UNIVERSIDAD DE EL SALVADOR
FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES
SEMINARIO DE GRADUACION EN CIENCIAS JURIDICAS AÑO 2004
PLAN DE ESTUDIO 1993

LA NECESIDAD DE LA REGULACIÓN JURÍDICA DE LA FIRMA ELECTRÓNICA EN EL SALVADOR.

TRABAJO DE GRADUACION PARA OPTAR AL TITULO DE:

LICENCIADO EN CIENCIAS JURIDICAS

PRESENTAN

Yuri Vladimir Argueta Velásquez
William Asvil Barahona
David Alberto Leiva Urías

DIRECTOR DE SEMINARIO
LIC. RAUL ANTONIO CHATARA FLORES

CIUDAD UNIVERSITARIA, SAN SALVADOR, NOVIEMBRE DE 2005.

UNIVERSIDAD DE EL SALVADOR

RECTORA

DRA. MARIA ISABEL RODRIGUEZ

VICERECTOR ACADEMICO

ING. JOAQUIN ORLANDO MACHUCA GOMEZ

VICERECTORA ADMINISTRATIVO

DRA. CARMEN ELIZABETH RODRIGUEZ DE RIVAS

SECRETARIA GENERAL

LICDA. ALICIA MARGARITA RIVAS DE RECINOS

FISCAL GENERAL

LIC. PEDRO ROSALIO ESCOBAR CASTANEDA

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

DECANA

LICDA. MORENA ELIZABETH NOCHEZ DE ALDANA

VICE DECANO

LIC. OSCAR MAURICIO DUARTE GRANADOS

SECRETARIO

LIC. FRANCISCO ALBERTO GRANADOS HERNANDEZ

COORDINADORA DE LA UNIDAD DE SEMINARIO DE GRADUACION

LICDA. BERTA ALICIA HERNANDEZ AGUILA

DIRECTOR DE SEMINARIO

LIC. RAUL ANTONIO CHATARA FLORES

AGRADECIMIENTOS

A mis padres: Por todo el apoyo que me brindaron a lo largo de mi carrera hasta culminar con mi trabajo de graduación. **A todas** las personas que me ayudaron a que esto fuera posible, y a esa persona especial que vino desde Canadá.

Yuri Vladimir Argueta Velásquez

A mis padres: por todo el apoyo, sacrificio y motivación que me brindaron en el desarrollo de la tesis. A mis hermanos por su ayuda incondicional a que esto fuera posible.

David Alberto Leiva Urías

A Dios: Por iluminarme y darme fuerza para lograr esa meta. **A mi madre:** por su sacrificio, comprensión y apoyo en el transcurso del desarrollo del trabajo de graduación.

William Asvil Barahona.

Un agradecimiento especial del grupo: A nuestro asesor **Lic. Raúl Antonio Chatara Flores,** por sus orientaciones claras y oportunas, sus recomendaciones y observaciones para mejorar la calidad de nuestro trabajo.

INDICE

INTRODUCCION

Desde un enfoque histórico acerca de lo que conocemos como firma, ha sido utilizada con la intención de expresar el consentimiento a la manifestación de voluntad vertida en el instrumento. Desde el punto de vista del derecho, se ha logrado otorgar valor jurídico a las distintas representaciones de esa autenticación o confirmación de la identidad de la persona de acuerdo con la sociedad y los momentos históricos. Básicamente, la firma sirve a los siguientes propósitos: consentimiento, solemnidad, prueba y forma, características que en su momento serán expuestas. Por otra parte puede decirse que firma es la manera habitual con que una persona escribe su nombre y apellido con el objeto de asumir las responsabilidades inherentes al documento que suscribe, en donde el carácter de habitualidad es decisivo para que un rasgo sea considerado la firma de una persona.

Una firma digital no es ajena a lo mencionado anteriormente, con la diferencia que se aparta un poco de sus representaciones habituales y cotidianas, ello se debe que es el resultado de la realización de un proceso matemático realizado con soporte tecnológico. Esta firma esta siendo utilizada en muchos países del mundo, la práctica demuestra que este es un medio seguro, con poco costo de autenticar y asegurar su integridad y confiabilidad. Existen sustanciales ventajas en la transmisión de la información por medio de redes, tales como Su disponibilidad instantánea en la cantidad deseada para ser trabajada directamente por el receptor, la rapidez de su envío y los costos prácticamente insignificantes para su transmisión.

Estos logros alcanzados por la tecnología posibilitan que actualmente, la mayoría de los ordenamientos jurídicos del mundo contengan legislaciones que adopten el instrumento y la firma digital otorga esa viabilidad e idoneidad dentro

de la amplitud del comercio electrónico, siendo este un concepto amplio que involucra cualquier transacción comercial efectuada por medios electrónicos, es decir, que involucra medios tales como el fax, telex, teléfono, EDIS e Internet.

En El Salvador este fenómeno tecnológico, también se ha hecho presente y se esta implementando a pesar de no contar con una ley especial como la poseen otros países como Canadá, España, Argentina, Colombia, Japón, etc. No obstante a ello, si figuran leyes aisladas que de una manera genérica regulan la compleja estructura y aplicación de la firma digital, entre estas podemos mencionar la Ley de Simplificación Aduanera y la Ley de Anotaciones Electrónicas de Valores en Cuenta.

Para generar un verdadero ambiente de seguridad y confianza lo cual es determinante en el uso de la firma digital, es necesario la creación de un ordenamiento jurídico en el que se prevea no solamente los pasos de cómo esta debe usarse, es importante además, construir una infraestructura la cual necesariamente debe de contener cuando menos las sanciones entre los diversos delitos que pueden originarse para su uso, tal como sucede con la Ley de Firma Electrónica Española.

Durante el desarrollo del presente trabajo de investigación, abordaremos con más amplitud en lo que se refiere a la firma electrónica y como esta se emplea en el comercio electrónico, así como el destacar sus características, que son la atribución, integridad, autenticación y no repudio, que mas adelante se profundizaran. También destacar las ventajas obtenidas con la implementación de la firma electrónica en Europa y América , además de referirnos a los antecedentes legislativos que se encuentran operando actualmente en nuestro país y las ventajas que ofrecería la regulación de la firma electrónica en el desarrollo del comercio electrónico.

CAPITULO I

ANTECEDENTES HISTORICOS DEL INTERNET

Sumario: *1.1 Antecedentes históricos de Internet.- 1.2. ¿Que es Internet?- 1.3. La Comisión de las Naciones Unidas Para el Derecho Mercantil Internacional (UNCITRAL).- 1.4 Ley Modelo sobre Comercio Electrónico de la UNCITRAL.- 1.5. Ley Modelo sobre Firmas Electrónicas de la UNCITRAL.-*

1.1. ANTECEDENTES HISTORICOS DEL INTERNET

Desde cualquier punto de vista que se pretenda abordar el tema del Internet, hay que partir de que nunca se ha tenido o había existido una red como esta en toda la historia de la humanidad, sin embargo siempre ha existido el propósito de establecer comunicación universal entre todos los pueblos, y es ese propósito el que finalmente, llevo a la creación y desarrollo del Internet.[1]

El inicio de la historia de lo que conocemos hoy en día como Internet lo podemos ubicar en los años setenta, con el establecimiento de los llamados "canales de paquetes autónomos de información", los paquetes autónomos, son un método para fragmentar mensajes en subpartes llamadas 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.

Tal y como lo expresa el autor Alejandro Reyes Krafft, al citar "Las leyes en la red: Problemas y Prospecto; la tecnología de los paquetes autónomos de información fue desarrollada en 1968 en los Estados Unidos, pero no fue hasta

[1] Reyes Krafft, Alfredo Alejandro. Firma Electronica y entidades de certificación. Cit. a :. Martínez Godinez Alonso: La contratación jurídica a través de medios electrónicos; Universidad Panamericana; tesis para optar al titulo de Licenciado en Derecho; 2000.

1969 cuando realmente esta tecnología fue usada por el departamento de defensa de los Estados Unidos, la cual utilizó este sistema, con la finalidad de establecer un canal experimental diseñado como medio de apoyo de investigación militar, concretamente con el objetivo real, de asegurar la orden de abrir fuego desde un centro de control a las bases de mísiles.[2]

Dicho canal se denominó ARPANET (Advance Research Project Agency Network), el cual utilizaba un protocolo de control de canal (NCP) como su protocolo de transmisión desde 1969 y hasta 1982.

El Internet que es conocido como el canal de canales, tuvo su origen exacto en 1972, pues 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 del ARPANET.

La visión propuesta de los principios arquitectónicos para lograr una interconexión internacional de canales, tal y como los circuitos independientes de ARPANET estaban 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 ejercito, 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 mas rápido, inclusive cuando dos usuarios de distintos lugares se

[2] Reyes Krafft, Alfredo Alejandro. Firma Electronica y entidades de certificación. Cit. a: The Laws of the net: Problems and Prospects, Godwin, M, Internet world, 1993.

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 el mensaje 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, este 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. Este último fue sustituido por NFSNET el cual con el tiempo sería suplido por el Canal Nacional de Investigación y Educación.

ARPANET fue de gran importancia para 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 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 influyo 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 correos electrónicos y los extendieron a lo que nosotros hoy en nuestros días le llamamos chatear.

A finales de los setenta y principios de los ochenta, otro tipo de tecnologías y canales comenzó a entrar, estos fueron los primeros canales de ventas y de investigación como BITNET y USENET[3].

Como 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 a 1970 varios modelos para conferenciar cara a cara o vía correo regular se han desarrollado, un modelo que tuvo gran importancia fue 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.

Otro sistema desarrollado fue THEORYNET, iniciado por Lawrence Landweber en la Universidad de Wisconsin, en 1977, THEORYNET proporcionó fácilmente recibo y envío de correspondencia para más de 100 científicos e investigadores en computación. En mayo de 1979, Lawrence tuvo un encuentro con representativos de ARPA, de la National Science Foundation 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)[4].

[3] Op. Cit. 23
[4] Op. Cit. 24

El CSNET, fue establecido por dos razones, por una parte, el UUCP, los modems 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 los sistemas de computo de ARPANET le daba en investigación y reclutamiento de estudiantes.

Durante 1980, el científico de ARPA Vinton Cerf, propuso un plan para una conexión de canales entre ARPANET y CSNET, este plan fue concebido por CSNET como un canal lógico compuesto de varios canales físicos. Las comunicaciones entre CSNET y ARPANET serian arregladas para ser transparentes, esto es, los servicios en cada canal serian accesados a través de una serie de protocolos.

La conexión entres estos canales podría ser a través de una conexión denominada Canal de valor agregado o VAN (VALUE ADDED NETWORK). La implementación entre estos canales y la importante decisión de hacer al TCP/IP disponible sin cargo, marco la fundación de lo que posteriormente seria conocido como INTERNET[5].

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 Winconsin. Este fue el principal impulsor del servicio de nombres de Dominio ahora utilizado ampliamente en los canales TCP/IP[6].

[5] Consultado en: www.findlaw.com
[6] Op cit. 26

USENET es un ejemplo de una arquitectura cliente-servidor. Un usuario conecta una maquina la cual se conecta a otra maquina la cual ha adquirido la correspondencia de USENET de todos 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 para que le sea enviado por la maquina a la que se encuentra conectada la suya. Si el artículo no se encuentra disponible por cualquier razón, aparece un mensaje que indica: “articulo 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[7].

Arpanet estableció entre otros canales de información 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.

En 1990 dejo de existir ARPANET y fue liberado el siguiente gran servicio de la red: ARCHIE (primer servicio de búsqueda en Internet). Al siguiente año apareció el servidor denominado World Wide Web conocido por “ www ” , que antecede a la mayoría de direcciones en Internet, que fue desarrollado por Tim Banners-Lee, del laboratorio europeo de estudios sobre Física de las Partículas (CERN). Banners 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

[7] Reyes Krafft, Alfredo. Firma Electrónica y Entidades de Certificación, México D.F, Facultad de Derecho. Pp. 27.

los llevara al texto o fuente de la cita o referencia. Pronto se vio la necesidad de relacionar ya no solo citas bibliograficas, sino partes completas de estudios, gráficas, dibujos, fotografías, archivos de sonido... lo que finalmente llevaría el sistema de navegación a su cúspide.

En 1991 salió a la venta la versión 3.1 de Windows, que popularizo la interfaz gráfica. Para 1992 se alcanzo un millón de servidores en línea y se conectó el banco Mundial; ese mismo año, la NSF retiró su inversión dejando así la posibilidad a otros tipos de financiamiento y, por lo tanto, a otros usos.
En 1993 se conecto a la red de la Organización de las Naciones Unidas, también apareció " Mosaic ", primer programa para acceder las paginas del servicio " www ", ahora conocido 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 mas usado, rebasando al servicio de transferencia de archivos (FTP), quien acaparaba la demanda de usuarios. Los sistemas multimedia que permiten ahora manejar textos, datos, audio, imagen y video han convertido a este 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 ejecutara aplicaciones sobre cualquier plataforma computacional, es decir, con cualquier sistema operativo. En ese año se alcanzaron 10,000,000 de servidores y desde entonces el crecimiento ha sido de grandes magnitudes, alcanzándose en Enero de 1999 40,000,000 de servidores conectados y mas de 1.6 millones de dominio.

Durante la época de los 90´s aparecieron los sistemas comerciales de conexión telefónica “dial up” que brindan al usuario domestico el acceso a la red mundial, mediante una renta anual o mensual (servicio de Internet). El único limite tecnológico hasta el momento es la capacidad del medio de transmisión (cableado telefónico y actualmente radio espectro y satélite).

Finalmente hay que decir, que en la actualidad el Internet es una federación de redes que esta en constante desarrollo y es de acceso general. Después de los investigadores, los alumnos en las universidades y los empleados de las instituciones publicas, 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 del Internet.

1.2. ¿QUÉ ES INTERNET?

Diferentes acepciones se han generado sobre este tópico a pesar de ser relativamente nuevo, algunas personas lo definen dependiendo de la actividad que realicen, para unos no es mas que un medio de 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 mas, es un medio de expresar sus ideas.[8]

Las características fundamentales de la operación en Internet son: Que se trata de una red **distributiva,** es decir computadoras que están interconectadas que pueden ser accesadas desde cualquier parte del mundo, es **interopable,** utiliza protocolos abiertos , de manera que distintos tipos de

[8] Vid. Reyes Krafft, Alfredo. Firma Electrónica y Entidades de Certificación, México D.F, Facultad de Derecho. Pp. 49.

redes pueden ser enlazados, permitiendo la diversidad de servicios a una variedad de usuarios (TPC/IP).

En síntesis el Internet es un canal mundial de telecomunicaciones informáticas, que esta integrado por muchos canales que a su vez están interconectados entre si, lo cual lo convierte en el medio de comunicación mas veloz que haya tenido la humanidad[9].

Como se señalo anteriormente el Internet fue creado hace aproximadamente 30 años por el Departamento de Defensa de los Estados Unidos como un canal experimental diseñado para apoyar la investigación militar. En un principio se le denominó ARPANET, sin embargo con el paso del tiempo se fueron desarrollando diversos canales para permitir a los estudiantes y universidades acceder al ARPANET, con fines educacionales.

Poco a poco han ido aumentado el número de canales que se han conectado al ARPANET, a tal grado que las grandes empresas mundiales, agencias gubernamentales, y los individuos o personas físicas están descubriendo y explorando el mundo del Internet.

Pero entre los diversos fines que proporciona el Internet, el más importante para nuestros fines jurídicos, es el del Comercio a través del Internet dado que las compañías tanto privadas como del sector público de diversos países, han visto beneficios que el Internet aporta al comercio mundial. Según José Manuel Villar abogado del Estado y Exsecretario General de

[9] Reyes Krafft, Alfredo. Firma Electrónica y Entidades de Certificación, México D.F, Facultad de Derecho. Pp. 51. Desde sus comienzos, esta red de canales conocida como Internet, ha crecido hasta el punto de englobar a mas de seis millones de canales interconectados con Internet y a mas de cuarenta millones de usuarios en todo el mundo, entre los que podemos incluir agencias gubernamentales, universidades, investigadores, compañías privadas y personas físicas.

Comunicaciones de España[10], define al comercio electrónico, en un sentido amplio, como cualquier forma de transacción o intercambio de información comercial basada en la transmisión de datos sobre redes de comunicación, como Internet.[11] Para nuestra investigación consideramos que el comercio electrónico no es mas que una modalidad especifica del comercio tradicional la cual es realizada por medio de ordenadores conectados a la red, mediante el intercambio electrónico de datos, en la cual compañías y personas físicas ofrecen sus productos y servicios.

El crecimiento del comercio electrónico es tan grande que nadie duda del profundo impacto económico y social que traerá en los próximos años y todos los actores involucrados, desde gobiernos a asociaciones de la industria y empresas individuales, tratan de tomar las medidas necesarias para aprovechar al máximo sus ventajas.[12]

Un sistema avanzado para el comercio electrónico como el que constituye Internet puede comprender actividades como:

a) Transferencia electrónica de fondos
b) Regulación gubernamental de intercambio de datos.

---

[10] Villar, José Manuel. Derecho de Internet, Contratación Electrónica y Firma Digital: Capitulo I "Una aproximación a la firma electrónica. Edit. Aranzadi. Pp.166.

[11] Villar, José Manuel. Capitulo I "Una aproximación a la firma electrónica. Edit. Aranzadi. Pp.166. el concepto de comercio electrónico no solo incluye la compra y venta electrónica de bienes, información o servicios, sino también el uso de la red para actividades anteriores o posteriores a la venta como: a) La Publicidad, b) La búsqueda de información sobre productos y proveedores, c) la negociación entre comprador y vendedor sobre precio y condiciones de entrega, d) La atención al cliente antes y después de la venta, e) la realización de tramites administrativos relacionados con la actividad comercial, f) la colaboración entre empresas con negocios comunes.

[12] Villar, José Manuel. Derecho de Internet, Contratación Electrónica y Firma Digital: Capitulo I "Una aproximación a la firma electrónica. Edit. Aranzadi. Pp.167.

c) Integración de consorcios, es decir de compañías con el fin de tener mayor competitividad en un mercado totalmente globalizado.
d) Soporte computacional para la colaboración en el trabajo.

El comercio electrónico puede combinar las ventajas de las computadoras como lo son la velocidad, rentabilidad y gran cantidad de datos, aunado a ello las ventajas que poseen las personas creatividad, flexibilidad y 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.[13]

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 computo.

Como resultado del crecimiento de Internet, muchas empresas temen que sus respectivos gobiernos impongan extensivas y represivas regulaciones en Internet y por lo tanto en el comercio electrónico sin embargo, durante esta época del comercio electrónico, es cuando debe establecerse un regulación adecuada que permita la “seguridad jurídica” de 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. Los gobiernos

[13] Reyes Krafft Alfredo Alejandro, Cit: La www una telaraña que se teje a plena luz del día, Fernández Flores, Rafael, en la revista red, nª 70, año VI, Julio de 1996, pp. 38-40.

quienes tienen un efecto en el desarrollo del comercio electrónico, ellos pueden facilitar mediante acciones el comercio en Internet o reducirlo, para ello deben de tener en cuenta la naturaleza para lo cual fue creada la red, es decir un medio de comunicación mundial.

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

a) Reduce costos para los compradores al incrementar la competencia permitiendo que cada vez más proveedores de bienes y servicios sean capaces de competir electrónicamente en un mercado abierto.

b) Reduce errores, tiempo y costos mayores en el procesamiento de información.

c) Reduce costos para los proveedores a través del acceso electrónico a bases de datos donde encuentran una oferta creciente.

d) Reduce el tiempo para completar las operaciones de negocios, particularmente en la reducción de tiempo transcurrido desde el pago hasta la entrega del producto.

e) Estimula la creación de mercados al facilitar y hacer mas barato el acceso a un mayor numero de clientes.

f) Facilita la entrada a nuevos mercados geográficos remotos.

g) Mayor calidad en los productos, especificaciones y estándares, gracias al aumento de la competencia.

h) Mayor rapidez en los negocios y en los procesos de mercado a través de la eliminación virtual de pasos, logrando la reducción a una sola transacción.

i) Reducción de inventarios y la virtual eliminación del riesgo de inventarios obsoletos a través de la creciente demanda de bienes y servicios por vía electrónica, lo cual permite la renovación constante de los inventarios por parte de los proveedores.

j) Disminución de costos a través del ahorro de gastos en comunicación y reducción personal, y

k) Reduce el uso de materiales que dañen el medio ambiente a través de la coordinación electrónica de actividades y movimiento de información en vez de objetos físicos.

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

Con una extensa variedad de transacciones electrónicas, el desarrollo de las aplicaciones del comercio electrónico requieren 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 la necesidad de contar con cierta infraestructura para integrarse al comercio electrónico, crea barreras para la inversión y gastos excesivos sobre todo para la mediana y pequeña empresa.

Actualmente podemos percibir la gran influenza 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 con una referencia a un sitio en la red, el cual provee mayor información sobre una compañía particular y sobre sus productos y servicios.

La aplicación del comercio electrónico requiere la interoperacion de comunicaciones, proceso de datos y servicios de seguridad. Estos servicios

serán proveídos por diferentes compañías; pero dada esta diversidad, ¿Cómo puede 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, la industria y el comercio.

1.3 LA COMISION DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL (UNCITRAL).

La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, CNUDMI o sus siglas en ingles UNCITRAL; es el órgano jurídico central del sistema de las Naciones Unidas en el ámbito del derecho mercantil internacional. Dicha comisión tiene como labor fomentar la armonización y unificación progresivas del derecho mercantil internacional mediante: La preparación o el fomento de la aprobación de nuevas convenciones internacionales, leyes modelo y leyes uniformes, así como el fomento de la codificación y una aceptación más amplia de las condiciones, disposiciones, costumbres y prácticas comerciales internacionales, El fomento de métodos y procedimientos para asegurar la interpretación y aplicación uniformes de las convenciones internacionales y de las leyes uniformes en el campo del derecho mercantil internacional,[14] etc.

La comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL), ha completado trabajos sobre modelos de ley que soporta el uso comercial de contratos intencionales en comercio electrónico. Estos modelos de ley establecen reglas y normas que validan y reconocen los

[14] Resolución 2205 (XXI) de la Asamblea General de la UNCITRAL.

contratos celebrados por medios electrónicos, establecen reglas para la formación de los contratos y su desempeño, definen las características para un escrito electrónico valido 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 técnicas en los tribunales y procedimientos de arbitraje.

Muchos 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 elegir la relación contractual entre ellas que mejor les convenga,
- Las reglas deben ser tecnológicamente neutras.
- Las reglas deben prever futuros desarrollos tecnológicos
- 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 aun no se encuentra en línea.

1.4. LEY MODELO SOBRE COMERCIO ELECTRONICO

La ley modelo sobre comercio electrónico de la UNCITRAL adoptada en el año de 1996 tiene por objeto facilitar el uso de medios modernos de comunicación y de almacenamiento de información, por ejemplo el intercambio electrónico de datos, el correo electrónico y la telecopia, con o sin soporte como

seria el Internet. Se basa en el establecimiento de un equivalente funcional de conceptos conocidos en el trafico que se opera sobre papel como serian 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 común. Como complemento de las normas generales, la ley modelo contiene normas para el comercio electrónico en áreas especiales, como seria el transporte de mercancías. [15]

1.5. LEY MODELO PARA LAS FIRMAS ELECTRONICAS

El creciente empleo de tecnologías de identificación electrónica en sustitución de las firmas manuscritas y de otros procedimientos tradicionales de autenticación ha planteado la necesidad de crear un marco jurídico especifico para reducir la incertidumbre con respecto a las consecuencias jurídicas que puedan derivarse del empleo de dichas técnicas modernas de identificación.

La finalidad de la Ley Modelo sobre Firmas Electrónicas[16] es ayudar a los Estados a establecer un marco legislativo moderno, armonizado y equitativo para abordar de manera mas eficaz las cuestiones relativas a firmas electrónicas. Esta ley modelo ofrece normas practicas para comprobar la fiabilidad técnica de las firmas electrónicas. La ley de firmas electrónicas supone una contribución importante a la Ley Modelo sobre Comercio Electrónico de la UNCITRAL, al adoptar un criterio conforme el cual puede determinarse previamente la eficacia jurídica de una determinada técnica de creación de una firma electrónica. Así pues, la ley sobre 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

[15] Vid. Ley sobre Comercio electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.
[16] Cfr. Considerandos de la Ley Modelo de Firmas Electronicas de la UNCITRAL.

firmas electrónicas 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 modelos para firmas electrónicas puede ayudar a configurar prácticas comerciales más armoniosas en el ciberespacio.

Los objetivos de la Ley Modelo de Firmas Electrónicas son el de permitir o facilitar el empleo de firmas electrónicas y el de conceder igualdad de trato a los usuarios de documentación consignada sobre papel y a los de información consignada en soporte informático, 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 sobre Firmas Electrónicas y la Ley Modelo 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.[17]

[17] Vid. Guia para la incorporación de la Ley modelo de la UNCITRAL, para las firmas electronicas al derecho interno. Segunda parte pag. 11. Cfr. Parrafo 24. 2001.

CAPITULO II

REGULACION INTERNACIONAL DE LA FIRMA ELECTRÓNICA

Sumario: 2*.1 Panorama Internacional: 2.1.1 Alemania, 2.1.2 Bélgica, 2.1.3 Dinamarca, 2.1.4 España, 2.1.5 Francia, 2.1.6 Irlanda, 2.1.7 Italia, 2.1.8 Japón, 2.1.9 Luxemburgo, 2.1.10 Portugal, 2.1.11 Reino Unido, 2.1.12 Suecia.- 2.2 Latinoamérica: 2.2.1 Colombia, 2.2.2 Argentina, 2.2.3 Chile, 2.2.4 Panamá, 2.2.5 Perú, 2.2.6 Venezuela, 2.2.7 Canadá, 2.2.8 Estados Unidos.- 2.3. La Firma Electrónica en España.- 2.4. La Junta Directiva de la Unión Europea.- 2.5. Organizaciones Internacionales.- 2.5.1. ONU.- 2.5.2 OCDE.*

2.1. PANORAMA INTERNACIONAL

En un mundo cada vez mas globalizado, los Estados se ven en la necesidad de implementar técnicas que permitan desarrollar con eficacia el comercio electrónico y contar con una regulación uniforme que garantice de una forma confiable sus operaciones realizadas por la red.

La UNCITRAL ha creado una Ley Modelo sobre Firmas Electrónicas, en la cual pretende crear un criterio uniforme a los países que adopten este sistema, muchos países del mundo han elaborado sus proyectos de Ley de firma Electrónica inspirada en esta Ley Modelo.

Actualmente entre los países que cuentan con una legislación en materia de Firma electrónica podemos enumerar a los siguientes:

2.1.1 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. Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations (Bundesgesetzblatt - BGBl. Teil I S. 876 vom 21. May 2001).

Published 16 May 2001. Official Journal Nº 22, 22 May 2001. In Force 22 May 2001.

2.1.2 BELGICA : se promulga la Ley que regula la firma electrónica en el 19 de Septiembre del año 2001.

2.1.3 DINAMARCA: Act 417 of 31 May 2000 on Electronic Signatures. Bill L 229. Executive Order on Security Requirements etc. for Certification Authorities. Executive Order Nº 923 of 5 October 2000.
Executive Order on Reporting of Information to the National Telecom Agency by Certification Authorities and System Auditors. Executive Order Nº 922 of 5 October 2000.

2.1.4 ESPAÑA: El Real Decreto Ley 14/1999 sobre Firmas Electrónicas. Septiembre de 1999, Instrucción sobre el Uso de la Firma Electrónica de los Fedatarios Públicos Orden de 21 de febrero de 2000 por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica. El Proyecto de Ley de firma electrónica, de 20 de junio de 2003 , ha introducido diversas modificaciones respecto del vigente Real Decreto ley 14/1999 de firma electrónica. Tras su ratificación por el Congreso de los Diputados, se acordó someterlo a una más amplia consulta pública y al posterior debate parlamentario para perfeccionar su texto, entre los puntos mas importantes que considera están: Promoción de Autorregulación de la Industria, Concepto de Firma Electrónica Reconocida, Declaración de prácticas de certificación, Documento Nacional de Identidad Electrónico y el más debatido, Certificados para Personas Morales, un caso distinto a la firma electrónica de los representantes de las personas morales, pues se persigue dar firma a las

empresas, no a sus representantes, si bien, evidentemente, con el objeto de que así se pueda distribuir entre sus empleados.[18]

2.1.5 FRANCIA : En el Decreto nº 2001-272 del 30 marzo 2001 se aprueba la Ley referente a la firma electrónica. du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l´informtion et relative à la signature électronique.

2.1.6 IRLANDA: se regula lo concerniente a firma electrónica y comercio electrónico, en la Ley de Actos de Comercio Electrónico del año 2000.

2.1.7 ITALIA (El 15 de marzo de 1997, fue publicado el "Reglamento sobre: Acto, Documento y Contrato en Forma Electrónica" aplicable a las diversas entidades de la Administración Pública, el 15 de abril de 1999 las reglas técnicas sobre firmas digitales y el 23 de enero del 2002 la ley sobre firma electrónica).

2.1.8 JAPÓN (1/04/2001 Ley sobre firma electrónica y Servicios de Certificación).

2.1.9 LUXEMBURGO : Règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, aupaiment électronique et à la création du comité "commerce électronique". Projet de règlement grand-ducal portant determination d´un système d´accréditation des organismes de certification et d´inspection, ainsi que des laboratoires d´essais et d´étalonnage et portant création de l´Office Luxembourgeois d´Accréditation et de Surveillance, d´un Comité de´accréditation et de´un Recueil national des auditeurs qualité et

[18] www.cmt.es

techniques. Texte amendé suite aux avis de la Chambre de commerce et de la Chambre des métiers.

2.1.10 PORTUGAL: la firma electrónica se regula en su decreto Ley 290-D/99.

2.1.11 REINO UNIDO: Actos de comunicación electrónica regula en el reino unido lo concerniente a firma electrónica. (Electronic Communications Act, 2000.)

2.1.12 SUECIA: Qualified Electronic Signatures Act (FSF 2000:832) .

2.2 LATINOAMERICA :

2.2.1 COLOMBIA

En Colombia existe la Ley de Comercio Electrónico en Colombia (Ley 527 de 1999) Su objetivo es la reglamentación y la definición del acceso y el uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, además del establecimiento de las Entidades de Certificación. [19]

Su ámbito de aplicación es el uso de firmas digitales en mensajes de datos Define como Firma Digital, al valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

Como Mensaje de Datos a la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como

[19] Sitio en Internet de la Corte Constitucional de Colombia. www.corteconstitucional.cl

pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.

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

En cuanto a la Supervisión y al control, estas recaen sobre las Entidades de Certificación autorizadas por la Superintendencia de Industria y Comercio.
Se equipara el valor probatorio de un mensaje de datos que uno en papel siempre y cuando contenga lo siguiente:
1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.
3. Está bajo el control exclusivo de la persona que la usa.
4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.
Si da Reconocimiento a Certificados Extranjeros las sanciones serán impuestas por la Superintendencia de Industria y Comercio de acuerdo con el debido proceso y el derecho de defensa, podrá imponer según la naturaleza y la gravedad de la falta, estas van de la Amonestación a la Revocación de la Autorización.

2.2.2 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 -firma digital en la Administración Pública- el 14/12/2001 Ley de Firma Digital para la República Argentina 25/506. [20]

2.2.3 CHILE (decreto 81/ 2002 Ley sobre documentos electrónicos, firma electrónica y servicios de certificación). [21]

2.2.4 PANAMÁ

(31/07/2001 Ley 43 de Comercio Electrónico). [22]

2.2.5 PERU

En Perú existe la Ley No. 27269 Ley de Firmas y Certificados Digitales (2000) Su Objetivo es utilizar la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad. [23]

Su Ámbito de Aplicación son aquellas Firmas electrónicas que, puestas sobre un mensaje de datos puedan vincular e identificar al firmante, y garantizar su integridad y autenticación.

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

---

[20] **www.jus.gov.ar/minis/nuevo/proyectocodigocivil.**
[21] Vid. Ley sobre documentos electrónicos, firma electrónica y servicios de certificación, de Chile.
[22] Vid. Ley de Comercio Electrónico de Panamá
[23] Proyecto de ley 5070-99. Ley de firmas electrónicas y certificados.

Como Certificado Digital a aquel documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.
Por su parte la Entidad de Certificación es aquella que cumple con la función de emitir o cancelar certificados digitales.

Existe una Entidad de Registro o Verificación que es la encargada de recolectar y comprobar la información del solicitante del Certificado, además identifica y autentica al suscriptor de firma digital y acepta y autoriza las solicitudes de emisión y cancelación de certificados digitales.

La Supervisión y el Control, corren a cargo de la autoridad administrativa designada por el Poder Ejecutivo; las Entidades de certificación intervienen en la emisión de certificados y pueden asumir las funciones de entidades de registro o verificación.

Esta ley no establece el Valor probatorio de la Firma Electrónica. Para que un Certificado Extranjero sea reconocido, este debe contar con el aval de una Entidad nacional. No existen Sanciones

2.2.6 VENEZUELA

Ley sobre Mensajes de Datos y Firmas Electrónicas (2001) Su Objetivo es otorgar y reconocer eficacia y valor jurídico al mensaje de datos, a la firma electrónica y a toda información inteligible en formato electrónico.
Su Ámbito de Aplicación son los mensajes de datos y firmas electrónicas.
Define a la Firma Electrónica como aquella información creada o utilizada por el signatario, asociada al mensaje de datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.

Como Mensajes de Datos a toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.

Como órgano de control, existe la Superintendencia de Servicios de Certificación Electrónica, como un servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión, en las materias de su competencia, dependiente del Ministerio de Ciencia y Tecnología. Los Proveedores de Servicios de Certificación, son los que emiten los certificados
La firma tendrá valor probatorio cuando vincule al signatario con el mensaje de datos y se pueda atribuir su autoría.

Cuando los certificados extranjeros estén garantizados por un proveedor de servicios de certificación acreditado, tendrán la misma validez y eficacia jurídica

Las Sanciones para los proveedores de servicios de certificación van de entre 500 a 2,000 Unidades Tributarias. [24]

2.2.7 CANADÁ (British Columbia Bill 13-2001, The Electronic Transactions Act).

El acto de las transacciones electrónicas que regula las relaciones comerciales realizadas a través de la red, establece el uso de la firma electrónica, establece en su apartado número trece numeral tercero, “que una firma electrónica es siempre requerida por las partes para realizar una transacción electrónica”.

[24] Sitio en Internet del gobierno de Venezuela. www.venezuela.com

También establece que la firma electrónica es usada para identificar a una persona y para indicar la aprobación de la información comunicada por el suscriptor. Al mismo tiempo esta Ley Canadiense le da la validez jurídica al documento electrónico y establece valor probatorio en juicio en caso de controversia.[25]

2.2.8 ESTADOS UNIDOS

La primera ley en materia de Firma Digital en el Mundo fue la denominada “Utah Digital Signatura Act”, publicada en mayo de 1995 en el Estado de UTAH, en Estados Unidos.

Su objetivo es facilitar mediante mensajes electrónicos y firmas digitales las transacciones. Procurar las transacciones seguras y la eliminación de fraudes. Establecer normas uniformes relativas a la autenticación y confiabilidad de los mensajes de datos, en coordinación con otros Estados.

Su ámbito de aplicación son las transacciones mediante mensajes electrónicos, su confiabilidad, así como las firmas digitales.

Esta ley, define a la Firma Digital como la “transformación de un mensaje empleando un criptosistema asimétrico tal, que una persona posea el mensaje inicial y la clave pública del firmante pueda determinar con certeza si la transformación se creó usando la clave privada que corresponde
a la clave pública del firmante, y si el mensaje ha sido modificado desde que se efectuó la transformación.”

Al Criptosistema Asimétrico, como aquel “algoritmo o serie de algoritmos que brindan un par de claves confiable.” Al Certificado, como aquel registro

[25] www.gp.gov.ca/statreg/state/E/1010_01

basado en la computadora que identifica a la autoridad certificante que lo emite; nombra o identifica a quien lo suscribe; contiene la clave pública de quien lo suscribe, y está firmado digitalmente por la autoridad certificante que lo emite.

En cuanto a la Supervisión y al control, estos recaen sobre la División, quien actúa como autoridad certificadora. También formula políticas para la adopción de las tecnologías de firma digital y realiza una labor de supervisión regulatoria.[26]

La emisión de los certificados corre a cargo de la autoridad certificadora que ha sido acreditada Se equipara el valor probatorio de un mensaje de datos que uno en papel siempre y cuando contenga una firma digital confirmada mediante la clave pública contenida en un certificado que haya sido emitida por una autoridad certificadora autorizada.

No se contempla el reconocimiento de certificados extranjeros, solo se menciona que la División puede reconocer la autorización emitida por Autoridades Certificadoras de otros Estados. No contempla sanciones.
ABA: 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”.

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.

[26] Idem.

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.

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).[27]

2.3. LA FIRMA ELECTRONICA EN ESPAÑA

El Real Decreto Ley 14/1999, de 17 de septiembre, sobre Firma Electrónica (1999) tiene como objetivo establecer una regulación sobre el uso de firma electrónica, atribuyéndole eficacia jurídica, además de establecer lineamientos para los prestadores de servicios de certificación.

Su Ámbito de Aplicación son las firmas electrónicas, su eficacia jurídica y la prestación al público de servicios de certificación.

Define a la Firma electrónica como un conjunto de datos, en forma electrónica, ajenos 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.

Define también a la Firma Electrónica Avanzada como aquella 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

[27] www.senate.state.mo.us/98info/billtext/intro/sb708

al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

Como certificado aquella certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad.

Como Prestador de Servicios de Certificación a aquella persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica.

La supervisión corre a cargo del Ministerio de Fomento a través de la Secretaría General de Comunicaciones. Existe un Registro de Prestadores de Servicios de Certificación en el Ministerio de Justicia, en el que se solicita su inscripción antes de iniciar actividades.

Cuando la firma electrónica avanzada esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá Valor probatorio Para otorgarle Reconocimiento de certificados extranjeros, estos deben cumplir los siguientes requisitos:

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

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

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

Las Sanciones son impuestas conforme a los siguientes parámetros:

a) Por la comisión de infracciones muy graves, se impondrá multa por importe no inferior al tanto, ni superior al quíntuplo, del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción o, en caso de que no resulte posible aplicar este criterio lo constituirá el límite del importe de la sanción pecuniaria.

b) La reiteración de dos o más infracciones muy graves, en el plazo de cinco años, podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España durante un plazo máximo de dos años.

c) Por la comisión de infracciones graves, se impondrá multa por importe de hasta el doble del beneficio bruto obtenido como consecuencia de los actos u omisiones que constituyan aquéllas o, en caso de que no resulte aplicable este criterio o de su aplicación resultare una cantidad inferior a la mayor de las que a continuación se indican, esta última constituirá el límite del importe de la sanción pecuniaria.

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

Instrucción sobre el Uso de la Firma Electrónica de los Fedatarios Públicos Orden de 21 de febrero de 2000 por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica. -Ley de Servicios de la Sociedad de Información-) Proyecto de Ley de Firma Electrónica: Promoción de Autorregulación de la Industria, Concepto de Firma Electrónica Reconocida, Time stamping, Declaración de prácticas de certificación, Documento Nacional de Identidad Electrónico y Certificados para Personas Morales.

2.4. LA DIRECTIVA DE LA UNIÓN EUROPEA

La Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para la firma electrónica (1999)

Su Objetivo es garantizar el buen funcionamiento del mercado interior en el área de la firma electrónica, instituyendo un marco jurídico homogéneo y adecuado para la Comunidad Europea, y definiendo criterios que fundamenten su reconocimiento legal.

Su Ámbito de aplicación se limita al reconocimiento legal de la firma electrónica y establece un marco jurídico para determinados servicios de certificación accesibles al público.

Define a la Firma electrónica a la realizada en forma digital integrada en unos datos, ajena a los mismos o asociada con ellos, que utiliza un signatario para expresar conformidad con su contenido y que cumple los siguientes requisitos:

1. Estar vinculada al signatario de manera única;
2. Permitir la identificación del signatario;
3. Haber sido creada por medios que el signatario pueda mantener bajo su exclusivo control.
4. Estar vinculada a los datos relacionados de modo que se detecte cualquier modificación ulterior de los mismos.

Como Dispositivo de creación de firma a los datos únicos, como códigos o claves criptográficas privadas, o un dispositivo físico de configuración única, que el signatario utiliza para crear la firma electrónica.

El Dispositivo de verificación de firma son los datos únicos, tales como códigos o claves criptográficas públicas, o un dispositivo físico de configuración única, utilizado para verificar la firma electrónica.

El Certificado reconocido es el certificado digital que vincula un dispositivo de verificación de firma a una persona y confirma su identidad, y que cumple con los requisitos establecidos en el Anexo Y de la ley.

El Proveedor de Servicios de Certificación es la persona o entidad que expide certificados o presta otros servicios al público en relación con la firma electrónica.

La Comisión ejerce la supervisión con ayuda del Comité de Firma Electrónica, de carácter consultivo, compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión. Los Estados miembros velarán porque la firma electrónica sea considerada como firma que cumple los requisitos legales de una firma manuscrita y produce los mismos efectos que la manuscrita cuando cumpla con los requisitos establecidos en ley.

Los Estados miembros velarán porque los certificados expedidos por un proveedor de servicios de certificación establecido en un tercer país tengan la misma validez que un local cuando cumplan con los siguientes requisitos:
1. El proveedor de servicios de certificación cumple los requisitos establecidos en la presente Directiva y ha sido acreditado en el marco de un sistema voluntario de
acreditación establecido por un Estado miembro;
2. Un proveedor de servicios de certificación establecido en la Comunidad, que cumpla las prescripciones del Anexo II, avala el certificado en la misma medida que los suyos propios;
3. El certificado o el proveedor de servicios de certificación están reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones internacionales.

2.5. ORGANIZACIONES INTERNACIONALES

La firma electrónica es uno de los temas quemas ha suscitado controversia, por cuanto de su aplicación se tienen consecuencias muy graves para el manejo general del comercio electrónico, en tal medida, organizaciones como la comunidad económica europea, se han preocupado por modelos que puedan ser implantados por todos sus miembros, de modo que se sobrepasen los problemas que una inadecuada legislación pueda generar. Como referencia puede citar el expediente interinstitucional numero 98\0325 COD. De 28 de febrero de 2000, en el cual se desarrollo el asunto de la siguiente forma; "posición común aprobada por el consejo con vistas a la adopción de la Directiva del parlamento Europeo y del consejo relativo a determinados aspectos jurídicos del servicio de la sociedad de la información, en particular al comercio electrónico en el mercado interno". En que señala, que todo Estado debe ajustar su legislación en cuanto a los requisitos y, especialmente, los requisitos formales que pueden entorpecer la celebración del tratado por vía electrónica; se debe examinar de forma sistemática que legislaciones necesitan proceder a dichos ajustes y este examen debe versar sobre todas las fases y actos necesarios para realizar el proceso contractual, incluyendo el registro del contrato; el resultado de dicho ajuste debería hacer posible contratos por vía electrónica; El efecto jurídico de la firma electrónica es objeto de la directiva 1999/93//CA del parlamente Europeo y del consejo, de 13 de diciembre de 1999, por la que se establece un marco común para la firma electrónica; el acuse de recibo expedido por un prestador de servicios puede consistir en suministrar en línea un servicio pagado; la presente directiva no afecta a la posibilidad que tienen los Estados miembros de mantener o establecer regímenes jurídicos específicos o generales en materias de contratos que pueden cumplirse por vía electrónica, en particular los requisitos en relación con la seguridad de las firmas electrónicas.

Lo anterior es tan solo un ejemplo de cómo el papel de la firma digital ha generado todo un proceso de cambio de las legislaciones en el ámbito internacional, en el caso presentado, se explica que haya sido necesario para la comunidad Europea, el establecer unos parámetros básicos respecto a los cuales se maneje el tema entorno a Internet.[28]

2.5.1. ONU

La organización de las Naciones Unidas por conducto de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNDUMI, mejor conocida por sus siglas en inglés UNCITRAL), con sedes tanto en Nueva York como en Viena, se compone por 37 países. Funciona desde 1968, elaborando múltiples convenciones, además de reglas de arbitraje, modelos de contratos, de cláusulas contractuales y guías jurídicas, pero sobre todo Leyes Modelo como la de Arbitraje, Comercio Electrónico y Firma Electrónica.

En la sesión del día 12 de diciembre de 2001, fue aprobada por el pleno de la 85ª Sesión Plenaria de la Asamblea General la Ley Modelo sobre las Firmas Electrónicas. Toda vez que esta Ley Modelo es la que ha sido más aceptada a nivel internacional, sus puntos más importantes serán analizados mas adelante.

2.5.2. OCDE

En marzo de 1997, la Organización para la Cooperación y el Desarrollo Económico publicaron su recomendación para el establecimiento de políticas sobre Criptografía, sin embargo solo establece una serie de lineamientos que se sugiere a los gobiernos adoptar al momento de legislar en materia de firma digital y de Entidades Prestadoras de Servicios de Certificación.

---

[28] Cfr. Cubillos Velandia, Ramiro y Rincón Cárdenas, Erick. Introducción Jurídica al Comercio Electrónico. Bogotá, D.C. Colombia. 2002. Capitulo II.

CAPITULO III

FIRMA ELECTRONICA – NOCIONES GENERALES

Sumario: *3.1.- Firma Autógrafa.- 3.1.1. Características de la firma autógrafa.- 3.1.2. Elementos de la firma.- 3.2. Firma electrónica y firma digital.- 3.2.1 Firma Electrónica Avanzada.- 3.3 Equivalencia funcional. 3.4 Neutralidad Tecnológica. 3.5 Prestadores de servicios de certificación.- 3.5.1 Certificados.- 3.5.2 Vigencia del certificado.- 3.6. Obligaciones de las partes, prestadores de servicios de certificación, usuarios y la parte que confía en el certificado.- 3.6.1. Obligaciones de los prestadores de servicios de certificación.- 3.6.2. Obligaciones del usuario o firmante.- 3.6.3. Obligaciones de la parte que confía en el certificado.- 3.7. Criptografía.- 3.8. Algoritmos.- 3.8.1. Algoritmo simétrico.- 3.8.2. Algoritmo asimétrico.- 3.9. Métodos de encripcion.- 3.9.1. Clave Publica.- 3.9.2. Clave Privada.*

3.1. LA FIRMA AUTÓGRAFA

No existe en nuestro país una regulación específica, sobre la firma, sus elementos, consecuencias o su concepto y las pocas referencias que existen son prácticamente aislados tal como sea mencionado.

En Roma, existía la Manufirmatio, que consistía en una ceremonia en que leído el documento por su autor, o el funcionario, se colocaba desenrollando y extendido sobre la mesa del escribano y luego de pasar la mano abierta sobre el pergamino en actitud de jurar, pero sin hacerlo, se estampaba el nombre, signo, o una o tres cruces, por el autor o el funcionario en su nombre, haciéndolo seguidamente los testigos. Más que un requisito, la Manufirmatio era en sí misma parte del espectáculo solemne en que se

realizaba el acto.[29] En la Edad Media, se inscribía una cruz a la que se le añadían diversas letras y rasgos. Estos signos se utilizaban como firma. Debido a que no sabían leer ni escribir, los nobles remplazaron esta práctica con el uso de sellos.[30]

"La diferenciación entre "firmas" y "signos" hizo que se empezase a entender que aquellas 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.[31]

Según el Diccionario de la Real Academia, la firma es el Nombre y apellido, o título, que una persona escribe de su propia mano en un documento, para darle autenticidad o para expresar que aprueba su contenido. Si se considera a la firma como un conjunto de signos, podemos distinguir que esta tiene una doble función por un lado el hecho de que vincula a la persona con el acto jurídico, esto es, se torna IDENTIFICADORA de la persona, puesto que determina su personalidad, así como sus derechos y obligaciones sobre el convenio de que se trata. Sin embargo este método no es totalmente fiable

[29] Reyes Kraff, Alfredo Alejandro. Firma Electrónica y Entidades de Certificación. México. Universidad Panamericana. 2002. p. 128 Cit. a : Floris. Margadant G. Derecho Privado Romano
[30] Op Cit p.128, cit a: Tomas y Valiente Francisco. EL ORDEN JURIDICO MEDIEVAL.. Madrid Marcial Pons, Ediciones Jurídicas y Sociales, S. A pp. 53-54.

[31] Op Cit p. 130, cit a : Acosta Romero, Miguel; NUEVO DERECHO MERCANTIL, La Firma en el Derecho Mercantil Mexicano pp. 537 a 562; editorial Porrua, Primera Edición; 15 de Agosto del 2000.

puesto que el mismo podría ser falsificado y su autoría deberá ser comprobada por un perito.

Existe también la AUTENTICACION que consiste en el proceso por medio del cual se revelan algunos aspectos de la identidad de una persona. Es decir el autor además de expresar su consentimiento, y toma como suyo el mensaje. Así, la firma autógrafa se utiliza para expresar el consentimiento de las partes sobre un contrato en particular.

3.1.1 CARACTERÍSTICAS DE LA FIRMA AUTOGRAFA

La firma autógrafa tiene las siguientes características:

IDENTIFICATIVA: Sirve para identificar quién es el autor del documento.

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.

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.[32]

3.1.2. ELEMENTOS DE LA FIRMA

ELEMENTOS FORMALES.- Son aquellos elementos materiales de la firma que están en relación con los procedimientos utilizados para firmar.

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.

El animus signandi. Es el elemento intencional o intelectual de la firma, consiste en la voluntad de asumir el contenido de un documento, que no debe confundirse con la voluntad de contratar.

---

[32] Vid. Reyes Krafft, Alfredo. Firma Electrónica y Entidades de Certificación, México D.F, Facultad de Derecho. Pp. 159. 2002.

ELEMENTOS FUNCIONALES. Tomando la noción de firma como el signo o conjunto de signos, podemos distinguir una doble función:

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. No es un método de autenticación totalmente fiable. En el caso de que se reconozca la firma, el documento podría haber sido modificado en cuanto a su contenido, falsificado, y en el caso de que no exista la firma autógrafa puede ser que ya no exista otro modo de autenticación. En caso de duda o negación puede establecerse la correspondiente pericial caligráfica para su esclarecimiento.[33]
Autenticación: El autor del acto expresa su consentimiento y hace propio el contenido del documento.

La firma es el lazo que une al firmante con el documento en que se pone[34], el nexo entre la persona y el documento. Para establecer ese lazo, la firma no necesita ni ser nominal ni ser legible; esto es, no requiere expresar de manera legible el nombre del firmante; en una palabra no requiere aptitud para desempeñar aquella función identificativa de la firma.

La firma, al constituir el lazo o nexo de la persona con el documento, debe ser documental y personal y ha de haber sido puesta en el documento por el firmante en persona. La idea anterior suele expresarse como “manuscritura”

[33] Vid. Cubillos Velandia Ramiro – Rincón Cardenas, Erick. Introducción Jurídica al Comercio Electrónico. Parte VI. p. 215, parrafo I. Medellin Colombia. Ediciones Jurídicas Gustavo Ibáñez. 2002..
[34] Vid. Reyes Krafft, Alfredo. Firma Electrónica y Entidades de Certificación, México D.F, Facultad de Derecho. Pp. 160. Cit a: La Firma Electronica: Comunicación discutida en sesion del pleno de academicos de numero el dia 5 de Junio del 2000. real academia de jurisprudencia y legislación; publicada en sus anales 2000. Antonio Rodríguez Adrados.

(escritura con la propia mano, del puño y letra del suscribiente), pero se debe ampliar a cualquier otra "grafía" puesta en el documento por el firmante mismo, es decir a toda "autografía", de ahí el término de "firma autógrafa". Es decir, lo que resulta destacar es la actuación del firmante mismo en el documento y en éste orden de ideas la "manuscritura" puede ser sustituida por cualquier otra "grafía" del firmante que necesariamente haya de ser personal, como hasta ahora viene ocurriendo con la huella digital pero no por otra grafía que pueda ser impuesta por un tercero o por procedimientos que permitan a terceros imponerla.[35]

El uso mercantil y bancario ha ido orientándose a que la "firma" pueda estamparse por medios mecánicos como pueden ser el facsímil y las máquinas de firma, para poder considerarla se requiere de un acuerdo previo entre las partes en el que se haga constar que el supuesto firmante asume la responsabilidad. Por lo anterior, se cuestiona que el denominativo de firma al símbolo estampado por un tercero por medio de facsímil o máquinas de firma.
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.

[35] Op. Cit. en términos generales la firma se refiere a una señal que hace una persona con la cual se identifica y da constancia sobre la manifestación de su voluntad, que se ve legitimada en la medida que se asegura que es dicha persona quien efectúa la manifestación de la voluntad. p 115.

En éste sentido es de considerar, 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, de ahí el concepto de la UNICITRAL de equivalente funcional de la firma.

3.2. FIRMA ELECTRÓNICA Y FIRMA DIGITAL

Existen diferentes tendencias en cuanto a las acepciones sobre firma electrónica, así algunos toman como un solo tipo de firma la denominada electrónica y la digital (Ley de Simplificación Aduanera, El Salvador), y existe otra tendencia que se inclina en distinguir como dos tipos de firma, así Apol-Lonia, Martínez Nadal, considera que firma electrónica puede ser cualquier método, símbolo basado en medios electrónicos utilizado o adaptado por una parte por la intención actual de vincularse o autenticar un documento cumpliendo todas o algunas de las características de una firma manuscrita y por otro lado entiende por firma digital aquella en la que necesariamente debe generarse utilizando un sistema de criptografía o de clave publica, a diferencia de firma electrónica que son tecnológicamente indefinidas, en tanto comprenden cualquier método, sin estar específicamente determinados, es decir que puede considerarse firma electrónica a aquella generada por cualquier método de encriptación por lo regular utilizada en redes cerradas en las cuales las partes operan acuerdan la determinación de este. Por lo anterior se deduce que la firma electrónica es tomada según esta tendencia, en forma genérica, y la firma digital en forma especifica, de tal modo que firma electrónica puede equipararse al genero y la firma Digital es una especie de firma electrónica.[36]

[36] Martínez Nadal, Apol-Lonia. Comercio electrónico, Firma Digital y Entidades de Certificación. Cap. I. pp.42. año 2001.

La firma digital, refiriéndonos aquella que use un sistema de encriptación asimétrica de clave publica, también es denominada firma electrónica avanzada (derecho español / mexicano) o refrendada (derecho colombiano); pero todas estas acepciones se refieren a aquel tipo de firmas que logran demostrar mediante la aplicación de un procedimiento de seguridad que permita identificar al signatario de un mensaje de datos y que a la vez se pueda demostrar que efectivamente dicha firma se encuentra relacionada inequívoca y exclusivamente al firmante.[37]

Existen diferentes acepciones de firma digital las cuales han sido adoptadas por diferentes países en sus legislaciones, así la Ley Peruana Nº 27269 establece en su Articulo tercero lo siguiente: "Art. 3º. firma digital: la firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de llaves únicas, asociadas una clave privada y una publica relacionadas matemáticamente entre si, de tal forma que las personas que conocen la clave publica no puedan derivar de ella la clave privada".[38]

Por otra parte la Ley de Utah de 1996 de los Estados Unidos de Norteamérica se refiere a la firma digital de la siguiente manera: Capitulo uno numeral diez, firma digital: "transformación de un mensaje empleando un criptosistema asimétrico tal, que una persona que posea el mensaje inicial y la clave publica del firmante puede determinar con certeza:

1. si la transformación se creo usando la clave privada que corresponde a la clave publica del firmante.
2. si el mensaje ha sido modificado desde que se efectúo la

[37] Cubillos Velandia Ramiro – Rincón Cardenas, Erick. Introducción Jurídica al Comercio Electrónico. Parte VI. p. 215, parrafo II. Medellin Colombia. Ediciones Jurídicas Gustavo Ibáñez. 2002..

[38] Vid. Ley Peruana nº 27269.

transformación."[39]

Por otro lado en nuestra legislación el primer borrador de proyecto de Ley de Comercio Electrónico define la firma electrónica en su Art. 3 como "…cualquier medio, método, símbolo o proceso electrónico que sustituye la firma manuscrita y se adhiere o se asocia lógicamente con un mensaje de datos aceptado y aprobado por una persona dándolo por autentico, impidiendo que el signatario pretenda desconocer la autoría de la misma posteriormente. [40]

Sin embargo consideramos que la definición de firma electrónica con mas aceptación es la establecida por la UNCITRAL, en su Ley Modelo para firmas electrónicas y así la define 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 aprueba la información recogida en el mensaje de datos".[41]

Después de haber apreciado las diferentes definiciones que puede tener la firma electrónica se puede llegar a tener una idea mas amplia de lo que ella significa, sin embargo es necesario conocer que es firma electrónica en términos prácticos, técnicamente puede decirse que 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).

La firma digital es generalmente asociada o identificada con la

[39] Vid. Ley de Utah de 1996 de los Estados Unidos de Norteamérica.
[40] Vid. Primer borrador del Proyecto de Ley de Comercio Electrónico, El Salvador
[41] Vid. Ley Modelo de Firmas Electrónicas de la UNCITRAL. Art. 2.

criptografía asimétrica también denominado criptosistema de clave asimétrica o publica, basados en el uso de un par de llaves asociados como una privada conocida solo por su titular que debe mantenerla en secreto o que incluso puede ocurrir que ni siquiera el titular conoce la clave privada que probablemente se mantendrá en una tarjeta inteligente y se podrá acceder a ella mediante un numero de identificación personal en la situación ideal mediante un dispositivo de identificación biométrica por ejemplo a través de reconocimiento de una huella digital, y una clave publica relacionada matemáticamente con ella y que puede ser accesible para cualquiera estando disponible incluso por directorios públicos de fácil acceso o en publicaciones en paginas de Internet.[42]

3.2.1 CARACTERISTICAS DE LA FIRMA ELECTRONICA

INTEGRIDAD

Entendida en dos vertientes, la primera respecto de la fiabilidad del método para generarla, comunicarla, recibirla o archivarla. Y la segunda como la forma de garantizar que la información en él contenida no fue alterada.

ATRIBUCIÓN

Es la forma en que podemos garantizar que las partes que se obligan en la relación jurídica son quienes dicen ser y expresan su voluntad libre de vicios.

Esta atribución a las personas obligadas en la relación jurídica que se pretende formalizar en un mensaje de datos, no es mas que una “firma electrónica”, la cual puede ser de dos tipos: “simple y avanzada”.

[42] Martínez Nadal, Apol-Lonia. Comercio electrónico, Firma Digital y Entidades de Certificación. Cap. I. pp.47. año 2001.

ACCESIBILIDAD

Se refiere a que el contenido de un mensaje de datos en el que se consignen contratos, pueda estar disponible al usuario (emisor, receptor, juez, auditor, autoridades, etc.) para ulterior consulta, siempre y cuando las dos características anteriormente anotadas.

Es importante recalcar que el medio físico a través del cual el contenido de un mensaje de datos se pone a disposición del usuario puede ser diferente de aquel en que se creó, ya que debe garantizar la integridad del mensaje de datos, no del medio físico que lo contiene. Esto es que el mensaje puede estar contenido en el disco duro de una computadora y ponerse a disposición del usuario en un disquete, el copiarse a ese medio físico distinto al que fue creado no lo hace de ninguna manera perder integridad.

NO REPUDIACION

Significa que la información intercambiada no puede ser cambiada o alterada por el suscriptor del mensaje de datos, ya que dicha información establece con toda certeza quien es el que emitió y lo vincula directamente a el, es decir con la firma electrónica se tiene la certeza de quien fue el autor del mensaje y que por lo tanto ratifica su contenido impidiendo su posterior repudiación.

3.2.2 FIRMA ELECTRÓNICA AVANZADA

Según la UNCITRAL, para que una firma electrónica sea considerada como fiable debe cumplir con lo siguiente:

a) Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;

b) Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante

c) Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y

d) Cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.[43]

Con lo anterior es factible garantizar:

Autenticación, para asegurar la identidad de la persona con la que se está comerciando.

Autorización, para asegurar que a esa persona es la indicada para llevar a cabo una operación concreta.

Privacidad, para garantizar que nadie más va a ver los intercambios de datos que se lleven a cabo.

Integridad, para asegurar que la transmisión no sea alterada en ruta o en almacenaje No Repudiación, para garantizar que quien envía el mensaje no puede negar que lo envió él.[44]

3.3. EQUIVALENCIA FUNCIONAL

El reto más importante es establecer equivalencia entre la firma electrónica con la firma autógrafa, dándole los mismos atributos y la misma validez jurídica.

Según la Ley Modelo, “Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea fiable y resulte igualmente apropiada para los fines con los cuales se generó o comunicó ese mensaje”. La firma electrónica entonces será fiable si hay acuerdo entre las partes para su uso (intercambio de claves y contraseñas), ahora bien, por disposición de ley y salvo prueba en contrario se considerará fiable a los efectos del cumplimiento del requisito a que

[43] Cfr. Ley Modelo de Firmas Electronicas. Art. 6 parrafo 3. 2001.
[44] Cfr. Ley Modelo de Firmas Electronicas. Art.6, Parrafo 4. 2001.

se refiere el párrafo anterior:

a) Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante.

Aquí se trata de la fiabilidad del método para generarla, comunicarla, recibirla o archivarla, es decir que la creación de la firma proviene de un método seguro y a la vez garantiza que la información contenida esta integra.

b) Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante.

En este segundo literal se cumple la característica de la atribución, es decir que las partes que intervienen en la relación jurídica son quienes dicen ser, ya que firman el documento y por lo tanto se tiene la certeza de con quien se esta tratando, ya que afirman el contenido del documento con su firma electrónica.

c) Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma.[45]

Es decir que la información intercambiada no puede ser cambiada o alterada, ya que dicha firma lo vincula directamente al mensaje y no puede provenir de nadie más.

En síntesis los literales anteriores hacen referencia a las características fundamentales de la firma electrónica como son la integridad, atribución y no repudio de la información consignada en el mensaje de datos, y a la vez confirmando la identidad del firmante y el contenido del mensaje de manera tal de vincularlo directamente a el con toda certeza, por medio de su firma.

De esta manera se pretende que la documentación consignada por medios electrónicos otorgue un grado de seguridad equivalente al del papel, junto con

[45] Vid. Ley Modelo de Firmas Electronicas, Art 6, parrafo 3-4. 2001.

su característica principal, mayor confiabilidad y rapidez

3.4 NEUTRALIDAD TECNOLÓGICA

Con el paso del tiempo la tecnología avanza a pasos agigantados, no podemos limitar el cumplimiento de las disposiciones de ley a una determinada tecnología, porque no sería justo para las demás y esto limitaría el desarrollo tecnológico.

La propia UNCITRAL, sobre el particular establece que: “Convencida de que la armonización tecnológicamente neutral de ciertas normas relativas al reconocimiento jurídico de las firmas electrónicas y el establecimiento de un método para evaluar de un modo tecnológicamente neutral la fiabilidad práctica y la idoneidad comercial de las técnicas de firma electrónica darán una mayor certidumbre jurídica al comercio electrónico.”

El reto es que estas reformas puedan lograr un equilibrio entre el proceso mas dinámico, que es la tecnología, con el mas lento, que es la creación leyes.

3.5 PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

Según la UNCITRAL, un Prestador de Servicios de Certificación, es aquella persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas.

Es un tercero confiable que acredita el vínculo existente entre una clave y su propietario. Además extiende un certificado de firma electrónica el cual está firmado con su propia clave, para así garantizar la autenticidad de la información.

La existencia de diversos Prestadores de Servicios de Certificación, permitirá que sea el propio usuario quien elija a aquella Entidad que le proporcione mayor confianza y/o seguridad.

3.5.1 CERTIFICADOS

Generalmente, cuando se nos habla de certificado, entendemos por tal un documento en el cual consta una información, emitido por una persona que da fe sobre el contenido del mismo. Según la Ley Modelo de Firma electronica de la UNCITRAL[46] el Certificado es todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma (clave privada).

Es un archivo que incorpora la clave pública de un sujeto y la relaciona con su clave privada, su validez consiste en que es la propia Agencia de Certificación o un agente, persona física, dependiente de él, quien actuando como tercero confiable, verifica la identidad de el firmante y da certeza a cualquier otra sobre tal información.

En este sentido puede decirse que un certificado digital es aquella información con respecto a la clave pública que ha sido firmada por una Autoridad Certificadora. La información normalmente encontrada en el certificado, actualmente se basa en el estándar X.509 v3. Los certificados dentro de éste estándar incluyen información de la identidad del propietario de la clave privada, el tamaño de la clave, el algoritmo usado y el algoritmo de hashing asociado, vencimiento y las acciones que se pueden realizar con este certificado.

[46] Vid. Ley Modelo de Firmas Electronicas art. 2. (UNCITRAL)

El certificado es esencial para PKI toda vez que permite asociar a una persona determinada una clave pública y por ende su privada. Esto es, el propio requerimiento de certificación que incluye algunos datos del solicitante constituye el antecedente del certificado.

3.5.2. VIGENCIA DEL CERTIFICADO

Un certificado siempre tiene un tiempo de vida finito, es decir, una fecha de vencimiento. Es posible tramitar certificados de forma electrónica, esto es sin requerir la presencia del titular y esto pudiera hacerse en tanto el certificado anterior esté vigente pues con esta firma electrónica el titular genera la solicitud del nuevo certificado.

Según el primer borrador de proyecto de ley de comercio electrónico de el Salvador, la vigencia de un certificado depende directamente de la voluntad de la persona titular de la firma, así establece en su art. 36: “el periodo de vigencia estará sujeto a la voluntad del titular de dicha firma de acuerdo a lo que se estableciere en el reglamento de esta Ley o en cualquier otra Ley que hubiere al respecto.”

Con esto la ley se refiere a que el titular de la firma decidirá cuanto tiempo durara la vigencia del certificado que adquiera en proporción a los parámetros de tiempo que la ley fije a efecto de que elija el periodo de vigencia.[47]

3.6 OBLIGACIONES DE LAS PARTES: PRESTADORES DE SERVICIOS DE CERTIFICACION, USUARIOS Y LA PARTE QUE CONFIA EN EL CERTIFICADO.

[47] Vid. Primer borrador del proyecto de ley de comercio electrónico , El Salvador. Art. 36.

Una de las principales situaciones por las cuales es necesario la existencia de una normativa que regule los aspectos de firma electrónica es la necesidad de regular el proceder de las partes que intervienen en el ámbito del funcionamiento de la firma electrónica, siendo los principales las entidades certificadoras, los firmantes y los terceros que confían en el certificado, debiéndose de regular los requisitos que deben cumplir cada uno de estos para poseer tal calidad respectivamente y la conducta o modo en que deben proceder conforme a las normas establecidas en la ley.

La Ley Modelo para firmas electrónicas y Comercio electrónico, se establecen parámetros y lineamientos generales dedicados en gran medida a la homogenización de criterios para que los diferentes países establezcan en sus legislaciones internas parámetros similares en relación a la actividad de los sujetos que se relacionan en el ámbito de aplicación de la firma electrónica.

3.6.1 OBLIGACIONES DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

De conformidad a la Ley de Modelo de Firmas Electrónicas de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, la obligación de los prestadores de servicios de certificación son las siguientes:

a) Actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas. A esto se le llama Declaratoria de Prácticas de Certificación y constituye el límite de Responsabilidad frente al Usuario y Firmante del Prestador de Servicios de Certificación;

b) Actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho el firmante en relación con el certificado o que estén consignadas en él sean exactas y cabales;

c) Proporcionar a la parte que confía en el certificado medios razonablemente

accesibles que permitan a ésta determinar mediante el certificado:

i) La identidad del prestador de servicios de certificación;

ii) Que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;

iii) Que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;

d) Proporcionar a la parte que confía en el certificado medio razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera:

i) El método utilizado para comprobar la identidad del firmante;

ii) Cualquier limitación de los fines o del valor respecto de los cuales puedan utilizarse los datos de creación de la firma (clave privada) o el certificado;

iii) Si los datos de creación de la firma (clave privada) son válidos;

iv) Cualquier limitación del alcance o del grado de responsabilidad que haya establecido el prestador de servicios de certificación;

v) Si existe un medio para que el firmante dé aviso de que los datos de creación de la firma (clave privada) no estén o puedan no estar en su poder;

vi) Si se ofrece un servicio para revocar oportunamente el certificado;

e) Proporcionar un medio para que el firmante dé aviso de que los datos de creación de la firma (clave privada) no estén o puedan no estar en su poder y, cuando se ofrezcan servicios de Registro de Certificados cerciorarse de que existe un servicio para revocar oportunamente el certificado;

f) Utilizar, al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables. Serán de cargo del prestador de servicios de certificación las consecuencias jurídicas que entrañe el hecho de no haber cumplido estos.

3.6.2. OBLIGACIONES DEL USUARIO O FIRMANTE

Cuando puedan utilizarse datos de creación de firmas (clave privada) para crear una firma con efectos jurídicos, cada firmante deberá:

a) Actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma (clave privada);
b) Sin dilación indebida, utilizar los medios que le proporcione el prestador de servicios de certificación, o en cualquier caso esforzarse razonablemente, para dar aviso en caso de que:
i) el firmante sepa que los datos de creación de la firma (clave privada) han quedado en entredicho; o
ii) las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma (clave privada) hayan quedado en entredicho;
c) cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el certificado o que hayan de consignarse en él son exactas y cabales.

3.6.3. OBLIGACIONES DE LA PARTE QUE CONFIA EN EL CERTIFICADO

Cuando una parte desea averiguar la firma digital generada por otra parte, la parte verificadora necesita tener acceso a la clave pública de la parte firmante con la seguridad de que se corresponde, realmente, con la clave privada de ese firmante.[48] Así como verificar aspectos de validez y confiabilidad. Entre los cuales podemos mencionar con base a la Ley Modelo de la UNCITRAL (CNUDMI) para firmas electrónicas, los siguientes:
a) Verificar la fiabilidad de la firma electrónica; o
b) Cuando la firma electrónica esté refrendada por un certificado:
i) Verificar la validez, suspensión o revocación del certificado; y

[48] Martínez Nadal, Apol-Lonia. Comercio electrónico, Firma Digital y Entidades de Certificación. pp.63año 2001.

ii) Tener en cuenta cualquier limitación en relación con el certificado.[49]

3.7. LA CRIPTOGRAFÍA

La criptografía se divide en dos grandes disciplinas: la criptologia y criptoanálisis. La primera es aquella en que los matemáticos e investigadores se dedican a inventar de manera constante nuevos algoritmos criptográficos, con la finalidad de hacerlos mas eficaces y menos vulnerables. Los criptoanalistas se encargan de estudiar y analizar minuciosamente la debilidad que pueda tener un algoritmo y atacan el diseño hasta poder descifrarlo.

La Criptografía es la ciencia de la seguridad de la información aunque muchas veces ha sido descrita como el arte o la ciencia de la escritura secreta. Por medio de ella se puede almacenar o transmitir información en una forma tal que permite ser revelada únicamente a aquellos que deben verla.[50]

Para muchos la criptografía es el arte o técnica de aplicar matemáticas complejas para aumentar la seguridad del flujo de información por medios electrónicos. En la práctica la criptografía consiste en problemas matemáticos sumamente difíciles.

La palabra viene del griego kryptos, que significa “oculto”. La criptografía está relacionada con el criptoanálisis, que es la práctica de violar los intentos de esconder información y es parte de la criptología, donde se incluye la criptografía y el criptoanálisis.

El origen de la criptografía data de el año 2000 AC., con los egipcios y

[49] Vid. Ley modelo de la UNCITRAL sobre firmas electrónicas. Art. 11.
[50] Martinez Nadal Apol-Lonia. “la criptografia es la ciencia que se ocupa de transformar mensajes en formas aparentemente inteligibles y devolverlos a su forma original. La Criptografía se ha usado durante siglos y ha sido especialmente útil durante las guerras.”p. 45.

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 carácter siguiente del alfabeto romano. No solo los romanos, sino los árabes y los vikingos hicieron uso de sistemas de cifrado.

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

En lugar de esto, dentro de la información digital que se desea proteger, debe colocarse algún tipo de marca codificada que sirva para identificar el origen, autenticar el contenido y asegurar la privacidad ante posibles intrusos.

La protección de la privacidad utilizando un algoritmo simétrico, como por ejemplo el contenido en el estándar DES (Data Encryption Standard), es sencillo en redes pequeñas, pero requiere el intercambio de la clave secreta de encriptación entre cada una de las partes. En la medida en que han proliferado las redes, el intercambio seguro de las claves secretas se ha vuelto costoso e inadecuado. Por tanto, el empleo aislado de esta solución, es inadecuado para grandes redes de comunicación. El estándar DES sufre una desventaja adicional: requiere que se comparta el conocimiento de la Clave Privada. Cada persona debe confiar en la otra respecto de la custodia de la clave secreta común y, además, no transmitírsela a nadie más. Teniendo en cuenta que el usuario debe tener diferentes claves para cada una de las personas con las que se quiere comunicar, debe compartir con cada una de ellas una de sus claves

secretas. Esto significa que desde el punto de vista de la implantación práctica, solamente se puede establecer una comunicación segura entre personas que tengan alguna relación previa. Por tanto, los aspectos fundamentales que DES no cubre son la autenticación y el no repudio. El hecho de que la clave secreta sea compartida implica que cada una de las partes no puede estar absolutamente segura de lo que la otra ha hecho con la misma. Incluso, una de las partes puede, maliciosamente, modificar los datos sin que un tercero pueda determinar la verdadera identidad del remitente ni quién es el culpable de la alteración. La misma clave que hace posible comunicaciones seguras puede ser empleada para crear documentos falsificados en nombre del otro usuario.

3.8. ALGORITMOS CRIPTOGRAFICOS

Un Algoritmo en general es la serie de reglas que no pueden ser ambiguas y deben tener una meta clara. Dicho de otra forma los algoritmos a forma de ejemplo pueden representarse como una serie de pasos previamente detallado con un fin ultimo el cual en terminología informática siempre será resolver problemas matemáticos. Los algoritmos pueden ser expresados en cualquier lenguaje, desde el inglés al francés, hasta lenguajes de programación de computadoras.

Los algoritmos criptográficos son la base para construir aplicaciones y protocolos de encripción, estos algoritmos criptográficos son algoritmos matemáticos y están diseñados de manera que se puedan llamar con diferentes conjuntos de datos para entrar en funcionamiento. Existen dos tipos generales de algoritmos basados en claves que son: Simétricos y Asimétrico.

3.8.1 ALGORITMO DE ENCRIPCIÓN SIMÉTRICO

Aquella en la que la llave de encripción es la misma de descripción. Por tanto estamos ante un criptosistema simétrico o de clave secreta cuando las

claves para cifrar o descifrar son idénticas; o fácilmente calculables una a partir de la otra.

Cuando la clave que va a encriptar el mensaje puede ser calculada desde la clave para desencriptar y viceversa se le conoce como algoritmo simétrico. En muchos de los algoritmos simétricos, la clave de encripción y para desencriptar es la misma. Estos algoritmos requieren que el emisor y el receptor tengan la misma clave antes de comunicarse. La seguridad de un algoritmo simétrico realmente recae en la clave. El divulgar la clave significa que cualquiera puede encriptar o desencriptar la información. La clave tiene que mantenerse en secreto tanto tiempo como la comunicación se quiere mantener en secreto.

Los algoritmos criptográficos simétricos toman el texto claro como entrada. Después usando una clave simétrica, sacan una versión cifrada del texto.

Se puede considerase éste algoritmo como relativamente seguro, y esto significa que el criptoanalista ha atacado al algoritmo por suficiente tiempo como para confiar que se trata de una matemática muy sólida y que no hay manera de romper los datos cifrados usando el algoritmo, a menos que se conozca o se adivine la clave, es decir que existe la posibilidad de que se adivine la clave y se tenga acceso a la información lo cual significa que guarda un considerable margen de falibilidad.

Ejemplo de cifrado y descifrado simétrico:

Cifrado simétrico

Clave simétrica

Descifrado

Simétrico

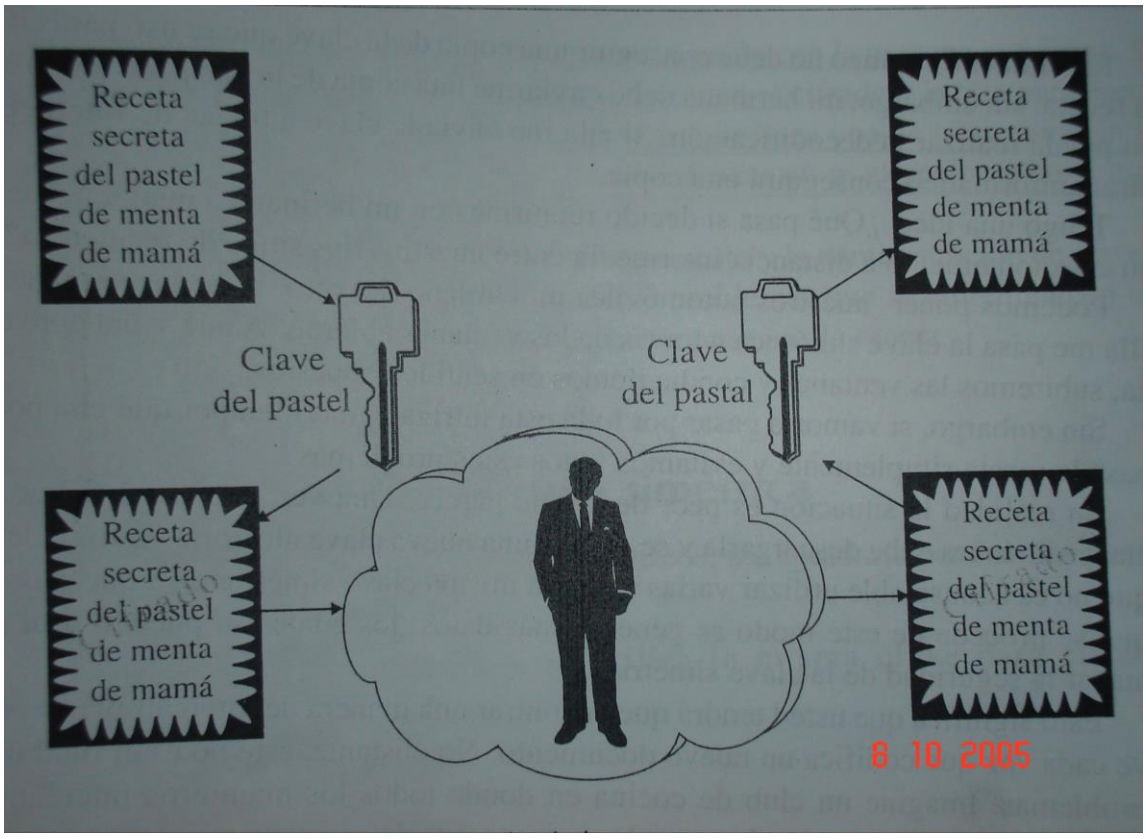
Clave simétrica

Un punto importante de estos algoritmos simétricos son las firmas digitales, como una técnica criptográfica para relacionar información con una persona, a continuación daremos algunos puntos importantes que deben tomarse en cuenta al momento de emplear algoritmos simétricos:

a) En esta criptografía se utiliza la misma clave para cifrar y descifrar.
b) El cifrado simétrico es rápido y seguro.

c) El texto cifrado es compacto.
d) Dado que la clave simétrica debe llegar al receptor, este tipo de cifrado esta sujeto a la interceptación.
e) La criptografía simétrica no se ajusta a las firmas digitales o a la aceptación.

Veamos otra grafica del cifrado y descifrado simétrico:



3.8.2 ALGORITMO DE ENCRIPCIÓN ASIMÉTRICO

A diferencia de la encripcion simétrica en la asimétrica si las claves para cifrar y descifrar son diferentes y una de ellas es imposible de calcular por derivación de la otra entonces estamos ante un criptosistema asimétrico o de

clave publica.

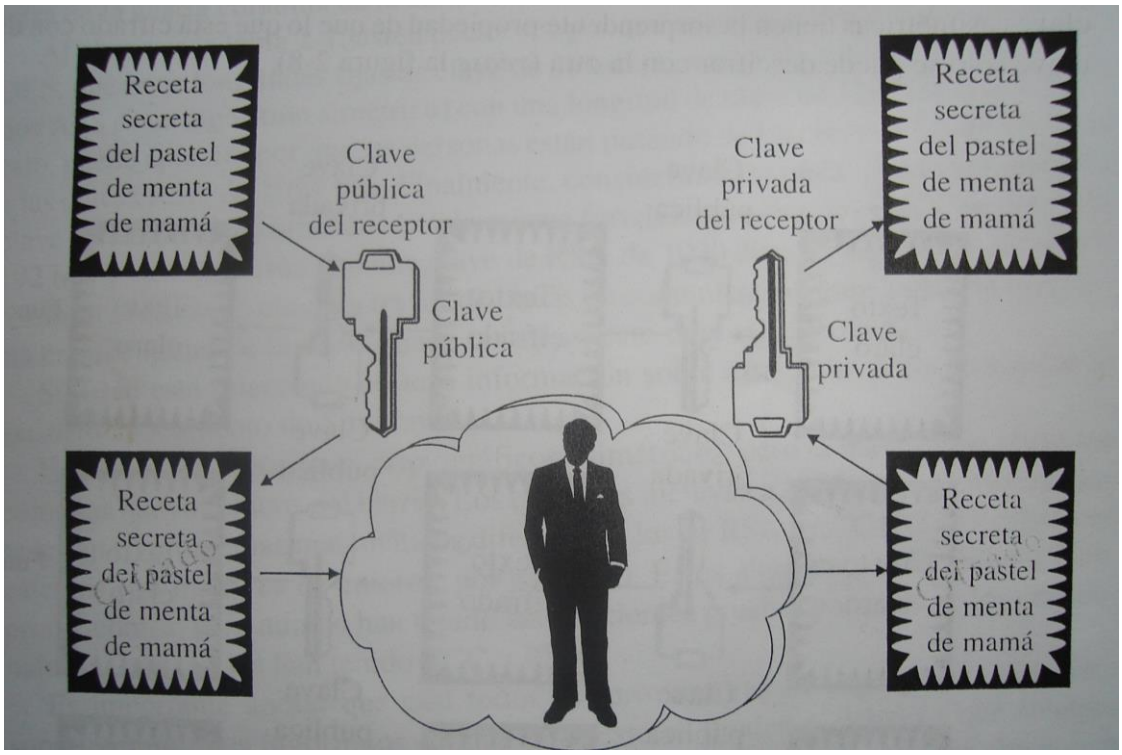
Esto quiere decir que si utilizamos un criptosistema de clave secreta o simétrica necesariamente las dos partes que se trasmiten información tienen que compartir el secreto de la clave, puesto que tanto para encriptar como para desencriptar se necesita una misma clave u otra diferente pero deducible fácilmente de la otra.

Los algoritmos asimétricos o también llamados de clave pública son diseñados de tal manera que una clave se usa para encriptar y una diferente para desencriptar. Esto ocasiona que teniendo la clave para desencriptar, no se puede calcular la clave de encripción. Estos algoritmos son llamados de “clave pública” porque la clave para encripción se puede publicar. Un completo desconocido puede usar la clave para encriptar el mensaje, pero sólo una persona puede desencriptar el mensaje. En estos sistemas, la clave de encripción es llamada clave pública y la clave para desencriptar se llama clave privada.

Al igual que la criptografía simétrica, también en la criptografía asimétrica hay algunos aspectos importantes que hay que considerar al momento de emplear este tipo de algoritmos:

a) se utilizan dos claves una para cifrar el contenido del mensaje y la otra para descifrarlo.
b) El cifrado asimétrico es seguro.
c) Debido a que no necesita enviara una clave al receptor, la codificación asimétrica no sufre la interceptación de claves.
d) La criptografía asimétrica soporta firmas digitales y aceptación.
e) El cifrado asimétrico es relativamente lento.
f) El cifrado asimétrico expande el texto cifrado.

Cifrado y descifrado de claves publica/ privada.

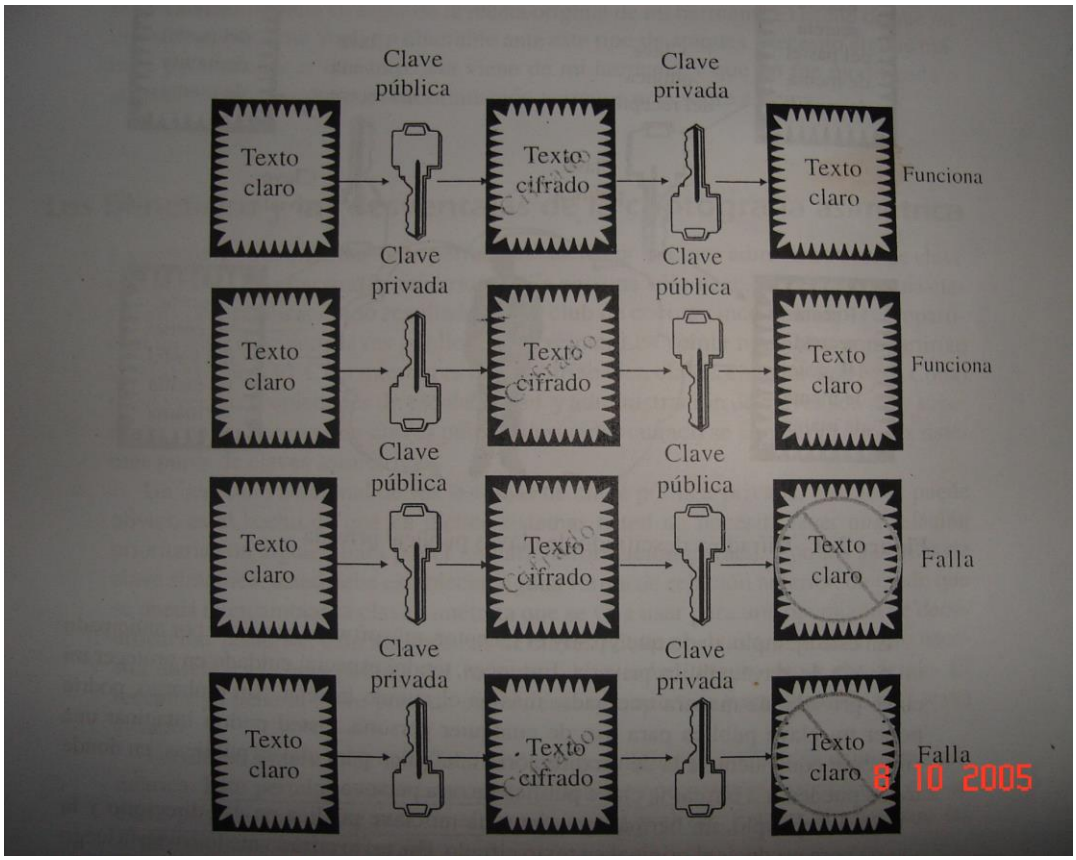


Cuando se completa la generación de una clave asimétrica, hay dos claves: una pública y otra privada. La primera es la que todo mundo conoce o al menos eso se desea y la otra es la que se guarda con mucha privacidad. Las claves asimétricas tienen la sorprendente propiedad de que lo que esta cifrado con una clave solo se puede descifrar con la otra.

Por ejemplo supongamos que uno es el receptor el software generara por anticipado mi pareja de clave publica y privada. Entonces, tendrá especial cuidado en proteger mi clave privada de manera que nadie mas en el mundo la sepa. Sin embargo mi clave pública deberá estar al alcance de cualquier persona, se supondría una situación equivalente a la de un directorio telefónico

para claves públicas.

Para ilustrarnos mejor veamos otro ejemplo del cifrado y descifrado asimetrico:



3.9 . MÉTODOS DE ENCRIPCIÓN

En las siguientes páginas se hablará de los algoritmos criptográficos más importantes usados hoy en día para la seguridad. Cada uno de los algoritmos es identificado por un nombre, un propósito, un rango de clave y por la fecha de creación. Todos los algoritmos tienen uno o más propósitos:

A) Encripción

Se usan simplemente para encriptar comunicación. Tanto el emisor como el receptor encriptan y desencriptan el mensaje usando el mismo algoritmo.

B) Firmas Digitales

Existen muchos algoritmos de firma electrónica. Todos ellos son algoritmos de clave pública con información secreta para firmar documentos e información pública para verificar las firmas. Muchas veces al proceso de firmado se le llama encriptar con una clave privada y la verificación se le llama desencriptar con una clave pública, pero esto es sólo verdadero para el algoritmo usado por RSA.

C) Hashing y Digest

Un algoritmo de hashing es una función matemática que toma una cadena de longitud variable y la convierte a una cadena de longitud fija. Es una manera de obtener una huella digital de los datos. Si se necesita verificar un archivo que pertenece a cierta persona se manda un valor de hashing para comprobarlo. Esto es muy usado en transacciones financieras. El algoritmo de hashing genera un valor para el mensaje.

El Digest es la representación del texto en forma de una cadena de dígitos, creado con una fórmula de hashing de una sola dirección. El encriptar un digest de un mensaje con una clave privada, genera una firma digital.

3.9.1. LA CLAVE PÚBLICA

La criptografía de clave pública usa un par de claves criptográficas. Si una clave sirve para encriptar la información, entonces únicamente la otra clave puede desencriptar la información. Si se conoce una de las claves no se puede fácilmente calcular la otra. Por consiguiente, en un sistema de clave pública se tiene lo siguiente:

a) Una clave pública: Que se hace público – se encuentra a disposición de todos.

b) Una correspondiente (y única) clave privada: Que se debe mantener en secreto y no se comparte a los demás.

Por medio de estos conceptos, podemos asociar los siguientes conceptos básicos:

a) Autenticación: Asegurarse que la entidad que envió los datos es quien dice ser.

b) Integridad: Asegurarse que la información no fue alterada (intencionalmente o sin intención) entre el emisor y el receptor o entre el momento que fue generado y el momento recibido.

c) Confidencialidad: Asegurarse que no cualquier entidad puede tener acceso a esa información que fue generada intencionalmente para una sola entidad.

La clave Pública usada para Encriptar Una persona en Internet usa la clave pública de otra cuando requiere enviar información confidencial. La información que será enviada estará encriptada usando una clave simétrica única, la cual será encriptada por la clave pública. Esta doble Encripción permite hacer el proceso más rápido, teniendo que encriptar con la clave pública únicamente la clave simétrica única de menor tamaño que la información. Se puede proveer de la clave pública al emisor o puede ser obtenida directamente del directorio donde ha sido publicada.

Una clave privada es usada para desencriptar la clave simétrica única y así desencriptar la información que ha sido encriptada por la clave pública correspondiente. La persona usando la clave privada puede asegurar que la información que recibe únicamente puede ser vista por ella pero no puede asegurar la identidad del emisor del mensaje.

Ejemplo de la criptografía asimétrica, en la que se usa un par de llaves: si A y B usan la misma la misma criptografía asimétrica, ambos tienen un juego de llaves, una publica que cualquier persona puede conocer y otra privada que solo su dueño conoce.

Si A envía un mensaje a B, llave publica de B y llave privada de B. A usa la llave publica de B para encriptar el mensaje que le envía B. A usa la llave publica de B para encriptar el mensaje que le envía. B usa la llave privada para

desencriptar el mensaje que le envió A y verifica la identidad de A con su clave publica.

De esta forma cuando se quiera establecer una comunicación segura con otra parte basta con encriptar el mensaje con la clave publica del sujeto para que a su recepción solo el sujeto que posea la clave privada pueda leerlo.

Si a A y B desean autenticar un documento, el proceso es al revés. A quiere enviar un documento a B, para que este lo autentique, es decir, para que B pueda comprobar que dicho documento solo pueda provenir de A. este proceso se conoce como firma digital. Cualquier persona que conozca la clave publica de A (todos la conocen), puede desencriptar el documento con esa llave. Es así como existe una llave privada de A y una llave publica de A. es así que A encripta el documento con su clave privada y lo envió a B. por lo que B desencripta el documento con la clave publica de A.

Estas claves públicas existen cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado de datos, se les llama criptosistema asimétrico. Una clave privada se mantiene en secreto, mientras que la segunda es publica. 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 cifrada. Los criptosistemas de clave publica, aunque más lentos que lo simétricos, resultan adecuados para los servicios de autenticación, distribución de claves de sesión y firmas digitales.

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 este 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 digital segura, ya 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.[51]

3.9.2. LA CLAVE PRIVADA

Si el emisor desea proveer una verificación de que es realmente esa persona, se usa una clave privada para firmar digitalmente el mensaje. A diferencia de una firma con la que firmamos papeles legales, la firma electrónica es diferente cada vez que se realiza. Un valor matemático único, determinado por el contenido del mensaje es calculado usando un algoritmo de "hashing" o "digestión" para después este valor sea encriptado con la clave privada, creando así la firma electrónica para este mensaje. El valor encriptado viene adjunto al mensaje o en un archivo por separado junto con el mensaje. La clave pública correspondiente con el valor recibido por el emisor. Si los valores concuerdan, el receptor sabe que la persona controlando la clave privada corresponde a la clave pública que envió la información. De esa manera también se asegura que la información no ha sido alterada desde que fue firmada.

Si un certificado de clave pública fue recibido con la información, entonces es validado con la Autoridad Certificadora que generó el certificado para asegurar que el certificado no ha sido falsificado y que la identidad del controlador de la clave privada es genuina.

Finalmente, si es posible, se revisa la lista de certificados revocados en la Autoridad Certificadora para validar que el certificado el válido.

Para encriptar información que será almacenada para uso propio (únicamente la persona que encripta la información podrá leerla) se usa la clave pública propia para poder desencriptar la información más adelante con la clave

[51] Reyes Krafft. Cit a: PEÑALOSA EMILIO. "la protección de los datos personales". Editorial Díaz Santos, España pp 114.

privada.

Es muy importante aclarar que la generación de las claves invariablemente debe partir del propio usuario, en la práctica el usuario baja una aplicación programada para generar el par de claves, conserva su clave privada y el requerimiento de certificación junto con su clave pública lo presenta ante una agencia de certificación o agente de ésta, se identifica y le genera un certificado.

CAPITULO IV
FIRMA ELECTRONICA EN EL SALVADOR

Sumario: *4.1. Comercio electrónico y Firma electrónica en El Salvador. Análisis reflexivo de la problemática.- 4.2. Ley de Simplificación Aduanera.- 4.3 Primer borrador del Proyecto de Ley de Comercio Electrónico (14-05-03). 4.4 Entidades Certificadoras.-*

4.1 COMERCIO ELECTRÓNICO Y FIRMA ELECTRÓNICA EN EL SALVADOR. ANÁLISIS REFLEXIVO DE LA PROBLEMATICA.

En la actualidad es innegable que cada ves mas personas de diferentes ocupaciones se apoyan en la tecnología para realizar diferentes actividades, así el uso de ordenadores es cada vez mas frecuente en el intercambio de todo tipo de información, de tal forma el comercio también se ha servido de la tecnología de los ordenadores para realizar operaciones comerciales a diferentes escalas, desarrollándose esta practica hasta convertirse en lo que hoy en día se conoce como Comercio Electrónico, el cual es definido por el Borrador de Proyecto de ley de Comercio Electrónico de El Salvador como "Toda acción comercial, financiera, tributaria o cualquier tipo de transacción que se realice por medio del intercambio de mensajes de datos o medios similares". [52]

En términos prácticos en El Salvador se ha venido desarrollando paulatinamente la practica del comercio electrónico y consecuentemente el uso de la firma electrónica, aunque no con la misma intensidad con la que la emplean en otros países con mayor desarrollo económico y tecnológico, que además cuentan con modernas legislaciones de vanguardia; Es importante señalar el crecimiento que en nuestro país ha tenido el comercio electrónico, debido a la estrecha relación con nuestro tema de investigación, ya que al

[52] Primer Borrador de Proyecto de Ley de Comercio Electrónico, de El Salvador Art. 3

hablar de desarrollo del comercio electrónico implícitamente hablamos de un desarrollo en el uso de la firma electrónica.

"En el comercio electrónico, el clásico documento de papel es sustituido por el novedoso documento electrónico. Correlativamente, desaparecen las tradicionales firmas manuscritas que pueden ser remplazadas usando métodos que son incluidos en el concepto amplio de firma electrónica".[53]

En ese orden de ideas, en la medida que el crecimiento de ese tipo de comercio, va permitiendo la creación de nuevos mecanismos o estrategias comerciales como lo es el uso de la red para realizar compras, efectuar pagos bancarios, etc., operaciones que necesitan el uso de la firma electrónica para su eficacia y efectividad.

"…la utilización de las nuevas tecnologías y los cambios que suponen, pueden generar riesgos he incertidumbres en los operadores económicos sobre cuestiones jurídicas tan esenciales, de entrada, como la validez y la eficacia de las transacciones electrónicas; así como otras cuestiones derivadas de la problemática del perfeccionamiento de un contrato celebrado por esos medios, la prueba de mismo, la distribución de riesgos y delimitación de responsabilidades entre los distintos sujetos intervinientes, la ley aplicable y la jurisdicción competente en caso de litigio".[54]

Los riesgos son casi inherentes al comercio electrónico sobre todo en las redes abiertas como el Internet, entre los más importantes pueden mencionarse:

---

[53] Martínez Nadal, Apol-Lonia. Comercio electrónico, firma digital y entidades de certificación. Año 2002. P. 41.
[54] Idem. P. 34

a) que el autor y fuente del mensaje haya sido suplantado,

b) que el mensaje sea alterado, de forma accidental o de forma maliciosa, durante la transmisión,

c) que el emisor del mensaje niegue haberlo transmitido o el destinatario haberlo recibido, y

d) que el contenido del mensaje sea leído por una persona no autorizada.

En tal sentido, es grave la falta de garantías sobre la autoría del mensaje electrónico, sobre su contenido, su integridad y aun sobre la existencia misma del mensaje, genera desde la óptica legal una inseguridad jurídica que genera dudas sobre la validez y eficacia de las transacciones electrónicas.[55]

Sin que exista una debida regulación que garantice a los usuarios la realización de sus operaciones con el menor riesgo posible, ofreciendo autenticidad, confidencialidad, integridad en el intercambio de mensajes de datos; conllevara a una apatía y desconfianza al uso de estos sistemas innovadores.

Tal como señala la Comisión Europea sobre comercio electrónico, existe una extendida inquietud respecto a la identidad y solvencia de los suministradores, su localización física y real, la integridad de la información, a protección de los datos personales, el cumplimiento de los contratos a distancia, las garantías de abono de los pagos, los recursos en caso de error o estafa, etc. [56]

En este tipo de sistema mercantil en la que se produce una transición a un comercio en el que se ha sustituido el papel y las firmas manuscritas por sus equivalentes electrónicos, los cuales deben de guardar a la vez la misma

[55] Op. Cit. p. 35
[56] Ob. Cit. pag. 36

valides y eficacia que aquellos. Por ello es que se buscan soluciones jurídicas y tecnológicas par brindar seguridad al comercio electrónico.

Por otro lado, no todo funciona de esa manera, ya que si existe una ley que regula el uso de la firma electrónica al menos en aspectos básicos o generales dirigido a un ámbito de aplicación especifico, y nos referimos pues, a la Ley de Simplificación Aduanera que es empleada en operaciones de carácter aduanal, importación y exportación de mercancía, pago de impuestos aduanales mediante el sistema de teledespacho; Esta ley establece el uso de la firma electrónica regulando solo aspectos básicos pero de suma importancia, que aunque no están regulados de una forma ordenada, trata de garantizar la Autenticidad, integridad y confidencialidad de la información que son los caracteres primordiales de la Firma electrónica. [57]

La ley Marítima Portuaria, por su parte también contempla el intercambio electrónico de datos, en los que se puede utilizar firma electrónica cuando se tengan que intercambiar documentos relacionados con el manejo de mercancías que se transportan por vía marítima, en tal sentido esta ley en su Art.90 establece: “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 en comunicarse electrónicamente, dichos documentos podrán ser sustituidos por un mensaje de intercambio electrónico d datos.

---

[57] Ley de simplificación aduanera, Republica de El Salvador, Decreto Nº. 529, del 13 de enero de 1999, Publicado en el Diario Oficial Nº. 23, Tomo 342, del 3 de febrero de 1999. Art. 8 inciso 1.

La firma podrá ser manuscrita, o bien estampada mediante facsímile o autenticada por un Código electrónico.[58]"

Cuando la Ley se refiere a una firma que sea autenticada por un código electrónico, esta haciendo alusión a una firma electrónica, sin embargo, no se establece en la ley a que disposiciones queda sujeta la utilización de este tipo de firma, circunstancia que reafirma el creciente uso de la firma electrónica y la necesidad de contar con una ley especial que regule los aspectos importantes relacionados con ella.

Por otra parte, el Ministerio de Economía ha elaborado el primer borrador, del proyecto de Ley de Comercio electrónico de fecha catorce de Mayo de 2003, que persigue establecer una regulación formal del comercio electrónico y de sus aspectos correlativos, siendo uno de estos la firma electrónica, expresa en ese sentido en su primer articulo que: "La presente ley tiene por objeto de normar la utilización de mensajes de datos y comunicaciones electrónicas, en cualquiera de sus formas, en el contexto de actividades legales, tanto comerciales como civiles en el ámbito nacional e internacional, de tal manera que ellas puedan ser certificadas válidamente, mediante procedimientos de seguridad electrónicos existentes y que a su vez permitan dar claridad, seguridad, autoría y autenticidad de las mismas". [59]

Según un articulo publicado por La prensa Gráfica el veintiuno de junio de presente año, el Centro Nacional de Registros(CNR) y el Colegio de Registradores de España firmaron el veinte de junio del año en curso, un acuerdo de asistencia técnica y cooperación para que el primero sea instruido

[58] Vid. Ley General Maritimo Portuario, decreto 994, del 19 de Septiembre de 2002, publicado en el diario oficial Nº 182, tomo 357, art. 90.
[59] Vid. Primer Borrador de Proyecto de Ley de Comercio Electronico, de El Salvador Art. 1.

en la creación de Firma Electrónica, para ser utilizada en transacciones por red en un novedoso sistema que permitirá al CNR una más pronta legalización de las pequeñas y medianas empresas(pymes), además de efectuar operaciones de registro de propiedades a través de internet, sin necesidad de desplazarse hasta las instalaciones de la institución.

El director ejecutivo del CNR, Felix Garrid Safie, aseguró que la adopción de un sistema de firma electrónica da mayor seguridad jurídica al país. Tras conocer el método, uso y aplicaciones, Safie cree necesario un marco jurídico que permita aplicar la nueva metodología incluso, si se desea al sistema bancario local.

Por su parte el presidente del colegio de registradores Nicolás Nogueles, explicó que por sistema de firma electrónica debe entenderse que cualquier persona creará su propia firma de forma sistematizada y con una serie de claves, que garantiza su inviolabilidad. Las firmas electrónicas serán enviadas en una especie de tarjeta de prepago con chip y en dispositivos similares a las memorias USB portátiles.[60]

4.2. LEY DE SIMPLIFICACION ADUANERA

La Ley de Simplificación Aduanera, inspirada en el crecimiento del tráfico comercial a nivel internacional y la profusión de negocios comerciales sobre todo regionales, sumado a la necesidad de adecuar los servicios aduaneros a los estándares mundiales de calidad y eficiencia en términos de eficiencia y facilitación del comercio internacional, que dentro de nuestro ordenamiento jurídico constituye, un importante avance en la modernización de

[60] Cfr. La Prensa Grafica. "Apoyo para una firma electrónica", articulo publicado el día martes 21 de Junio. Pp 13. 2005.

nuestra legislación en lo que a comercio electrónico y firma electrónica se refiere.

Tal como se ha mencionado en el transcurso de este trabajo, aún no existe en nuestro país una Ley de Firma Electrónica, no obstante a ello, la ley de simplificación aduanera, regula aspectos primordiales para la utilización de la firma electrónica, con la única limitante presenta que el campo de aplicación esta restringido exclusivamente al sector aduanero sea marítimo, terrestre o aéreo y que la validez de la firma solo es vigente para este sistema.

De tal manera, es necesario definir el ámbito de aplicación de la Ley, y en ese sentido el articulo 1 establece…" La presente Ley tiene por objeto establecer el marco jurídico básico para la adopción de mecanismos de simplificación, facilitación y control de las operaciones aduaneras, a través del uso de sistemas automáticos de intercambio de información." En tal sentido, en el Art. 1-A la Ley exige de la función pública y de los usuarios, la transmisión electrónica de la información relativa a los actos, operaciones o regimenes aduaneros en los que participen. Podemos mencionar dentro de estos novedosos métodos, el denominado Sistema de Teledespacho, el cual consiste básicamente en permitir el flujo o transferencia de datos en forma electrónica, la declaración y destino de mercancías. En este sistema las conexiones son realizadas a través de una red privada denominada Virtual Private Network(VPN), sistema que permite la transferencia de datos entre usuarios de Teledespacho, Bancos y Aduanas, sin que otras personas que utilizan el Internet tengan acceso a estos datos.[61]

[61] www.diescoean.com.sv

De acuerdo con el Art. 6, este sistema para asegurar la integridad de flujos de información deberá estar estructurado por procedimientos que aseguren la autenticidad, confidencialidad, integridad y no repudiación de la información transmitida.

Posteriormente en el inciso tercero, continua refiriéndose al sistema de teledespacho y lo define como “aquel 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”.

Seguidamente esta ley en su articulo 8, menciona a las entidades de certificación, en las que faculta a empresas para que provea servicios de certificación, con la finalidad de originar un control jerarquizado que permita mayor transparencia, el articulo 8 literalmente expone que: “ A efectos de garantizar la autenticidad, confidencialidad e integridad de la información y de impedir su posterior repudiación, se establecen sistemas de certificación de la información transmitida, para lo cual, se autorizará la intermediación de empresas que provean servicios de certificación de dicha información, llamadas en adelante entidades certificadoras”. Entre las funciones principales de estas entidades es la de emitir certificados de firma digital o electrónica. Aunque la Ley no de una definición taxativa de firma electrónica se deduce del texto de la ley en su articulo 8 inciso tercero lo que para efectos de la misma constituye firma electrónica, cuando establece “…y para la ejecución de las distintas actuaciones que conforman el sistema de teledespacho y para el intercambio de información en general, cada usuario autorizado, contará con 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 vinculación de ambas llaves o clases constituye la firma digital o electrónica, que para los efectos legales se constituye en el sustituto digital de la firma manuscrita que en el marco del intercambio electrónico de datos permite al receptor de un mensaje electrónico verificar con certeza la identidad proclamada por el transmisor, impidiendo a este último desconocer en forma posterior la autoría del mensaje. Los usuarios del sistema, conocidos además como suscriptores, tendrán la obligación de guardar secreto acerca de las llaves privadas que les hayan sido asignadas y responderán por las consecuencias legales que se deriven de un uso indebido de tales llaves, ya sea por parte de él mismo o de terceras personas no autorizadas".

La ley, en la anterior disposición, en ocasión de establecer un imperativo para los usuarios del sistema de teledespacho, a la vez describe lo que constituye firma electrónica, que en realidad constituye no solo un firma electrónica sino más bien una firma digital, o firma electrónico avanzada.

Del tenor del articulo citado se nota claramente la equivalencia funcional que la ley funcional que la ley hace entre firma electrónica y la firma manuscrita, en el sentido que dota a aquella de los mismos efectos legales de esta ultima, otorgándole a la firma electrónica igual valides y eficacia de una firma tradicional.

Es preciso mencionar que la validez y eficacia de una firma electrónica, esta directamente relacionada con la autenticidad que le otorgan las entidades certificadoras a las que se refiere la ley en comento, y para cumplir con esa función las entidades que sean autorizadas para operar, emitirán los

respectivos certificados que permitan a los usuarios del sistema una interacción segura en la red informática habilitada para el intercambio electrónico de datos, esta seguridad a su ves esta directamente relacionada con el uso de la firma electrónica.

Esta ley, en su artículo 8-A, establece las funciones de las entidades certificadoras las cuales consisten en:

a) Ejercer la potestad jurídica de otorgar fe pública en el marco del intercambio electrónico de datos, respecto de la pertenencia de las firmas digitales a personas naturales o jurídicas y de los términos en que se ha generado y transmitido un mensaje de datos;

Esta función que otorga la ley, en el sentido que otorga fe pública a las entidades certificadoras, puesto que la fe publica es una facultad que la ley otorga a los funcionarios públicos, cabe entonces, que surja la interrogante de si las entidades certificadoras tienen tal calidad, o simplemente es una situación que paso por alto el legislador al momento de otorgar a estas entidades de tal función.

En otras legislaciones, como es el caso de México, las entidades certificadoras dan fe de la autenticidad de las firmas electrónicas, pero no pueden dar fe pública, entonces, los encargados de dar fe pública sobre la autenticidad de las firmas electrónicas en el ámbito del intercambio de mensaje de datos serian aquellos funcionarios que ejerzan el notariado electrónico.

b) Generar el par de llaves privadas y pública, a solicitud expresa, virtualmente o por escrito, de una persona natural o jurídica;

c) Asignar las llaves públicas a los suscritos o a las personas naturales o jurídicas que así lo soliciten, verificando el cumplimiento de los requisitos que al efecto se establezcan y determinando fehacientemente la identidad y la capacidad de obrar de las personas naturales y la personería jurídica de los representantes legales de las personas jurídicas;

d) Expedir o emitir los certificados respectivos, esto es, los documentos electrónicos que, añadidos a la llave pública como datos e información características del firmante, acreditan o respaldan la vigencia y la correspondencia entre una clave pública y la persona que es titular de dicha llave, utilizando sistemas que garanticen la seguridad técnica y criptográfica de los procesos de certificación. Para estos efectos, la entidad certificadora podrá publicar el certificado en su sitio WEB de Internet, otorgarlo directamente o enviarlo a los sistemas del suscriptor de la llave pública, o entregarlo sin costo a cualquiera que lo solicite;

e) Llevar un registro magnético o directorio público en línea, tanto de las llaves públicas como de los certificados o documentos electrónicos que acrediten o respalden la correspondencia entre dicha clave pública y la persona que sea su titular;

f) Tomar medidas técnicas y administrativas tendientes a evitarla falsificación de llaves públicas y certificados; y,

g) Las demás que otras disposiciones legales o reglamentarias les otorguen.

Además se establece en su artículo 8- C, los deberes siguientes:

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

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

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

d) Rendir a favor del Fisco una garantía global, bancaria o de compañía de seguros, por el monto que se fije por el Ministerio de Hacienda;

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

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

g) Efectuar los avisos y publicaciones conforme a lo dispuesto por esta Ley;

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

i) Permitir y facilitar la realización de las auditorías por parte del Ministerio de Hacienda o de la entidad a quien corresponda dicha

función de acuerdo con las normas que a futuro rigen el comercio electrónico;

j) Elaborar los reglamentos que definan sus relaciones con el suscriptor y la forma de prestación del servicio; y,

k) Llevar un registro de los certificados emitidos.

Además de las entidades certificadoras en el sistema de teledespacho intervienen los suscriptores, es decir las personas a quienes se les asigna la firma electrónica, para los cuales la ley establece los preceptos a que deben sujetarse para utilizar la firma electrónica en este sistema. Así establece también para estos una serie de deberes que deben cumplir, así el artículo 8-D, establece los siguientes deberes para los suscriptores:

a) Certificadora, utilizando un método autorizado por ésta;

b) Suministrar la información que requiera la entidad certificadora;

c) Mantener el control de la firma digital, especialmente de su clave o llave privada;

d) Solicitar oportunamente la revocación de los certificados; y,

e) Los demás que les impongan las Leyes o Reglamentos de la República.

En términos generales puede verse que esta ley hace referencia a aspectos relevantes de la firma electrónica, pero al mismo tiempo al establecer en su

objeto, el cual es crear un marco “básico”, para poder aplicar la firma electrónica en una red cerrada conocida como teledespacho.

Podemos hoy en día a la firma digital como una verdadera institución jurídica que debe unificarse, siendo aplicable a cualquier sector, y a todo lo relacionado con la transmisión de datos por medios telemáticos en los que se requiera autenticar la autoría del consentimiento por medios electrónicos.
Dentro de todo esta abundante actividad, en las que el intercambio electrónico de datos, debido al constante innovación de la tecnología, es necesario que la ley prevea consecuencias ante la posibilidad de que se puedan violentar los sistemas bajo las tecnologías existentes y pueda alterarse la integridad de los mensajes de datos y la misma Firma Digital, es por ello que la “Ley especial para Sancionar Infracciones Aduaneras” tipifica conductas de acuerdo quede acuerdo a su disvalor jurídico, son acreedoras de una sanción de tipo penal. Siendo por este motivo que es la primara en regular delitos de carácter informáticos que en relación con la clasificación que hace el código penal pueden considerarse como delito graves, por superar la pena aplicable los tres años de prisión, en tal sentido el Art. 24 de esta ley establece infracciones y sanciones penales informáticas de la siguiente manera:

Será sancionado con prisión de tres a cinco años, quien:

a) Acceda, sin la autorización correspondiente y por cualquier medio, a los sistemas informáticos utilizados por la Dirección General;

b) Se apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación diseñado por o para tal autoridad o sus bases

de datos, que de manera exclusiva y en el ejercicio de sus controles y servicios utilizare la Dirección General;

c) Dañe los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyen el funcionamiento de los sistemas informáticos o de comunicaciones, diseñados para las operaciones de la Dirección General, con la finalidad de entorpecerlas u obtener beneficio para sí o para otra persona;

d) Facilite el uso del código y la clave de acceso, asignados para ingresar en los sistemas informáticos. La pena será de uno a tres años si el empleo se facilita culposamente; y,

e) Manipule el sistema informático o de comunicaciones a fin de imposibilitar cualquier control que con base en dicho sistema exista la posibilidad de realizar.[62]

Es notable el desarrollo que en cuanto a legislación informática ha adquirido El Salvador en lo que va del siglo, siendo el pionero el sector de Aduanas en aplicar este tipo de legislación de vanguardia, no solo al contemplar la regulación formal de firma electrónica sino también para sancionar penalmente infracciones aduaneras en el ámbito informático. Sin embargo se esta conciente de que la brecha es considerable en relación a los avances necesarios legislativos, que requiere un país competitivo.

[62] Cfr. Ley Especial para sancionar infracciones aduaneras. Art. 24. Decreto Nº 551, del 20 de septiembre de 2001, publicado en el diario oficial Nº 204, tomo Nº 353, del 29 de Octubre de 2001.

4.3. PRIMER BORRADOR DE PROYECTO DE LEY DE COMERCIO ELECTRONICO (14-05-03)

En El Salvador, actualmente se esta elaborando un proyecto de ley, por iniciativa del Órgano Ejecutivo, que actualmente se encuentra en la etapa de elaboración y redacción del texto, nos referimos, a LA LEY DE COMERCIO ELECTRONICO, la cual se encuentra en preparación por el Ministerio de Economía, y en ese sentido nos enfocaremos a hacer un análisis sobre su primer borrador.

.

Actualmente el Ministerio de Economía ha elaborado un primer borrador de este proyecto de ley, tomando como base constitucional lo dispuesto en el Art. 101 de la Carta Magna, en la parte que hace referencia al deber del Estado de promover el desarrollo económico y social mediante el incremento de la producción, la productividad, y bajo una visión de un mercado globalizado en el que El salvador no debe de quedarse al margen si desea incorporarse al comercio de la mayoría de mercados competitivos y tecnificados. Para tener una mejor idea de los fundamentos que guarda este proyecto de ley, es necesario revisar sus considerándos de este, los cuales son los siguientes:

I.- Que el Art. 101 inciso segundo de la Constitución de la República establece que es obligación del Estado, fomentar el Desarrollo Económico y Social del país.

II.- Que en el contexto de la globalización, el comercio electrónico constituye una forma innovadora y actualizada para la realización de actividades socio-económicas, lo cual abre las puertas a nuevas oportunidades para el desarrollo económico con más eficiencia y genera múltiples ventajas en las diversas actividades humanas, reduciendo los tiempos transaccionales, costos y mejor utilización de los recursos.

III.- Que con la expansión en el uso de Internet, la cual se ha convertido en un foro mundial de interrelación social, cultural y económico, en nuestro país, se vienen realizando diversas actividades comerciales por vía electrónica, sin que exista una regulación legal de las mismas.

IV.- Que con una normativa jurídica que regule el Comercio Electrónico, se supera cualquier incertidumbre en dicho medio transaccional; y se coadyuva al desarrollo de actividades socio-.económicas por vía electrónica, así como también constituye un insumo importante para estimular la inversión.

Con la sola lectura de estos considerándos es posible formarse una idea acerca de los fines que persigue este proyecto de ley, que podría resumirse en poca palabras en la obtención de un marco legal de comercio electrónico que ofrezca seguridad en sus operaciones, lo cuál se traduce en desarrollo económico para el país.

Existen muchos puntos determinantes incorporados en la justificación de esta ley, estos los podemos ordenar de la siguiente manera:

1. Fomentar el desarrollo económico y social del país;
2. Oportunidades para el desarrollo económico con más eficiencia y múltiples ventajas;
3. Reducir los tiempos transaccionales, costos y mejor utilización de los recursos;
4. El uso de Internet, la cual se ha convertido en un foro mundial de interrelación social, cultural y económico;
5. En nuestro país, se vienen realizando diversas actividades comerciales por vía electrónica, sin que exista una regulación legal de las mismas;

6. Una normativa jurídica que regule el Comercio Electrónico, se supera cualquier incertidumbre en dicho medio transaccional

Con la implementación de una ley de comercio electrónico, se busca establecer un marco jurídico adecuado a los novedosos caracteres del comercio electrónico, en tal sentido define su objeto en el primer articulo estableciéndolo así: “La presente ley tiene por objeto normar la utilización de mensajes de datos y comunicaciones electrónicas, en cualquiera de sus formas, en el contexto de actividades legales, tanto comerciales como civiles en el ámbito nacional e internacional, de tal manera que ellas puedan ser certificadas válidamente, mediante procedimientos de seguridad electrónicos existentes y que a su vez permitan dar claridad, seguridad, autoría y autenticidad de las mismas.”

El objeto de esta ley es primordialmente normar en los aspectos referentes a la transferencia electrónica de datos para su legal y eficiente utilización, en el contexto del comercio electrónico, quedando para los demás aspectos sustantivos, la aplicación del derecho común.

Para toda ley es imprescindible fijar y delimitar al ámbito de aplicación al que va dirigida, no siendo esta ley la excepción, así esta ley hace dentro del Art. 2 la especificación de los sectores del comercio a los que será dirigida su aplicación, y así establece:

“La presente Ley será aplicable a todo tipo de comunicación o información transmitida en forma de mensaje de datos, así como a toda clase de documentos en que las Leyes requieran soporte material y firmas manuscritas, siempre que la información contenida en los mensajes de datos sean legibles, estén disponibles para ser usados y presentados en cualquier momento y exista una razonable seguridad que la información que contienen se ha mantenido sin alteración desde el momento que fue generada; salvo en los siguientes casos y materias:

1. Derecho sucesoral
2. Derecho de familia
3. Aquellos actos jurídicos o contratos para los cuales otras leyes exijan expresamente formalidades especiales que no queden cubiertas por esta ley.
4. Aquellas advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón del riesgo que implica su comercialización, uso o consumo.
5. Cuando sea contrario a normas de tratados y convenios internacionales ratificados por El Salvador.

No se considerará que un mensaje de datos cumple con los requisitos del inciso anterior, si el iniciador o su sistema electrónico de envío no permite que el destinatario imprima o guarde dicho mensaje o que el mismo no pueda ser recuperado posteriormente por cualquier medio técnico.”

Este es el ámbito de aplicación que hasta el momento se ha establecido para ley de comercio electrónico, que por ahora solo constituye un Primer Borrador, al cual es posible realizarle todas las modificaciones que el Órgano Ejecutivo considere pertinentes antes de presentarlo formalmente a La Asamblea Legislativa.

En relación a la firma electrónica el presente proyecto de Ley en su articulo 3 la define como cualquier medio, método, símbolo o proceso electrónico que sustituye la firma manuscrita y se adhiere o asocia lógicamente con un mensaje de datos aceptado y aprobado por una persona dándolo por auténtico, impidiendo que el signatario pretenda desconocer la autoría de la misma posteriormente.

En relación a este precepto, debe revisarse lo que la Ley Modelo sobre Firmas Electrónicas de la UNCITRAL, define como firma electrónica y en ese sentido establece en su Art. 2 “ Para los fines de la presenta ley:

a) Por “firma electrónica” se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos.“

Es importante notar lo dispuesto en el Art. 10 del borrador en comento, ya que se refiere a la firma de documentos y dispone que “ Cuando la ley exija la existencia de una firma manuscrita en un documento en forma material, se entenderá satisfecho dicho requerimiento en relación con un mensaje de datos, cuando: ”

b) …”el mensaje de datos ha sido firmado con una firma electrónica de acuerdo con los requisitos de la presente ley.”

Como se puede notar, se prevé el uso de la firma electrónica en el Borrador ya que esta se encuentra directamente relacionada con la firma de documentos que contienen obligaciones adquiridas dentro del comercio electrónico y validadas mediante la Firma Electrónica, que es tomada con la misma aceptación de la firma manuscrita y con los mismo efectos como firma. A efectos de hacer una comparación para revisar la armonía y homogeneidad del Primer Borrador en relación a lo establecido en el Art.6 de la Ley Modelo de firmas electrónicas de la UNCITRAL que establece:

“Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica

que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea fiable y resulte igualmente apropiada para los fines con los cuales se generó o comunicó ese mensaje.”

En el primer borrador se dedica el capitulo V, Art. 32 y siguientes a la regulación de la firma electrónica en el cual se establecen disposiciones generales atinentes a la misma, así mismo detalla en su Art., 33 los requisitos esenciales para la valides de la firma electrónica consistentes en:

a) Que garanticen la confidencialidad del mensaje.
b) Que sean susceptibles de verificación la autoría e identidad del emisor.
c) Que estén bajo el control exclusivo de la persona que la use
d) Que estén ligados a la información o mensaje de datos.
e) Que no altere la integridad del mensaje.

Dentro del mismo capitulo V se incorporan los deberes y responsabilidades de los suscriptores, las cuales consisten en:

a) Aceptar la firma electrónica que le asignen las entidades de certificación.
b) Actuar con la debida diligencia y tomar las medidas de seguridad necesarias para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada de si firma.
c) Suministrar toda la información que requiera la entidad de certificación.
d) Solicitar oportunamente la revocación de los certificados.
e) Cumplir con las obligaciones derivadas del uso ilegal de su firma.

Además, establece aspectos importantes para la firma electrónica como la vigencia de la misma, la cual dependerá de la voluntad del titular, así también en su Art. 36 establece las obligaciones del suscriptor las cuales a la vez dependen de la vigencia de la misma.

El borrador del proyecto de ley, siempre en lo relativo a la firma electrónica, mas adelante en el Capitulo VI, Art.37 ubica las disposiciones relativas a las entidades de certificación y certificados, tomando como tales aquellas publicas o privadas, nacionales e internacionales, que estén jurídica y tecnológicamente capacitadas para emitir certificados electrónicos, de esta forma el proyecto establece la debida autorización que estas entidades deben de tener para operar , aunque el borrador aun no establece quien será la entidad encargada de dar dicha autorización, establece los requisitos que debe tener la entidad certificadora para poder ser autorizada, estableciendo las condiciones siguientes:

a) Ser persona Jurídica
b) Contar con la capacidad financiera y humana suficiente para poder prestar los servicios autorizados como entidad de certificación
c) Contar con la capacidad y elementos técnicos necesarios para la generación de firma electrónica, la emisión de certificados de autenticidad de firma electrónica.
d) Garantizar un servicio de suspensión, cancelación y revocación, rápido y seguro de los certificados que emita

Los certificados que emitan las entidades certificadoras deberán tener requisitos indispensables que vinculen al titular con la firma electrónica, por ello el anteproyecto establece que los certificados de firma electrónica deben contar al menos con:

a) Nombre y dirección del suscriptor
b) Nombre y dirección donde realiza sus actividades la entidad de certificación.
c) Contar con un método seguro para identificar al suscriptor.
d) Numero de serie del certificado.

e) Fecha de emisión del certificado.

Debe de recalcarse que el proyecto de ley requiere de la aplicación de un reglamento para su cumplimiento, por ello es de deducir que muchos aspectos sobre la firma electrónica serán desarrollados conforme a las disposiciones del respectivo reglamento mientras no se emita una LEY ESPECIAL DE FIRMA ELECTRONICA.

La existencia de un Borrador de anteproyecto de ley de firma electrónica demuestra la iniciativa del Ejecutivo por medio de Ministerio de Economía que nace de la necesidad de regular el comercio electrónico por medio de una ley, que por consecuencia regula la firma electrónica aunque en sus aspectos mas básicos debido a que en el comercio electrónico es inminente la posibilidad que se contraigan obligaciones dentro de su plano virtual, por ello, es así necesario la suscripción de tales obligaciones por los mismos medios digitales es decir utilizando una firma electrónica que reúna los requisitos legales para su validez y aceptación; no obstante que el Borrador que se comenta representa un progreso significativo en la modernización o al menos actualización de nuestra legislación, la firma electrónica requiere de mayor exactitud es decir que necesita de una regulación mas amplia que contemple detalladamente todos sus aspectos de manera que en caso de un eventual conflicto la firma electrónica sea eficaz según sus fines y pueda determinarse con plena seguridad la autenticidad de la firma en el caso concreto, es necesario así una legislación que exija la existencia de un soporte físico y tecnológico con el que deban de contar los usuarios, entidades certificadoras así como las autoridades en lo referente a la firma .

4.4. ENTIDADES CERTIFICADORAS

Según la UNCITRAL, un Prestador de Servicios de Certificación, es

aquella persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas[63].
Es un tercero confiable que acredita el vínculo existente entre una clave y su propietario. Además extiende un certificado de firma electrónica el cual está firmado con su propia clave, para así garantizar la autenticidad de la información.

La existencia de diversos Prestadores de Servicios de Certificación, permitirá que sea el propio usuario quien elija a aquella Entidad que le proporcione mayor confianza y/o seguridad.

Según lo dispone la Ley de Simplificación Aduanera las Entidades Certificadoras constituyen empresas intermediarias que serán autorizadas por el Ministerio de Hacienda para que puedan fungir como tales, estableciendo requisitos para que puedan operar, además de las funciones y deberes que estas tienen.

En el Salvador es requisito que la entidad certificadora sea una Persona Jurídica, con capacidad tecnológica para brindar los servicios de generación y certificación de firma electrónica o digital. Actualmente existen ya operando diversas entidades de certificación, entre ellas: Distribuidora Global Salvadoreña, Aracavi, S.A. de C.V., Servicios Electrónicos Digitales, UNISOFT, IDESAC, MAP S.A. de C.V., y en especial, la Primera y mas destacada certificadora, conocida como DIESCO EAN EL SALVADOR, entidad certificadora que opera en al país con el propósito de consolidar el comercio electrónico por medo de estándares internacionales (EANCOM/EDIFACT/XML), desarrollados bajo el contexto del intercambio electrónico de datos, mas

[63] CFR. Ley modelo de la UNCITRAL para las firmas electrónicas.

conocido como EDI, a través de la red mundial Internet a desarrollado e implementado los siguientes proyectos, en conjunto con las instituciones u organizaciones según se describe en cada proyecto.
El trabajo desarrollado a la fecha, se ha enfocado en los sectores comercial, aduanal (importaciones) y financieros.

Esta entidad certificadora se ha desarrollado en diversos aspectos, en los cuales tiene aplicación la Firma Electrónica entre los cuales se encuentran el TELEDESPACHO, el cual consiste en el sector aduanal en los tramites de importación por Internet.

Desde enero del 2002, existen más de 250 empresas (usuarios) realizando transacciones reales por Internet con la Dirección General de la Renta de Aduanas de nuestro país (envío de la declaración de mercancías/póliza por Internet), agilizando en gran medida el procesamiento de la información para la importación de mercadería. Los principales usuarios son empresas de courier, agencias aduanales, maquilas y empresas industriales (importadores/exportadores directos).

El intercambio de información, particularmente de la declaración de la mercancía y la respectiva respuesta por parte de la Dirección de Aduanas, se hace bajo estándares EDIFACT, con un modelo de seguridad altamente confiable que contempla el uso de certificados digitales, firma digital y criptográfica (infraestructura estándar de la llave pública/privada).

La DIESCO en El Salvador, cuenta con su autoridad certificadora, la primera entidad certificadora cerrada en el país, ya que como se sabe, 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.[64] Estos mecanismos de seguridad permiten asegurar el envío y la recepción de la información, ya que el emisor, al firmar el documento electrónico y al validarlo con su certificado digital, esta dotando a dicho documento con las siguientes características de seguridad: no repudio, autenticación e integridad del emisor del mensaje. Adicionalmente este mensaje firmado se codifica (cifra) para que viaje por Internet en un lenguaje en que solo las partes involucradas pondrán entenderlo. Esta autoridad certificadoras es puntual en aclarar que los certificados digitales emitidos por ella solo certifican al usuario, no la información y su uso es únicamente para teledespacho por Internet (tramites de importación por Internet con la Dirección General de la Renta de Aduanas).

Desde Octubre de 2002, con el objetivo de facilitar al usuario el teledespacho el poder realizar una orden de pago de los impuestos de importación desde su oficina, y así evitar tener que enviar a alguien a certificar cheques para poder retirar la mercadería en las diferentes aduanas del país, el Ministerio de Hacienda tuvo a bien contratar los servicios de consultoria DIESCO EAN en El Salvador para el desarrollo de una plataforma de pago electrónico, en adelante TELEPAGO, actualmente este sistema cuenta con la participación de bancos como: Banco Cuscatlan, Banco Salvadoreño, Banco Americano, Citibank, Banco de Comercio.

El modelo de seguridad para telepago esta basado en estándares internacionales EAN - UCC, bajo los servicios de autenticidad, no repudio, integridad y confidencialidad más el uso de certificados digitales, y el uso de llaves públicas y privadas. [65]

---

[64] www.diescoean.com.sv.
[65] www.diescoean.com.sv.

CAPITULO V
ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACION DE CAMPO

Sumario: 5.1 Entrevista realizada a usuarios del teledespacho que operan con firma electrónica en la aduana terrestre de el salvador.- 5.2 Análisis del resultado de la entrevista realizada en almacenes siman, al departamento de ventas por Internet.- 5.3 análisis de la información obtenida en la entrevista dirigida al licenciado David Rodríguez, gerente de servicio al cliente de diesco ean el salvador, entidad certificadora en el sistema de teledespacho.- 5.4 Conclusiones.- 5.5 Recomendaciones.

5.1. ENTREVISTA REALIZADA A USUARIOS DEL TELESPACHO QUE OPERAN CON FIRMA ELECTRÓNICA EN LA ADUANA TERRESTRE DE EL SALVADOR.

INTRODUCCION

En nuestra investigación de campo se utilizó la técnica de investigación denominado entrevista estructurada o dirigida, la cual consiste en entrevistar al informante clave. llamados así porque se encuentran en una posición muy importante la cual les permite proporcionar información que otras personas desconocen o darían incompleta, bajo este método las entrevistas fueron dirigidas a tres instituciones, la primera fue desarrollada en la administración General de Renta de Aduanas, cuya dependencia esta ubicada en la Aduana Terrestre de San Bartolo, la segunda entrevista fue realizada al jefe del departamento de Ventas por Internet de Almacenes Siman y la tercera y ultima fue hecha al Gerente de Atención al Cliente de DIESCO EAN, lic. David Rodríguez.

ANALISIS

La primera entrevista que fue elaborada en la aduana de San Bartolo nuestro informante clave fue: el Licenciado Moisés García jefe de la Unidad Atención al Usuario.

Los resultados obtenidos de la primera entrevista son los siguientes; se trabajo con un esquema sencillo el cual nos permitiera obtener la mayor cantidad de información posible, que reflejaran información practica, la entrevista se inicio estableciendo cual era e sistema que se había utilizado hasta que se incorporo el sistema de Teledespacho, se nos explicó que aproximadamente hace una década los procedimientos eran realizados de forma manual todo era hecho por mecanismos de bajo rendimiento y poca capacidad. Posteriormente con la implementación del sistema de teledespacho el trabajo de captura e información permitió un avance y desarrollo muy notable, de cuyo avance se desprenden las características siguientes:

1. Celeridad (tiempo): ya no es necesario desplazarse hasta las aduanas o fronteras físicamente para la declaración de mercaderías.
2. ubicación: La declaración de mercaderías puede realizarse desde cualquier parte del mundo u oficina.
3. pluralidad: todas las aduanas están enlazadas y cuentan con un acceso a consultas de transito o del estado de mercaderías desde la terminal del usuario al sistema de teledespacho.

No esta demás mencionar que la declaración de mercaderías puede todavía realizarse por medio de escritos formales pero solamente en algunos casos, tales serian por ejemplo: los equipajes procedentes del extranjero, todo este procedimiento forma parte del sistema llamado SIDUANEA, cuyo significado es sistema aduanero sistematizado.

Otra de las preguntas realizadas estuvo basado en los requisitos que exige la Dirección General de Renta de Aduanas para hacer uso del sistema de teledespacho, de la cual se nos dijo que este debería ser primeramente un auxiliar de la función pública:

1. En el caso de los agentes aduaneros lo primero es obtener las resoluciones de la DGRA, para poder tener acceso a los sistemas informáticos y la designación de llaves o claves de acceso para la declaración de mercaderías, transito internacional, pagos electrónicos y “firmas electrónicas”.
2. hacer contrato con las compañías que prestan los servicios de certificación.
3. contratar el servicio y el soporte técnico de Internet y línea dedicada (IP Publico).

De la anterior pregunta se desprende inevitablemente el determinar como están constituidos los sistemas informáticos a la aduana. La forma de acceder al sistema es a través de perfiles de usuarios, esto significa que existen categorías como agentes aduaneros, transportistas, gestor de encomiendas, etc.

Consecuentemente en el mismo orden se cuestiono si existe un método que facilite la identificación exacta de quien realiza la declaración de mercaderías, de la cual efectivamente se cuenta con un código personal que representa su identidad el cual es otorgado por la Aduana y además a esta poseen unas claves de acceso que son creadas por el mismo usuario (firmas electrónicas), las cuales deben de ser confidenciales y exclusivas para cada uno y solamente ellos y la aduana poseen conocimiento.

Se pregunto además si la información intercambiada no puede ser alterada, de la cual se nos dijo, que por el hecho de ser llaves personales e intransferibles es difícil que se de el caso, pero si esto ocurriera el usuario puede solicitar nuevos accesos.

Por otro lado como es conocido quien hace uso de procesadores de información ésta siempre es susceptible de perdidas por diversas razones propias o ajenas a su voluntad y es por esta razón que es responsabilidad de la Aduana generara copias de respaldo lo que permite garantizar la existencia fidedigna de la base de datos dicho respaldo son llamados back up y están hechos todos los días, si los problemas son hechos por los usuarios se aplican sanciones que pueden ser tributarias o personales.

Cambiando el enfoque práctico del uso del sistema de teledespacho se formulan las siguientes interrogantes: ¿Considera necesario que exista una ley que regule el uso exclusivo de la firma electrónica? La respuesta obtenida fue la siguiente: si es necesario ¿por qué? Porque permite y otorga garantías al usuario estableciendo derechos y obligaciones, aunque la Ley que regula esta parte es la Ley de Simplificación Aduanera pero esta se queda corta en algunos casos más complejos que puedan surgir en el quehacer aduanero.

Finalmente al preguntar cuales son los beneficios obtenidos con la implementación de la firma electrónica en el sistema de teledespacho, sin mayor problema se refirió a:

1. mayor eficiencia en el despacho de las mercaderías (disminución de tiempo)
2. Reducción de costos en concepto de desplazamiento.
3. mayor transparencia en los trámites.

5.2. ANALISIS DEL RESULTADO DE LA ENTREVISTA REALIZADA EN ALMACENES SIMAN, AL DEPARTAMENTO DE VENTAS POR INTERNET.

INTRODUCCION

La segunda entrevista la llevamos a cabo en la empresa de Almacenes Siman, ya que esta es una empresa de sólido prestigio con diversas áreas que ofrecen diversos productos al cliente, y para fines de nuestra investigación el área del Departamento de ventas por Internet es nuestro campo a investigar.

Se elaboro una guía de entrevista la cual fue elaborada con siete preguntas que a nuestro criterio son las que reúnen las inquietudes mas importantes a efectos de poder dar un análisis concreto y posteriormente a brindar conclusiones y recomendaciones, sobre la base de los datos recolectados.

ANALISIS

Esta entrevista fue realizada al Lic. Javier Campos jefe del Departamento de Ventas por Internet de Almacenes Siman.

La entrevista se realizo preguntando ¿Cuál era el sistema que utiliza Almacenes Siman para identificar usuarios y que genere las condiciones de seguridad y confianza? La respuesta fue que no identificaban usuarios, es decir se utiliza un password, no utilizan firmas electrónicas para identificarlos, respuesta que se complementó con la segunda pregunta, ¿porque no utilizaba la firma electrónica en el proceso de ventas por Internet? nos manifestó que no había existido la necesidad de hacerlo, ya que Siman lo hace de la forma que se mencionó (usuario + pass Word), y por el sistema de pago de la tarjeta Credisiman. Aunque nos menciono que si se había contemplado el uso de la firma electrónica para futuras operaciones a través del Internet.

Pero eso nos llevo a preguntarle que a pesar de contar con un sistema de identificación como el lo mencionó seguro, ¿como puede asegurarse de la identidad de aquel con quien realizan la operación?, y nos manifestó que un

banco que recibe la información del cliente e investigan su record verificando la identidad de la persona, y que a pesar de ese procedimiento no es del todo seguro, de con quien están realizando la operación.

Posteriormente le preguntamos de cómo ellos pueden asegurarse que la información intercambiada no ha sido modificada en el proceso de envío, y el nos contesto que usan protocolos de seguridad SSL (secure socket layers) y certificados con Verising, que es una compañía que se encarga de acreditar a las empresas que realizan operaciones comerciales por Internet como sitios seguros y que la información que en ese momento una persona esta observando es única y personal.

Almacenes Siman realiza estas operaciones con regulación interna de la empresa, es esta la que establece las condiciones en las cuales se va regir la contratación, ya que en el país no existe Ley que regule el comercio electrónico y mucho menos la firma electrónica, y eso nos llevo a preguntarle si conocía del proyecto de Ley de Comercio electrónico que actualmente se encuentra en la fase de desarrollo del texto en el Ministerio de Economía, y nos manifestó que no conocía de dicho proyecto.

Esta fue la entrevista de forma dirigida que realizamos al jefe de ventas por Internet de Almacenes Siman, de lo cual podemos manifestar claramente que a pesar del sistema que la empresa utiliza, no se ha percatado de manera objetiva del uso que generaría la implementación de la firma electrónica en sus operaciones realizadas por Internet, el desconocimiento de esta herramienta tecnológica y jurídica limita el desarrollo del comercio electrónico.

En el caso de las Aduanas se ha podido observar como la Ley de Simplificación Aduanera regula la firma electrónica de una manera breve, la

misma Ley hace referencia a la regulación del Comercio electrónico y todos sus métodos de seguridad, en las aduanas se ha podido observar como la firma electrónica ha facilitado los tramites de declaración de mercaderías agilizando los tramites y lo que es mas importante “teniendo un soporte jurídico” que avale y garantice las operaciones realizadas a través de la red.

Si bien es cierto que almacenes Siman regula de forma unilateral parte del comercio electrónico a través de sus protocolos de seguridad sin necesidad de la firma electrónica, ésta como la forma mas idónea y segura para la privacidad, integración, confidencialidad y no repudiación de la información en las operaciones realizadas por Internet, no puede darse de forma aislada, porque precisamente los beneficios de la implementación de esta técnica de seguridad deben darse en todos los ámbitos del comercio electrónico. Los mismos clientes de Almacenes Siman necesitan que la información que intercambian con la empresa sea transparente y que sea tutelado por una ley.

Podemos concluir que La empresa debe de ofrecer al cliente un entorno de la forma mas segura, es decir que el protocolo de seguridad que ellos utilizan puede ser bueno, pero el cliente necesita que su información adquiera un valor jurídico, porque es la única manera en que garantiza de un ejercicio justo y reciproco del cumplimiento de las obligaciones que ambas partes adquieren.

5.3 ANALISIS DE LA INFORMACION OBTENIDA EN LA ENTREVISTA DIRIGIDA AL LICENCIADO DAVID RODRIGEZ, GERENTE DE SERVICIO AL CLIENTE DE DIESCO EAN EL SALVADOR, ENTIDAD CERTIFICADORA EN EL SISTEMA DE TELEDESPACHO.

Cuando se realizó esta entrevista se nos manifestó que la empresa DIESCO EAN EL SALVADOR, brinda a los usuarios de teledespacho servicios de creación de firma electrónica generando una clave publica y una clave privada, para lo cual vende a sus clientes un software de seguridad, al cual denominan Modulo de Seguridad para SIDUNEA.

Se preguntó porque era necesario contar con ese software o Modulo de seguridad para utilizar la firma, y se nos explicó que solo este software es indispensable en el proceso de elaboración de la Firma electrónica.

En relación a los requisitos que la empresa exige al solicitante de una firma electrónica, se nos contestó que éstos, varían dependiendo de si se trata de una persona natural o una empresa, en el primer caso, el solicitante debe contar con referencias bancarias, presentar constancia de trabajo, y el acuerdo de autorización por el Ministerio de Hacienda o por la Aduana, en el segundo caso, ser empresa legalmente constituida, y comprobar esta situación, presentar las seis ultimas declaraciones de IVA, y acuerdo de autorización por el Ministerio e Hacienda, entre los mas básicos.

Al preguntar sobre el proceso que se seguía para obtener una firma electrónica, se nos explicó que cuando un usuario compra el software de seguridad, se le otorga una licencia para su uso, la cual es individual o sea que solo puede ser usada en una sola maquina o PC(computadora) y la

computadora debe de contar con los requisitos mínimos de capacidad que se exige para usar el sistema de teledespacho para lo cual se nos proporciono un hoja con tales requisitos y que consisten en: Procesador Pentium II, III, VI, disco duro de 20 GB(Giga Bytes), ram(memoria) de 256 o mas, sistema operativo Win 98 segunda edición, unidad de CD en buen estado, el modem que determinará la empresa certificadora; Se nos advirtió que estos requisitos pueden ir cambiando según las actualizaciones que se vayan tomando por la certificadora.

Además se nos manifestó el software de seguridad no funciona solo, y que es necesario adquirir los programas necesarios para la creación de las claves y el necesario para poder encriptar los documentos que se generen en el Sidunea para, continuó añadiendo que una vez creada la firma, o sea las claves privada y publica, se procede a publicar ésta ultima en su sitio web para que los demás usuario también puedan conocerla y así poder encriptar(descifrar) los mensajes que provengan de este nuevo usuario.

Al usuario se le entrega un certificado Digital, el cual sirve para validar la firma, que es indispensable para el usuario pueda operar en el sistema de teledespacho, esta operación se puede realizar por medio un lector de tarjeta inteligente o por el disco duro de la computadora, esto ultimo queda a opción del usuario que puede optar por tomar el lector de tarjeta inteligente o de la otra manera.

La duración de estos certificados es de un año, siendo necesario renovar su vigencia anualmente, y es obligatoria hacerlo, pues si el certificado digital ya esta vencido no es fiable la firma y el usuario no puede operar mas. Cada certificado cuesta unos $100 USD.

También las actualizaciones del software de seguridad son anuales y son obligatorias para seguir operando ya que es necesario darle soporte y mantenimiento al software para que se pueda operar en buenas condiciones y bajo las normas de seguridad que van evolucionando, para lo cual se toma como base los diferentes acuerdos que dicten las diferentes entidades, por ello se ofrece este servicio al cual denomina como soporte preventivo y de evolución a las diferentes aplicaciones.

El soporte técnico que se brinda comprende entre otros, el servicio de soporte técnico telefónico, soporte remoto a usuarios, consultorio de implementación de software de seguridad, solución a fallas del software, detectar posibles fallas de comunicaciones, soporte de respaldote la información, monitoreo permanente de las transacciones y de los sistemas de funcionamiento, visitas periódicas al cliente, estos servicios constituyen el soporte técnico ordinario necesario para mantener en buen estado el funcionamiento e los sistemas operativos del Sidunea, y servicio de soporte técnico evolutivo es aparte y sirve para actualizar el software de seguridad según las nuevas aplicaciones que se pueden ir tomando por las diferentes entidades.

5.4 CONCLUSIONES

La firma electrónica tiene un ámbito de aplicación muy grande, en muchos países no solo se ha referido a aspectos meramente mercantiles, sino también a lo gubernamental y a lo jurídico.

En la mayoría de estos países se ve la utilidad que tiene la firma electrónica en el uso de las relaciones a través de la red Internet y en otras redes cerradas de menor numero de usuarios en los campos antes mencionados. Estos han unificado criterios y principios rectores a sus legislaciones internas mediante la creación de un ordenamiento jurídico en el cual reúnan los requisitos esenciales para la utilización de la firma electrónica.

Ejemplo de ello es el caso de la Ley de Firma Electrónica de España que reúne todos los requisitos que la firma de be contener y toma como base para ello los lineamientos establecidos en la Ley Modelo para Firmas Electrónicas de la UNCITRAL., la cual pretende la unificación en lo posible de la normativa de firma electrónica.

En El Salvador la firma electrónica tiene hasta el momento una regulación aislada como es el caso de la Ley de Simplificación Aduanera que brinda un soporte jurídico para el funcionamiento de su sistema de teledespacho, y de la Ley General Marítimo Portuario que la regula en su art. 90 en lo referente a la transferencia electrónica de datos; lo cual a pesar de esta breve regulación hace hasta el momento las únicas dos leyes que regulan la firma electrónica.

Por lo tanto concluimos:

I. Por la necesidad que tiene El Salvador de abrirse paso a mercados internacionales es imprescindible que actualice sus capacidades tecnológicas a estándares competitivos que le permita estar a nivel de otros países mas desarrollados con los que existen vínculos comerciales originados de acuerdos mercantiles, para lo cual necesita principalmente actualizar su legislación interna como soporte jurídico que genere confianza adecuado que brinde seguridad para la utilización de la firma electrónica.

II. Considerando que los sectores que han implementado firma electrónica lo han hecho paulatinamente de manera que han tenido la necesidad de crear para ello una legislación privativa para su sector, de igual forma aquellos que pretenden implementarla, presentan esta misma tendencia, lo que inminentemente producirá que los criterios de creación validez y eficacia de la firma sean divergentes de un sector a otro que afecta la aceptación y confiabilidad de la firma electrónica quebrantando la seguridad jurídica que esta brinda, tomando en cuenta que para la aplicación de las leyes prevalece el principio de especialidad.

III Con la implementación de una Ley que regule de manera uniforme la complejidad de aspectos que conlleva la utilización de la firma electrónica de manera armoniosa en los diferentes ámbitos que requieran su aplicación, esta se regularía formalmente bajo una ley que contemplan la diversidad de operaciones que se realizan tanto en una red cerrada como el teledespacho y una abierta como el Internet, en los que se requiera la utilización de la firma electrónica.

IV. La necesidad de regulación de la firma electrónica esta directamente relacionada con el interés generar confianza para estimular a que diversos sectores opten por gozar de los beneficios que brinda.

V. La dispersidad de normas sobre la firma electrónica implicaría la necesidad de contar con una firma electrónica distinta para cada ámbito de aplicación, dependiendo de los requisitos del sector en que se utilizaría, sea público o privado, en una red cerrada o en una red abierta.

Que diversos sectores privados que realicen operaciones por medio la red impongan las directrices de forma unilateral, creando regulaciones internas aisladas, lo cual implicaría que el efecto de esa firma se vería reflejado solo en el sector especifico en que se aplica; vulnerando los principios plasmados en nuestra constitución de igualdad jurídica, seguridad jurídica y legalidad de las leyes, que protegerían al consumidor de buena fe.

VI. Con esta nueva normativa jurídica que regule la actividad del comercio electrónico conjuntamente con la firma electrónica se superaría cualquier incertidumbre, o temor en dicho medio tecnológico e interactúan al desarrollo de actividades socioeconómicas por vía electrónica y sin lugar a duda también significa un estimulo importante para la inversión nacional y extranjera

5.5 RECOMENDACIONES

I. En vista de que sectores de importancia muestran indicios en su interés por implementar firma electrónica es necesario la creación uniforme para ella aplicable a cualquier sector, de tal manera que se cuente con un marco jurídico al que debe someterse el sector que pretenda utilizarla.

II. Es conveniente que nuestro El Salvador se apoye en la experiencia que otros países han adquirido respecto de la aplicación de firma electrónica, para optar por una legislación de firma más adecuada a nuestra realidad socioeconómica.

III. Es necesario contar con una ley firma electrónica que sea suficiente y eficaz y que abarque todos los sectores en que se utiliza la transferencia electrónica de datos en que se requiera su utilización, de modo que todos estos campos de aplicación se rijan bajo los mismos parámetros, condiciones, procedimientos, infracciones. Y consecuentemente brinde seguridad jurídica.

IV. Bajo la necesidad de homologar las normas reguladoras de la firma electrónica, es pertinente tomas en cuenta las directrices básicas que ofrece la ley modelo de firma electrónicas de la UNCITRAL, así como la experiencia adquirida en la aplicación del sistema de teledespacho regulado por la ley de simplificación aduanera

V. Es necesario que se determine en la regulación de firma electrónica la calidad probatoria del documento electrónico, en el sentido de que se clasifique como un público o autentico, para efectos de valoración en juicio.

VI. Que se determine en la Ley de Firma electrónica si las entidades certificadoras obtienen la calidad de funcionario público en cuanto la ley las faculta para otorgar fe publica, por ello es necesario que se les confiera otorgar fe del documento o de la firma electrónicamente y no fe publica en estrictu sensu.

BIBLIOGRAFIA.

LIBROS.

CUBILLOS VELANDIA RAMIRO- RINCON CARDENAS, ERICK. **"Introducción jurídica al Comercio Electrónico"**, Gustavo Ibáñez Ediciones jurídicas, Colombia Bogota, 2002.

TOMAS Y VALIENTE FRANCISCO. **"El orden jurídico medieval"** Madrid marcial pons., ediciones jurídicas y Sociales S. A, 2001.

MARTINEZ NADAL APOL-LONIA. **"Comercio electrónico, firma digital y entidades de certificación"**. 2001.

RAFAEL MATEU DE ROS, JUAN MANUEL CENDOYA MENDEZ DE VIGO. **"Derecho de Internet, contratación electrónica y firma digital"**. Editorial Aranzandi, 2002.

VILLAR JOSE MANUEL. **"Derecho de Internet: contratación electrónica y firma digital"**. Editorial Aranzandi, 2002.

TESIS

REYES KRAFFT, ALFREDO ALEJANDRO. **"Firma electrónica y entidades de certificación". Universidad Panamericana"**, México 2000.

LEGISLACION

Constitución de la republica de El Salvador de 1983. versión comentada FESPAD. El Salvador 2001.

Ley de Simplificación Aduanera Decreto Nº. 529, del 13 de enero de 1999, Publicado en el Diario Oficial Nº. 23, Tomo 342, del 3 de febrero de 1999.

Ley General Marítimo Portuario Decreto Nº. 994, del 19 de Septiembre de 2002, publicado en el Diario Oficial Nº. 182, Tomo 357, del 10 de Enero de 2002.

Primer borrador del proyecto de ley de Comercio Electrónico, 2003.

Ley Peruana de Comercio Electrónico nª 27269. 2002

Ley de Utah de 1999 de los Estados Unidos de Norteamérica.

Ley Modelo de Comercio Electrónico de la UNCITRAl, 85ª sesion plenaria de 16 de Diciembre de 1996.

Ley Modelo de Firmas Electrónicas de la UNCITRAL, Naciones Unidas, Nueva York . 2002.

Asamblea General de la Uncitral: Resolución 2205 (XXI), 2002.

SITIOS EN INTERNET

- Diesco EAN El Salvador: E-Comerce y Firma Electrónica. On line: www.diescoean.com.sv, consulta el 12 de Octubre de 2004.
- Quienes somos: consulta de leyes, Entidades de certificación. On line: www.mh.gob.sv, consulta 15 de Diciembre de 2004.
- Corte Suprema de Justicia: Consulta de Leyes. On line: www.csj.gob.sv, consulta 20 de Diciembre de 2004.

- Asamblea Legislativa: Biblioteca, Consulta de leyes. On line: www.asamblea.gob.sv, consulta 20 de Febrero de 2005.
- Aduanas de El Salvador: Teledespacho, leyes aduaneras. On line: www.aduana.gob.sv, consulta 12 de Abril de 2005.
- Firma electrónica y entidades de certificación. On line: www.bibliotecacervantes.com/tesis. , consulta 22 de Abril de 2005.
- Corte Constitucional de Colombia. On line: www.corteconstitucionaldecolombia.cl, consulta 20 de Agosto de 2005.
- Ministerio de Justicia de Argentina: Proyecto de Código Civil. On line: www.jus.gov.ar/minis/nuevo/proyectocodigocivil, consulta 12 de Septiembre de 2005.
- Digital signature act. On line: www.esis.ee/ist2004/text/101, consulta 22 de Agosto de 2005.
- Digital signature. On line: www.gp.gov.ca/statreg/stat/E/01010_01, consulta 25 de Agosto de 2005.
- Electronics Comunications and Transaccions Act 2002: Nº 25 of 2002. On line: www.internet.org.za/ect_act, consulta 02 de Septiembre de 2005.
- SB 708 – Introduced Bill Text: Senate Bill Nº 708, 89 TH General Assembly. On line: www.senate.state.mo.us/98info/billtext/intro/SB708, consulta 10 de Septiembre de 2005.

ANEXOS

Universidad de El Salvador

Facultad de Jurisprudencia y Ciencias Sociales

Cuestionario para la recolección de información sobre la Necesidad de la Regulación Jurídica de la Firma Electrónica en El Salvador

Dirigido a: Los usuarios del sistema de Teledespacho en las Aduanas de El Salvador

1. ¿Cuál era el sistema que se utilizaba para realizar la declaración de mercaderías en las aduanas, antes que entrara en vigencia la Ley de Simplificación Aduanera?

_____

_____

_____

2. ¿Cuál es la diferencia con la vigencia de la Ley de Simplificación Aduanera, el cual incorpora el sistema de teledespacho?

_____

_____

_____

_____

3. ¿Actualmente para la declaración de mercaderías sin el uso del sistema de teledepacho, puede realizarse de otra manera? Si___ No___ ¿Por qué?

_____

_____

_____

_____

4. ¿Cuál es el procedimiento formal para el uso del Teledespacho?

_____

_____

_____

_____

5. ¿Existe un método que permita la identificación exacta de quien realiza la declaración de mercaderías?

_____

_____

_____

_____

6. ¿Cómo pueden asegurarse que la información intercambiada no ha sido alterada en el proceso de envío?

_____

_____

_____

_____

7. ¿En caso de la perdida de información por problemas técnicos, cual es el procedimiento a seguir?

_____

_____

_____

_____

8. ¿Considera necesaria que existiera una Ley que regulara el uso exclusivo de la Firma Electrónica?

_____

_____

_____

_____

9. ¿Existe alguna institución que funja como intermediaria entre la Administración y los usuarios del teledespacho? Si___ No___

10. Si su respuesta anterior fue afirmativa, ¿A que institución se refiere?

_____

_____

_____

11. ¿Cuáles son los beneficios obtenidos con la implementación de la Firma Electrónica en el Sistema de Teledespacho?

_____
_____
_____
_____
_____

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

SEMINARIO DE GRADUACION

GUIA DE ENTREVISTA AL LIC. JAVIER CAMPOS, JEFE DE VENTAS POR INTERNET DE ALMACENES SIMAN.

1. ¿ CUAL ES EL SISTEMA DE CONTROL QUE UTLIZAN PARA IDENTIFICAR A LOS USUARIOS EN LAS VENTAS POR INTERNET, QUE GENERE LAS CONDICIONES DE SEGURIDAD Y CONFIANZA, SI ES QUE LO TIENEN?

_____
_____
_____

2. ¿UTILIZAN LA FIRMA ELECTRONICA EN SUS OPERACIONES? SI ___ NO___ ¿Por qué?

_____
_____
_____

3. ¿ COMO PUEDEN ASEGURARSE DE LA IDENTIDAD DE AQUEL CON QUIEN ESTAN REALIZANDO LA OPERACIÓN?

_____
_____
_____

4. ¿ COMO PUEDEN TENER LA CERTEZA DE QUE LA INFORMACION INTERCAMBIADA NO HA SIDO ROBADA, ALTERADA O CONOCIDA POR PERSONAS AJENAS?

_____
_____
_____

5. ¿EXISTE ALGUN TIPO DE REGULACION JURIDICA ESPECIAL ACTUALMENTE BAJO LA CUAL ALMACENES SIMAN REALICE SUS OPERACIONES A TRAVES DEL INTERNET? SI___ NO___ ¿Por qué?

_____
_____
_____

6. ¿CONOCE USTED LA EXISTENCIA DE UN ANTEPROYECTO DE LEY DE COMERCIO ELECTRONICO? SI___ NO___

7. ¿EXISTE LA POSIBILIDAD DE NEGOCIAR LOS TERMINOS DE UN CONTRATO EN EL INTERNET? SI___ NO___ ¿Por qué?

_____
_____
_____

MUCHAS GRACIAS

COMERCIO

- Actividad de cambio por la que se aproximan los bienes del productor al consumidor.

COMERCIO TRADICIONAL

COMERCIO ELECTRONICO

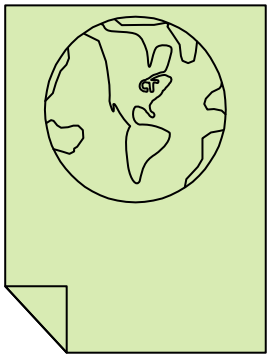
Es aquella metodología moderna de hacer negocios que detecta la necesidad de las empresas, comerciantes y consumidores de reducir los costos y mejorar la calidad de los bienes y servicios, así como minorizar el tiempo de entrega de los mismos.

COMERCIO ELECTRONICO

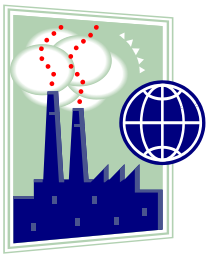
Comunicaciones por Internet

Sector Publico

Administración Publica.

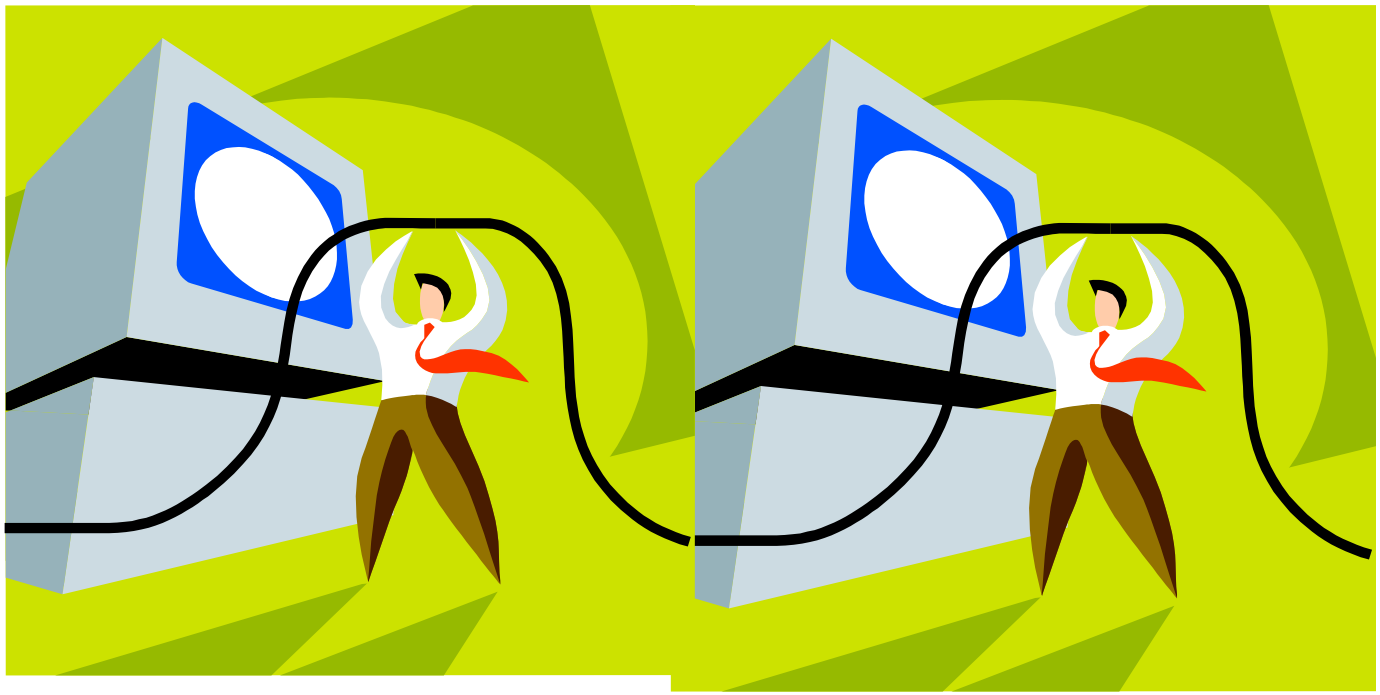


Sector Privado



- Empresa
- Consumidores

TRANSFERENCIA ELECTRONICA DE DATOS



Problemática

- Riegos en comunicaciones sobre redes abiertas
  - Posibilidad de acceso no autorizado a informaciones privadas
  - Posibilidad de suplantación de personas (identidades)
  - Posibilidad de modificación ilegítima de informaciones
  - Posibilidad de rechazo de acciones realizadas (repudio)
  - Falta de confianza en *servicios telemáticos*
  - Dificultad de puesta en marcha y aceptación de servicios complejos, teletramitación, negocios-e ...

Problemática

- Es necesario
  - Poder garantizar la identidad de las personas y las entidades
  - Poder garantizar la privacidad de las informaciones
  - Poder garantizar la integridad de las informaciones
  - Mejorar los controles de acceso a servicios
  - Poder sustituir procesos *físicos* a otros *virtuales*
  - **. . . proporcionar confianza en los servicios**

- Garantizar la identidad de las personas y entidades
  - ✓ Firma electrónica y certificación digital
- Garantizar la privacidad de las informaciones
  - ✓ Cifrado de datos
- Garantizar la integridad de las informaciones
  - ✓ Firma electrónica
- Mejorar los controles de acceso a servicios
  - ✓ Firma electrónica y certificación digital
- Sustituir procesos *físicos* a otros *virtuales*
  - ✓ Firma electrónica, cifrado de datos, almacenamiento ...

Firma Electrónica

- firma electrónica puede ser cualquier método, símbolo basado en medios electrónicos utilizado o adaptado por una parte por la intención actual de vincularse o autenticar un documento cumpliendo todas o algunas de las características de una firma manuscrita

FIRMA ELECTRONICA AVANZADA

Aquella en la que necesariamente debe generarse utilizando un sistema de criptografía o de clave publica

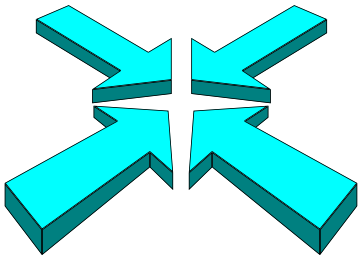
- “transformación de un mensaje empleando un criptosistema asimétrico tal, que una persona que posea el mensaje inicial y la clave publica del firmante puede determinar con certeza:
- si la transformación se creo usando la clave privada que corresponde a la clave publica del firmante.
- si el mensaje ha sido modificado desde que se efectúo la transformación.”
-

[1] Vid. Ley de Utah de 1996 de los Estados Unidos de Norteamérica.

LA SOLUCION TECNICO + LEGAL

- Una Infraestructura de Clave Pública (PKI)
  - **abierta**
  - **que refleje lo legal en lo técnico**
  - **integrable en proyectos de teleAdministración**
  - **orientada a facilitar el desarrollo de servicios y no a su propio crecimiento**

Confidencialidad **Autenticidad**



No Repudio **Integridad**

La solución legal

SOPORTE LEGAL HOMOLOGADO DE FIRMA ELECTRONICA

Ej.:

Europea

- **Directiva europea 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica**

España

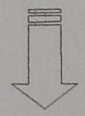
- **Real Decreto-ley 14/1999, de 17 de septiembre, por el que se regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación**

El Salvador

- **Ley de Simplificación Aduanera.**

OBJETIVO DEL TELEDESPACHO

Simplificar y mejorar los controles aduaneros, íntegrando los servicios relacionados con los procesos de importación y exportación, tanto de entidades públicas como privadas, haciendo de los documentos electrónicos y redes públicas (Internet) el principal medio de intercambio de información

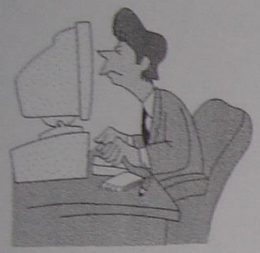


Se reduce al máximo el uso de papel
Trámites expeditos en frontera

Sistema Integrado de Información con todas las intituciones involucradas en la import / export.

3 11 2005

TELEDESPACHO PAGO ELECTRONICO



ENVIA ORDEN
PAGO AL BANCO
(PAYMUL)

OBTIENE RECIBOS
DE ADUANA Y
DEL BANCO

INTERNET

OBTENIDO No REGISTRO, GENERA
EN MODBRK LA FACTURA ELECTRONICA

INGRESA AL SISPAGO E INTEGRA LOSDATOS
DE LA FACTURA ELECTRONICA

ENVIA AL CLIENTE
RESPUESTA
INTEGRADA DE
BANCO Y ADUANA

RECIBE ORDEN DE
PAGO, VALIDA Y LO
CARGA A LA
CUENTA DEL
CLIENTE

VALIDA Y REALIZA EL
CONTROL DE PAGOS

ENVIA NUMERO DE
RECIBO (APERAK)

ENVIA NOTA DE
CREDITO(CREADV)

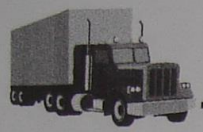
ADUANA

TESORERIA

BANCO

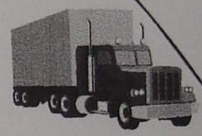
3 11 2005

IMPORTACION DE MERCANCIAS

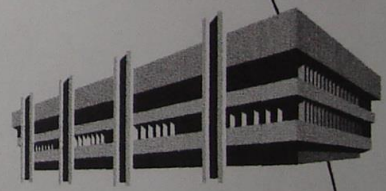


TRANSPORTISTA O IMPORTADOR LLEVA LA DECLARACION, DE TRANSITO INTERNO O INTERNACIONAL, CON EL NUMERO DE AUTORIZACION DE REGISTRO DE LA ADUANA Y CODIGO DE LA ADUANA

CONTROLADOR DE MEDIOS DE TRANSPORTE, ESTAMPA FECHA Y HORA DE INGRESO



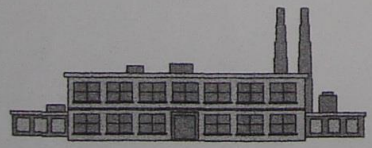
OFICIAL ADUANERO VERIFICA/LIQUIDA, DE SER INSPECCION FISICA TRASLADA A CONTADOR VISTA PARA SU VERIFICACION INMEDIATA, DE SER LA DECLARACION DE OTRA ADUANA GENERA TRANSITO ELECTRONICO Y REMITE A ADUANA RESPECTIVA.



ADUANA DE FRONTERA

SI EL RESULTADO ES LEVANTE AUTOMATICO DESPACHA MERCANCIAS A BODEGAS DEL CLIENTE

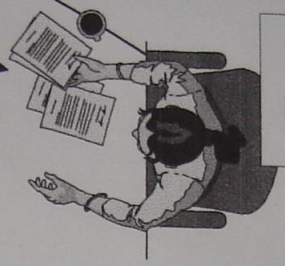
EMPRESA



3 11 2005

VERIFICACION INMEDIATA

EL OFICIAL ADUANERO ANOTA EL CODIGO 03 Y ENTREGA LA DOCUMENACION AL CONTADOR VISTA PARA SER REVISADA



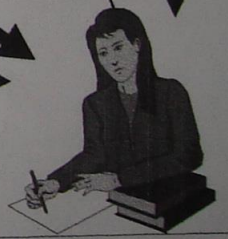
SE REALIZA AFORO DOCUMENTAL Y FISICO

MAYOR O MENOR

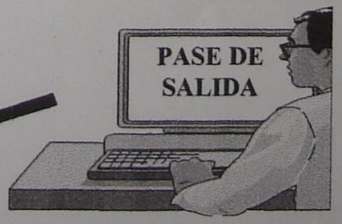
IGUAL

ELABORA HOJA DE DISCREPANCIAS Y HOJA DE LIQUIDACION CORRECTA

NOTIFICA DISCREPANCIA REALIZAN PAGO



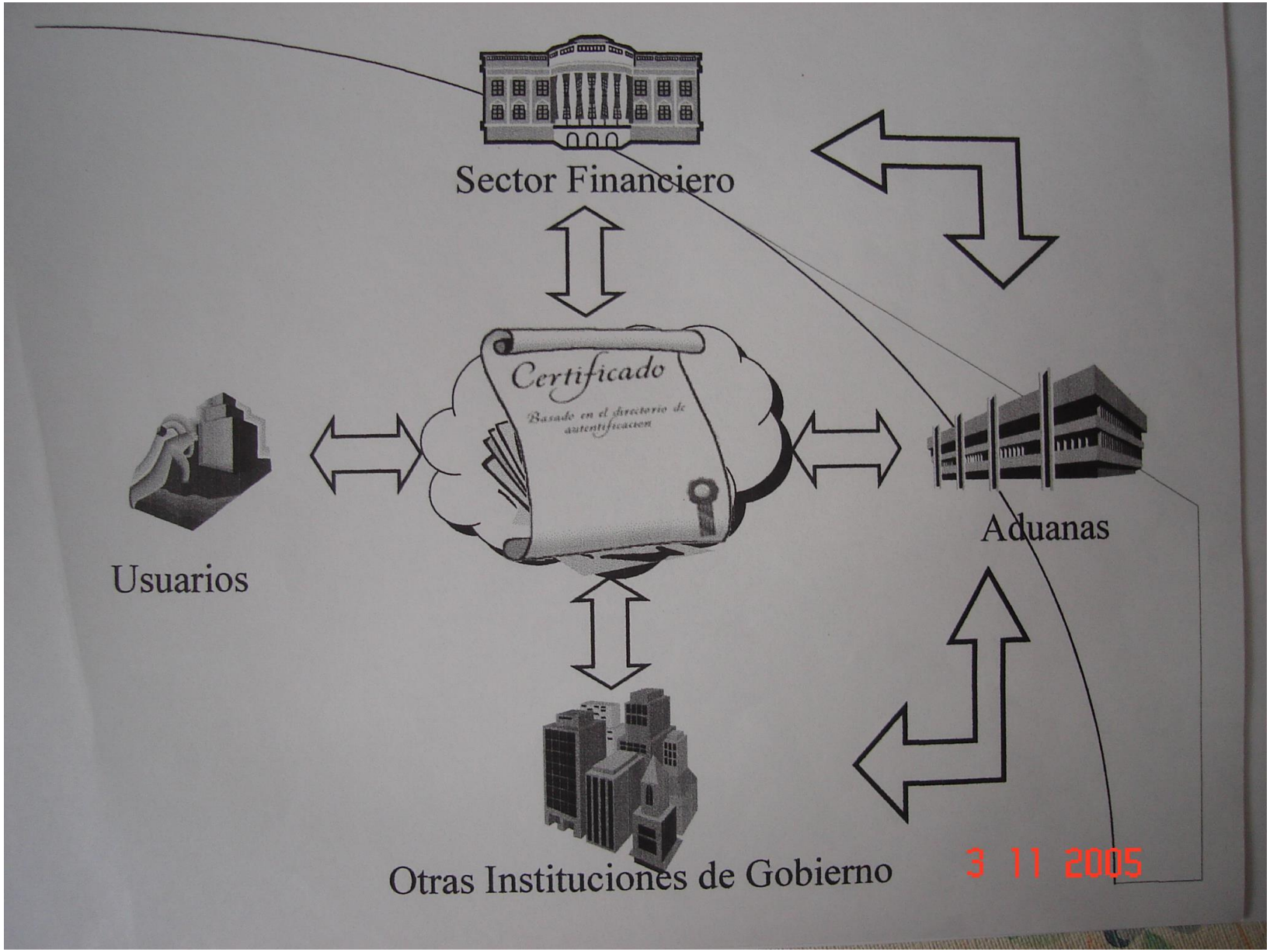
FIRMA Y SELLA DECLARACION



PASE DE SALIDA

SALIDA

3 11 2005


Sector Financiero
Certificado
Basado en el directorio de autentificacion
Usuarios
Aduanas
Otras Instituciones de Gobierno
3 11 2005


QUIENES PARTICIPARAN EN LA RED DE TELEDESPACHO POR INTERNET
BCR
INDUSTRIA
COMERCIO
AGENTES ADUANALES
TRANSPORTE
SECT. FINANCIERO
AUTORIZACIONES
ADUANAS
3 11 2005

SISTEMAS DE SEGURIDAD

- Seguridad Aplicativa Documental
  - Certificados Digitales
  - Firma Electrónica
- Seguridad de Redes: Implementación de Redes Virtuales
  - Llaves compartidas
  - Segmentación de áreas de Seguridad y Control de Accesos
- Seguridad Jurídica
  - Ley de Simplificación Aduanera

3 11 2005

TELEDESPACHO UN SISTEMA SEGURO

- ES UN SISTEMA INTEGRADO DE INFORMACION ENTRE CLIENTES, BANCOS, ADUANAS E INSTITUCIONES RELACIONADAS QUE PERMITEN ESTABLECER CONEXIONES A TRAVES DE UNA RED PRIVADA, VPN (VIRTUAL PRIVATE NETWORK)

el Congreso y el Ayuntamiento

FOTO DE LA PRENSA/ALFREDO HERNÁNDEZ

CORTÉS. *El mandatario Saca, junto al presidente del Congreso de los Diputados, el socialista Manuel Marín, durante la visita que el gobernante hizo al hemiciclo, el día de ayer.*

FOTO DE LA PRENSA/ALFREDO HERNÁNDEZ

RECIBIMIENTO. *El alcalde de Madrid, Alberto Ruiz-Gallardón, saluda al presidente salvadoreño y a su comitiva a su llegada al ayuntamiento de la capital española, en la puerta del Sol.*

3-11-2004

Apoyo para una "firma electrónica"

El Centro Nacional de Registros (CNR) y el Colegio de Registradores de España firmaron ayer un acuerdo de asistencia técnica y cooperación para que el primero sea instruido en la creación de la llamada "firma electrónica", para ser usada en transacciones por red y que es a prueba de falsificaciones.

El novedoso sistema permitiría al CNR una más pronta legalización de las pequeñas y medianas empresas (pymes), además de efectuar operaciones de registro de propiedades a través de internet, sin necesidad de desplazarse hasta las instalaciones de la institución.

El director ejecutivo del CNR, Félix Garrid Safie, aseguró que la adopción de un sistema de firma electrónica da mayor seguridad jurídica al país. Tras conocer el método, uso y aplicaciones, Safie cree necesario un marco jurídico que permita aplicar la nueva metodología incluso, si se desea, al sistema bancario local.

Por su parte, el presidente del colegio de registradores, Nicolás Nogueles, aseveró que se atrevía a firmar el documento de cooperación por la "forma moderna y profesional" en que es manejado el CNR.

Nogueles explicó que por sistema de "firma electrónica" debe entenderse que cualquier persona creará su propia firma de forma sistematizada y con una serie de claves, que garantiza su inviolabilidad. Las firmas electrónicas son transportadas en una especie de tarjeta de prepago con chip y en dispositivos similares a las memorias USB portátiles.