UNIVERSIDAD DE EL SALVADOR

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES
SEMINARIO DE GRADUACIÓN EN CIENCIAS JURÍDICAS AÑO 2008
PLAN DE ESTUDIOS 1993

"NECESIDAD DE UN MARCO LEGAL
QUE REGULE LA INTERVENCIÓN DEL NOTARIO EN LA
CONTRATACIÓN ELECTRÓNICA EN EL SALVADOR".

TRABAJO DE GRADUACIÓN PARA OBTENER EL GRADO DE:

LICENCIADO (A) EN CIENCIAS JURÍDICAS

PRESENTAN:
ORELLANA, DANIEL EDUARDO
PORTILLO BARRIERE, VERÓNICA ARGENTINA

DIRECTOR DE CONTENIDO:
DOCTOR JOSÉ NICOLÁS ASCENCIO HERNÁNDEZ

CIUDAD UNIVERSITARIA, SAN SALVADOR, JUNIO DE 2009

UNIVERSIDAD DE EL SALVADOR

MÁSTER RUFINO ANTONIO QUEZADA SÁNCHEZ
RECTOR

MÁSTER MIGUEL ÁNGEL PÉREZ RAMOS
VICE-RECTOR ACADÉMICO

MÁSTER OSCAR NEO NAVARRETE ROMERO
VICE-RECTORA ADMINISTRATIVO

LICENCIADO DOUGLAS VLADIMIR ALFARO CHÁVEZ
SECRETARIA GENERAL

DOCTOR RENÉ MADECADEL PERLA JIMÉNEZ
FISCAL GENERAL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

DOCTOR JOSÉ HUMBERTO MORALES
DECANO

LICENCIADO OSCAR MAURICIO DUARTE GRANADOS
VICE-DECANO

LICENCIADO FRANCISCO ALBERTO GRANADOS HERNÁNDEZ
SECRETARIO

LICDA. BERTA ALICIA HERNÁNDEZ ÁGUILA
COORDINADORA DE LA UNIDAD DE SEMINARIO DE GRADUACIÓN

DOCTOR JOSÉ NICOLÁS ASCENCIO HERNÁNDEZ
DIRECTOR DE SEMINARIO

Agradecimientos

DIOS Y A LA VIRGEN DE GUADALUPE, *En primer lugar quiero agradecer a ellos por ser la base fundamental de todo este trabajo, porque sin ellos jamás se hubiera logrado, Gracias Diosito y Virgencita por haberme dado la fortaleza para continuar y la sabiduría para saber que escribir.*

A MIS PADRES, *Francisca del Rosario Barriere de Portillo y José Roberto Portillo Chávez, porque sin ustedes yo no estuviera aquí, gracias por haberme dado la vida y por haberme inculcado la perseverancia, gracias también por el apoyo tanto económico como moral que sin ello no hubiese sido posible realizar este trabajo… muchas gracias, y aunque a veces no me porto bien y nunca lo digo ¡¡LOS AMO MUCHO!! Y quiero que se sientan orgullosos de mí y este triunfo también es de ustedes.*

A MI NOVIO Y COMPAÑERO DE TESIS, *gracias porque si no hubiera sido por ti yo nunca hubiera llegado hasta donde estoy ahora, gracias por todas esas veces que me aconsejaste y me diste ánimo para seguir cuando estaba a punto de rendirme y las veces que no me dejaste salirme de clases, jaja!, gracias por que por eso termine todo esto. Quiero decirte que este triunfo es de los dos, ambos hicimos que este sueño se hiciera realidad y estoy muy orgullosa de haberlo logrado contigo a mi lado. Gracias… ¡TE AMO!*

A MIS AMIGOS: *Gracias también a ellos que me ayudaron en el transcurso de mi carrera y me brindaron toda su amistad, apoyo (Xiomy, Litzardo, Edwin Orlando, Pingüi, Lorena, Cindy, Rafa.) ya que con los muchos momentos alegres que tuvimos y que aun tenemos se hizo más fácil llevar la carga de la carrera. Por eso hoy les agradezco toda esa amistad y apoyo que me brindaron y quiero desearles muchos*

éxitos y que primero Dios sigamos con esta amistad tan bonita que hemos formado, ¡GRACIAS NIÑOS, los aprecio mucho!

A NUESTRO ASESOR: *Un agradecimiento especial a nuestro asesor de tesis el Dr. José Nicolás Ascencio por sus consejos y porque él es una parte fundamental de este trabajo.*

A todos… GRACIAS!

VERÓNICA ARGENTINA PORTILLO BARRIERE

Agradecimientos

A DIOS. *Por haberme iluminado cada día, y poder culminar una meta en vida. Le agradezco por haberme ayudado hasta el último día de realización de este trabajo de graduación, y porque aun se que él me seguirá ayudando el largo camino que me falta por recorrer. Y puedo decir que hasta aquí Dios me ha ayudado.*

A MI ABUELA. *Por ser una persona que me ha aconsejado a lo largo de toda mi vida y más aun en mi carrera. Gracias a ella y a la de mi madre he salido adelante. Gracias "Mamá Súper" (como cariñosamente le decimos sus nietos) por su apoyo incondicional.*

A MI MADRE. *Quien sin ella no existiría en este mundo, que sin ella no podría decir que he terminado una página más de mi vida, y en lo personal me siento orgulloso de ella que siendo madre soltera me empujo a ser un hombre de bien y que gracias a sus consejos junto con los de mi familia, buscare ser justo y tomar las mejores decisiones a lo largo de mi vida profesional.*

A MI HERMANA. *Quien es la razón para mi superación ya que espero que mi ejemplo llegue a su vida y que reflexione sobre el camino que debe de seguir en el futuro.*

A MI FAMILIA. *Por ser un pilar fundamental en mi vida, por haberme ayudado no solo económicamente, sino que por sus consejos, regaños y mostrarme el mejor camino a seguir en mi vida como estudiante y ahora como profesional.*

A MI NOVIA. *Quien no solo fue un apoyo moral en la realización de esta tesis sino que también fue parte de ella ya que como compañera de tesis le agradezco que me haya soportado todo este tiempo, que me corrigiera cuando me equivoque, que me*

ayudara cuando más lo necesitaba. Gracias por ser una parte fundamental en mi vida. Je t´aime.

A LA UES. *Como cariñosamente le llamamos todos los que hemos salido de ella, ya que como estudiante le debe mucho a esta institución por ser la que me formo académicamente, pero en mi caso particular le debo mucho mas por haber sido un estudiante becado y que sin esa ayuda, no estaría dando estos agradecimientos.*

A MIS AMIGOS. *Quienes estuvieron conmigo no solo físicamente sino que me llevaron en sus pensamientos y sus oraciones, pero en especial quiero agradecer a Rosa, América, Ada, Wilson, Delmy y Clarisa por su apoyo a lo largo de mi carrera, ¡muchas gracias amigos!*

A MI ASESOR. *Le doy gracias por haberme dado sus consejos y haberme guiado a lo largo de este trabajo. Gracias Doctor Ascencio por su apoyo.*

DANIEL EDUARDO ORELLANA

ÍNDICE

CONTENIDO **PAGINA**

INTRODUCCIÓN

Los avances en las comunicaciones y la utilización de los medios informáticos para el registro y la transmisión de datos es uno de los hechos que más ha revolucionado el panorama actual de las relaciones de mercado. El tráfico jurídico se ha visto necesariamente transformado en cuanto a sus formas y usos por el desarrollo y la creciente utilización de las tecnologías de la información y la comunicación. En el análisis del panorama actual del tráfico económico, uno de los aspectos de interés jurídico es la utilización de las técnicas informáticas como base en las relaciones de mercado.

Los conceptos de globalización de la economía y la contratación en masa supusieron retos de estudio jurídico que claramente ponían de manifiesto la falta de adecuación de muchas de las instituciones jurídicas que tradicionalmente habían sido la base de la regulación legislativa mercantil. Esto impuso la toma de conciencia sobre la necesidad de adaptación del Derecho Positivo a los cambios operativos del mercado, esfuerzo que fue realizado en el ámbito legislativo y que planteaba no pocos escollos sobre la base de la velocidad vertiginosa de los cambios operados en la realidad a regular; a ello se unía la exigencia de planteamientos de uniformidad legislativa por la internacionalización de las relaciones que ha pasado ya de ser una tendencia y es hoy una realidad ampliamente estudiada.

En este ámbito el avance tecnológico de los medios de información y la liberalización de las comunicaciones jugaron desde el primer momento un papel de generadores de la nueva configuración del marco del mercado hacia el que tendía de forma irreversible la economía global. Dentro de estos

fenómenos de acortamiento de distancias en todos los órdenes uno de los avances más interesantes para el Derecho y de mayor influencia es el cambio protagonizado por las técnicas de comunicación informática o telemática, que facilitan una transmisión de datos de enormes posibilidades en cuanto a su contenido y volumen; si el uso de medios de comunicación en las relaciones comerciales como el teléfono o el telégrafo ya fue reconocido por el legislador como un ámbito y técnica de necesaria regulación, los avances informáticos a los que estamos asistiendo lógicamente se plantean como un reto de claro interés jurídico. Las denominadas autopistas de la información y las aplicaciones y efectos derivados del uso de las redes informáticas rebasan el mero concepto de medio de comunicación de datos para crear un mundo de relaciones virtuales en el que la información es tan sólo una utilidad más al lado de las amplias posibilidades de relaciones sociales de todo orden que se plantean.

El presente trabajo de investigación cuenta con siete capítulos en los que se va desglosando el tema de investigación, en el primer capítulo se abordan la historia del notariado latino desde sus inicios a nivel internacional, es decir cómo fue evolucionando la institución del notariado en los países europeos como Grecia, Egipto, Roma entre otros, hasta nuestro país con las legislaciones que le han dado vida al notariado. Otra institución que también ha dado un gran salto cualitativo en su evolución ha sido el comercio que con la ayuda de los que conocemos como Internet ha creado un nuevo tipo de comercio que es el comercio electrónico. Vamos a estudiar cómo se origino el comercio, el Internet y el comercio electrónico y toda la evolución que han tenido hasta llegar a la actualidad.

En el Capitulo Segundo que se denomina Aspectos Doctrinarios del Comercio Electrónico, donde se hace alusión a la globalización como un factor sumamente importante del surgimiento de las nuevas tecnologías y por

ende del comercio electrónico, así mismo entramos a lo que es el comercio electrónico con su definición, las ventajas y las desventajas que presenta para el comerciante y para los consumidores, los factores que influencian el comercio electrónico, así como el documento electrónico y la contratación electrónica la contratación electrónica, y en este punto el concepto de contrato, la naturaleza jurídica, las modalidades de este tipo de contratación, los principios jurídicos en los que se basa, los elementos de validez y la forma en que se da el consentimiento por medios electrónicos, concluyendo con la seguridad en la contratación electrónica y las amenazas a la misma como los llamados hacker y cracker.

El Capítulo Tercero que se denomina Herramientas de la Seguridad Informática para la Protección de la Contratación Electrónica, en que se hace referencia a lo que denominamos las herramientas de la seguridad informática como las autoridades de certificación, los certificados electrónicos, la firma digital así como la criptografía, todo en el sentido de brindar seguridad a las transacciones por medios electrónicos.

El Capitulo Cuatro corresponde a la legislación tanto nacional como internacional de la contratación electrónica y del ciber notario, y hacemos una mención al proyecto final de la Ley de Comunicación Y Firma Electrónica de El Salvador, que está siendo estudiado por la Secretaria técnica del Ministerio de Economía para ser entregado a la Asamblea Legislativa para su aprobación y convertirse en ley de la República.

El Capítulo Cinco constituye el tema central de la investigación, es decir la intervención del notario en la contratación electrónica, aquí se desglosa la función que deberá tener un ciber notario ante un contrato electrónico, estudiamos los diferentes servicios que puede brindar, la

importancia de su implementación así como veremos un ejemplo práctico de una situación en la que una persona busca los servicios de un ciber notario

El Capitulo Seis alude al análisis de los resultados de la investigación de campo, donde se desglosan los resultados de las encuestas donde se examinó a cien abogados y notarios sobre su conocimiento acerca de la contratación electrónica y su opinión acerca de la intervención del notario en la contratación electrónica, así mismo se hace el análisis de las respuestas que dieron las personas entrevistadas.

Concluimos el trabajo de investigación con el capitulo siete donde se encuentran las conclusiones y las recomendaciones a las que llegamos a lo largo de la investigación.

CAPITULO I

MARCO HISTÓRICO DEL NOTARIADO, DEL INTERNET Y DEL COMERCIO ELECTRÓNICO

SUMARIO: *Introducción. 1.1 Síntesis Histórica del Notariado Latino. 1.2 Origen y Evolución del Internet. 1.3 Origen y Evolución del Comercio. 1.3.1 Edad Antigua. 1.3.2 Edad Media. 1.3.3 Edad Moderna.*

Introducción

En el presente Capitulo se desarrollaran los aspectos históricos de los principales conceptos en los que se fundamenta nuestra investigación, como lo son el notariado, el Internet y el comercio electrónico. Siendo estos aspectos muy importantes ya que nos establecen el inicio de las instituciones jurídicas y como estas han cambiado con el transcurso del tiempo, siendo el ciber-notario una de estas figuras novedosas que han nacido gracias a la evolución de estas instituciones jurídicas, considerándose una de las herramientas para la seguridad en estos medios.

1.1 Síntesis Histórica del Notariado Latino.

Sin duda las sociedades antiguas alcanzaron un alto grado de desarrollo en todos los aspectos como el comercio, las artes, la industria e incluso el derecho, sociedades como los Hebreos, Romanos, Egipcios y Griegos son quizás las más conocidas por sus grandes avances en todas las ramas del conocimiento y podemos atribuirles una cantidad impresionante de

contratos grabados en piedra, mármol y ladrillo encontrados en ciudades de Grecia, Egipto, Roma, entre otras.

Pero se dice que con el derecho nació el notariado y estas sociedades, también se ocuparon de desarrollar este ámbito del derecho, sin embargo no podemos establecer exactamente el origen del notariado, tampoco que en qué lugar se origino, ni a quien corresponde su invención, pero podemos mencionar que antes de Cristo ya existía por lo menos cercano a lo que conocemos como tal, así podemos mencionar como ejemplo lo establecido por la Biblia en el libro de Rut, capitulo 4, versículos del 7 al 9 y 11: "Había ya desde hacía tiempo esta costumbre en Israel tocante a la redención y al contrato, que para la confirmación de cualquier negocio, el uno se quitaba el zapato y lo daba a su compañero; y esto servía de testimonio en Israel; Entonces el pariente dijo a Booz: Tómalo tú. Y se quitó el zapato; Y Booz dijo a los ancianos y a todo el pueblo: Vosotros sois testigos hoy, de que he adquirido de mano de Noemí todo lo que fue de Elimelec, y todo lo que fue de Quelión y de Mahlón…Y dijeron todos los del pueblo que estaban a la puerta con los ancianos: Testigos somos."[1] Como podemos ver con este ejemplo antes de Cristo ya existían personas a las que se les entregaba la potestad de servir como testigos y dar fe de los actos que ante ellos se otorgaban, por lo que podríamos decir que son los notarios antiguos. Sin embargo no existe fecha exacta del nacimiento de esta institución, pero las distintas sociedades han dejado plasmado el gran desarrollo que del notariado tuvieron, así para los hebreos se observo un sistema orgánico en donde a los que eran designados para ejercer la función notarial se les denominaba "*scribae",* cargo que eran considerado de alto rango concedido únicamente a la casta sacerdotal.

[1] Santa Biblia, "Versión de Reina Valera, 1960", libro de Ruth, capitulo 4 versículos del 7 al 9 y 11.

Los scribaes se clasificaban según las funciones que realizaban, así las personas que autorizaban los actos del Rey ya fuera en el momento de emitir leyes y de administrar justicia, o ya presenciando las grandes ceremonias del Estado; además que tenían funciones de consejero de Estado quienes eran denominados *Scribae Regis (Escriba del Rey)*, la segunda clasificación era la de las personas que daban fe de las ceremonias del culto y de las solemnidades públicas del mismo, estos se denominaban *Scribae Templis (Escriba del Estado)*, y los últimos eran los que podríamos considerar como los más cercanos a lo que conocemos como notarios, ya que eran los que daban fe de los actos del pueblo a estos se les denominaba *Scribae Populis (Escriba del pueblo).*

Entre los egipcios existieron dos clases de escribanos: los primeros eran los llamados **Escribanos de gobierno:** Estos se consideraban como personas de dotes superiores, con títulos obtenidos capaces de igualar a escrito todas sus normas jurídicas y sociales[2]. En segundo lugar estaban los llamados **Escribanos Privados:** que se consideraban que tenían funciones similares a las que hoy se les denominan propias del Notariado, en el campo privado. Como una nota curiosa entre los egipcios sobresalen que fueron ellos los que introdujeron la fecha en el documento, el nombre del otorgante, el texto y el nombre del escriba; incluyendo una lista de testigos[3].

Entre los griegos también existieron personas que se dedicaban a la redacción de documentos que eran otorgados por los miembros de la población. Entre los notarios griegos se conocieron los Singrafos que

[2] Girón, J. Eduardo. El Notario Práctico o Tratado de Notaria. 4ª edición, Editorial Tipografía Nacional, Guatemala, noviembre de 1932,página 13

[3] Córdova Rogel, Karen Marisol y Otros. Tesis de la Universidad de El Salvador: Alcances que Presenta la Función Notarial en la Ley del Notariado y Frente al Anteproyecto de dicha Ley, en lo Relativo a las Actuaciones Notariales que se Realizan en el Exterior. Año 2006, Pagina 10

escribían en un registro público toda clase de contratos, los que sin esta solemnidad carecían de valor ante la ley. Según la historia cada tribu tenía dos singraphos a los que se les daba privilegios y honores especiales[4].

Roma es otra civilización que desarrollo el notariado, pero primeramente no despertó en los romanos ningún interés científico ya que su estudio y el ejercicio de las funciones de notario se impusieron como trabajo obligatorio a los esclavos, para quienes estaba reservado el desempeño de oficios degradantes.[5] Pero esto cambio con la llegada del cristianismo cuando se señala para la institución una era de reparaciones y de interés científico, es entonces cuando se reglamentan sus principios, se aceptan sus doctrinas, es decir se eleva a la categoría de institución jurídica.

Los primeros en reconocer la importancia del notariado fueron los emperadores romanos Arcadio y Honorio, ellos fueron los que elevaron a cargo público el ejercicio de sus funciones; mandaron que estas fueran desempeñadas por hombres libres y vecinos honorables de cada localidad y más tarde por funcionarios ministeriales de la confianza de los gobernadores de cada provincia, ordenaron retribuir a estos con crecidos sueldos y concedieron a la clase preeminencias y distinciones.[6]

Como ejemplos de las personas que desempeñaban cargos de notarios en Roma podemos mencionar: **Los Notariss o Notarius:** A quienes se les encargaba tomar razón, por medio de notas o minutas, de los actos en que intervenían por razón de su ministerio. Estos posteriormente tomaron el nombre de *Cursores o Logographi*, porque escribían tan rápido como

[4] Girón. J Eduardo. Obra citada pagina 17
[5] Idem.
[6] Idem.

hablaban; **los Scribaes:** Eran las personas que estando investidas con algún cargo público o autorizados para dar fe de actos judiciales o extrajudiciales, sabían el arte de escribir.[7] Eran acompañantes de los gobernadores o pretores de provincia y tenían por obligaciones principales la de escribir los decretos, redactar las sentencias, arreglar las cuentas del Estado y custodiar los archivos y documentos de la provincia en la que servían; **los Tabeliones o Tabulariis:** Quienes escribían los actos o contratos en pequeñas tablas cubiertas de cera o albayalque[8]. Eran oficiales escribientes que empezaron por reproducir en las "Tabulas Leyes", tarea que les era remunerada, convirtiéndose después en oficio, realizaban tareas de censo, y por su hábito de custodiar documentos, se inició la práctica de entregárseles los testamentos, contratos y otros actos[9].

En nuestro país el notariado nació como tal con la disolución de la República Federal de Centroamérica por la legislación que se originó, pero que no fueron suficientes y fue necesario el surgimiento de otras leyes que se adecuaran al dinamismo de la época. Pero el decreto más significativo que reguló el notariado fue el decreto de fecha de 15 de abril de 1853 que contemplaba las situaciones de fallecimiento de escribanos y que se retiraran o se trasladaran a otros estados ya sea permanentemente o de forma temporal, por estas circunstancias se debía entregar el protocolo al archivo de la Corte Suprema de Justicia, entre otras situaciones. En 1857 el Código de Procedimientos Judiciales y de Fórmulas se convirtió en la primera ley en regular completamente el notario. Después en 1881 se creó el Código de Procedimientos Civiles que a partir de la tercera reedición en 1948 en el

[7] Girón. J Eduardo. Obra citada página 17
[8] Girón. J Eduardo. Obra citada. Pagina 17
[9] Córdova Rogel, Karen Marisol y Otros. Tesis de la Universidad de El Salvador: Alcances que Presenta la Función Notarial en la Ley del Notariado y Frente al Anteproyecto de dicha Ley, en lo Relativo a las Actuaciones Notariales que se Realizan en el Exterior. Año 2006, Página 16

Capitulo Tres se regulo al notario. Sin embargo en 1930 el cinco de septiembre surge la Ley de Notariado que fue anexada al Código de Procedimientos Civiles en el capítulo dedicado el notario. Hasta llegar a la actual Ley de Notariado que surgió por el Decreto Legislativo número 218 del día 6 de diciembre de 1962 y aprobada y promulgada el día siete de diciembre de 1962[10].

Es obvio que la institución notarial no ha existido desde siempre, sin embargo, no existe un estado de civilización avanzada, que no tenga un sistema notarial, cualesquiera que sean su tipo o sus características.

Y más aún con la aparición de la contratación electrónica es mucho más importante que el notario esté presente en las negociaciones de este tipo, porque así como lo hemos venido estudiando la historia ha venido evolucionando así es como el notario debe evolucionar con ella. El ciber notario es una institución nueva que ha surgido por esa misma necesidad que hizo que nacieran los tabulareis, los escribas y otros funcionarios que hemos estudiado en el desarrollo de este tema para satisfacer a la sociedad de seguridad, orden y paz. Y que el Estado está obligado a garantizar independientemente cual sea su condición, su ideología o sistema de mercado. Por lo que el Estado de El Salvador está obligado por la historia y la misma sociedad a crear leyes que beneficien a la sociedad y así crear instituciones novedosas como la de comercio electrónico, firma digital y ciber notarios, por los mismo indicios de que la sociedad salvadoreña ha empezado a utilizar estas instituciones y la necesidad que estas se amplíen con la creación de un marco legal que regule dicha institución.

[10] Luís Vásquez López. Derecho y Práctica Notarial. San Salvador. Pág. 13

1.2 Origen y Evolución del Internet.

El concepto de Internet surgió como un proyecto militar lanzado por el Departamento de Defensa de los Estados Unidos en 1958, como parte de la respuesta al lanzamiento del primer satélite soviético en la época de la Guerra Fría, el Sputnik, por lo que este creo **ARPA**[11] (Agencia de Proyectos de Investigación Avanzada) con el objeto de potenciar la investigación científica[12].

Este proyecto militar-académico[13] fue creado, por el aporte de muchas ideas que se pensaron aun veinte años antes que naciera este proyecto, por lo que podemos decir que este, surgió con aportes significativos de ensayos y trabajos de investigación para formar de lo que hoy conocemos como Internet. Muchas personas fueron los que aportaron a este proyecto con sus ideas, en los aspectos doctrinarios de lo que hoy es Internet. Así se construyeron las primeras computadoras u ordenadores como lo es el Mark1[14] y la ENIAC (Integrador y Computador Electrónico Numérico)[15], con

[11] ARPA es acrónimo de la expresión en inglés Advanced Research Projects Agency ("Agencia de Proyectos de Investigación Avanzada"), denominación del organismo del Departamento de Defensa de Estados Unidos creado en 1958 como consecuencia tecnológica de la llamada Guerra Fría, y del que surgieron, una década después, los fundamentos de ARPANET, red que dio origen a Internet. La agencia cambió su denominación en 1972, conociéndose en lo sucesivo como DARPA (Defense Advanced Research Projects Agency o "Agencia de Proyectos de Investigación Avanzada de la Defensa"). http://es.wikipedia.org/wiki/ARPA

[12] Gracia, Mexia Pablo. Principios De Derecho De Internet, Segunda Edición, Editorial Tirant Blanch. año 2005 Valencia. Pág. 89

[13] El cual unió a cuatro ordenadores de los cuales ARPA proporciono los fondos a varios departamentos de informática de universidades norteamericanas, así como algunas empresas privadas.

[14] El Harvard Mark I o Mark I fue el primer ordenador electromecánico construido en la Universidad Harvard por Howard H. Aiken en 1944, con la subvención de IBM. Tenía 760.000 ruedas y 800 kilómetros de cable y se basaba en la máquina analítica de Charles Babbage. El computador Mark I empleaba señales electromagnéticas para mover las partes mecánicas. Esta máquina era lenta (tomaba de 3 a 5 segundos por cálculo) e inflexible (la secuencia de cálculos no se podía cambiar); pero ejecutaba operaciones matemáticas básicas y cálculos complejos de ecuaciones sobre el movimiento parabólico de proyectiles. La Mark I era una máquina digna de admirar, pues sus longitudes eran grandiosas, medía unos 15,5 metros de largo, unos 2,40 metros de alto y unos 60 centímetros de ancho, pesaba aproximadamente unas cinco toneladas. Pero lo más impresionante fueron unas cubiertas de cristal que dejaban que se admirara toda la maquinaria de su interior. http://es.wikipedia.org/wiki/Mark_1

[15] ENIAC, siglas de Electronic Numerical Integrator And Computer (Integrador y Computador Electrónico Numérico), primer ordenador digital universal totalmente electrónico. El ENIAC, diseñado por John William

los conceptos de arquitectura de Von Newman como lo son: Unidad Central de Proceso, con sus unidades aritmético-lógicas y de control, unidades de entrada/salida, memoria principal y auxiliar. Y basado en estos conceptos fueron creados los primeros ordenadores de instituciones públicas, universidades y empresas privadas[16]. Otros científicos que aportaron grandes ideas para el desarrollo en internet son los que a continuación detallaremos y de los cuales uno de ellos es J.C.R Licklider[17] que en 1962 laboro en el MIT (Massachussets Institute of Tecnology o Instituto Tecnológico de Massachussets) quien escribió el ensayo "Red Intergaláctica". La cual consistía en una red interconectada globalmente de la que cada uno pudiera acceder desde cualquier lugar del planeta a datos y programas. Así también este se convirtió en el director del proyecto de ARPA y aposto por mover el Proyecto al sector privado, específicamente a las universidades estableciendo que eran estas las instituciones más idóneas para entender y desarrollar esta red de telecomunicaciones sentando así el inicio de ARPANET.[18] [19]

Mauchly y John Presper Eckert, fue construido entre 1943 y 1946 en la Universidad de Pensilvania. Esta computadora —inicialmente un proyecto militar— era capaz de realizar varios cientos de multiplicaciones por minuto. Sin embargo, su programa estaba físicamente determinado mediante el cableado del procesador, y tenía que ser modificado manualmente. Los diseñadores mejoraron este aspecto en su siguiente creación, el EDVAC (Electronic Discrete Variable Automatic Computer, Computadora Automática Electrónica de Variable Discreta), cuyo sistema de almacenamiento electrónico era mucho más avanzado. El ENIAC pesaba 30 toneladas y contenía 18.000 válvulas de vacío; permaneció en uso hasta 1955. Microsoft ® Encarta ® 2007. © 1993-2006 Microsoft Corporation. Reservados todos los derechos.

[16] Gracia, Mexia Pablo. Ob. Cid. Pág. 90

[17] Licklider nació el 11 de marzo de 1915, en St. Louis, Mo, EE.UU. Se graduó en psicología, fue uno de los primeros en reconocer que el máximo potencial de los ordenadores sólo puede lograrse mediante la mejora de la capacidad del usuario humano para interactuar con la computadora. A su vez, percibió que el equipo informático puede hacer algo más que proporcionar datos. También podría ayuda a sus usuarios en el pensamiento, la comprensión y la toma de decisiones. http://www.um.es/docencia/barzana/BIOGRAFIAS/Biografia-JCR-Licklidder.php

[18] García, Mexia Pablo. Ob Cid. Pág. 162.

[19] La red de computadoras ARPANET (Advanced Research Projects Agency Network) fue creada por encargo del Departamento de Defensa de los Estados Unidos ("DoD" por sus siglas en inglés) como medio de comunicación para los diferentes organismos del país. El primer nodo se creó en la Universidad de California, Los Ángeles y fue la espina dorsal de Internet hasta 1990, tras finalizar la transición al protocolo TCP/IP en 1983. http://es.wikipedia.org/wiki/ARPANET

Otros científicos que aportaron en gran manera al desarrollo del Internet fueron, Lawrence Roberts[20] y Thomas Merrill quienes en 1965 habían conectado, por primera vez dos ordenadores mediante una línea telefónica de baja velocidad, con este experimento se pudo comprobar que era factible el intercambio de información entre dos ordenadores, pero que también la conmutación de circuitos que entonces se utilizaba en la red telefónica era muy inadecuada ya el nivel de descarga era de 1.200 bits/s[21].

Así como también en 1972 se creó el primer lenguaje de programación del disco C. Y en se mismo año Ray Tomlinson desarrollo el primer programa de correo electrónico el cual llamo usuario@maquina. El signo de la @ se eligió arbitrariamente de los símbolos no alfabéticos del teclado. Y en los años de los 80´s, se inicio la era de la conexión de redes no solo locales sino que internacionales, por lo que era necesario ver esa heterogeneidad de ordenadores y redes interconectas por lo que surgió en 1983 en base a la idea de los protocolos de comunicación.

En 1990 ARPANET, el origen del Internet, se cierra formalmente en 20 de años aproximadamente de vida ya que había crecido para ese entonces de 4 a 600, 000 ordenadores en 5,000 redes separadas a lo largo de más de 100 países. Pero no solo era la interconexión lo que hizo famoso a este nuevo mecanismo de comunicación[22]. Ya que poseía muchos errores y

[20] Nacido en Connecticut, Estados Unidos en 1937, es un científico estadounidense, considerado uno de los padres de Internet. Doctorado por el Instituto Tecnológico de Massachusetts (MIT), en 1967 entró a trabajar en la Agencia de Investigación de Proyectos Avanzados de Defensa (DARPA) en la cual colaboró con Robert Kahn y Vinton Cerf en la creación de ARPANET, la primera red de conmutación de paquetes. Máximo ejecutivo de Telenet, la primera operadora de datos a través de conmutación de paquetes, desarrolló el protocolo X25 en el cual se basaría la red europea EUNet. El 2002 fue galardonado con el Premio Príncipe de Asturias de Investigación Científica y Técnica junto con Robert Kahn, Vinton Cerf y Tim Berners-Lee. http://es.wikipedia.org/wiki/Lawrence_Roberts

[21] García, Mexia Pablo. Ob Cid. Pág. 162.

[22] Cremades Javier, Miguel Ángel, Fernández Ordóñez, Rafael Illista. Régimen Jurídico de Internet. Primera edición. Editorial la Ley Madrid. 2002. Página 97.

lentitud en las conexiones que tenían y aunque las primeras herramientas de búsqueda y acceso a la información se encontraron en estos modelos, no estaban integrados, no eran de uso fácil su utilización. Sino que fue en 1989 en el CERN (Organización Europea para la Investigación Nuclear)[23] el científico Tim Berners-Lee concibe el concepto de del uso del Hipertexto[24] (Protocolo de Transferencia de Hipertexto o HTTP)[25] y el Lenguaje de Marcas de Hipertexto o HTML[26] través de maquinas conectadas a Internet, dando nacimiento al World Wide Web y dando paso a una nueva era en la historia e Internet. Por lo que no menos importantes fue la concepción del navegador para visualizar las páginas definidas en HTML. De alguna forma este navegador fue el que revitalizo el interés por Internet, ya que el navegador representaba el interfaz cómodo y vistoso. Se dice que era cómodo porque no tenía complejos comandos que memorizar, simplemente un golpe con el ratón, un clic para navegar por la información. Vistoso porque permitía visualizar todo tipo de información multimedia, aunque en un

[23] La Organización Europea para la Investigación Nuclear (nombre oficial), comúnmente conocida por la sigla CERN (sigla provisional utilizada en 1952, que respondía al nombre en francés Conseil Européen pour la Recherche Nucléaire, es decir, Consejo Europeo para la Investigación Nuclear), es el mayor laboratorio de investigación en física de partículas a nivel mundial. Está situado en la frontera entre Francia y Suiza, entre la comuna de Meyrin (en el Cantón de Ginebra) y la comuna de Saint-Genis-Pouilly (en el departamento de Ain). Como una instalación internacional, el CERN no está oficialmente ni bajo jurisdicción suiza ni francesa. Los estados miembros contribuyen anualmente 1.000 millones CHF (aproximadamente € 664 millones, US$ 1.000 millones). http://es.wikipedia.org/wiki/CERN

[24] El concepto de hipertexto se remonta en realidad al año de 1945 en que Van-nevar Bush describe un dispositivo foto-electro-mecánico llamado Memex (de memory extensión), que podía hacer y seguir enlaces en documento en microfichas. El termino hipertexto propiamente como tal fue acuñado por Ted Nelson en 1965. Entonces los documentos enlazados se encontraban en el disco duro local.
Cremades Javier, Miguel Ángel, y otros. Ob. Cid. Pág. 97.

[25] Es un protocolo de transferencia de información que permite la comunicación directa y única entre el navegador de un ordenador y el ordenador de la red al que se quiere acceder. Se establece una conexión independiente por cada elemento de la pagina web que se desea ver (imágenes, texto y marcos que, a su vez, son nuevas páginas web). Para que todos los documentos, localizados en múltiples ordenadores sean accesibles, la red debe compartir un espacio de nombres y direcciones común, lo que se logra a través del servicio de directorio IP (Numero de identificación de cada máquina conectada) a partir de nombres fáciles de recordar.
Gracia, Mexia Pablo. Ob. Cid. Pág. 61.

[26] Es el lenguaje habitual utilizado para mostrar información en Internet. HTML es un subconjunto del SGML (Standard Generalized Markup Language), utilizando en edición electrónica. Su facilidad de hipertexto permite que una palabra cualquiera contenida en un texto pueda considerarse clave y convertirse en un enlace que encamina a otro texto con ella relacionada. Esta técnica, que ya existía para la operación en un ordenador, Berners-Lee la modifico para que funcionara en una red de ordenadores y la optimizo incorporando prestaciones multimedia. Ídem. Pág. 61.

principio las capacidades multimedia fueron muy primitivas y estas fueron siendo incorporadas poco a poco[27]. Lo que en un principio abarco un pequeño dominio en el CERN (Organización Europea para la Investigación Nuclear), creció por lo que Berners-Lee escribió el programa *Enquire,* que permitía añadir al final de cada documento una lista de referencias desde las cuales se podía enlazar como los documentos relacionados. Por lo que el pequeño domino en el CERN (Organización Europea para la Investigación Nuclear), creció fuera de sus límites y se optimizo. Primero fue llamado Web (telaraña), luego paso a ser Wide Web (gran telaraña) por el éxito que tuvo entre los usuarios y finalmente alcanzó el ámbito mundial, llegando a ser World Wide Web por haber pasado las fronteras físicas de los países. Los cuales en resumen son los datos contenidos en un ordenador que se quieren poner a disposición de la WWW. El cual estaba apoyado de tres conceptos fundamentales para lo que conocemos hoy como WWW que son:

a) Lenguaje de Marcas de Hipertexto (HTML).
b) Protocolo de Transferencia de Hipertexto (HTTP).
c) Localizador Uniforme de Recursos (URL)[28]

[27] Siguiendo la idea de la incorporación de medios multimedia en las páginas web podríamos decir que Marc Anderessen, entonces estudiante de NCS, el que introdujo en 1993 la posibilidad de incluir imágenes en las páginas web cuando construyo un navegador que llamo Mosaic. Y este fue contratado por Clark en 1994 para fundar una empresa que iba a basar su negocio precisamente en los navegadores web; creando a Netscape, que durante muchos años fue el navegador más utilizado por muchos años. Hasta que Microsoft entro en la carrera de los navegadores y en 1995 creó su navegador que gano aceptación con el Internet Explorer. Los navegadores poco a poco fueron ampliando sus capacidades de forma que eran capaces de entender los protocolos y formatos de representación: VRLM o Lenguaje de Modelado de Realidad Virtual, para la representación de modelos tridimensionales; Java para representación de comportamientos por medio de applets, que eran pequeñas aplicaciones incorporadas a los navegadores. De alguna manera podemos decir que estos se convirtieron en la ventana universal a la que asomarse a internet era rápido, sencillo y cómodo.
Cremades Javier, Miguel Ángel, y otros. Ob. Cid. Pág. 98.

[28] Es la dirección que está asociada con la dirección IP (Internet Protocol) a través del servicio de directorio DNS (Domain Name System). Consta de cuatro partes diferentes:

Modo_de_acceso://identificación_del_host/ruta/fichero. El modo_de_acceso especifica el protocolo empleado para ofrecer el servicio, que puede ser:

Ftp: transferencia de ficheros; file: fichero local; htt: transferencia de páginas web; https: transferencia a páginas web seguras (cifradas); mailto: dirección de correo electrónico; news; telnet: terminal virtual; entre otros.
La identificación_del_host consiste en la dirección completa del sitio (site) al que queremos ir. Se estructura pro dominios (host.subdominio.dominio).

Establecido plenamente el Internet a nivel mundial, en nuestro país en el año de 1994 se dieron los primeros movimientos que llevarían al país a un acceso fijo a la red, entre los precursores de esta iniciativa se encuentran Consejo Nacional de Ciencia y Tecnología (CONACYT), Fundación Salvadoreña para el Desarrollo Económico y Social (FUSADES), Universidad de El Salvador (UES), Universidad Centroamericana "José Simeón Cañas" (UCA), Universidad Don Bosco, Centro Cultural Salvadoreño, Escuela Superior de Economía y Negocios, Embajada de los Estados Unidos, entre otros; quienes en la ciudad de San Salvador el día 2 de septiembre de mil novecientos noventa y cuatro acuerdan constituir el grupo coordinador del "Proyecto SVNet: Internet en El Salvador"[29]. Por lo cual en nuestro país se ha convertido en un fenómeno relativamente nuevo solo teniendo catorce años de ser implementado y siendo que a nivel de servidores hogar ha tenido aun menor tiempo de desarrollo. En el Salvador como antecedentes más inmediatos de estos tenemos a empresa IANA (Internet Assigned Numbers Authority) y el InterNIC (Internet Network Information Center) que dio la administración del dominio de Nivel Superior "SV" al país para el envió de mensajería y la primera pagina Web que abrió al país al ciberespacio[30] fue la

---

El host no normalmente indica el tipo de servicio empleado. Algunos valores frecuentes son:

1. www World Wide Web. Acceso a páginas web.
2. ftp File Transfer Protocol. Transferencia de ficheros.
3. irc Internet Relay Chat. Comunicación interactiva entre usuarios.

El subdominio identifica la organización que ofrece el servicio y que estará registrado en InterNIC (Network Information Centres), organismo encargado de registrar los nombres.

A ruta detallada el nombre del directorio y/o subdirección donde está la información específica.

Por ejemplo la dirección URL donde se encuentra la historia del mismo que es la pagina del Senado de Estados Unidos es el siguiente:

http://www.senado.es/historia/index.html

En ella se identifican los conceptos antes descritos: 1. modo_de_acceso http. 2. identificion_del_host www.senado.es. 3. host www, 4. subdominio senado, 5. dominio .es, 6. ruta /historia. 7. fichero index.html.

Cremades Javier, Miguel Ángel, Fernández Ordóñez, Rafael Illista. Régimen Jurídico de Internet. Primera edición. Editorial la Ley Madrid. 2002. Página 102.

[29] Raúl Armando Aguilar Moran, Evelyn Yesenia Hernández Núñez Y Florencio De Jesús Vargas Consuegra. Tesis "El Comercio Electrónico en EL Salvador". Universidad de El Salvador, Facultad de Jurisprudencia y Ciencias Sociales, San Salvador, 2002.

[30] Ciberespacio, entorno creado por la interconexión de redes planetarias de sistemas informáticos. El término se aplica en la actualidad de forma generalizada a Internet, pero su utilización original en ficción científica se refería a un concepto mucho más ambicioso y especulativo: la inmersión total de los sentidos del ser humano en un

pagina de ANTEL que dio origen al tráfico comercial y telecomunicaciones en nuestro país.

En octubre de ese año se estableció un acuerdo con UUNet, en Virginia, EE.UU. para manejar el tráfico de correo electrónico de El Salvador, bajo el dominio SV. En diciembre se instaló y configuró exitosamente un nodo UUCP (Copiador de Unix a Unix)[31] de correo electrónico en el CONACYT con este propósito, y los primeros mensajes con direcciones terminadas en SV comenzaron a circular en Internet.

En febrero de 1996 ANTEL completó la instalación de los primeros enlaces dedicados a Internet en territorio salvadoreño, siendo éstos el de la Universidad Centroamericana José Simeón Cañas y el de la Universidad Don Bosco. El siguiente mes vieron la ciberluz los sitios Web de estas dos universidades, así como los de SVNet y la página principal de El Salvador, convirtiéndose así en los primeros sitios Web de El Salvador que residían en un servidor ubicado físicamente en El Salvador[32].

En conclusión podemos decir que Internet fue creado por distintos conceptos en diferentes años o décadas pero con un mismo objetivo que era la conexión de ordenadores y el intercambio de información a nivel mundial. Además podríamos decir que la información no solo es útil para el consumo del ser humano en insumos de educación, noticias y intercambio de tecnologías sino que también es para lo que es el desarrollo del comercio

---

entorno generado artificialmente. La experiencia sensorial de la persona sería generada por la máquina y suministrada directamente al cerebro.
Microsoft ® Encarta ® 2007. © 1993-2006 Microsoft Corporation. Reservados todos los derechos.

[31] UUCP (acrónimo del inglés Unix to Unix Copy, Copiador de Unix a Unix) es un conjunto de comandos Unix usado para copiar archivos desde servidores usando redes de marcado telefónico. http://es.wikipedia.org/wiki/UUCP

[32] Raúl Armando Aguilar Moran, Evelyn Yesenia Hernández Núñez Y Florencio De Jesús Vargas Consuegra. Ob. Cid. Pág. 90

electrónico, el cual es una base hoy en día que sostiene al mercado mundial y en la mayoría de casos las economías de grandes potencias en el mundo, claro ejemplo es la bolsa de valores de Estados Unidos el cual depende ahora en día del 100% de la información que obtiene del Internet para saber el comportamiento del mercado. Así como es una herramienta que fue creada para el ser humano para poderse desarrollar este. Y así el comercio electrónico podemos decir que viene ligado a la función notarial electrónica que nace gracias a la creación del Internet que ha podido darnos esta ventana de exploración en un campo a un desconocido para el Derecho y que ha empezado a explotar para el beneficio de la misma sociedad. En El Salvador ha tenido un impacto positivo el uso del Internet ya que muchas empresas hoy en día han empezado a utilizar el ciberespacio como una herramienta de comercialización lo cual debe de ser tomado por nuestro ordenamiento jurídico y de las instituciones encargadas de su creación, para regular este y evitar en un futuro conflictos por su falta de regulación.

1.3 Origen y Evolución del Comercio.

El comercio como una actividad humana ha acompañado al hombre desde tiempos ancestrales, ha evolucionado de muchas maneras; pero debe aclararse que su significado y fin se ha conservado por lo que se entiende por comercio el proceso y los mecanismos utilizados necesarios para colocar las mercancías, que son elaboradas en las unidades de producción en los centros de consumo en donde se aprovisionan los consumidores, último eslabón de la cadena de comercialización. Dentro del contexto en estudio la palabra “comercio” se refiere a una serie cada vez mayor de actividades que tienen lugar en redes abiertas (compraventa, publicidad, comercio y

transacciones de toda índole) las cuales conducen a un intercambio de valor entre dos partes.

En líneas generales y, con un sentido amplio, el comercio implica la investigación de mercado con el fin de interpretar los deseos del consumidor, la publicidad que anuncia la existencia del producto, la posibilidad de adquirirlo, y en qué lugar, a la vez que se utilizan medios que permitan persuadir, la venta al por menor y finalmente la adquisición por parte del público.

1.3.1 Edad Antigua

Aunque desde épocas muy primitivas existió el deseo y el interés del intercambio de objetos, fue hasta la era neolítica, cuando el hombre empezó a especializarse en actividades determinadas y se presentaron las relaciones comerciales. Estas se efectuaron en forma de trueque y eran productos que solo los producen en ciertas zonas las que tenía esta modalidad.

Después las primeras civilizaciones urbanas de oriente, China e India fueron el inicio del primer periodo histórico del desarrollo comercial; estas fueron el punto de encuentro e intermediarios entre los fenicios, griegos y europeos y los del Mediterráneo occidental los que se convirtieron en la principal ruta comercial en el mundo (ruta de la seda). Un factor de desarrollo fue la moneda como forma de pago.

1.3.2 Edad Media

En la edad media a partir del siglo V, fue en decadencia el comercio ya que las invasiones de los germanos, musulmanes y otros rompieron esa unidad de comercio que existía y casi desapareció este intercambio comercial internacional en el mundo occidental hasta aproximadamente el siglo XIII. En la época feudal el comercio tenia escasa importancia y se limitaba a un ámbito local, excepto para algunos productos que se debían traer de otras regiones o países (como metales, sal, tejidos, joyas entre otros), además de la poca importancia de la moneda y las leyes tributarias y gremiales, que dificultaba las relaciones entre amplias áreas comerciales, por lo que la ruta mediterránea dejo paso a una ruta nueva como la musulmana o islámica. Así paso por muchos siglos el dominio de esta ruta.

1.3.3 Edad Moderna.

La revolución industrial fue el cambio total a lo que fue el comercio y se inicio entre la mitad del siglo XVIII y durante todo el siglo XIX en Inglaterra y Japón por lo que hubo un gran cambio de la producción utilizando maquinas.

El desarrollo de veleros y de transportes eficientes durante los siglos XV y XVI ayudó a una rápida expansión del comercio. A medida que descendía el coste de transportar grandes cargamentos a larga distancia, el grano empezó a importarse a gran escala desde el Báltico hasta los Países Bajos y otros países de Europa. Las nuevas rutas oceánicas entre Europa y el Este permitieron importar desde Asia, con menores costos, un mayor volumen de mercancías del que se podía transportar por tierra. El

descubrimiento de América creó un comercio de nuevos bienes como tabaco y madera[33].

La explotación española vino con el tránsito Europeo hacia las costas americanas utilizo como medio la conquista y la colonización para imponer no solo sus costumbres, sino, también su moneda, así tenemos por ejemplo la explotación española de las grandes minas mexicanas y peruanas de oro y plata, la cual transformó por completo el comercio. Por fin, Europa poseía un bien —los metales preciosos— que tenían una gran demanda en el lejano Oriente. A cambio de los bienes asiáticos, Europa ofrecía monedas de plata acuñadas en México, España, Italia y Holanda. El comercio de bienes de primera necesidad creció a una velocidad asombrosa[34].

Así el comercio evoluciono de gran manera creándose después el comercio electrónico que se da en los inicio del siglo XX, cuando a principio de la década de 1920, en los Estados Unidos surgió la venta utilizando catálogos, impulsados por grandes tiendas de mayoreo. Este sistema de venta, que para su época se puede considerar de impacto revolucionario consistió en una revista con fotos ilustrativas de los productos a vender, lo que revoluciono el ámbito de los contratos, y así también la necesidad de regularlos y de que el notario les diera la suficiente seguridad y así tuviera mayores funciones por lo que este fue el inicio del comercio moderno.

Además a finales de los años de 1960 y principios de los años de 1970 la Agencia de Proyectos de Investigación Avanzada (ARPANET) de Estados Unidos de América había sentado las bases para el desarrollo de lo

[33] Flores Cárcamo, Erick Roberto, y otros. Tesis UES, "Efectos Jurídicos Generales por la Falta de Normativa Legal Expresa que Regula las Compraventas Mercantiles por Medios Electrónicos. " San Salvador, Febrero de 2003. Página 10
[34] Ídem.

que sería Internet, a través de la cual empleando la tecnología se enlazan documento científicos proveniente de diferentes computadoras a los que se les puede integrar texto, música entre otros[35]. Lo que más impacto este tipo de comercio fue la creación del World Wide Web en 1991 con la creación de los protocolos de transferencia de información con la Fundación Nacional para la Ciencia (NSFNET)[36].

Y es así que con la influencia de la tecnología esta rama ha ido diversificándose y haciendo que el comercio se convierta en lo que hoy se conoce como comercio electrónico que pasa a ser una herramienta en el mundo para comunicar a todos y que puedan comercializarse productos vía trans-oceánica.

En El Salvador el comercio electrónico, tuvo como pioneros en 1999 a Almacenes Simán S.A. de C.V. A mediados del año 2000, el Banco Cuscatlán, Banco Salvadoreño y Banco Agrícola lanzaron las primeras tarjetas de crédito orientadas a realizar compras en Internet.

En Enero de 2002, las agencias aduanales empezaron a realizar transacciones por Internet con la Dirección General de la Renta de Aduanas, utilizando por primera vez la firma digital en el país agilizando en gran medida el procesamiento de la información para importación de mercadería y mayor agilidad en las transacciones comerciales que se realizan ahí.

[35] Galán Cortez, Jeannie Elizabeth y otros. Tesis UES "La Firma Digital como Medio de Seguridad y Consentimiento en las Transacciones del Comercio Electrónico". San Salvador. 2008. Págs. 2 y 3.

[36] Acrónimo inglés de National Science Foundation's Network. La NSFNET comenzó con una serie de redes dedicadas a la comunicación de la investigación y de la educación. Fue creada por el gobierno de los Estados Unidos (a través de la National Science Foundation), y fue reemplazo de ARPANET como backbone de Internet. Desde entonces ha sido reemplazada por las redes comerciales. http://es.wikipedia.org/wiki/NSFNET

En Agosto de 2002, surge el primer Centro Comercial en Línea de El Salvador, implementado por NetCom S.A. de C.V[37].

Y ahora ha surgido mas empresas que comercializan por medio de Internet así tenemos COEX Café, Grupo Q entre otros que ofrecen su servicio por la Web.

[37] Galán Cortez, Jeannie Elizabeth y Otros. Ob. Cid. Páginas 3 y 4.

CAPITULO II

ASPECTOS DOCTRINARIOS DEL COMERCIO ELECTRÓNICO.

SUMARIO: *Introducción. 2.1 Globalización, como Factor Socio Económico del Surgimiento de Nuevas Tecnologías y el Surgimiento del Comercio. 2.2. Comercio Electrónico 2.2.1 Definición del Comercio Electrónico. 2.2.2 Ventajas y Desventajas del Comercio Electrónico. 2.2.2.1 Ventajas. 2.2.2.2 Desventajas. 2.2.3 Factores que Influencian el Comercio Electrónico. 2.3. Documento Electrónico. 2.3.1 Concepto de Documento Electrónico. 2.3.2 Principios Rectores en la Interpretación de los Documentos Electrónicos. 2.3.3 Características del Documento Electrónico. 2.3.4 Naturaleza Jurídica del Documento Electrónico. 2.3.5 Clasificación del Documento Electrónico. 2.3.6 Seguridad Jurídica del Documento Electrónico. 2.4 Contratación Electrónica. 2.4.1 Concepto de Contrato Electrónico. 2.4.2 Modalidades de la Contratación Electrónica. 2.4.3 Naturaleza Jurídica del Contrato Electrónico. 2.4.4 Principios Rectores de la Contratación Electrónica. 2.4.4.1 Principio de Equivalencia Funcional. 2.4.4.2 Principio de Neutralidad Tecnológica. 2.4.4.3 Principio de Buena Fe. 2.4.4.4 Principio de Libertad de Comercio. 2.4.4.5 Principio Protectorio. 2.4.5 Elementos de Validez del Contrato Electrónico. 2.4.5.1 Capacidad para Contratar. 2.4.5.2 El Objeto debe ser Lícito. 2.4.5.3 La Causa debe ser Lícita. 2.4.5.4 El Consentimiento por Medios Electrónicos. 2.4.5.4.1 Formación del Consentimiento por Medios Electrónicos. Oferta y Aceptación. 2.4.5.4.2 Vicios del Consentimiento en el Contrato Electrónico. 2.4.5.4.3 Lugar de Perfeccionamiento del Contrato Electrónico. 2.4.5.4.4 Tiempo de Perfeccionamiento del Contrato Electrónico. 2.4.6 Amenazas a la Seguridad Informática. 2.4.6.1 Concepto de Seguridad Informática. 2.4.6.2 Hacker. 2.4.6.3 Cracker.*

Introducción

En el presente capitulo se abordan los aspectos doctrinarios del comercio electrónico, iniciando con uno de los factores que más ha influenciado el comercio, es decir la globalización ya que con el avance de ella ha ido evolucionando el comercio, ayudado también por el avance de la tecnología, como vimos en el capitulo anterior el comercio ha tenido una gran evolución por medio de la tecnología, con ayuda de las maquinas y los

medios de transporte y ahora con los medios de comunicación como el Internet, esto ha creado un nuevo tipo de comercio que es a nivel global.

Y con el comercio electrónico ha surgido la contratación electrónica, considerándose como una ventaja para las personas, ya que las negociaciones son mucho más ágiles y rápidas y beneficiosas. Pero a la vez surgen las grandes dudas de cómo realizar estos contratos y la inseguridad que hay en la Web, con todos los peligros para la seguridad como los hacker y cracker y los famosos virus informáticos que son una gran amenaza cuando se trata de documentos de suma importancia como es un contrato electrónico.

2.1 Globalización, como Factor Socio Económico del Surgimiento de Nuevas Tecnologías y el Surgimiento del Comercio.

Cuando se habla de Globalización en el sector económico se alude principalmente a que el sistema de producción de bienes se opera a escala mundial, este proceso de globalización ha sido posible ya que ha sido sustentado por el gran avance tecnológico que ha existido y valiéndose del gran avance de las comunicaciones, como lo es la informática[38].

Este sistema mundial único de relaciones económicas, políticas, sociales, entre otras, tiene como surgimiento el siglo XVI, con la expansión colonial de las sociedades europeas y la causa más importante que llevo a que este sistema se expandiera es el modo de producción capitalista, cuyo

[38] Folleto Educativo de la Cátedra del Curso Jurídico Filosófico Político, del área Política, Tema "Reflexiones en Torno al Proceso de Mundialización y Globalización". Año 2003

motor, el principio capitalismo, el comercio mundial, la evolución de las tecnologías, la revolución de los transportes y los medios de comunicación.

La globalización es un proceso multidimensional que comprende las esferas económicas, sociales, políticas y culturales[39].

Según la Enciclopedia Salvat[40], la globalización es el proceso histórico de interrelación e interdependencia creciente de todas las sociedades del planeta en un único sistema mundial, de relaciones económicas, políticas y culturales.

Otra de las definiciones que podemos mencionar de la globalización es la de que es una tendencia de los mercados y de las empresas a extenderse, alcanzando una dimensión mundial que sobrepasa las fronteras nacionales.[41]

Este concepto de globalización, desde sus inicios se ha utilizado para describir los cambios en las economías nacionales, cada vez más integradas en sistemas sociales abiertos e interdependientes, sujetos a los efectos de la libertad de los mercados, las fluctuaciones monetarias y los movimientos especulativos de capital. Los ámbitos de la realidad en los que mejor se refleja la globalización son la economía, la innovación tecnológica y el ocio.

Actualmente el termino de globalización es utilizado en muchas esferas, como la de los negocios, la de los medios de comunicación, así

[39] Pleitez, Rafael. Ponencia presentada en el Foro del COLPROCE: "La Doctrina del Neoliberalismo y el Proceso de Globalización en los Países Subdesarrollados" 1998, publicada en la Revista "Realidad", sin edición, Distribuidora de Publicaciones de la Universidad Centroamericana José Simeón Cañas, San Salvador, página 501
[40] Navarro, Francesc, y otros. La Enciclopedia, volumen nueve, Salvat Editores. Madrid, 2004. página 6921
[41] Microsoft® Encarta® 2007. © 1993-2006 Microsoft Corporation. Reservados todos los derechos.

como la de la sociología, y con matices y connotaciones tan distintas que hasta se ha perdido su definición inicial, convirtiéndose en fuente de ambigüedad entre los grupos.

Este modelo se presento con las características siguientes: 1. la producción en serie; 2. el consumo en masas; y, 3. la organización científica del trabajo. Esta última se considero como la fuente de esta productividad creciente que consistió en técnicas para optimizar los tiempos y espacios de la producción en serie[42].

En la globalización, como lo mencionamos al principio, el constante desarrollo de las nuevas tecnologías informáticas ha sido una fuerte influencia permitiendo el paso de una economía de productos a una economía de símbolos, en donde se ha sustituido la creación de riqueza por transacciones invisibles que son posibles gracias a la tecnología electrónica e informática desarrolladas en la últimas décadas. Antes el dinero seguía a las mercancías hoy gracias a esta tecnología el capital viaja vía ordenador de un lugar a otro al margen de las mercancías, nos referimos al comercio electrónico ya que en este nuevo comercio se ayuda de la red para el intercambio de mercancías haciéndolo más fácil, siendo que cada persona, comprador y vendedor pueden estar en diferentes países e incluso continentes los que a través de una computadora hacen sus negocios.

Así la globalización ha traído a los países la contratación masificada donde casi se desconoce la autonomía de la voluntad y se debilita la teoría del consentimiento, a esto el Derecho ha reaccionado creando la legislación adecuada de protección al consumidor, en algunos casos con jerarquía

[42] Folleto Educativo de la Cátedra del Curso Jurídico Filosófico Político, del área Política, Tema "Reflexiones en Torno al Proceso de Mundialización y Globalización". Año 2003

constitucional[43], esto es lo que ha pasado con la contratación electrónica ya que se han creado, a nivel internacional, la legislación que venga a regular esta actividad para la protección de los derechos de su propia sociedad.

En conclusión decimos que la globalización ha significado la perceptible perdida de fronteras del quehacer cotidiano en las distintas dimensiones de la economía, la información, la tecnología y en si la sociedad civil, sin embargo conlleva consecuencias positivas y negativas, nacen nuevas ideas, nuevas figuras contractuales con un dominio vertiginoso de la tecnología, esperando obtener el mejor resultado jurídico al menor costo.

2.2. Comercio Electrónico.

Podemos decir que los tres cambios tecnológicos decisivos para la aparición y funcionamiento de la sociedad han sido el creciente uso de la información de forma digital, el incremento vertiginoso de las redes electrónicas y la creación de la telaraña mundial World Wide Web (www). Las repercusiones generales de estos tres sucesos de innovaciones tecnológicas son innumerables y trascendentes y constituyen el fundamento de una sociedad informatizada y por ende del comercio electrónico ya que este ha sido muy importante para las economías de todos los países siendo que muchas de las transacciones se están realizando por medios electrónicos.

Cada día son más los negocios que se realizan utilizando medios electrónicos y cada vez son más aceptados en nuestra sociedad. Pero en este tipo de contratación, en muchas ocasiones, surgen dificultades, tanto en

[43] Highton de Nolasco, Elena Inés y Angélica Generosa Elvira Vitale. La Función Notarial en la Comunidad Globalizada, 1ra edición, Santa Fe, Editorial Rubinzal-Culzoni, 2005. página 28

orden jurídico como de orden técnico. Por lo que en el presente tema analizaremos estos problemas y daremos un análisis de estos a la luz de nuestro ordenamiento jurídico.

2.2.1 Definición del Comercio Electrónico.

Debe entenderse por "electrónico" la infraestructura mundial de tecnologías y redes de la informática, las telecomunicaciones que permiten el procesamiento y la transmisión de datos digitalizados. El desarrollo de este tipo de comercio está relacionado con el origen de Internet, siendo este creado por el Departamento de Defensa de los Estados Unidos de América en 1973, dando inicio a la nueva era informática, y con este se empezaron a crear las primeras páginas que comercializaban productos diversos y así estar más cerca de sus clientes y diversificar sus ventas, siendo estas en masa.

Existen muchas definiciones de diversos autores de comercio electrónico, de las cuales solo mencionaremos algunas para entender lo que es el comercio electrónico.

Como definiciones del comercio electrónico podemos mencionar que es "el acto de interposición intersubjetiva entre el comerciante y su cliente el cual usa un medio electrónico[44]

Otra definición de este nuevo comercio es la que da Davara Rodríguez quien nos dice que: "es tanto la compra de productos o servicios por Internet,

[44] Bernal Ríos Robles, Articulo Electrónica "Firma Digital: Legalidad en las Transacciones Comerciales Electrónicas y su Entorno. Perfección de los Contratos en Línea. Incorporación del Derecho al Impulso Digital

como la transferencia electrónica de datos entre operadores de un sector en un mercado, o el intercambio de cantidades o activos entre entidades financieras o la consulta de información con fines comerciales a un determinado servicio o un sin fin de actividades de similares características realizadas por medios electrónicos"[45].

Una tercera definición de lo que conocemos como comercio electrónico es la concebida por la Comisión Europea en la que se menciona que el comercio electrónico es "el conjunto de cambios sociales y organizativos que se han producido en el ámbito de la información y las comunicaciones como resultado de la aplicación de las nuevas tecnologías al mismo[46]

"El comercio electrónico es un concepto amplio que involucra cualquier transacción comercial efectuada por medios electrónicos, implica un amplio rango de operaciones, incluyendo: intercambio de información, ventas, pagos electrónicos, distribución y asociaciones virtuales; además incluye niveles de alta tecnología de informática y de telecomunicaciones, por tal razón las empresas ven al comercio como una manera de modernizar las operaciones actuales, alcanzar nuevos mercados y servir mejor a los clientes."[47]

Al tomar en cuenta lo anterior se puede concluir que comercio electrónico es un concepto amplio que involucra cualquier transacción comercial efectuada por medios electrónicos tales como: el fax, el télex[48], el

[45] Davara Rodríguez, Miguel Ángel. "Manual de Derecho Informático". Ediciones Aranzandi. España. 1997 Pág. 197 y 198.
[46] Cuestiones mundiales publicación electrónica del Us s, volumen 2, número 4, octubre de 1997, citado por Flores Carcomo, Erick Roberto y otros. Tesis UES: "Efectos Jurídicos Generales por la Falta de Normativa Legal Expresa que Regula las Compraventas Mercantiles por Medios Electrónicos", Febrero de 2003, página 81
[47] www.utem.sl/cyt/derecho/firma.html
[48] Sistema telegráfico de comunicación, que se sirve de un transmisor semejante a una máquina de escribir y de un receptor que imprime el mensaje recibido.

teléfono, los EDI e Internet. No obstante nos limitaremos a considerarlo de la siguiente manera: “Comercio electrónico es la parte del comercio que se desarrolla a través de redes (cerradas y abiertas) mediante la relación entre oferta y demanda, para lo cual se utilizan herramientas electrónicas y telecomunicaciones, con el objeto de agilizar el proceso comercial[49].

2.2.2 Ventajas y Desventajas del Comercio Electrónico.

El comercio electrónico como una nueva actividad comercial ofrece ciertas ventajas que pueden servir para un mejor desempeño en el ámbito del comercio por medios electrónicos así como ciertas desventajas propias de ser una nueva forma de comercio.

2.2.2.1 Ventajas.

El uso del comercio electrónico brinda a los usuarios muchas ventajas, mencionamos unas de ellas a continuación:

- Permite el acceso a más información; ya que la naturaleza de la red faculta al usuario para realizar búsquedas profundas, que ellos mismos inician y controlan, en consecuencia, las actividades de mercadeo electrónico, son impulsadas por los clientes quienes son los que buscan el producto deseado. Creando así la misma Web motores de búsqueda que facilitan al usuario a encontrar la información en esa gran telaraña, así

[49] Arrué Echegoyén, Carolina Esmeralda Masin Masin y Natalia Margarita Vázquez Lara, Manuel Alejandro. Tesis “La Seguridad Jurídica Que Proporciona El Estado Al Utilizar La Firma Digital Como Medio De Expresión Del Consentimiento”. Universidad De El Salvador, Facultad de Jurisprudencia y Ciencias Sociales, San Salvador, año 2004.

tenemos que los más famosos buscadores son Google, Altavista, Yahoo, entre otros.

- Facilita la investigación y comparación de mercados; ya que la red tiene la capacidad de acumular, analizar y controlar grandes cantidades de datos, permitiendo al usuario confrontar el producto que desea comprar y acelera el proceso para encontrar exactamente lo que busca.

- Reduce los costos y precios; conforme aumenta la capacidad de los proveedores para competir en un mercado electrónico, abierto, se produce una baja en los costos y precios, de hecho, tal incremento en la competencia mejora la calidad y variedad de los productos y servicios. Ya que reduce los costo de producción además que elimina los intermediarios los cuales hace que el producto tenga un mayor valor, y deja solo una relación más directa en productor y consumidor.

De lo anterior podemos decir que el comercio electrónico no es un obstáculo para la libre comercialización de productos, no solo encerrándonos a productos de software, sino que también es capaz de comercializarse productos muebles en la Web y hasta inmuebles, por lo que el contrato por medios electrónicos es una alternativa que tienen los consumidores, siempre pensando entonces en brindarles seguridad a través de las figuras del notario electrónico, protocolo electrónico y las firmas digitales.

2.2.2.2 Desventajas.

El comercio electrónico también presenta desventajas, tales como:

- **Entorno empresarial y tecnológico cambiante:** Aunque anteriormente señalamos como una ventaja la rebaja en los costos y precios del producto, podemos ver que la empresa necesita hacer una inversión inicial y constante en la implementación de un sistema operativo que cumpla con los requisitos mínimos para ofrecer a sus clientes una buena calidad en sus sistemas de compras y financieros. Ya como hemos visto la tecnología va a pasos agigantados por lo que una empresa que tiene el reto de integrarse a un comercio electrónico debe de estar preparado para poder comprar los productos más recientes en sistemas y ordenadores para poder servir mejor a las personas que les compran el producto.

- **Privacidad y seguridad:** una más de las desventajas del comercio electrónico es que la mayoría de los usuarios no confían en la red como un canal de pago; ya que las compras y pagos de servicios se realizan utilizando el número de la tarjeta de crédito, cualquiera que transfiera datos de una tarjeta de crédito mediante la red no puede estar seguro de la identidad del vendedor, en forma similar no lo está sobre la del comprador, es decir que quien paga no puede asegurarse de que su número de tarjeta de crédito no sea utilizado para algún propósito malintencionado, por otra parte el vendedor no puede asegurarse que el dueño de la tarjeta rechace lo que compró. Esto es dado por el mismo fenómeno de delincuencia que posee cada país el cual varía según el grado de desarrollo que poseen pero, aun así podemos decir que existe un alto grado de desconfianza de las personas de la realización de ciertas transacciones electrónicas por no saber o no poder utilizar los medio necesarios para dar seguridad jurídica a dichos actos jurídicos.

- **Cuestiones legales, políticas y sociales:** existen algunos aspectos que son extensivos en torno al comercio electrónico, por ejemplo validez de

la firma digital, legalidad de un contrato electrónico, perdida de derechos sobre las marcas. Esto puede tomarse como una desventaja ya que en muchos países de Latinoamérica no se cuenta con una legislación específica de comercio electrónico que pueda regular todos los aspectos anteriormente mencionados. Esto sin contar con la poca promoción de parte de los gobiernos para el comercio electrónico; ya que este vendría a aumentar y desarrollar las economías de nuestros países.

Por lo de lo anterior y sobre todo por el ultimo planteamiento, es necesario que en El Salvador se dé una aprobación de ley de los contratos celebrados por medios electrónicos para así como lo hemos dicho anteriormente, pueda garantizar el Gobierno los principio de su creación como de brindar seguridad jurídica así como también ayudar en que las personas tenga acceso a las herramientas que existen en nuestros manos para que satisfagan sus necesidades.

2.2.3 Factores que Influencian el Comercio Electrónico.

Tres son según Fernando Hernández Jiménez Casquet[50], los aspectos más importantes que influencian al comercio electrónico y al ordenamiento jurídico: rapidez e inmediatez de las comunicaciones; la seguridad, confidencialidad y autenticación; y el carácter transnacional de las transacciones electrónicas. Estos aspectos condicionan la eficacia de la aplicación del Derecho Sustantivo que rige las transacciones comerciales, de la aplicación del Derecho de Obligaciones a los contratos electrónicos y justifican, en ocasiones, la necesidad de medidas regulatorias

[50] García Mexía, Pablo y otros. Principios de Derecho de Internet. 2ª Edición, Editorial Tirantto Blanch. Valencia. Año 2005. Pág. 432.

complementarias aplicables a las transacciones electrónicas, como por ejemplo la intervención de un ente certificador (ciber notario) para dar fe y además que cumplan los requisitos legales dichos contratos.

La Rapidez E Inmediatez De Las Comunicaciones. Los nuevos medios de comunicación electrónica conllevan la aparición de nuevas formas de negocio que además de realizarse entre ausentes, están caracterizados por la rapidez e inmediatez de las comunicaciones. Por lo que los conceptos de inmediatez y contratación a distancia, aspectos aparentemente contradictorios, se unen en los procedimientos electrónicos de contratación y con el auge de métodos empresariales. Ya en la práctica y por la necesidad de las personas de realizar sus negocios aceptan acuerdos de voluntades sin tener en cuenta el lugar en que se emiten, los medios que se utilizan (telefax, video llamada o correos electrónico, entre otros) o la naturaleza jurídica del contrato. Entonces la rapidez y la inmediatez constituyen un factor que influencia el nacimiento de la contratación electrónica porque se justifica por la propia celeridad del tráfico mercantil, que exige la máxima rapidez en la conclusión del contrato.

.

Por lo que la rapidez en estos contratos es clave para su realización. Además que esta distinción no se puede ubicar entre contratos empresariales o contratos de consumidor final. Por lo que la inmediatez y la rapidez son características imprescindibles que deben de contar todos los contratos electrónicos; en el cual se realiza por medios electrónicos y además que entre la aceptación y la oferta se produce de inmediato sin poder ver una apreciación de estas a simple vistas.

Otro caso es *La Confidencialidad, Confianza y Autenticación*[51] es otro factor que influye al ordenamiento jurídico y que es uno de los factores críticos para el desarrollo del comercio electrónico, especialmente en la esfera de los consumidores, y es que sea capaz de garantizar unos niveles de seguridad suficiente a los actores y de garantizar a los mismo confianza para realizar transacciones a través de medios electrónicos. Y la peculiaridad del comercio electrónico frente al comercio tradicional es la cuestión de seguridad; ya que se pierde el contacto físico entre las partes y la gran variedad de negociaciones que se dan en forma esporádica hacen crecer el miedo con respecto a la ausencia de soporte documental físico que acredite el consentimiento y contenido de los mismos, así como la identidad de los firmantes y la no modificación de los datos. Pero todo esto tiene sus respuestas en los mecanismos y los nuevos instrumentos que se desarrollan en los ordenamientos jurídicos de cada país. Como lo es la firma electrónica y los certificados que son los que brindan esa seguridad y confianza a los contratos y que se desarrollaran más adelante.

Y por ultimo otro factor que influye en el comercio electrónico es *La Ampliación del Alcance del Comercio Electrónico más allá de las Fronteras Nacionales Convirtiéndose en Transnacional.* Un efecto jurídico que afecta el Internet y por lógica el comercio electrónico es su dificultad de regir en un ordenamiento jurídico, ya que por su característica mundial, difuso e innovador este plantea nuevas perspectivas y retos por lo que para Fernando Hernández Jiménez-Casquet[52] son tres las respuestas que puede dar para este dilema de la legislación de cada país y estas son:

[51] García Mexía, Pablo y otros. Ob. Cid. Pág. 435.
[52] García Mexía, Pablo y otros. Ob. Cid. Pág. 436.

1. La armonización de normas estatales y la celebración de tratados internacionales;

2. La adaptación de las normas de conflicto de Derecho Internacional Privado a las nuevas modalidades de contratación y

3. La aparición de mecanismos extrajudiciales de solución de conflictos y códigos de conducta de adhesión voluntaria y carácter privado[53].

2.3. Documento Electrónico

La celebración de todos los actos sobre plataformas electrónicas se funda en un concepto de Documento Electrónico. Es un concepto de importancia fundamental, dado que se trata del presupuesto básico tanto de la existencia del "Comercio Electrónico" como del denominado "Ciber Notario". Todos ellos han sido objeto de estudio por parte de la doctrina como, objeto de regulación jurídica[54]. De ahí que a fin de comprender, estudiar y sistematizar estas materias de creciente impacto en el cotidiano vivir de las personas, se hace necesario que comprendamos la noción de Documento Electrónico

Sin embargo, no nos podemos quedar en el plano netamente teórico de lo que es el Documento Electrónico. Es menester que profundicemos la importancia práctica que, en la actualidad, tiene en el mundo jurídico como también analizar los efectos jurídicos específicos, los cuales, permiten

[53] "Son un fenómeno de especial relevancia, pues se trata de procedimientos bastante adecuados al carácter no territorial y no estatal del Internet. Asimismo, el ámbito de aplicación de estos códigos de conducta previsiblemente tendera a traspasar las fronteras estatales"… García Mexía, Pablo y otros. Ob. Cid. Pág. 436

[54] Ver Capitulo Cuatro que se refiere al Marco Normativo de la Contratación Electrónica, Firma Digital y Ciber Notario.

transformar al Documento Electrónico en una plataforma jurídicamente segura que genere la confianza necesaria requerida en la celebración de todo negocio jurídico. De ahí que ha surgido la regulación del Documento Electrónico y el nacimiento del ciber notario.

2.3.1 Concepto de Documento Electrónico.

El Documento Electrónico: Es un conjunto de impulsos eléctricos que recaen en un soporte de computadora, y que sometidos a un adecuado proceso, permiten su traducción a lenguaje natural a través de una pantalla o de una impresora[55].

Otra idea señala que Documento Electrónico: "es todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria".[56]

Al referirnos al documento electrónico se alude a que el lenguaje magnético constituye la acreditación, materialización o documentación de una voluntad ya expresada en las formas tradicionales y en que la actividad de una computadora o de una red solo comprueban o consignan electrónica, digital o magnéticamente un hecho, una relación jurídica o una regulación de intereses preexistentes. Se caracterizan porque solo pueden ser leídos o conocidos por el hombre gracias a la intervención de sistemas o dispositivos traductores que hacen comprensibles las señales digitales[57].

---

[55] Ver. www.aaba.org.ar-Mail:aabacoin.pccp.com.ar

[56] César Edgardo Castaneda Espinoza, Violeta Elizabeth Escalante Escalante y José Mario Hernández Lazo. Tesis "El Documento Electrónico como Medio de Prueba para Acreditar Judicialmente las Obligaciones Derivadas de dicha Contratación". Universidad de El Salvador. Página 83.

[57] Arrué Echegoyén, Carolina Esmeralda, Masin Masin, Natalia Margarita y Vázquez Lara, Manuel Alejandro. Tesis "La Seguridad Jurídica que Proporciona el Estado al Utilizar la Firma Digital como Medio de Expresión del Consentimiento". Universidad de El Salvador. 2004. Pág. 150.

Por lo que al referirnos a documento electrónico podemos decir que es todo aquel soporte digital que es transferido electrónicamente de un ordenador, o cualquier otro dispositivo que tenga conexión de Internet a otro con las mismas propiedades utilizado un lenguaje binario[58] que luego es transformado por medio de procesos electrónicos a un lenguaje alfanumérico, por medio del cual puede ser observado por medio de una pantalla o ser impreso y que tenga este eficacia jurídica como medio de prueba.

2.3.2 Principios Rectores en la Interpretación de los Documentos Electrónicos.

El documento en soporte electrónico, informático y telemático posee los mismos principios en cuanto a su validez jurídica que el documento tradicional en papel, así como posee principios propios como toda institución jurídica nueva, de los cuales podemos mencionar:

Principio de Inalterabilidad: Hace referencia a que el contenido del documento no se puede alterar, y que si esto ocurre existen medios para

---

[58] El sistema binario desempeña un importante papel en la tecnología de los ordenadores. Los primeros 20 números en el sistema en base 2 son 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111, 10000, 10001, 10010, 10011 y 10100. Cualquier número se puede representar en el sistema binario, como suma de varias potencias de dos.
Puesto que sólo se necesitan dos dígitos (o bits), el sistema binario se utiliza en los ordenadores o computadoras. Un número binario cualquiera se puede representar, por ejemplo, con las distintas posiciones de una serie de interruptores. La posición 'encendido' corresponde al 1, y 'apagado' al 0.
Además de interruptores, también se pueden utilizar puntos imantados en una cinta magnética o disco: un punto imantado representa al dígito 1, y la ausencia de un punto imantado es el dígito 0. Los biestables —dispositivos electrónicos con sólo dos posibles valores de voltaje a la salida y que pueden saltar de un estado al otro mediante una señal externa— también se pueden utilizar para representar números binarios. Los circuitos lógicos realizan operaciones con números en base 2. La conversión de números decimales a binarios para hacer cálculos, y de números binarios a decimales para su presentación, se realizan electrónicamente. "Sistema numérico." Microsoft® Student 2007 [DVD]. Microsoft Corporation, 2006. Microsoft ® Encarta ® 2007. © 1993-2006 Microsoft Corporation. Reservados todos los derechos.

comprobar dicha alteración, llegando a carecer de valor real el documento, convirtiéndose en falso.

Principio de Autenticidad: Un documento es autentico habiendo sido generado por quien dice ser su autor. Por lo que la firma digital (como se verá más adelante), se presume que pertenece exclusivamente a la persona que consta como titular del documento, pues cada parte de la relación se encuentra determinada, de lo anterior podemos decir la clave privada empleada en la emisión de la firma digital contenida en el documento electrónico ha sido empleada por quien es su legitimo propietario.

Principio de Seguridad: Con el desarrollo de algunas técnicas que se emplean en el documento electrónico, este es al menos, equivalente en cuanto a seguridad, al instrumento escrito y firmado sobre un soporte de papel.[59]

Estas características del documento electrónico permiten que éste no sea la simple trascripción sino la reproducción completa y fiel de la forma y contenido del documento original preexistente. Por lo que son propias de él.

Principio de Integridad: Se presume que el mensaje de datos recibido corresponde al enviado, por cuanto una vez ha sido firmado digitalmente, en caso de llegarse a modificar cualquier parte del mismo, a través de los sistemas técnicos se puede comprobar tal cambio. Por lo tanto, se tiene como presunción legal que el mensaje recibido corresponde al enviado y en caso de considerarse que ha sido modificado, el *onus probandi*

[59] Arrué Echegoyén, Carolina Esmeralda, Masin Masin, Natalia Margarita y Vázquez Lara, Manuel Alejandro. Tesis "La Seguridad Jurídica que Proporciona el Estado al Utilizar la Firma Digital como Medio de Expresión del Consentimiento". Universidad de El Salvador. 2004. Pág. 151.

está en manos del interesado, quien en tal evento deberá probar que las normas de seguridad establecidas no fueron respetadas. Este principio está muy ligado al principio de autenticidad por ser los que resguardan la seguridad del documento electrónico.

En conclusión, integridad significa que la información enviada a través del mensaje de datos no carece de alguna de sus partes, como tampoco ha sido transformado. En tal sentido, la integridad es uno de los requisitos esenciales con los cuales se le da plena validez jurídica al documento electrónico y es por eso que se confía en la firma digital pues esta asegura dicha integridad en el mensaje.

Principio del No Repudio: El principio de no repudio es cuando un documento electrónico ha sido firmado, lo que se manifiesta en ese momento que hay una aceptación expresa de dicho contenido; por ende, cuando un mensaje de datos se encuentra firmado sea por una simple firma electrónica, sea por medio de firma digital, se infiere que el autor del mensaje que consta en el certificado, debidamente expedido, está manifestando que su voluntad es la consignada en dicho documento y por lo tanto no puede negarse a los efectos que del mismo se derivan, estando obligado, según los parámetros establecidos en el mismo pues se ha determinado que dicho documento es veraz y tiene pleno efectos.

2.3.3 Características del Documento Electrónico.

Cuando hablamos de características del documento electrónico nos referimos a lo especial o particular que esta institución jurídica posee y que la distingue de otras similares a esta dando la particularidad del mismo.

Entre las características más importantes de los documentos podemos mencionar:[60]

- Utiliza como lenguaje los códigos binarios que se descifran mediante tecnología informática.

- Su contenido es representativo pues, reproduce palabras, datos, cifras, operaciones matemáticas, sonidos, diseños gráficos o imágenes (multimedia).

- Que sea almacenado o guardado. Es decir, si la información no es guardada en alguna clase de medio, no constituye documento electrónico, porque no establece con certeza la prueba producida por el mismo sistema.

- Que se permita su uso posterior. Es decir, debe permitir que el documento puede ser reutilizado cuantas veces sea necesario.

- No existe diferencia entre original y copia.

- No existe una firma manuscrita sino una digital.

- Se produce la supresión del soporte de papel, actualmente se tiende a sustituir el documento escrito en papel por el electrónico, aunque ello no deje de lado la seguridad que aun brinda el papel.

[60] Castaneda Espinoza, César Edgardo y otros. Tesis UES "El Documento Electrónico como Medio de Prueba para Acreditar Judicialmente las Obligaciones Derivadas de Dicha Contratación". San Salvador, 2005. página 83-84

- Permite identificar cuadros de información, es decir, identifica y registra todo lo que realiza en el acto o contrato.

- Permite su reconocimiento mutuo, de las partes al momento de contratar.

- Es inalterable, una vez realizado la firma de dicho estos no se pueden modificar, eliminar por medio de la seguridad del sistema que así no lo permite.

- Durabilidad, El documento electrónico perdura en el tiempo debido a que el soporte en el que se da su reproducción, es de carácter indeleble, es decir, que permanece estable en el tiempo y no puede ser alterado sin dejar huella alguna.

2.3.4 Naturaleza Jurídica del Documento Electrónico.

En cuanto a su naturaleza jurídica se estima que el documento informático constituye una nueva forma de soporte electrónico surgida al amparo de las modernas técnicas de la electrónica, al cual le es perfectamente asimilable toda la teoría civil y comercial de la contratación, con adaptaciones obvias, que debe ser generado por la vía legislativa y cuyo valor probatorio debe ser similar al del documento per cartam, una vez adaptado por la vía legal.

Así considerado, el documento informático, podrá ser tenido como instrumento privado o público, en la medida que se cumplan o no los requisitos que cada legislación contempla. Es así que este podría en un

futuro convertirse en un documento público electrónico y sería afirmativa la ubicación en este documento la intervención del notario cumpliendo los siguientes requisitos. a) Una adecuación técnica de la informática, destinada a satisfacer los requerimientos jurídicos propios de la teoría de la contratación y del acto escriturario formal y b) una adecuación del Derecho a los condicionamientos esenciales de la informática, sin que se afecten los principios generales y particulares destinados a proteger la escritura pública y a fiscalizar la labor cautelar del Notario[61].

2.3.5 Clasificación del Documento Electrónico

El Documento Electrónico puede ser clasificado de dos formas las cuales son:

- **En un Sentido Material.**

Tengamos presente desde ya que en la actualidad su materialidad tiende a separarse de éste, permitiendo así la existencia del documento electrónico, cuyo ser se manifiesta a través de un sistema de conformación electrónica presente en un Hardware[62] adecuado y que se expresa a través de un lenguaje binario, conformado por bits o unidades mínimas de información, manteniéndose intocado el documento en su realidad intelectual.

[61] MSc. Yanixet Formentín Zayas. Profesora Instructora de la Facultad de Derecho de la Universidad de Camaguey. Cuba. www.monografias.com.

[62] hardware. (Voz ingle.). m. Inform. Conjunto de los componentes que integran la parte material de una computadora.

- **En un Sentido Históricos o Jurídicos.**

Según se atienda al valor agregado que contienen: serán simplemente históricos, en aquellos casos en que cumplan con una finalidad representativa, como puede ser el caso de un diploma que deje constancia de un hecho; pero si a dicha finalidad representativa se le agrega un valor de eficacia, éste se transformará en jurídico, en cuanto supondrá una capacidad probatoria; será el caso del diploma que deja constancia, ya no de un simple hecho, sino de aquel que tiene connotación jurídica: el de quien obtiene un título profesional; éste, en efecto, amerita y prueba que tal persona es un profesional en la materia que el diploma indica.

En este segundo caso, el documento implicará una -evidentia, esto es, que entre éste y su autor hay una inmediación o adecuación entre actum y dictum, entre el acto que ha tenido lugar en un momento dado y la narración hecha en el documento, en el decir de Rafael Núñez Lagos.

Es por lo dicho, que se acostumbra distinguir entre documento e instrumento, en cuanto el primero no necesariamente deberá pertenecer a la esfera del Derecho, en tanto que el segundo sí es plenamente jurídico, ya que posee eficacia. De este último, agreguemos finalmente que si además de eficacia, es indubitado esto significa no sujeto a dudas en relación con su contenido, y con plena correspondencia entre actum y dictum, será además, instrumento público.

Otros tratadistas clasifican al Documento Electrónico en diferentes ramas de acuerdo a la naturaleza por la cual fue creada o herramienta que

es creada y entre ellas tenemos. De acuerdo al grado de conservación de los documentos electrónicos estos pueden clasificarse en[63]:

De carácter Volátil: Como los datos contenidos en las memorias de circuitos RAM (Random Access Memory), los cuales se pierden inmediatamente al cortar la energía a la computadora.

Permanentes: Son aquellos contenidos en algunas memorias de masa como discos compactos, cintas y floppy disk. A diferencia de la anterior categoría, los datos allí almacenados desaparecen sólo al ser borrados, en caso contrario se mantienen en el tiempo.

Inalterables: Son aquellos que una vez grabados no pueden ser alterados, sólo leídos. Dentro de estos encontramos las memorias ROM (Read Only Memory), que consiste en un circuito o chip integrado a la computadora o que se le puede incorporar a la voluntad y los CD-ROM, que son una memoria de masa contenida en un disco láser.

2.3.6 Seguridad Jurídica del Documento Electrónico.

Para poder analizar la seguridad jurídica con la que cuenta el documento electrónico debemos primero analizar el significado de seguridad informática, la que podemos definir como el conjunto de técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados.[64] Los

[63] Arrué Echegoyén, Carolina Esmeralda, Masin Masin, Natalia Margarita y Vázquez Lara, Manuel Alejandro. Ob. Cid. Pág. 152

[64] "Revista de Ciencias Jurídicas", Universidad de Costa Rica, Facultad de Derecho, Numero 102, septiembre-diciembre año 2003, Colegio de Abogados, San José. Página 39

daños que se mencionan incluyen el mal funcionamiento del hardware, la perdida física de datos y el acceso a bases de datos de personas no autorizadas y esto en el comercio electrónico es muy peligroso ya que cuando se realiza un contrato electrónico se debe tener la plena seguridad de los que intervienen en el contrato y del contenido del mismo.

Por lo que la seguridad jurídica del documento electrónico debe comprender su *autenticidad, su integridad, su disponibilidad y* lo que se ha dado en llamarlo en el ámbito jurídico como "*el no repudio*"[65]. Es decir para que un documento electrónico sea seguro debe cumplir a cabalidad con los principios y las características que mencionamos al inicio del tema del documento electrónico. Todos estos principios y los medios tecnológicos como la firma digital y los certificados electrónicos entre otros ayudan a dar esa seguridad al documento los cuales desarrollaremos en los capítulos siguientes para un estudio más profundo de cada uno de ellos.

2.4 Contratación Electrónica.

El comercio electrónico ha venido a implementar figuras que no son consideradas por leyes y que divergen en gran medida de los principios tradicionales del derecho comercial y civil, convirtiéndose en un reto para los legisladores en el sentido que no es aceptable la adecuación funcional de los nuevos elementos al marco legal existente, siendo lo apropiado la creación de un marco jurídico especial que lo regule.

[65] Highton de Nolasco, Elena Inés y Angélica Generosa Elvira Vitale. La Función Notarial en la Comunidad Globalizada, 1ra edición, Santa Fe, Editorial Rubinzal-Culzoni, 2005.

La forma de contratación del siglo XXI es y seguirá siendo una contratación fuertemente sujeta a los impactos de la tecnología de la información. La electronificación de los contratos clásicos contenidos tanto en el Código Civil como en el Mercantil, han evolucionado por lo que el derecho no se puede sustraer a estos cambios, por lo cual deberá adaptarse a las nuevas instituciones; y a derogar leyes y crear nuevas.

Y es así como se van creando nuevas modalidades para contratar como el que hoy conocemos como contrato electrónico o telemáticos, por lo que en el presente tema desarrollaremos las definiciones de este contrato, las modalidades a las que se sujeta, los principios jurídicos que los rigen y que son los que brindan la interpretación de los mismos, entre otras cosas, que nos servirán para establecer la importancia de la intervención del notario en los mismos.

2.4.1 Concepto de Contrato Electrónico

Antes de analizar el concepto de contrato electrónico, debemos entender que es Contratación Electrónica que "es aquella que se realiza mediante la utilización de algún elemento electrónico, cuando este tiene o puede tener una incidente real y directa sobre la formación de la voluntad o el desarrollo o interpretación futura del acuerdo".[66]

[66] Davara Rodríguez, Miguel Ángel. "Manual de Derecho Informático". Ediciones Aranzandi. España. 1997 Pág. 198. El cual hace referencia a los contratos de ventas a distancia "los celebrados sin la presencia física simultanea del comprador y vendedor y la aceptación del comprador por un medio de comunicación a distancia de cualquier naturaleza.

Para Juan Farina[67] son "contratos celebrados por medios electrónicos cuando la transacción es efectuada por elemento que emplea el electrón[68] tales como fax, los ordenadores, el correo electrónico, los pagos electrónicos y los sistemas de transferencia de fondos, los EDI (Electronic Data Interchange), e Internet.

Otra definición podemos decir que contratos electrónicos son los que la oferta y la aceptación se trasmite por medios electrónicos o telemáticos, no importando si las partes contratantes están o no en comunicación directa[69].

2.4.2 Modalidades de la Contratación Electrónica

En materia de contratación electrónica se presentan varias fases que comprenden el consentimiento por redes y el lugar de celebración de los mismos. Por lo que dichos efectos jurídicos de la exteriorización de la voluntad dependerán si son entre empresa-consumidor o empresa-empresa[70]. Por lo que podemos decir que existen dos y con los últimos años una tercera, modalidad en las contrataciones electrónicas como lo son las siguientes:

- ✓ ***Contratación Abierta:*** Esta contratación es la más famosa y conocidas por todos los que navegan por Internet, y es la que se da en plataformas Web que ofrecen la posibilidad de comprar bienes y servicios. Este sistema permite a cualquier persona que tenga una conexión a Internet

[67] Farina, Juan. Contratos Comerciales Modernos. Modalidades de Contratación Empresarial. Tercera edición, Editorial Astrea, Buenos Aires, 2005, página 128
[68] Entendido como la partícula más pequeña de la electricidad.
[69] Cremades Javier, Miguel Ángel, Fernández Ordóñez, Rafael Illista. Régimen Jurídico de Internet. Primera Edición. Editorial la Ley Madrid. 2002. Página 115.
[70] http://www.elnotariado.com/ver_nota.asp?idnoticias=511

acceder a un sitio Web y hacer una comprar. Al margen de las páginas Web se puede decir que se hace en pocos segundos y de manera sencilla: tras llenar un formulario de pedido se hace clic en un icono o link a efectos de enviar el pedido al oferente, el cual envía una notificación en el que informa que su pedido esta en procesamiento y el plazo de recepción de los bienes solicitados.

Por lo que decimos que es abierta porque cualquier persona, a pesar de no conocer ni tener relación previa con el empresario puede concluir un contrato electrónico con dicha persona[71].

- ✓ ***Contratación Cerrada:*** esta se lleva a cabo con un número determinado de sujetos, normalmente socios comerciales que se conocen entre sí. Es precisamente el hecho de conocer entre si y la decisión de mantener esta relación comercial duradera lo que convierte a estos en un grupo cerrado[72].

Por lo que la tecnología EDI se ha utilizado mayormente por estos grupos cerrados. Por ello, esta tecnología utiliza redes privadas o con redes gestionadas, operado por proveedores de servicios de valor añadido que prestan servicio en relación con la instalación de estos.

Pero esta tecnología con el paso de los años ha venido cambiando y es así que en 1998 se empezó a abrirse, al utilizar no solo redes privadas sino redes con conexión a Internet, con las típicas contrataciones en Internet de “uno a uno”. Por lo que surgieron las contrataciones semi-cerradas.

[71] Cremades Javier, Miguel Ángel, Fernández Ordóñez, Rafael Illista. Ob. Cid. Págs. 550 y 551
[72] Ídem Pág. 551

✓ ***Contratación Semi-cerrada:*** las cuales se caracterizan por utilizar redes con Internet, que están a disposición de cualquiera, pero por otro lado, se utilizan sistemas de seguridad que permiten excluir a terceros del uso del sistema y por tanto de la contratación. Igualmente, y en el plano de lo jurídico, para la participación en estos sistemas se requiere que el empresario firme un acuerdo que fije las reglas de participación en el mismo, y que incluye diferente aspectos jurídicos respecto a los contratos electrónicos concluidos utilizando este sistema. El tipo más utilizado en la contratación de este tipo es la compraventa y el contrato de suministro. Debe de notarse que desde un plano económico se puede decir que en estos tipos de contrato es donde se mueve la mayor cantidad de dinero[73].

Por lo que podemos decir que este ultimo sistema es el que se está utilizando mas para mover el capital de las grandes empresas y en la que se necesita medios de seguridad para impedir la intromisión de terceros ajenos a estos contratos y por lo que es necesario la intervención de un tercero de confianza que certifique la autenticidad de dicho contrato como lo es la figura del ciber notario.

2.4.3 Naturaleza Jurídica del Contrato Electrónico

Hay dos cuestiones que se deben de estudiar para conocer la naturaleza jurídica del contrato electrónico y sus implicaciones legales:

1. El Carácter Civil O Mercantil De Los Mismos.
2. La Aplicación De Las Normas De Protección De Los Consumidores A Los Contratos Electrónicos.

[73] Ídem. Pág. 553.

Para el carácter civil o mercantil de los mismos, se debe de señalar, la aplicación del régimen general contractual de los códigos civil y mercantil a la contratación electrónica[74], es así como ya lo hemos venido diciendo que los contratos tanto en papel y electrónicos no tiene diferencia mayor que el soporte en que son hechos. Por lo que siguiendo esta lógica se dice que un contrato es mercantil en aquellos en lo que participe un sujeto mercantil[75], que recaigan sobre cosas típicamente mercantiles[76] o el acto es un acto mercantil (en masa, por empresa y que recaiga sobre una cosa mercantil)[77]. Así se dice que los contratos tendrán naturaleza civil siempre y cuando no exista un sujeto mercantil o que recaiga sobre cosas mercantiles. Esto último es importante ya que como sabemos los contratos tanto mercantiles y civiles tienen tratamientos distintos tal es el caso que en los contratos mercantiles los intereses son diferentes en cuanto a la cuantificación de los mismos (en el comercio es del doce por ciento en base al artículo 960 C. Com. y el seis por ciento para los contratos civiles), además de la prescripción de una y otro cambian así los que establece el Código de Comercio es menor el tiempo los que establece en el Código Civil.

---

[74] García Mexía, Pablo y otros. Principios de Derecho de Internet. 2ª Edición, Editorial Tirantto Blanch. Valencia. Año 2005. Pág. 448.

[75] Art. 2.- Son comerciantes:
I.- Las personas naturales titulares de una empresa mercantil, que se llaman comerciantes individuales.
II.- Las sociedades, que se llaman comerciantes sociales.
Código de Comercio. D.L. Nº 671, del 8 de mayo de 1970, publicado en el D.O. Nº 140, Tomo 228, del 31 de julio de 1970.

[76] Art. 5.- Son cosas mercantiles:
I.- Las empresas de carácter lucrativo y sus elementos esenciales.
II.- Los distintivos mercantiles y las patentes.
III.-Los títulos valores.
Código de Comercio. D.L. Nº 671, del 8 de mayo de 1970, publicado en el D.O. Nº 140, Tomo 228, del 31 de julio de 1970.

[77] Art. 3.- Son actos de comercio:
I.- Los que tengan por objeto la organización, transformación o disolución de empresas comerciales o industriales y los actos realizados en masa por estas mismas empresas.
II.- Los actos que recaigan sobre cosas mercantiles.

Además de los indicados, se consideran actos de comercio los que sean análogos a los anteriores.
Código de Comercio. D.L. Nº 671, del 8 de mayo de 1970, publicado en el D.O. Nº 140, Tomo 228, del 31 de julio de 1970.

En segundo lugar la protección del consumidor, ya que como sabemos el carácter de inmediatez y rapidez que rige el comercio electrónico, no se puede dejar de lado el derecho del consumidor como un derecho constitucional que tiene todas las personas y que resulte afectado por este tipo de contratación y por ende cada legislación en base a su realidad le darán un tratamiento efectivo para su protección, así en España podemos señalar que todo contrato electrónico será reconocido como un contrato civil, por los rasgos que posee y para proteger a los consumidores y no verse en la incertidumbre a la hora de incoar una acción judicial, la cual se la pueden declarar improponible[78].

2.4.4 Principios Rectores de la Contratación Electrónica

Como toda ciencia, disciplina, estudio o rama de conocimiento se basan siempre por ciertos principios encontrando en ellos las características principales que los diferencian de los demás, así la contratación electrónica como una nueva institución jurídica también se rige por ciertos principios, los cuales a continuación detallamos:

2.4.4.1 Principio de Equivalencia Funcional.

Este principio constituye el principal fundamento del comercio electrónico y por consiguiente de la contratación electrónica ya que se trata de un requisito *sine qua non* de este nuevo comercio que sin este no podría desarrollarse con la seguridad y confianza jurídica que se requiere.

[78] García Mexía, Pablo y otros. Principios de Derecho de Internet. 2ª Edición, Editorial Tirant Lo Blanch. Valencia. Año 2005. Pág. 449.

Este principio se puede simplificar diciendo que la función jurídica que cumple la instrumentación escrita y autógrafa respecto de todo acto jurídico, o su expresión oral, la cumple de igual forma la instrumentación electrónica a través de un mensaje de datos con independencia del contenido, extensión, alcance y finalidad del acto así instrumentado.[79]

Es decir que este principio de equivalencia funcional es la base fundamental para evitar la discriminación de los mensajes de datos electrónicos con respecto a las declaraciones de voluntad expresadas de manera escrita o tradicional, en este sentido no se altera ni se modifica el actual régimen de las obligaciones, ni de los contratos. El comercio electrónico no implica una modificación de la teoría de las obligaciones y de los contratos sino que se convierte en un nuevo soporte y un medio de transmisión de las voluntades, pero sin negar que su utilización ha establecido un cambio significativo en la interpretación del derecho aplicable a los contratos como consecuencia necesaria de la presencia de lagunas jurídicas.

2.4.4.2 Principio de Neutralidad Tecnológica

Este principio se orienta a que las normas del comercio electrónico, pueden abarcar las tecnologías que propiciaron su reglamentación, así como las tecnologías que se están desarrollando y están por desarrollarse. En consecuencia, las tecnologías electrónicas incipientes deben ser comprendidas por las normas en la misma medida y extensión en que lo son

[79] Rincón Cárdeno, Erick. Contratación Electrónica. Primera Edición, Centro Editorial Universidad del Rosario, Bogotá, 2006, Página 30

las tecnologías plenamente operativas al día de la aprobación de la ley nacional aplicable.[80]

En este sentido se dice que es un pilar importante de la interpretación legal, ya que es la concreción real y necesaria del entorno dentro del cual la ley se va a aplicar, de modo que la interpretación realista permite que se desarrolle acorde a los hechos y a las situaciones en concreto es decir que este acorde con el constante desarrollo de las nuevas tecnologías.

2.4.4.3 Principio de Buena Fe

La buena fe se consagra como un principio general del derecho, que puede ser entendido de dos diferentes maneras: subjetiva o psicológica y objetiva o ética[81].

Para Guillermo Cabanellas la buena fe es la Rectitud, honradez, hombría de bien, buen proceder. Creencia o persuasión personal de que aquel de quien se recibe una cosa, por título lucrativo u oneroso, es dueño legítimo de ella y puede transferir el dominio[82].

Este principio constituye la reafirmación del fundamento que orienta a todo el Derecho, especialmente cuando se hace referencia al intercambio nacional e internacional de bienes y servicios. Pero al referirse al comercio electrónico se convierte en relevante por las características del intercambio que se realiza por medio de los soportes tecnológicos está fundamentada en

[80] Rincón Cárdeno, Erick. Contratación Electrónica. Ob. Cid. Página 30-31
[81] Palés, Marisol Directora de Diccionarios, texto y educación. Diccionario Electrónico Jurídico Espasa Calpe, S. A. Editora Celia Villar, Fundación Tomás Moro, Creación y realización electrónica: Planeta Actimedia, S.A, Madrid, 2001.
[82] Cabanellas, Guillermo. Diccionario Jurídico Elemental. 12ª Ed. Buenos Aires: Heliasta, 1997. Pág. 521.

la confianza entre los contratantes de modo que el desarrollo de la misma está íntimamente ligado no solo a la convicción de que se está obrando bien sino que también que con su obrar se está permitiendo que el co-contratante alcance aquellas causas por las cuales celebró el contrato.

2.4.4.4 Principio de Libertad de Comercio

Este principio establece que la prestación de estos servicios de comercio electrónico se realizará en libre competencia, sin que se puedan establecer restricciones para los servicios de la sociedad de la información.

La prestación de servicios de la sociedad de información no debe estar sujeta a autorización previa. Esta afirmación implica que las transacciones que se realicen mediante vía digital no tendrán limitaciones salvo las prohibiciones penales y civiles que se establecen en El Salvador con respecto a los objetos que no están en el comercio (el comercio de niños por ejemplo).

Entonces este principio establece que se deben eliminar barreras legales basadas en documentos escritos que se oponen a la transacciones electrónicas, se debe también reafirmar los derechos de las partes para decidir sobre los medios tecnológicos que son apropiados para autenticar sus transacciones, así mismo garantizar a todas las partes la posibilidad de defender un sistema de autenticación en los tribunales.[83]

[83] Rincón Cárdeno, Erick. Ob Cid. Página 31

2.4.4.5 Principio Protectorio

Este principio establece la necesidad de que en el comercio electrónico haya una protección de parte de una norma jurídica eficaz, contra los posibles inconvenientes que se generan con su utilización, en el que se respeten los derechos de los usuarios contra terceros.

En nuestro país no es aplicable a cabalidad este principio porque no existe una legislación que regule expresamente el comercio electrónico.[84]

2.4.5 Elementos de Validez del Contrato Electrónico

Sabemos que para la formación de un contrato es necesario que se cumplan requisitos que le brindan validez al mismo, según nuestra legislación [85] se establece que para que una persona se obligue con otra por un acto, contrato o declaración de voluntad es necesario en primer lugar que sea legalmente capaz, segundo que haya un consentimiento libre de todo vicio, tercero que el objeto por que se contrata sea licito y cuarto que la causa por la que se contrata sea licita. Como el contrato electrónico es básicamente un contrato común, ya que lo electrónico le viene como una nueva modalidad para realizar el contrato por lo que se le aplican las mismas reglas que a los contratos realizados en una base en papel.

[84] Según la opinión de Licenciado Elí Valle, Asesor Jurídico del Ministerio de Economía, se estaba trabajando en un proyecto de Ley de Comercio Electrónico, pero que lamentablemente quedo solo en borrador y sin esperanzas que pase a más. Sin embargo se trabaja en un proyecto de Ley de Comunicación Y Firma Electrónica, que para él es más necesaria.

[85] Artículo 1316 del Código Civil.

2.4.5.1 Capacidad para Contratar

La capacidad es uno de los primeros requisitos que se deben cumplir para que el contrato sea válido, cualquiera que sea la naturaleza del contrato es necesaria la capacidad de ambos contratantes.

La capacidad la podemos definir como "la aptitud de una persona para adquirir derechos y poderlos ejercer por si sola"[86]. Se clasifica en *capacidad de goce o adquisitiva y capacidad de ejercicio.* La primera es la aptitud de una persona para adquirir derechos, para ser titular de ellos, para poder ser sujeto de derecho. Sin esta capacidad una persona no puede adquirir por sí misma y sus actos son completamente nulos[87].

La capacidad de ejercicio es la capacidad de una persona para poder ejercer personalmente, por si misma los derechos que le competen.[88] La persona que es privada de esta capacidad de ejercicio puede ser titular de derechos, incorporándolos a su patrimonio y obtener todos los beneficios pecuniarios que sean susceptibles de producir, pero para hacerlos valer requiere el ministerio de otra persona.

Así como a modo de ejemplo podemos decir que si un menor de edad realiza una transacción electrónica esta quedaría perfeccionada o no este contrato, para dar respuesta a esto podríamos decir que en un primer momento si quedaría perfeccionado este contrato, ya que el principio de buena fe nos dice que todo contrato celebrado por medios electrónicos se tendrá por valido, y esto es porque, siendo un contrato electrónico este posee

[86] Alessandri y Somarriva, Curso de Derecho Civil. Las Fuentes de las Obligaciones en Particular. Tomo IV. Redactado y puesto al día por Antonio Vodanovic H., Santiago de Chile, Editorial Nacimiento, 1999, página 76
[87] Véase el artículo 1318 del Código Civil.
[88] Alessandri y Somarriva. Obra citada, página 177

dos pares de claves, una pública y una privada y la clave privada es la que la persona que la posee debe de resguardar bien, y en dado caso que por descuido un menor tenga acceso a ella, es responsabilidad del que la posee.

2.4.5.2 El Objeto debe ser Lícito.

Según el artículo 1331 del Código Civil toda declaración de voluntad debe tener por objeto una o más cosas que se trata de dar, hacer o no hacer, pudiendo ser el mero uso de la cosa o su tenencia. Este para ser valido debe llenar ciertos requisitos que son: *debe ser real, determinado y licito.*

Real: quiere decir que debe existir realmente, es decir que si por ejemplo, le vendo una casa o un carro a otra persona, este carro o casa debe existir, porque si no existe entonces el contrato no tendría objeto.

Determinado: esto quiere decir que se debe especificar el objeto por el cual se hace el contrato, es decir la cantidad y la calidad del objeto.

Licito: Este es el requisito más importante del objeto. En nuestra legislación en el artículo 1333 del Código Civil establece que hay objeto ilícito en todo lo que contraviene al derecho público salvadoreño. Y el artículo 1335 establece un listado de objetos ilícitos[89] , es decir que si el objeto de algún

[89] Código Civil, Art. 1335.- Hay un objeto ilícito en la enajenación:
1º De las cosas que no están en el comercio;
2º De los derechos o privilegios que no pueden transferirse a otra persona;
3º Lo hay también en la enajenación de las cosas embargadas por decreto judicial, o cuya propiedad se litiga, a menos que preceda autorización judicial o el consentimiento de las partes; pero aun sin estas condiciones, no podrá alegarse lo ilícito del objeto contra terceros de buena fe, tratándose de bienes raíces, si la litis o el embargo no se hubieren anotado con anterioridad a la enajenación.
Tampoco habrá objeto ilícito en la enajenación tratándose de los casos especificados en el artículo 721.

contrato recae en cualquiera de los estipulados en el artículo mencionado, el contrato es nulo porque su objeto es ilícito.

2.4.5.3 La Causa debe ser Lícita

Este requisito de validez se encuentra contemplado en los artículos del 1338 al 1340 del código civil. El primero de ellos establece que no puede haber obligación sin una causa real y licita, pero que no será necesario expresarla y el inciso segundo del mencionado artículo se define *causa* y manifiesta que es el motivo inmediato que introduce a contraer la obligación; y también manifiesta una definición de *causa ilícita,* y establece que es la prohibida por la ley, o contraria a las buenas costumbres o al orden público.

Se debe observar que para que el consentimiento por medios electrónicos sea válido, en primer lugar, que las personas sean capaces, lo que genera serios problemas ya que los contratantes nunca están en presencia del otro, sin embargo las precauciones para evitar defraudaciones en los últimos años se han vuelto más fuertes y están a cargo del proveedor de los productos o servicios que se ofrecen a través de la red, también debe observarse que el objeto y la causa de la contratación sean licitas[90], podemos observar que el contrato electrónico en realidad es igual que un contrato tradicional en lo que a requisitos de validez se refiere, ya que la contratación electrónica es únicamente una nueva forma de contratar, sin cambiar los requisitos establecidos en las leyes, es un nuevo soporte que si antes se realizaba en papel ahora se realiza por medio de una computadora. Pero queda plantada la duda. ¿Cómo se manifiesta el consentimiento cuando

[90] Rincón Cárdenas, Erick. Contratación Electrónica. Ob. Cid. Página 38

el contrato es electrónico?, a lo que en el siguiente tema se le dará respuesta.

2.4.5.4 El Consentimiento por Medios Electrónicos

Según Alessandri y Somarriva en su obra Las Fuentes de las Obligaciones, el consentimiento se puede definir como: "el acuerdo de voluntades de dos o más personas con un objeto licito.[91]" En el acto unilateral se denomina voluntad, pero esto se observa en la contratación tradicional (refiriéndose a la contratación que se realiza en soporte papel), pero cuando hablamos de contratación electrónica entonces surgen las dudas de cómo se manifiesta el consentimiento en esa situación, ¿se manifestara de la misma manera que en la contratación tradicional?, o ¿habrá diferencia?, esto es lo que trataremos de dar respuesta en el presente tema, en donde analizaremos como se da el consentimiento por medios electrónicos y si pueden generarse los vicios del consentimiento que conocemos.

2.4.5.4.1 Formación del Consentimiento por Medios Electrónicos. Oferta y Aceptación.

Para la formación de un contrato el consentimiento es uno de los elementos más importantes[92], ya que está íntimamente ligado a la voluntad de los contratantes, además si en el consentimiento se presenta algún vicio puede recaer en una nulidad que puede ser relativa e incluso absoluta.

[91] Alessandri Y Somarriva, obra citada. Página 176
[92] Alessandri Y Somarriva, Curso de Derecho Civil. Las Fuentes de las Obligaciones en Particular. Tomo IV. Redactado y puesto al día por Antonio Vodanovic H., Santiago de Chile, Editorial Nacimiento, 1999, página 76

Este consentimiento, para considerarse valido, debe reunir ciertos requisitos los cuales son: *que sea serio,* porque debe existir la intención, el propósito de crear un vínculo jurídico *y que se exteriorice,* debe darse a conocer externamente. Sin estos requisitos el contrato puede recaer en una nulidad.

Tanto en la contratación tradicional como en la contratación electrónica, el consentimiento se completa con la oferta y la aceptación de ambas partes, tenemos que para la formación del contrato se requiere que una de las partes tome la iniciativa y le proponga al interesado el objeto del contrato así como las condiciones y las modalidades por las cuales se va a regir el mismo y así la otra persona puede manifestar su conformidad y de esta manera nace el vinculo contractual.

El consentimiento electrónico está constituido por fases las cuales son las siguientes: motivación, intención, deliberación, decisión, expresión o manifestación, transmisión y conocimiento, por el oferente[93]. Estas fases son por las que pasa el aceptante. El sistema informático, una vez activado expresa la declaración de voluntad de un modo totalmente electrónico y telemático, es decir que si no hay un acuerdo de las partes no existirá contrato.

Si bien es cierto que la evolución del derecho a dejado de lado los formalismos de la legislación tradicional, sigue siendo de suma importancia la manifestación de la voluntad de las partes para que el contrato pueda materializarse, por lo que con el contrato electrónico es igual, recordemos la contratación electrónica no implica un cambio en la teoría de las obligaciones

[93] Galán Cortez, Jeannie Elizabeth, y otras. Tesis UES. La Firma Digital Como Medio De Seguridad Y Consentimiento En Las Transacciones Del Comercio Electrónico. 2006, página 91

o el implemento de una nueva sino que es únicamente un nuevo soporte de los contratos, ya no son impresos en papel sino que por medio de un programa de computadora.

- ✓ **La Oferta.**

Se encuentra constituida por la voluntad del que propone el contrato[94], y se puede definir como "el acto por el cual una persona propone a otra la celebración de un contrato sobre bases determinadas"[95]. En lo que respecta a la **oferta electrónica** la podemos definir como "la declaración unilateral de voluntad que una persona realiza a través de medios de comunicación y/o medios informáticos, invitando a otra persona a que la celebración de una convención quedará perfecta con la sola aquiescencia de ésta".[96] Otra definición de oferta electrónica es la establecida en la Convención De Las Naciones Unidas Sobre Los Contratos De Compraventa Internacional De Mercaderías[97], en el artículo 14.1 "la propuesta de celebrar un contrato, dirigida a una o varias personas determinadas, constituirá oferta si es suficientemente precisa e indica la intención del oferente de quedar obligado en caso de aceptación".

Como todas las instituciones jurídicas tiene ciertos requisitos que siendo la voluntad de uno de los contratantes debe hacerse con la *intención de producir el vinculo jurídico[98],* es decir que no es válida una oferta que no tenga la intención de obligarse, por ejemplo cuando un padre hace una promesa a su hijo que si obtiene buenas calificaciones le dará un obsequio

[94] Alessandri y Somarriva, obra citada, página 78
[95] Ídem.
[96] Rincón Cárdenas, Erick. Contratación Electrónica. Página 39
[97] Hecha en Viena el 11 de abril de 1980.
[98] Rincón Cárdenas, obra citada.Página 79

eso no es oferta porque no existe la intención de obligarse. Otro requisito es que la intención *se exteriorice*[99]*,* esa exteriorización puede ser expresa o tacita, expresa cuando se hace en términos explícitos y es tacita cuando se deduce de ciertas circunstancias. También debe ser *completa y voluntaria.*

La oferta electrónica se puede clasificar en base a las ofertas realizadas a través de las nuevas tecnologías de la información y la comunicación: 1) Aquellas realizadas vía fax, télex e inclusive por teléfono; 2) Aquellas realizadas a través de Internet.

En la referida convención en su parte II "formación del contrato", artículos 14 al 17 se establece lo concerniente a la oferta electrónica, en donde el artículo 15 establece el momento en que la oferta surtirá efectos y determina que es cuando llegue al destinatario. Pero para saber si esa oferta ha sido enviada por la persona quien dice ser en el artículo 13 de la Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional[100]*,* establece la atribución de los mensajes de datos[101], determinando que si una oferta se entenderá presentada por el oferente cuando sea enviado por el mismo oferente, pero también expone otra situación que si no ha sido enviada por el oferente, también se entenderá que proviene de él cuando se haya enviado por una persona facultada para actuar en nombre del oferente o por medio del un sistema de información.[102]

---

[99] Ídem.
[100] Aprobada por la Asamblea General de las Naciones Unidas en la 85a. sesión plenaria, del día 16 de diciembre de 1996.
[101] Artículo 2 Definiciones
Para los fines de la presente Ley: Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax.
"Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional".
[102] Artículo 13

En la contratación electrónica tanto la oferta como la aceptación deberán proponerse y celebrarse por similares medios. Sin embargo, basta que sólo sea electrónica la aceptación para que el contrato se tenga por tal, así, mientras no exista una oferta electrónica, como por ejemplo algún artículo ofertado por catálogo en formato papel pero adquirido a través una llamada telefónica.- No ocurre lo mismo en caso que sólo la oferta sea electrónica, ya que se puede haber recibido la oferta vía correo electrónico pero celebrarse el contrato de compra-venta en un documento escrito con formato papel.

Para que una comunicación constituya oferta consideramos que a la luz de nuestro sistema normativo salvadoreño, bastará con que "contenga los elementos esenciales del contrato" (determinando con claridad el objeto del mismo).

Con la oferta concluye la primera fase o etapa de la formación del consentimiento en un contrato electrónico y por consiguiente de su perfeccionamiento, ya que la sola declaración de voluntad del oferente no es apta, para producir efectos jurídicos, esto implica que la declaración se hace en doble vía tanto como el que ofrece como el que la acepta o la rechaza, y esto constituye la segunda fase que es la aceptación de la oferta, la que analizaremos a continuación.

Atribución de los mensajes de datos
1. Un mensaje de datos proviene del iniciador si ha sido enviado por el propio iniciador.
2. En las relaciones entre el iniciador y el destinatario se entenderá que un mensaje de datos proviene del iniciador si ha sido enviado:
a) Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje; o
b) Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

- ✓ **La Aceptación.**

La aceptación es el acto por el cual una persona, a quien va dirigida una oferta, expresa su voluntad a adherir a ella".[103] La aceptación electrónica se define como la "declaración unilateral de voluntad que una persona realiza a través de medios de comunicación y/o medios informáticos, manifestando su conformidad a una propuesta recibida por ella"[104].

Así como la oferta la aceptación tiene ciertos requisitos generales que debe llenar para que se forme el consentimiento, los cuales son: 1) *debe ser voluntaria y 2) debe manifestarse externamente.* Es un acto voluntario porque, como se dijo anteriormente el consentimiento es una declaración de voluntad del contratante, íntimamente ligada a la libertad que tiene la persona de contratar o no, por lo que al recibir una oferta tiene el derecho de aceptarla o rechazarla según sus intereses, por lo que si el contratante acepta la oferta obligado por cualquier circunstancia constituye un vicio del consentimiento y acarrea una nulidad absoluta.

Se debe exteriorizar, porque al derecho solo le interesa la manifestación externa de una idea, no es aceptada una manifestación del pensamiento que solo se queda en eso, en pensamiento. Sin embargo existen excepciones en las que el silencio constituye una manifestación de voluntad, que es cuando ese silencio se encuentra unido a ciertas circunstancias[105]:

1. Cuando así se hubiere estipulado.

[103] Alessandri y Somarriva, Obra Citada, página 83
[104] Rincón Cárdenas, Obra Citada.Página 40
[105] Alessandri y Somarriva, Obra Citada, página 83

2. El caso contemplado en el artículo 1885 del Código Civil, que establece la obligación de las personas que por su cargo o profesión tienen de aceptar o no el encargo en el menor tiempo posible si no lo hacen su silencio se mira como una aceptación tacita.[106]
3. Cuando entre dos o más personas se celebra frecuentemente un contrato.
4. Cuando en cualquier forma del contrato ha tenido su origen en insinuaciones que ha hecho el destinatario.

Existen otros requisitos que son necesarios para que se conforme el consentimiento en cuanto a la aceptación, y ellos son los siguientes[107]:

1) Debe ser Congruente: esto se refiere a que la manifestación de la aceptación debe tener relación con la oferta sin que varíe en los objetos, la cantidad, la calidad y el valor.
2) Debe darse mientras la oferta este vigente: la oferta se encuentra vigente mientras no produzca dos hechos jurídicos; la retractación y la muerte o incapacidad sobrevenida del oferente, que se encuentra regulados en el Código de Comercio en el Art. 969[108].
3) Debe ser oportuna: se entiende que la aceptación es oportuna cuando se otorga dentro del plazo legal que es el señalado como periodo de validez por la ley, o bien el plazo voluntario o convencional establecido por las partes, caso en el cual no existirían inconvenientes.

---

[106] Art. 1885.- Las personas que por su profesión u oficio se encargan de negocios ajenos, están obligadas a declarar lo más pronto posible si aceptan o no el encargo que una persona ausente les hace; y transcurrido un término razonable, su silencio se mirará como aceptación.

Aun cuando se excusen del encargo, deberán tomar las providencias conservativas urgentes que requiera el negocio que se les encomienda.

[107] Galán Cortez, Jeannie Elizabeth, y otras. Tesis UES. La Firma Digital Como Medio De Seguridad Y Consentimiento En Las Transacciones Del Comercio Electrónico. 2006, página 98

[108] La Retractación ocurre cuando el oferente puede dejar sin efecto la propuesta emitida mientras esta no haya sido aceptada; en las ofertas electrónicas realizadas por correo electrónico es fácil que se de esta figura, pero en las ofertas permanentes que se dan en línea resulta muy difícil por el hecho que el cliente compra en el mismo momento que accede a la pagina respectiva.

4) Debe ser pura y simple. en un contrato electrónico, en el cual la oferta es electrónica, la forma de la aceptación deberá de ser electrónica, y deberá ir dirigida al oferente, no puede dirigirse a persona diferente a este.

En el artículo 18 de la Convención De Las Naciones Unidas Sobre Los Contratos De Compraventa Internacional De Mercaderías, establece lo que se va a entender por aceptación y en qué momento surte efectos, y determina que surte efecto en el momento en que la indicación de asentimiento llegue al oferente en el plazo que se haya fijado al respecto, (si se fijo un plazo), o dentro de un plazo razonable, habida cuenta de las circunstancias de la transacción y en particular, de la rapidez de los medios de comunicación empleados por el oferente.

Y al terminar esta fase de la aceptación electrónica el contrato entonces es perfeccionado, así lo establece el artículo 23 de la mencionada convención.

Pero tanto el consentimiento en la contratación tradicional como en la contratación electrónica, pueden contener vicios así como los conocemos, el error, fuerza y el dolo, en el siguiente apartado vamos a analizar cada uno de ellos y la forma en que inciden en el consentimiento en la contratación electrónica.

2.4.5.4.2 Vicios del Consentimiento en el Contrato Electrónico

Como lo mencionábamos en el apartado anterior, el consentimiento sea en la contratación tradicional o en la contratación electrónica, puede adolecer de vicios error, fuerza y dolo.

Sabemos que para que un contrato sea valido no basta con el consentimiento de las partes y que este sea serio y declarado de conformidad a lo prescrito en la ley, es indispensable además que sea libre, consciente y con pleno conocimiento de causa, sin estas características se dice que el consentimiento adolece de vicios.

Un consentimiento viciado es, en realidad, consentimiento aunque dado en condiciones irregulares, es decir que la persona que bajo error, dolo o fuerza, ha expresado su voluntad, aunque no es libre, pero al fin y al cabo se considera como una manifestación de la voluntad.

- ✓ **Error.**

Al error se le define como el "concepto equivocado de la ley, de una persona o de una cosa; es el falso concepto de la realidad; consiste en creer verdadero lo falso y falso lo verdadero".[109] Es decir el error implica conocimiento pero equivocado. Es por tal razón que se considera un vicio ya que la ley quiere que el consentimiento se exprese con pleno conocimiento de causa y el que ignora una cosa o el que le atribuye una calidad diferente no procede con pleno conocimiento de causa.

[109] Alessandri y Somarriva, obra citada, página 110

El error se puede clasificar en *error de hecho*[110] *y error de derecho*[111], el primero es el concepto equivocado que se tiene de una persona[112], cosa o suceso; y el segundo es el concepto equivocado o la ignorancia que se tiene de la ley, el desconocimiento de sus preceptos[113], es así que el contrato ejecutado bajo la influencia de un error de derecho es válido y quien lo sufre no puede invocarlo; aunque ignore los efectos o consecuencias del contrato, es válido y surtirá todos los efectos queridos por la voluntad de las partes o la ley.

El error es el que puede presentar alguna especialidad en el ámbito de la contratación electrónica; error que puede darse, bien, durante la formación de la voluntad de negociar (vicio del consentimiento propiamente dicho), bien, en el momento de la declaración de la misma, lo que supone una divergencia entre la voluntad exteriorizada o declarada y la voluntad interna. Por ejemplo una equivocación por parte del destinatario del objeto al pulsar el icono o botón de aceptación o una aceptación de una oferta que en realidad no es tal sería un error obstativo, es la equivocación en la ejecución de un programa por parte de uno de los contratantes. No obstante cuando dicho error se produce por la negligencia del aceptante estando perfectamente clara la operatividad del programa debía tratarse de un error inexcusable.

El contrato electrónico será anulable, si contiene errores acreditados en la fase de declaración, impidiendo que lo declarado, que era lo que se quería emitir, coincida con lo que realmente se emitió o recibió. Para lograr apreciar el vicio del error en el consentimiento, es necesario que éste se

[110] Articulo 1324, 1325 y 1326 del Código Civil.
[111] Artículo 1323 del Código Civil.
[112] El error sobre la persona sólo invalidará el contrato cuando la consideración de ella hubiere sido la causa principal del mismo.
[113] Alessandri y Somarriva, obra citada, página 110

haya producido plenamente y estar perfeccionado el contrato con el error, porque si no, no habrá contrato que anular[114].

Dentro de las causas de errores que pueden ocurrir en la contratación electrónica, se pueden señalar las siguientes[115]:

- *Pérdida o demora:* cuando el documento ha sido enviado y no fue recibido por la otra parte, debido a extravió o demora en la recepción.
- *Repetición:* es casi imposible distinguir un documento electrónico original de una copia, por lo que se hace necesario que se le dote de alguna marca o signo que permita diferenciarlos.
- *Manipulación ilícita:* el documento declarado no contiene los mismos caracteres que el recibido, debido a que las partes no detectaron la intervención en el momento de la perfección del contrato y lo hacen en una fase de cumplimiento posterior.
- *Confidencialidad.*
- *Repudio*: negar el envío o la recepción del mensaje.
- *Fallos técnicos en la transmisión*: da como resultado que se intento la transmisión pero no se consiguió o no es recibida por el destinatario; o hay transmisión errónea del contenido o en la identificación de las partes.
- *Imposibilidad de comunicación:* protocolos no adecuados o sistemas incompatibles.
- *Contradeclaraciones*: documentos electrónicos con fecha posterior al contrato.

[114] Galán Cortez, Jeannie Elizabeth, y otras. Tesis UES. La Firma Digital Como Medio De Seguridad Y Consentimiento En Las Transacciones Del Comercio Electrónico. 2006, página 103
[115] Ídem.

- *Software*: manipulación intencionada, cambio del programa, virus devastador o con funciones especificas como recopilar datos, códigos o errores de programación.
- *Indebida manipulación o errores del dueño*.

✓ **Fuerza**

El segundo de los vicios del consentimiento es el de la *fuerza*, que se define como la presión que se ejerce sobre una persona por actos materiales o amenazas para inducirla a consentir.[116]

La fuerza, según el artículo 1327 del Código Civil, es "el acontecimiento ajeno a la voluntad que infunde a una persona temor de verse expuesta a ella, su consorte o alguno de sus ascendientes o descendientes capaz de producir en quien la padece una impresión fuerte o un mal irreparable o grave".

La fuerza expone al contratante, a la persona respecto de quien se ejerce, ya sea a un sufrimiento presente o al temor de un sufrimiento futuro, que puede ser moral[117] o material[118], y es el propósito de verse libre de este sufrimiento o de evitarlo el que la decide a consentir, entonces en si no es la fuerza lo que vicia el consentimiento sino el temor al que está expuesto la persona.

En cuanto a la contratación electrónica la fuerza se puede manifestar, cuando si a una persona se obliga mediante amenazas a dar una declaración

[116] Alessandri y Somarriva, obra citada, página 135
[117] Es moral cuando consiste en amenazas, cuando no es un mal presente, es decir cuando se le expone a sufrir un daño sino se celebra el acto de que se trata.
[118] Es fuerza material cuando a una persona golpea a otra para que consienta. Cuando se utiliza los golpes.

no querida bien sea directamente forzando su realización o indirectamente, forzando la entrega de las claves, sistemas criptográficos o instrumentos necesarios al titular para realizar la contratación. Es decir que la fuerza en la contratación electrónica sucederá como todo acto que infunda un justo temor de verse expuesta a ella sea el sujeto que se pretende contrate o su familia.

- ✓ **Dolo**

El dolo es el tercer y último vicio del que podría adolecer el consentimiento, en nuestra legislación vigente[119], se define como la intención positiva de inferir injuria a la persona o propiedad de otro. El dolo como vicio de la contratación, tiene como objetivo el engaño, y el ánimo de lograr la declaración mediante el artificio utilizado. Por lo que en la contratación por medio electrónico lo podemos ver cuando una persona realiza una transacción por otro para apropiarse de un bien o servicio en base al trabajo de la otra persona, así como también cuando se trata de engañar por ser un contrato a distancia a una persona haciéndole creer que es otra para realizar una transacción y adueñarse del dinero o el bien de esta persona que quiere contratar.

2.4.5.4.3 Lugar de Perfeccionamiento del Contrato Electrónico.

Este aspecto es de gran importancia para la contratación electrónica y el comercio electrónico ya que esta fija la competencia, la ley aplicable y el carácter nacional o internacional de estos tipos de contratos. Ahora bien como se ha establecido los contratos electrónicos su soporte es uno electrónico, virtual e inmaterial, el cual es muy difícil establecer un lugar fijo

[119] Artículo 42 inciso final, Código Civil.

de realización de estos tipos de contratos, ya que el lugar jurídico el cual está establecido por su dominio, puede ser que no coincida con el lugar real en donde efectivamente esta el sujeto con quien se ha contratado.

Por lo que la doctrina nos ha dado un principio general que se sigue en estos tipos de contratos y es que se fija el lugar en donde las partes han pactado (derecho dispositivo o libertad de contratar, articulo 23 de la Constitución[120]). Ahora bien ¿Qué pasara en el caso de aquellos contratos e que las partes guarden silencio o no pacten nada sobre este aspecto? Pues a esta interrogante la deberá de resolver cada legislador en base al marco legal que ha establecido para regular el comercio electrónico, y en el cual existen diferentes puntos de vista para tratar este punto; así como grupo daremos una postura uniforme en base a la Ley Modelo sobre Comercio Electrónico o conocida comúnmente como UNCITRAL[121], ya que en sus articulo 3 numeral 1) nos estable "En la interpretación de la presente Ley habrán de tenerse en cuenta su origen internacional y ***la necesidad de promover la uniformidad de su aplicación*** y la observancia de la buena fe." Su objetivo como norma internacional, es estandarizar la normativa sobre la interpretación de los contratos electrónicos y que buscan mejorar el tráfico mercantil electrónico a nivel internacional.

Desarrollando la idea anterior podemos decir que la Ley Modelo UNCITRAL en su artículo 15 nos establece "Un mensaje electrónico se considera expedido en el local donde el remitente tenga su establecimiento y recibido en donde el destinatario tenga su establecimiento. De esto podríamos decir que se tomara el lugar del domicilio el establecimiento

[120] Este apartado se ha desarrollado en el Capitulo Cuatro de la presente tesis, lo que respecta a las leyes nacionales, siendo la Constitución la máxima ley que rige el ordenamiento jurídico salvadoreño y que es de obligatorio cumplimiento.
[121] A la que nos referiremos como Ley Modelo o Simplemente UNCITRAL en adelante.

principal, aunque haya sido emitido en otro local o sucursal. Ahora bien si no se puede definir este, entonces la misma ley en el numeral 4 literal a) del mismo artículo nos dice que se tomara la residencia habitual del oferente, independientemente del lugar donde este el equipo informático que emitió el mensaje.[122]

Otra teoría del lugar donde se perfecciona los contratos electrónico es la derivada de la relación de consumo, es decir que la fuerte influencia del derecho de protección al consumidor, la cual ha sido a bien retomada por la legislación españolo, es decir que el domicilio del consumidor se tomara como lugar de celebración de dicho contrato; siendo esta una forma de protección a la parte más débil de la cadena de comercialización como lo es el consumidor final.

Las anteriores son reglas generales de interpretación de los contratos electrónicos que buscan resolver este aspecto de gran importancia para la contratación ya que sirven para brindar seguridad jurídica a las personas que deseen contratar por medios electrónicos.

2.4.5.4.4 Tiempo de Perfeccionamiento del Contrato Electrónico

En cuanto al establecimiento del tiempo en que se perfecciona un contrato electrónico, es importante establecer dicho momento, ya que desde ese momento empieza a surtir los efectos jurídicos de dicho contrato, así como también el nacimiento de los derechos y obligaciones de ambas partes. Por lo que la Ley Modelo no da una teoría especifica de cuanto para

[122] Noelia, Aída. Simposio Argentino de Informática y Derecho. Tema "Comercio Electrónico", del 11 al 12 de septiembre del año 2001. fuente de internet: wwww.alfa-redi.org/rdi-articulo.shtml?x=936

establecer este momento en el tiempo y la forma de determinarlo, pero si da criterios que deben de ser considerados muy en cuenta para determinar con mayor exactitud el hecho en el tiempo. Así se tomara como parámetros el momento en que se considera realizado la oferta como el de la aceptación.

De tal manera que se tiene recibida la oferta por el aceptante en que el mensaje de datos que la contiene entra al sistema de información designado por el aceptante y este mismo criterio se toma con la aceptación que hace el oferente, y se tiene recibida cuando entra en el sistema de información del oferente. Ahora bien la Convención de las Naciones Unidas sobre los Contratos de Compraventas Internacional de Mercaderías[123] nos establece que se tendrá por perfeccionado el contrato con la recepción de la aceptación o efectivo conocimiento, por parte del oferente, según el artículo 23 de dicha Convención que nos establece "El contrato se perfecciona en el momento de surtir efecto la aceptación de la oferta conforme a lo dispuesto a al presente Convención. Y así también el artículo 18 numeral 2) que dice "la aceptación de la oferta surtirá efecto en el momento en que la indicación del asentimiento llegue al oferente. Por lo que siguiendo este tipo de contratos opinamos como grupo son los más adecuados criterios que El Salvador debería de tomar en cuenta para la modernización del Estado y las relaciones contractuales que surgen por internet.

En el país en el nuevo borrador de Ley de Comunicación y Firma Electrónica retoma este punto y toma el criterio que para que un contrato se perfeccione la teoría de la aceptación o efectivo conocimiento lo cual se plantea en el artículo 13[124] de la misma.

[123] Ver Capitulo Cuatro referente a los tratados internacionales de la contratación electrónica.
[124] Reglas para la determinación del recibo del mensaje.

2.4.6 Amenazas a la Seguridad Informática

La seguridad es un aspecto muy importante en cualquier transacción comercial, en el sentido que el cliente debe estar seguro que no será defraudado por su proveedor, y por el otro lado el proveedor debe estar seguro que el cliente cumplirá con su obligación de pago, para esto se establecen mecanismos en el comercio convencional, tales como la celebración de contratos, firma de títulos valores, entre otros, todo esto para afianzar a las partes involucradas en la transacción comercial y salvaguardar los intereses de cada una de ellas.

Por lo que las más avanzadas técnicas de la informática han buscado mecanismos los cuales puedan ayudar a mantener la seguridad que toda persona busca al celebrar un contrato. Por lo que el comercio electrónico no es la excepción a esta exigencia por parte de los usuarios.

Con la contratación electrónica surgen ciertos riesgos, como lo es "El Riesgo de Transferencia de Información", ya que como hemos visto anteriormente las transacciones comerciales de este tipo de comercio se hacen a través de la Red, en donde transita muchísima información, y a la vez hay muchas personas que están al asecho de esa información, los famosos Hacker y Cracker, los cuales son una amenaza muy grande para el E-Commerce. En este sentido el cliente tiene mucha desconfianza de introducir sus datos personales y su número de tarjeta de crédito o débito por el temor a ser interceptado y que haya una "Usurpación de Identidad".

Art. 13 – El recibo del mensaje, se comprobará por el sistema de la recepción y tendrá lugar cuando el mensaje de datos ingrese al repositorio destinatario, encontrándose a disposición de éste para su acceso. Las partes no podrán pactar lo contrario a esta disposición.

Pero qué hacer cuando la seguridad se ve vulnerada por terceras personas, como los famosos Hacker y los Cracker, que son considerados una verdadera amenaza para la comercialización electrónica, en el presente tema analizamos como actúan estas personas, y porque se consideran amenazas, para la seguridad en Internet.

2.4.6.1 Concepto de Seguridad Informática

Para empezar debemos comprender que significa la seguridad informática y según Rodolfo Lomáscolo, la seguridad en Internet consiste en "implementar mecanismos para que cuando se reciba un mensaje o se realice una transacción por medios electrónicos, se asegure la integridad del contenido y la identidad del remitente y del receptor. Las contraseñas y palabras clave ya no son un mecanismo suficientemente fiable y seguro, ya que éstas pueden ser interceptadas durante su transmisión, de lo que desgraciadamente nos damos cuenta muy tarde o cuando la prensa se hace eco de un caso de estafa electrónica"[125].

Este autor expresa en su artículo publicado en www.markenting.com, dice "En el caso de las grandes corporaciones y organizaciones empresariales la preocupación por la seguridad en Internet es fácil de entender: las organizaciones necesitan proteger la confidencialidad de la información reservada. Por otra parte, los usuarios también deberían vigilar de cerca todo lo referente a la protección de sus datos y a la identidad de las

[125] Calderón Orellana, Mayra Jeannette, Delgado Ramírez, Juan Carlos Y Rivas Hernández, Nelson Orlando. Tesis de UES "Técnicas y Procedimientos de Auditoría para obtener Evidencias Virtuales en Empresas que Realizan Comercio Electrónico en El Salvador". Ciudad Universitaria San Salvador. Año Enero de 2005. Pág. 67.

fuentes y destinatarios de los mismos."[126] Por lo que es una prioridad guardar toda información la cual no debe de saber un tercero en los cuales son asuntos muy privados de cada persona.

Teniendo esto en cuenta podemos ahora decir que existen dos tipos de seguridad informática: la seguridad interna y la externa las cuales son fundamentales para poder brindar esa seguridad jurídica que quieren las personas tanto naturales como jurídicas.

La Seguridad Interna: Es aquélla que intenta mantener privados y accesibles sólo para los usuarios autorizados, aquellos datos internos o sensibles de la organización en cuestión. Son las redes internas o de seguridad que solo están conectadas a los ordenadores de la misma empresa sin tener conexión con el exterior.

La Seguridad Externa: Puede parecer más compleja de controlar, aunque en realidad no lo es tanto, ya que los usuarios externos no utilizan el sistema interno de la empresa, en principio no deberían disponer de ninguna clave de acceso, aunque sea a nivel de visitante, por lo que con dedicación y conocimiento se pueden crear sistemas altamente seguros.

Un ejemplo de un mecanismo de defensa para la seguridad interna son los Firewall que permiten aislar la red interna de la externa, con control del tipo de protocolo que circula, su origen y destino. El Firewall logra el balance optimo entre seguridad y accesibilidad, de esta manera la empresa puede obtener todas las ventajas que ofrece el libre manejo de su información sabiendo que esta se encuentra completamente protegida.

[126] Calderón Orellana, Mayra Jeannette, Delgado Ramírez, Juan Carlos Y Rivas Hernández, Nelson Orlando. Obra Citada. Pág. 66

Si una empresa tiene una red interna conectada a Internet o a una Intranet[127] corporativa se necesita un firewall para mantener las normas de seguridad entre ellas. El firewall mantiene separada su red interna (de la cual usted tiene control) de diferentes tipos de redes externas (de las cual usted NO tiene control). El firewall controla la entrada y salida de trafico protegiendo su red de intromisiones indeseadas[128].

La función del firewall es ser una sólida barrera entre su red y el mundo exterior. Este permite habilitar el acceso a usuarios y servicios aprobados.

Hoy no se puede decir que la conexión a Internet o a cualquier otra red abierta no se pueda realizar de forma segura, existen las herramientas y la mayoría de ellas seguro que se encuentran incorporadas en el sistema operativo de sus servidores y estaciones de trabajo.

2.4.6.2 Hacker

El avance de la era informática ha introducido nuevos términos en el vocabulario de cada día. Una de esas palabras es *hacker*, una palabra que aun no se encuentra en los diccionarios pero que ya se encuentra en la mente de todas las personas que alguna vez se interesaron por la informática y leyeron algún periódico, hoy es una palabra que causa temor entre los empresarios, legisladores y autoridades que desean controlar a los que se

[127] Una Intranet está basada en un sitio con tecnología de Internet que está ubicado en los servidores internos de la organización (aunque no siempre tenga que ser así), por supuesto se presupone la seguridad suficiente para que no puedan entrar intrusos. http://www.marketinet.com/ebooks/manual_de_intranet/manual_de_intranet.php?pg=1

[128] Merlat, Máximo, Paz, Gonzalo, Sosa, Matias, Martínez, Marcelo, Estudiantes de 5to. Año Ing. en Sistemas. www.monografias.com. Seguridad Informática. Tema: Hackers

divierten descifrando claves para ingresar a lugares prohibidos y tener acceso a información indebida.

Un hacker es una persona que mediante ingeniería inversa realiza: seriales[129], keygens[130] y cracks[131], los cuales sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican, sin que en absoluto pretenda ser dañino para el usuario del mismo[132]. Para la cultura popular hacker es aquella persona que, con ayuda de sus conocimientos informáticos consiguen acceder a los ordenadores de los bancos y de los negociados del gobierno. Bucean por información que no les pertenece, roban software caro y realizan transacciones de una cuenta bancaria a otra.

El principal objetivo de los Hackers no es convertirse en delincuentes sino "pelear contra un sistema injusto" utilizando como arma al propio sistema. Su guerra es silenciosa pero muy convincente. Se dedican a la penetración de sistemas informáticos a través de la red[133].

[129] Método para transmitir datos secuencialmente, es decir, bit por bit. http://diccionario.babylon.com/serial

[130] Un keygen es un programa informático, generalmente ilegal, que al ejecutarse genera un código para que un determinado programa de software de pago en su versión de prueba (Shareware) pueda ofrecer los contenidos completos del programa. Normalmente los keygen son archivos ejecutables (en formato *.exe) que se ejecutan sin necesidad de ser instalados. Es muy común el pensar que un keygen y un crack son lo mismo. Lo cierto es que, aunque se utilizan para lo mismo, usan sistemas diferentes: mientras que un keygen es un ejecutable que genera un código para poder desbloquear el programa, un crack simplemente hace una modificación sobre el programa para poder "completarlo". http://es.wikipedia.org/wiki/Keygen

[131] Recibe el nombre de crack un tipo de programa que realiza una modificación permanente o temporal sobre otro o en su código, para obviar una limitación o candado impuesto a propósito por el programador original. Algunas legislaciones consideran este tipo de programas ilegales por facilitar la vulneración de los derechos de autor de códigos no libres o comerciales. A veces también es llamado "medicina". http://es.wikipedia.org/wiki/Crack

[132] Calderón Orellana, Mayra Jeannette y Otros. Tesis UES. "Técnicas y Procedimientos de Auditoria para Obtener Evidencias Virtuales en Empresas que Realizan Comercio Electrónico en El Salvador". Facultad de Ciencias Económicas. 2005, página 62

[133] Calderón Orellana, Mayra Jeannette y Otros. Tesis UES. "Técnicas y Procedimientos de Auditoria para Obtener Evidencias Virtuales en Empresas que Realizan Comercio Electrónico en El Salvador". Facultad de Ciencias Económicas. 2005, página 62

Pero no se deben confundir con los llamados *cracker*, ya que estos son personas que siempre buscan molestar a otros, piratear software protegido por leyes, destruir sistemas muy complejos mediante la transmisión de poderosos virus, entre otras situaciones. Se diferencian con los hackers porque no poseen ningún tipo de ideología cuando realizan sus trabajos[134].

Es necesario que se sepan cuáles son los métodos que los hackers utilizan para perpetrar ataques a la seguridad informática (confidencialidad, integridad y disponibilidad de la información) de una organización o empresa, y que armas podemos implementar para la defensa, ya que saber cómo nos pueden atacar (y desde donde), es tan importante como saber con qué soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo. Sin olvidar que éstas últimas siempre son una combinación de herramientas que tienen que ver con tecnología y recursos humanos (políticas, capacitación).

2.4.6.3 Cracker

El término **cracker** (del inglés *crack*, romper) tiene varias acepciones, entre las que podemos observar las siguientes:

- Es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

[134] www.monografias.com

El término deriva de la expresión "criminal hacker", y fue creado alrededor de 1985 por contraposición al término hacker, en defensa de éstos últimos por el uso incorrecto del término. Se considera que la actividad realizada por esta clase de *cracker* es dañina e ilegal.

En ocasiones el *cracking* es la única manera de realizar cambios sobre software para el que su fabricante no presta soporte, especialmente cuando lo que se quiere es corregir defectos o exportar datos a nuevas aplicaciones, en estos casos (sólo en estos casos) en la mayoría de legislaciones no se considera el *cracking* como actividad ilegal.

Por ello los crackers son temidos y criticados por la mayoría de hackers, por el desprestigio que les supone ante la opinión pública y las empresas, son aquellos que utilizan sus conocimientos técnicos para perturbar procesos informáticos. Pueden considerarse un subgrupo marginal de la comunidad de hackers.

Las herramientas de "cracking" son los programas y aplicaciones que ayudan al *cracker* a lograr su fin, aunque estos programas no necesariamente debieron estar diseñadas para ese fin específico.

Entre los crackers existen diferentes tipos de los cuales podemos mencionar:

- ✓ *Pirata*: Su actividad consiste en la copia ilegal de programas, rompiendo su sistema de protección y licencias. Luego el programa es distribuido por Internet, CD’s.

- ✓ *Lamer*: Se trata de personas con poco conocimiento de informática, que normalmente buscan herramientas fáciles de usar para atacar a ordenadores, sin saber mucho de ellas, en ocasiones causando grandes daños.

- ✓ *Phreaker*: Son los crackers en línea telefónica. Se dedican a atacar y romper sistemas telefónicos ya sea para dañarlos o hacer llamadas gratuitas. Generalmente para dañarlos

- ✓ *Trasher*: Traducido al español es basurero, se trata de personas que buscan en las papeleras de los cajeros automáticos para conseguir claves de tarjetas, números de cuentas bancarias e información general para cometer estafas y actividades fraudulentas a través de Internet.

- ✓ *Insiders*: Son los crackers corporativos, empleados de la empresa que atacan desde dentro, movidos usualmente por la venganza. Los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema.

- ✓ *Mercenarios:* Que se ofrecen para romper la seguridad de cualquier programa informático que se le solicite y que contenga alguna protección para su instalación o ejecución.

Podemos concluir diciendo que la contratación electrónica y el comercio electrónico representan una nueva modalidad constitutiva de obligaciones, pero no como nueva fuente de obligaciones sino que una nueva modalidad para expresar la voluntad de obligarse, que se derive de los avances

tecnológicos que facilitan la transmisión electrónica de mensajes de datos, haciendo más ágiles las transacciones electrónicas. Esto claro con la ayuda de la Globalización Económica que ayuda a que las transacciones del comercio moderno sean más ágiles, por lo cual se necesita mayor control de estos creando sistemas de seguridad como lo hemos desarrollado que ayuden al desenvolvimiento de las personas en esta era cibernética.

CAPITULO III

HERRAMIENTAS DE LA SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LA CONTRATACIÓN ELECTRÓNICA

SUMARIO: *Introducción. 3.1 Autoridades de Certificación. 3.1.1 Definición. 3.1.2 Naturaleza Jurídica. 3.1.3 Requisitos Mínimos para su Funcionamiento. 3.1.4 Importancia de las Autoridades de Certificación. 3.1.5 Funciones De Las Entidades De Certificación. 3.2 Certificados Electrónicos. 3.2.1 Definición de Certificados Electrónicos. 3.2.2 Clases de Certificados Electrónicos. 3.2.2.1 Los Certificados según las Comprobaciones de los Datos que Realizan. 3.2.2.2 Certificados según la Directiva UIT-T X.509 (200 S). 3.2.3 Contenido de los Certificados Electrónicos. 3.3 Criptografía. 3.3.1 Definiciones. 3.3.2 Sistemas Criptográficos. 3.3.2.1 Sistema Simétrico. 3.3.2.2 Sistema Asimétrico. 3.3.2.3 Función Hash. 3.4 Firma Digital. 3.4.1 Firma Autógrafa o Manuscrita. 3.4.1.1 Elementos de la Firma Autógrafa o Manuscrita. 3.4.2 Firma Digital. 3.4.2.1 Tipos de Firma Digital. 3.4.3 Funcionamiento de la Firma Digital. 3.4.4 Eficacia Jurídica de la Firma Digita. 3.4.5 Firma Digital Certificada por Ciber Notarios.*

Introducción

Como se ha establecido en el capitulo anterior existen diferentes niveles de seguridad y peligro en el uso del Internet, por lo que este capítulo lo hemos denominado “Herramientas de Seguridad Informática para la Protección de la Contratación Electrónica”, para resaltar el uso de mecanismos y procedimientos que ayudan a proteger la confidencialidad e integridad de los datos que se envían por medios electrónicos. Como lo son tanto la firma digital, los certificados y las entidades de certificación que son herramientas que ayuda a mantener esa confianza en el sistema de transacciones electrónicas.

Por lo que desarrollaremos todas estas herramientas o mecanismos para hacer más confiables las transacciones electrónicas. Por lo que

tomamos como base para desarrollar el tema central de nuestra investigación que es el Ciber notario y su intervención en la contratación electrónica.

3.1 Autoridades de Certificación.

Una de las herramientas que la seguridad informática utiliza para darle seguridad jurídica a las transacciones electrónicas son las entidades certificadoras o autoridades de certificación, que son entidades que se encargan de emitir certificados, que a su vez sirven para distribuir una clave pública, asociar de forma segura la identidad de una persona concreta a una firma digital determinada.

En el presente tema vamos a determinar la función de estas entidades en el comercio electrónico, la naturaleza jurídica de las mismas, así como la importancia que tienen para la seguridad jurídica en las transacciones electrónicas.

3.1.1 Definición.

Al hablar de autoridades de certificación debemos de hacer una pequeña pausa para su definición y aclarar que a esta figura jurídica se le ha atribuido varias denominaciones según la legislación aplicable en cada país, de las cuales solo mencionaremos algunas y que no cambian la esencia del concepto de dicha institución sino que denotan en mayor medida el grado de laborar que realizan en cada legislación; así tenemos que se le suele llamar Autoridad de Certificación, Entidad Certificadora, Autoridad Emisora, Proveedor o Prestador de Servicios de Certificación o simplemente

Certificador; lo cual podemos dar paso a las definiciones de dicha institución jurídica.

Podemos decir que las autoridades de certificación son terceros de confianza que, cumpliendo determinados requisitos, son reconocidos y autorizados para emitir un certificado digital que identifique a una persona o entidad; pero no solamente emiten los certificados, sino que también se ocupan de la gestión de los mismos de forma que los puedan revocar y renovar cuando se den determinadas circunstancias, al tiempo que proporcionan listas y directorios de certificados y, en su caso, gestionan también distintos tipos de certificados con los limites que se establezcan y las condiciones que se pacten[135].

Apol-Lonia Martínez Nadal, en su obra Comercio Electrónico, Firma Digital y Autoridades de Certificación, establece que la autoridad de certificación es una entidad dedicada a la emisión de certificados que contienen información sobre algún hecho o circunstancia del sujeto del certificado, en el caso de los certificados de clave pública, certificados que vinculan un par de claves con una persona determinada de forma segura, cubriendo así la necesidad de servicios de terceras partes de confianza en el comercio electrónico de los tenedores de pares de claves asimétricas.

La Directiva UIT-T X.509 (200 S)[136], la define como aquella autoridad a la cual uno o más usuarios han confiado la creación y asignación de

[135] Davara Rodríguez, Miguel Angel. Manual de Derecho Informático. Séptima Edición, Editorial Aranzadi S.A. Madrid. 2005. Pág. 469.

[136] Unión Internacional de Telecomunicaciones. "Recomendación UIT-T X.509 Tecnología de la información-interconexión de sistemas abiertos-El directorio: Marco para certificados de Claves Publicas y Atributos. Pág. 5. La presente Recomendación | Norma Internacional define un marco para certificados de clave pública y para certificados de atributo. Otros conjuntos de normas pueden utilizar estos marcos para perfilar su aplicación a infraestructuras de clave pública (PKI) y a infraestructuras de gestión de privilegios (PMI). Asimismo, la presente Recomendación | Norma Internacional define un marco para la prestación de servicios de autenticación por el

certificados de clave pública. Facultativamente, la autoridad de certificación puede crear las claves de los usuarios.

Así tenemos que las autoridades certificantes o autoridades de certificación según la Dra. Leonor Guini[137] los define como terceros de confianza en un término genérico que abarca cualquier entidad de confianza de las parte intervinientes en una transacción para proporcionar servicios de seguridad. Dentro del concepto de tercero de confianza encontramos aquella autoridad que emite certificados y distribuye clave pública asociando de forma segura la identidad de una persona concreta con una clave pública determinada; a la cual se dé denotara el nombre de Autoridad de Certificación propiamente dicho.

Por lo que podemos generar el siguiente postulado en base a lo que hemos visto anteriormente ***"que toda autoridad de certificación es un tercero de confianza pero no todo tercero de confianza es autoridad de certificación"***. Porque existen terceros de confianza que no son autoridades de certificación como los Ciber notarios que son considerados como terceros de confianza pero son personas naturales que podrían tener funciones de certificación pero nunca llegar a ser entidades y así otros tipos de terceros de confianza como los proveedores de servicios de certificación.

Otra definición de autoridad de certificación es la que establece que esta entidad se dedica a la emisión de certificados de clave pública que

---

directorio a sus usuarios. Describe dos niveles de autenticación: autenticación simple que utiliza una contraseña como verificación de la identidad alegada, y autenticación fuerte con credenciales formadas utilizando técnicas criptográficas. Si bien la autenticación simple ofrece cierta protección limitada contra el acceso no autorizado, sólo se debe utilizar la autenticación fuerte para proporcionar servicios seguros.

[137] Dra. Leonor Guini. Asesora legal de la Oficina Nacional de Tecnologías de Información (ONTI), Argentina. Tema "Firma Digital Autenticada por Notario Electrónico. Tercero de Confianza. Autoridad Certificantes". http://www.elnotariado.com/ver_nota.asp?id_noticia=3244

contiene información sobre algún hecho o circunstancia del sujeto del certificado[138].

Y por último la Ley de Simplificación Aduanera, define a las entidades certificadoras como empresas que provean servicios de certificaciones de la información transmitida. [139]

3.1.2 Naturaleza Jurídica.

Al hablar de las autoridades de certificación podemos decir que poseen una característica especial en cuanto a su naturaleza jurídica como lo es la catalogación como entidad privada o pública, y ésta particularidad es otorgada por la opción legislativa de cada país en el cual se pretende regular dicha institución, basándose cada país en diversos factores, como por ejemplo, los intereses políticos o económicos (habilitar infraestructuras, equipos, personal entre otros), lo cual le dará la connotación de público o privado (ya sea por concesión o por un ente eminentemente privado), es decir que una entidad de certificación es pública o privada esto va a depender de parte de quien reciba los fondos para operar, de la forma en la que se constituya y de lo que establezcan las leyes.

Así siendo pública la institución, gozaría de mayor credibilidad al poder dar certificación a los proveedores comerciales de certificados, sería un ente controlador el cual teniendo esa connotación de pública se inclinaría a actuar en base a un interés público, en lugar de favorecer a un interés privado como

[138] Arrué Echegoyén, Carolina Esmeralda y otros. Tesis de UES "La Seguridad Jurídica que proporciona el Estado al Utilizar la Firma Digital como Medio de Expresión del Consentimiento". San Salvador. Noviembre de 2004. Pág. 97.
[139] Articulo 8 inciso primero de la Ley de Simplificación Aduanera.

lo haría una entidad privada, incluso se consideran más estables que las entidades privadas.

Así mismo las entidades de certificación públicas gozan de la facultad de poder desempeñar muchos papeles: por un lado puede desempeñarse como una entidad certificadora de otras entidades también certificadoras generalmente privadas y más pequeñas; y por otro lado puede desempeñarse como una entidad certificadora para los ciudadanos únicamente para las relaciones con la administración.

Mientras que las entidades privadas de certificación pueden dedicarse a la certificación ofreciendo el servicio de certificación a terceros como parte de su giro principal como empresa mercantil, o bien únicamente de forma complementaria a esa actividad o a efectos internos puramente organizativos.[140]

Doctrinariamente cuando se habla de la naturaleza de las entidades se hace una distinción cuando se trata de diferenciarlas ya que al tener un carácter público estas se denominan Autoridad o Entidad de Certificación, porque se considera que reviste de una cierta fuerza, seguridad y garantías a la actividad que realizan, mientras que al gozar de un carácter privado, a estas generalmente se les conoce como Proveedor o Prestador de Servicios de Certificación, debido a que esa connotación les atribuye una naturaleza comercial evitando la apariencia de naturaleza pública[141].

[140] Martínez Nadal, Apol-Lonia. Comercio Electrónico, Firma Digital y Autoridades de Certificación. Tercera Edición, Estudios de Derecho Mercantil, Cívitas, Madrid, 2001, página 151
[141] Arrue Echegoyén, Carolina Esmeralda y otros. Ob. Cid. Pág. 99.

En nuestro país tenemos una entidad de certificación que presta sus servicios en la Dirección General de Aduanas en El Salvador que se denomina Certicamara, que anteriormente era una dependencia de la Cámara de Comercio de El Salvador, pero que actualmente es una entidad de certificación de carácter privado[142].

3.1.3 Requisitos Mínimos para su Funcionamiento

Toda entidad de certificación para su funcionamiento debe de reunir ciertos requisitos legales los que están determinados en cada legislación, en los que deben reunir los conocimientos tanto técnicos como una experiencia necesaria, de forma que ofrezca confianza, fiabilidad y seguridad.

Por lo que deben de poseer un sistema de licencia que las acredite para dar un nivel mínimo de confianza que las partes puedan utilizar para confiar las transacciones que realizan.

El documento WP. 71 del 31 de Diciembre de 1996 de la Secretaria de las Naciones Unidas en su párrafo 44[143] nos indica los requisitos mínimos que debe de reunir una entidad certificadora, sin perjuicio de las que se pueden incorporar en cada legislación y que ayuden a dar esa seguridad jurídica a todas las personas, los cuales son:

---

[142] Esta entidad certificadora nació como ente con personalidad jurídica con el Decreto Legislativo Nº 523 de fecha 30 de agosto de 2001, publicado en el Diario Oficial numero 353 de fecha 5 de octubre de 2001, junto con las reformas a la Ley de Simplificación Aduanera, en las que se autoriza el funcionamiento de las entidades certificadoras, constituyéndose Certicamara como una entidad de carácter privado, facultada por el Ministerio de Hacienda, brindando servicios de emisión de certificados, revocación de certificados, publicación de certificados y almacenamiento de certificados. Galán Cortez, Jeannie Elizabeth y otros. Tesis UES. "La Firma Digital como Medio de Seguridad y Consentimiento en las Transacciones del Comercio Electrónico", 2006, página 64

[143] Alfredo Alejandro Reyes Krafft. Tesis "La Firma Electrónica y las Entidades de Certificación". Universidad Panamericana, México D.F. año 2002. Pág. 232

- Independencia, es decir ausencia de un interés financiero o de otro tipo en las transacciones que realiza.

- Experiencia en tecnología de clave pública y familiaridad con procedimientos de seguridad apropiados.

- Aprobación de equipo y programas que es un requisito técnico que utilice un sistema seguro y de confianza por parte de la autoridad de certificación para el desarrollo de sus actividades.

- Selección y administración de personal, el cual debe de ser competente, tanto desde el punto de vista de gestión como de la técnica, y de confianza.

- Seguridad Interna, consiste en un sistema en el que no se pueda sustraer información privada, la cual afectaría a los usuarios del sistema. Por lo que debe de mantenerse un control interno con el personal.

- Existencia de un plan para casos de emergencia, estas deben de poseer un plan de contingencia y de recuperación de datos frente a desastres, los cuales pueden ser desastres naturales o humanos, en los primeros tenemos los casos fortuitos y de fuerza mayor que son desarrollados en la legislación civil, y los desastres humanos o ciber-desastres, son aquellos que pueden ser producidos por técnicos de la informática (Cracker y piratas informáticos) que ingresando a un sistema o intentando ingresar a un sistema, lo infecta con un virus o cualquier herramienta tecnológica digital, pudiendo causar en su momento un congelamiento o paralizar las operaciones de una

empresa certificadora. Para los que debe estar preparada para salvar dicha información.

- Recursos y capacidad financiera para asumir la responsabilidad por el riesgo de pérdida, es decir un requisito financiero que garantice los daños, por error o negligencia o como resultado de una omisión o acción de la autoridad certificante.

- Un seguro, que cubra dichos daños.

De lo anterior podemos decir que las empresas certificadoras o entidades que certifiquen a las entidades certificadoras deben de poseer una experiencia y conocimiento grande en el área de informática jurídica y seguridad informática para poder proteger a las personas de terceros que solo deseen dañarlos.

Las entidades certificadoras, deberán ser personas jurídicas que además de estar capacitadas tecnológicamente para prestar servicios de generación y certificación de firma digital, deberán cumplir para su autorización con los requisitos legales y reglamentarios, que al efecto se establezcan. Una vez autorizadas para operar, dichas entidades estarán dotadas de la potestad de otorgar fe pública respecto a que una fecha y horas específicas, personas perfectamente individualizadas realizaron una transmisión electrónica de datos en determinados términos. La información así certificada, no podrá ser negada o repudiada posteriormente. Pero el proveedor de servicios de certificación puede perfectamente ser una persona natural, pudiendo ser un notario.

Por lo que en nuestro país la única empresa certificadora que existe actualmente es CERTICAMARA, como única institución que ha cumplido dicho requisitos.

3.1.4 Importancia de las Autoridades de Certificación.

Como sabemos la entidad de certificación es cualquier entidad de confianza de las partes intervinientes en una transacción para proporcionar servicios de seguridad; es decir aquella especifica tercera parte de confianza que desempeña de forma fundamental la función de emisión de certificados[144].

La importancia de estas instituciones radica en el crecimiento acelerado que se tiene de la participación en las transacciones electrónicas, ya que con ello se vuelve indispensable la creación de entidades que brinden confianza a estos negocios no solo en el ámbito técnico sino que también en el ámbito jurídico.

Estas instituciones se han convertido en una base importante para el comercio electrónico, ya que permiten conocer a los emisores de una oferta y aceptación de actos jurídicos y las partes intervinientes en un contrato.[145]

Además que las entidades de certificación pueden considerarse una especie de fedatario, así como también un tercero disipador de conflictos que pueden originarse con respecto a la contratación electrónica, ya que determinan al autor y la exactitud del mensaje de datos que se envía, es así

[144] Martínez Nadal, Apol-Lonia. La Ley de Firma Electrónica. 2ª edición, Cívitas, Madrid, 2001, página 101
[145] Galán Cortez, Jeannie Elizabeth y otros. Tesis UES. "La Firma Digital como Medio de Seguridad y Consentimiento en las Transacciones del Comercio Electrónico", 2006, página 51

que si el desarrollo de esa actividad es correcto adicionalmente implica la tranquilidad por parte del Estado en referencia al orden público en las relaciones con sus subordinados.[146]

3.1.5 Funciones De Las Entidades De Certificación.

Las autoridades de certificación como toda entidad tienen definidas sus funciones específicas. La actividad certificante de una certificadora asegura el vinculo entre la clave pública y el titular de la clave privada, también puede desempeñar otras funciones como autenticar fechas y horas de las transacciones, publicaciones de certificados, emisión de certificados de clave pública, servicios de registro en otras. Funciones que detallaremos a continuación.

Generación y Registro de Claves:

En el sistema de generación de claves, es esencial que las claves sean únicas y estén a prueba de manipulaciones, por ello las autoridades de certificación deben utilizar, en caso de ser ellas quienes las crean. Y al ser creadas debe de velar que queden registradas y guardadas en su sistema.

Identificación de Solicitantes de Certificados:

La emisión de certificados exige el reconocimiento previo de todos aquellos elementos característicos y únicos que son propios del solicitante; a estos caracteres se les denomina “Identificadores Intrínsecos”, tales como:

[146] Cubillos Velandia, Ramiro y Rincón Cárdenas, Erick. Introducción Jurídica al Comercio Electrónico. Ediciones Jurídicas Gustavo Ibáñez. 1ra Edición, Colombia. 2002. página 257

fotografía, firma manuscrita, huellas dactilares, timbre de voz, fondo de ojos, marcas de nacimiento, etc.

Emisión de Certificado

La entidad de certificación emite los certificados digitales únicos y perfectamente identificables a través de su número de serie.

Almacenamiento en la Autoridad de Certificación de su Clave Privada

Las autoridades de certificación son firmantes digitales en la emisión de certificados digitales, para ello deben disponer de una clave privada que sólo conocen ellos y que custodian con niveles de seguridad iguales o superiores a los declarados públicamente, dado que todo el valor reside en que cada agencia de certificación es la única capaz de generar las firmas que llevan su identificador, es de mucha importancia que esas claves privadas se almacenen y gestionen de forma segura.

Mantenimiento de las Claves Vigentes y Revocadas

Deben de almacenar los certificados emitidos mientras estos son válidos, de este modo, en el caso de que uno de los suscriptores pierda su certificado, podrá pedirle a la autoridad emisora que la envíe de nuevo una copia.

Cuando un certificado ha sido revocado el ente emisor debe de incluirlo en su lista de certificados revocados porque es desde ese momento en que la revocación del certificado tiene efecto y que puede invalidar cualquier operación que se haga con fecha posterior.

Servicios de Directorio

Este servicio de directorio es ofrecido por todas las autoridades de certificación, y es aquél en el que pueden obtener la clave pública certificada de cualquier miembro con quien quiere ponerse en contacto o establecer relaciones de algún tipo.

De todo lo anterior podemos decir que las autoridades de certificación son entes capaces de realizar una función que protege los intereses de sus usuarios a los que debe de brindar todas las garantías.

Otra cuestión importante, en la definición de los parámetros en los que una autoridad certificante actúa y por las cuales se delimita su competencia. Por lo que una autoridad certificante se diferencia de las entidades de certificación y aun de los terceros de confianza. Lo anterior es producto de la doctrina que es aplicada en cualquier parte del mundo para que sirva de insumo a una ley que regule la contratación electrónica por medio de certificados que es regulado por una entidad certificadora.

En el caso de El Salvador existe legislación en donde se regula las autoridades de certificación en el rubro de las exportaciones e importaciones en Aduanas, las cuales la Ley de Simplificación Aduanera en su artículo 8-A establece las funciones de la empresa que hoy por hoy realiza el trabajo de empresa certificadora y que fue tocado en temas anteriores, por lo que podemos contrastar las funciones que se dan doctrinalmente con los que la ley establece y podemos ver que no hay un cambio significativos con estos.

3.2 Certificados Electrónicos

Ahora que hemos establecido que son las Entidades Certificadoras y cuáles son sus funciones, es necesario para seguir con el desarrollo de nuestra investigación, desarrollar una de las funciones fundamentales de estas entidades, que es la emisión de certificados electrónicos, por lo que a continuación vamos a estudiar estos documentos que a medida que avanza la contratación electrónica se vuelven sumamente importantes para la verificación de la persona que emite un determinado mensaje de datos, o que realiza una oferta a otra para contratar, ya que como sabemos esta contratación se basa en la ausencia física de las partes, es decir que los contratantes no se encuentran presentes personalmente sino que se comunican por medio de Internet o por medio de correos electrónicos, por lo que se hace necesario establecer la identidad de los mismos para evitar problemas o fraudes.

3.2.1 Definición de Certificados Electrónicos.

Como hemos visto anteriormente en las transacciones electrónicas, las autoridades certificadoras son necesarias para evitar posibles fraudes, estas entidades emiten un certificado que vincula al solicitante con su firma digital, sin embargo la utilización de estas firmas plantea un serio problema en cuanto a que si la persona que envió el mensaje es quien verdaderamente dice ser y esto se acentúa a medida que el comercio electrónico avanza entre personas extrañas que están a miles de kilómetros de distancia. Por lo tanto se hace necesaria la implementación de medidas de seguridad, tales como las entidades de certificación (así como vimos anteriormente), esto

para que esta entidad ayude a asociar una determinada persona o entidad a la firma electrónica.

El grupo de trabajo de la CNUDMI[147] define al certificado como "un archivo electrónico que indica una clave pública junto con el nombre del suscriptor el certificado como el sujeto del certificado y confirma que el firmante potencial identificado en el certificado posee la clave privada correspondiente.[148]

Según el Real Decreto- Ley 17/1999 sobre firma electrónica de España, certificado es "la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad".

Otro concepto de certificado digital es la que se establece en la Recomendación UIT-T X.509 (200 S), que el certificado es la clave publica de un usuario, junto con alguna otra información, hecha infalsificable por cifrado con la clave privada de la autoridad de certificación que la emitió.[149]

Puede definirse también, como aquel documento electrónico generado y firmado digitalmente por una entidad de certificación que vincula un par de claves con una persona determinada vinculando su identidad.

---

[147] La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) (establecida en 1966) es un órgano subsidiario de la Asamblea General de las Naciones Unidas con el mandato general de promover la armonización y unificación progresivas del derecho mercantil internacional. Desde su creación, ha preparado una amplia gama de convenciones, leyes modelos y otros instrumentos relativos al derecho sustantivo aplicable a las operaciones comerciales o a otros aspectos del derecho mercantil que repercuten en el comercio internacional. La CNUDMI se reúne una vez al año, normalmente en verano, alternativamente en Nueva York y en Viena. http://www.uncitral.org/uncitral/es/about/origin_faq.html

[148] Martínez Nadal, Apol-Lonia. Comercio Electrónico, Firma Digital y Autoridades de Certificación. 3ª edición. Cívitas, Estudios de Derecho Mercantil. Madrid. 2001. Pág. 147

[149] Esta definición se refiere al certificado de clave pública, porque como se verá más adelante existen varias clases de certificados, y en la normativa se establecen tres clases, de autoridad, de atributo y de clave pública, los que se desarrollaran más adelante.

También lo podemos definir como un documento electrónico capaz de identificar la certificadora que lo emite, nombra o identifica al subscriptor, consigna la llave pública al mismo y que además está firmado digitalmente por la autoridad certificadora que lo emite. Es decir que el certificado digital es como un documento de identidad electrónico que garantiza la identidad de las personas tanto físicas como jurídicas que realizan contrataciones por medio de Internet.

3.2.2 Clases de Certificados Electrónicos.

Las entidades de certificación pueden emitir varios tipos de certificados según sea los servicios que se brindan, los interesados pueden elegir de entre los grupos de certificados el que más le conviene. Entre ellos tenemos:

3.2.2.1 Los Certificados según las Comprobaciones de los Datos que Realizan.

- ✓ **Certificados de Clase 1**: Corresponde a los certificados más fáciles de obtener e involucran pocas verificaciones de los datos que figuran en él: sólo el nombre y la dirección de correo electrónico del titular.

- ✓ **Certificados de Clase 2**: En los que la Autoridad Certificadora comprueba además el Documento de Identidad, el número de la Seguridad Social y la fecha de nacimiento.

✓ **Certificados de Clase 3**: En la que se añaden a las comprobaciones de la Clase 2 la verificación de crédito de la persona o empresa mediante un servicio del tipo Equifax o Duns&Bradstreet.

✓ **Certificados de Clase 4**: Que a todas las comprobaciones anteriores suma la verificación del cargo o la posición de una persona dentro de una organización.

3.2.2.2 Certificados según la Directiva UIT-T X.509 (200 S). [150]

✓ **Certificados para Autoridad de Certificación (AC)**: Que identifican a las propias Autoridades Certificadoras, y es usado por el software cliente para determinar si pueden confiar en un certificado cualquiera, accediendo al certificado de la AC y comprobando que ésta es de confianza. Toda persona o entidad que desee obtener un certificado debe pagar una cuota a las Autoridades de Certificación, cuota que irá en función de la clase del certificado y del uso que se le vaya a dar al mismo (ambas están relacionadas).

✓ **Certificado de Clave Pública:** Se realiza con el fin de que un usuario sea capaz de confiar en una clave pública para otro usuario, por ejemplo, para autenticar la identidad de dicho usuario, la clave pública será obtenida de una fuente de confianza. Dicha fuente, denominada una autoridad de certificación (CA) certifica una clave pública, expidiendo un certificado de clave pública, que vincula la clave pública a la entidad que posee la clave privada correspondiente. El certificado, tiene las propiedades siguientes:

[150] Ver pie de página 136 de pagina 84.

- Cualquier usuario con acceso a la clave pública de la autoridad de certificación puede recuperar la clave pública que fue certificada;

- Ninguna parte distinta de la autoridad de certificación puede modificar el certificado sin que se pueda detectar (los certificados no se pueden falsificar).

Debido a que los certificados no se pueden falsificar, se pueden publicar situándolos en el directorio sin necesidad de realizar ningún esfuerzo especial para protegerlos.

Un certificado de clave pública asocia la clave pública y el nombre distinguido único del usuario que el mismo describe. Por consiguiente: a) una autoridad de certificación tendrá que cerciorarse de la identidad de un usuario antes de crear un certificado para él; b) una autoridad de certificación no expedirá certificados para dos usuarios con el mismo nombre.

Un certificado de clave pública es una información disponible públicamente, y no se necesita emplear medidas de seguridad específicas con respecto a su transporte al directorio. Como éste es producido por una autoridad de certificación fuera de línea a nombre de un usuario que recibirá una copia del mismo, el usuario necesita solamente almacenar esta información en su inserción de directorio en un acceso ulterior al directorio. Alternativamente, la CA podría custodiar el certificado para el usuario, en cuyo caso a este agente tendrían que otorgársele derechos de acceso adecuados.

- ✓ **Certificado de Atributo**: Estructura de datos, firmada digitalmente por una autoridad de atributo, que vincula algunos valores de atributo con

información de identificación de su titular. El cual permite identificar una cualidad, estado o situación. Este tipo de certificado va asociado al certificado personal. (p.ej. Médico, Director, Casado, Apoderado de..., etc.). Un certificado de atributo es una estructura diferenciada de un certificado de clave pública de sujeto. Un sujeto puede tener múltiples certificados de atributo asociados con cada uno de sus certificados de clave pública. No se requiere que la misma autoridad cree el certificado de clave pública y el certificado o certificados de atributo para un usuario; de hecho, la separación de tareas aconsejará a menudo actuar de otra forma. En entornos en los que diferentes autoridades tienen la responsabilidad de expedir certificados de clave pública y de atributo, el certificado o certificados de clave pública expedidos por una autoridad de certificación (CA) y el certificado o certificados de atributo expedidos por una autoridad de atributo (AA) se firmarán utilizando claves de firma privadas diferentes. En entornos en los que una única entidad es tanto la CA, que expide certificados de clave pública, como la AA, que expide certificados de atributo, se recomienda encarecidamente que se utilice para firmar certificados de atributo una clave diferente de la clave utilizada para firmar certificados de clave pública.

3.2.3 Contenido de los Certificados Electrónicos.[151]

Como hemos visto anteriormente el uso de los certificados es para la identificación de los solicitantes el cual es firmado digitalmente por la autoridad de certificación utilizando la clave privada del titular. Y todo esto nos lleva a garantizar la autenticidad del documento y la integridad de su contenido.

[151] Ver anexo II.

En cuanto al contenido del certificado como grupo tomaremos las recomendaciones de UNCITRAL, y el proyecto de Ley de Comunicaciones Y Firma Electrónica, que está siendo estudiado por la secretaria técnica del Órgano Ejecutivo para ser presentada a la Asamblea Legislativa, para su aprobación, este proyecto lo vamos a analizar más a fondo en el capitulo siguiente que trata de la legislación aplicable a la contratación electrónica.

Como primer punto desarrollaremos los requisitos que establece UNCITRAL:

1. Que las especificaciones exigidas sean las menos posibles, y en todo caso hay que evitar datos personales que invadan la privacidad de las personas tales como, sus fechas de nacimiento;

2. Basta que solo se tengan los datos para reconocer e identificar al titular del certificado y a la entidad certificadora;

3. Se incluirá una clave pública del titular, los cuales serian el número de serie del certificado, la fecha de emisión, el tiempo de validez del certificado.

Es así que UNCITRAL ha establecido que estos requisitos pueden ser ampliados por cada legislación pero no así se pueden restringir, ya que un certificado que no contenga estos requisitos no se considerara como tal, quedando inválido todo acto que se realice con él.

El Proyecto mencionado también ha establecido el contenido que deberá tener el certificado electrónico, en el artículo 46 del mismo y manifiesta:

1. Identificación del proveedor de servicios de certificación que proporciona el certificado electrónico, indicando su domicilio y dirección electrónica.

2. Fecha de la acreditación y caducidad asignada al proveedor de servicios de certificación por la SIGET por medio de la Gerencia de Acreditación de Servicios de Certificación.
3. Identificación del titular del certificado electrónico, indicando su domicilio y dirección electrónica.
4. La clave pública del titular del certificado.
5. Las fechas de inicio y vencimiento del periodo de vigencia del certificado electrónico.
6. El Algoritmo empleado para la generación de la firma electrónica.
7. Un serial único de identificación del certificado electrónico.
8. Cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que esté sometido el certificado electrónico.
9. Indicación de la ruta de certificación.

3.3 Criptografía.

Como se ha venido desarrollando, el uso del Internet ha ido aumentando paulatinamente en el mundo y El Salvador no es la excepción a esta revolución tecnológica[152], y siendo el Internet un espacio muy poco explorado y conocido, es necesario crear mecanismos que ayuden a dar seguridad jurídica a los actos que se realicen y que tengan trascendencia en el ámbito jurídico. Por lo que surge la criptografía como una herramienta de codificación y la cual se ha venido desarrollando desde mucho tiempo atrás, siendo en el medio tecnológico su mayor trascendencia e importancia con la firma digital. Por lo que es importante su definición y los sistemas que se crean con ella.

[152] Ver anexo III.

3.3.1 Definiciones

Dos conceptos que no podemos separar cuando hablamos de seguridad informática son la criptografía y la firma digital los cuales son la base del comercio electrónico actual, para realizar contrataciones electrónicas por lo que es importante definir estos conceptos.

El uso del Internet ha traído aparejado el problema de la inseguridad en el manejo, protección y confidencialidad de la información entre usuarios, la inseguridad del documento electrónico ha dado lugar a crear estrategias para lograr la integridad y la autenticidad de la información, tanto en el contenido como en el cuidado de que ésta no sufra cambios de forma al viajar a través de la red. Esa protección se logra mediante la criptografía.

El término de la criptografía se define como el arte de la escritura secreta. Se define como "la ciencia que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlos a su forma original.[153]

Según la Real Academia Española como: "el Arte de escribir con clave o un modo enigmático". [154] Otros lo definen como el arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que solo puedan ser leídos por las personas a quienes van dirigidos.[155]

Podemos decir que el mayor reto que afronta la criptografía es el medio por el cual se envía el mensaje para desencriptar una información

[153] Martínez Nadal, Apol-Lonia. Comercio Electrónico, Firma Digital y Autoridades de Certificación. Tercera Edición, Estudios de Derecho Mercantil, Cívitas, Madrid, 2001, página 45
[154] Cubillos Velandia, Ramiro y Rincón Cárdenas, Erick, obra citada. Pág. 208
[155] http://es.wikipedia.org/wiki/criptograf%c3%ADa

para que este no sea descubierto por lo que el concepto de criptografía quedo un poco obsoleto y se retomo mejor el concepto de *criptosistema de clave pública,* el cual desarrollaremos a continuación con la evolución que ha tenido este arte al cual algunos lo catalogan como ciencia.

3.3.2 Sistemas Criptográficos

Como hemos visto el problema de la falta de seguridad en la contratación electrónica, es lo que ha llevado a crear soluciones para dar confianza y evitar este problema, la criptografía es una de estas soluciones, cuyo objetivo principal es el de proporcionar comunicaciones seguras sobre canales no seguros, pero esta también tiene ciertos sistemas para ser implementada como lo son: el *sistema simétrico y el sistema asimétrico,* los que a continuación desarrollaremos.

La criptografía se basa en algoritmos, es decir problemas matemáticos verdaderamente difíciles, un algoritmo es un conjunto de pasos necesarios para resolver un problema matemático, pero en el ámbito de la informática estos se implementan como partes de un programa principal en la que usualmente realiza una operación matemática sobre varios conjuntos de datos. Estos son también llamados *algoritmos criptográficos,* aunque también se conocen como sistemas criptográficos y se dividen en tres: *simétricos, asimétricos y hash.*

Antes de desarrollar los sistemas es sumamente necesario establecer que son las claves, porque son sumamente importantes para los algoritmos criptográficos ya que son la base de los mismos, ya sean simétricos o asimétricos, una clave criptográfica es similar a las llaves normales que se

utilizan para abrir cualquier cerrojo, siempre y cuando se utilice la llave correspondiente y en la manera correcta por lo que ahí se encuentra la similitud ya que para cada algoritmo o encriptación es necesaria la clave correspondiente.

3.3.2.1 Sistema Simétrico

Históricamente, el primer tipo de criptosistema conocido empleaba la misma clave para cifrar que para descifrar por lo que su invulnerabilidad dependía, en primera instancia, del mantenimiento en secreto de la clave empleada.[156] Este sistema es el más antiguo ya que se considera que fue utilizado por los egipcios, estos son los que utilizan una misma clave tanto para encriptar como para desencriptar una información.

Cuando se emplea la misma clave en las operaciones de cifrado y descifrado se dice que es un sistema simétrico o de clave privada, estos sistemas tienen la ventaja de ser bastante rápidos mucho más que los de clave pública o asimétricos y resultan apropiados para encriptar grandes volúmenes de datos.

Podemos definir el sistema de encriptación simétrica como "la utilización de una misma clave secreta privada utilizada únicamente entre dos personas en las operaciones de cifrado y descifrado de datos y si esta persona tuviese relación con más usuarios cada uno tendría su clave para poder descifrar el documento que el emisor haya enviado". Es decir que las dos partes que se comunican tendrían que ponerse de acuerdo de antemano

[156] Cremades Javier, Miguel Ángel, Fernández Ordóñez, Rafael Illista. Régimen Jurídico de Internet. Primera edición. Editorial la Ley Madrid. 2002. página 1317

sobre la clave que se usará en el negocio. Esta situación acarrea ciertos inconvenientes ya que la clave debería viajar junto con los datos, lo que hace demasiado arriesgado dicho negocio ya que podría caer en manos equivocadas o ser interceptado en el camino, esto es quizás el mayor inconveniente que se atribuye a este sistema porque es muy difícil lograr que las partes conozcan la misma clave sin que terceras personas tengan conocimiento de ella, ya que quien tenga la clave puede descifrar el contenido de los datos encriptados.

Además de la ventaja de ser rápidos y de que es fácil intercambiar los papeles entre el emisor y el receptor, tiene la ventaja de que aportan al receptor la seguridad de que el emisor es quien dice ser, es decir que este tipo de sistema no solo mantiene la confidencialidad sino que también identifica y autentica al emisor, aunque esta identidad pueda ser fabricada, por lo que no se deben considerar para una firma digital.

Como ejemplos de este tipo de sistema podemos mencionar esta:

"Enigma": Que es un sistema empleado en Alemania durante la Segunda Guerra Mundial, en el que las claves se distribuían a diario en forma de libros de códigos. Cada día, un operador de radio, receptor o transmisor, consultaba su copia del libro de códigos para encontrar la clave del día. Todo el trafico enviado por ondas de radio durante aquel día era cifrado y descifrado usando las claves del día.[157]

Algunos de los ejemplos de los algoritmos simétricos que se utilizan en este sistema son:

[157] http://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica

DES: Este fue diseñado por IBM a principios de los años 70 y que originariamente se conocía con el nombre de *Lucifer*. Utiliza una clave simétrica de 64 bits, de los cuales 56 son usados para la encriptación mientras que los ocho restantes son de paridad y se usan para la detección de errores en el proceso. Sin embargo el tamaño pequeño de las claves ha permitido romper con fuerza bruta este sistema en varias ocasiones es por eso que ya no es considerado como seguro. [158]

IDEA (Algoritmo Internacional de Cifrado de Datos): En criptografía, International Data Encryption Algorithmo IDEA (del inglés, Algoritmo Internacional de Cifrado de Datos) es un cifrador por bloques de 64 bits, diseñado por Xuejia Laiy y James L. Massey de la Escuela Politécnica Federal de Zúrich y descrito por primera vez en 1991. Fue un algoritmo propuesto como reemplazo del DES (Data Encryption Standard). IDEA fue una revisión menor de PES (Proposed Encryption Standard, del inglés Estándar de Cifrado Propuesto), un algoritmo de cifrado anterior. Originalmente IDEA había sido llamado IPES (Improved PES, del inglés PES Mejorado).

IDEA fue diseñado en contrato con la Fundación Hasler, la cual se hizo parte de Ascom-Tech AG. IDEA es libre para uso no comercial, aunque fue patentado y sus patentes se vencerán en 2010 y 2011. El nombre "IDEA" es una marca registrada y está licenciado mundialmente por MediaCrypt.[159]

BLOWFISH: Algoritmo simétrico que fué creado por Vruce Schneier, autor del libro “Applied Criptography”, utiliza claves de hasta 448 bits y es

[158] http://personal.telefonica.terra.es/web/criptologia/tercera4.html
[159] http://es.wikipedia.org/wiki/IDEA

resistente a ataques, por ello es considerado como unos de los algoritmos más seguros, sin embargo no es utilizado masivamente. Schneier diseñó Blowfish como un algoritmo de uso general, que intentaba reemplazar al antiguo DES y evitar los problemas asociados con otros algoritmos. Al mismo tiempo, muchos otros diseños eran propiedad privada, patentados o los guardaba el gobierno. Schneier declaró “Blowfish no tiene patente, y así se quedará en los demás continentes. El algoritmo está a disposición del público, y puede ser usado libremente por cualquiera”.[160]

3.3.2.2 Sistema Asimétrico

El sistema asimétrico fue creado por Differ y Hellma en 1976, quienes concibieron la idea de un criptosistema en el que no es necesario transferir una clave secreta entre emisor y receptor. Por lo que este criptosistema se denomina *criptosistema de clave pública (PKI)*, la cual se basa en dos claves una pública y una privada, que funcionan simultáneamente.

Por lo que este criptosistema se basa en el conocimiento general de la clave publica de la cual se identifica al sujeto, y por otro lado, para que dicho sujeto sepa el contenido de los datos enviados por su propia clave necesita de otra clave que sea privada, por lo que ya no es necesario que ambos conozcan la clave secreta, de modo que basta el conocimiento de la clave publica a la cual el interesado le asigna una clave secreta para acceder a la información. Por lo que nadie puede desencriptar ese mensaje sin ambas claves.

[160] http://es.wikipedia.org/wiki/Blowfish

Como ejemplo podemos decir que tenemos dos claves X y Z, teniendo que X es la clave privada y Z la clave pública, con el sistema asimétrico si el texto es encriptado con la clave X, deberá ser des encriptado con la clave Z y viceversa.[161]

En este tipo de cifrado se han creado varios algoritmos que son utilizados para la generación de ambas claves, así en Estados Unidos el más utilizado es la RSA[162] ideado en 1997, por los criptógrafos estadounidenses Rivest, Shamir y Adlema[163] (cuyas iníciales constituyen las siglas del algoritmo). Pero aparte de este algoritmo existen otros que desarrollaremos brevemente y son:

Diffle-Hellman: Este fue el primer algoritmo de clave pública inventada. Pero tiene problemas al no crear algoritmos indefinidos que ayuden a encriptar información, por lo que no se considera un algoritmo propiamente como tal, pero si es utilizado para crear llaves públicas y privadas.

ECC (Comprobación de errores y corrección): es un algoritmo que es muy poco utilizado pero a diferencia del RSA, éste sí puede encriptar

[161] Revista Jurídica, Universidad Pontificia Católica de Puerto Rico. Revista de Derecho Puertorriqueño, Nº 1, volumen 39. enero-abril de 2000. Pág. 44

[162] Este algoritmo inventado por Rivest, Shamir y Adleman, posee un inconveniente que tiene la dificultad de encriptar grandes volúmenes de información por lo que es utilizado en conjunto con el sistema simétrico.
El sistema criptográfico con clave pública RSA es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye (en forma autenticada preferentemente), y otra privada, la cual es guardada en secreto por su propietario. Una clave es un número de gran tamaño, que una persona puede conceptualizar como un mensaje digital, como un archivo binario o como una cadena de bits o bytes. Cuando se quiere enviar un mensaje, el emisor busca la clave pública de cifrado del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, éste se ocupa de descifrarlo usando su clave oculta. Los mensajes enviados usando el algoritmo RSA se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes (mayores que 10100) elegidos al azar para conformar la clave de descifrado. http://es.wikipedia.org/wiki/RSA

[163] Cremades Javier, Miguel Ángel, Fernández Ordóñez, Rafael Illista. Régimen Jurídico de Internet.
Ob. cit. Pág. 1320

grandes cantidades de información. ECC ("Error checking and correction") se basa en un algoritmo más complejo y se utiliza en computadoras de gama alta, como servidores de red. El sistema trabaja en conjunción con el controlador de memoria, y anexa a los bits de datos, los bits ECC, que son almacenados junto con los de datos. Estos bits extras, junto con la decodificación correspondiente, sirven para realizar la comprobación en el momento de la lectura.

Su diferencia principal con la paridad es que puede detectar el error de un bit y corregirlo, con lo que generalmente el usuario no detecta que se ha producido un error. Dependiendo del controlador de memoria utilizado, el sistema ECC también puede detectar errores de 2, 3 y 4 bits (sumamente raros), aunque en este caso no puede corregirlos; en estos casos devuelve un error de paridad. Hay que tener en cuenta que la verificación de errores (ECC o paridad) depende más de la placa base (tipo de controlador de memoria utilizado) que de la memoria en sí. La memoria pone el almacenamiento, pero es el controlador el que decide como se utilizará. Generalmente para poder utilizar una memoria ECC es necesario un controlador que pueda utilizar esta tecnología.[164]

Ahora bien como todo sistema, el sistema asimétrico tiene también sus debilidades las cuales podemos mencionar.

1) La necesidad de garantizar autenticidad de las claves públicas. Es así que A y B realizan un negocio y C siendo un enemigo de A, puede divulgar una clave la cual será clave de C, alegando ser A, por lo que B puede enviar su llave pública y así C podría conocer la información de A y utilizarla en su

[164] http://es.wikipedia.org/wiki/ECC

contra, y sin que se enteren ni A o B. Por lo que la solución a esto son las Notarias Electrónicas conocidas en Europa como Ciber Notarios, que se ocupan de dar veracidad de las personas que están contratando, los cuales darían fe de la clave pública del destinatario de un mensaje.

2) El cifrado de clave pública es muy lento en sus operaciones de cifrado y descifrado, de 5 a 20 veces de lo que es la clave secreta o simétrica. Por lo que este método es muy poco utilizado en un sistema puramente asimétrico.

Todo lo anterior es importante ya que ambas claves son generadas simultáneamente, tanto la clave pública como la privada, en un algoritmo matemático y por eso se guarda una relación estrecha entre ellos, lo que permite que una vez una información sea encriptado, solo puede ser des encriptado si se utilizan ambas llaves. Por lo que estas son la base de la firma digital, la llave publica es necesaria para encriptar un mensaje de datos cuyo destinatario es el de la clave privada, así como para verificar la identidad del firmante, y por otro lado la clave privada es necesaria para descifrar el criptograma y de suma importancia porque con esta firma el mensaje.

3.3.2.3 Función Hash

Una tabla hash o función hash[165] es una estructura de datos que une las llaves o claves con valores. Funciona transformando la clave con un algoritmo hash (se define el hash o huella dactilar digital como la característica de un ítem de dato, por ejemplo un valor de comprobación

[165] Algoritmo que transforma una secuencia de bits en otra menor, y que se aplica tanto para la creación como para la verificación de la firma digital. Apol-Lonia Martínez Nada. Comercio Electrónico, Firma Digital y Autoridades de Certificación. Tercera Edición, Editorial Civita Estudios de Derecho Mercantil, Madrid. 2001. Pág. 51

criptográfico o el resultado de la ejecución de una función de cálculo unidireccional sobre los datos, que es suficientemente peculiar del ítem de datos y que no es factible, mediante calculo, hallar otro ítem de datos que posea las mismas características; asimismo se define la función unidireccional como aquella función matemática cuyo cálculo es fácil, pero que, cuando se conoce un resultado, no es factible mediante cálculo, hallar cualquiera de los valores que pueden haber sido suministrado para obtenerlo)[166], es decir la función hash es una huella digital única, la cual verifica la autenticidad de los contratantes.

Por lo que podemos decir que el procedimiento de una función hash es complicado el cual trataremos de dar una breve explicación para efectos de entender cómo funciona esta tabla. Podemos decir que la función hash, transforma una secuencia de bits en otra menor, y que se aplica tanto para la creación como para la verificación de la firma digital. Así se aplica la criptografía asimétrica sobre la totalidad del mensaje y esto resulta menos costosa para la empresa y más accesible a los usuarios, y esto sirve si en especial es extenso el mensaje que se pretende codificar. Así sobre el mensaje inicial se aplica una función hash, y se obtiene un resumen de este, el cual es único y se le denomina compendio de huella digital única ya que es imposible que otra computadora cree otro igual, y la alteración de este produce un resultado del hash diferente.

Así el mensaje que no pesa mucho es cifrado por la clave privada de criptografía asimétrica del firmante. Y finalmente el resumen inicial, total y en claro y la firma digital son remitidos conjuntamente al destinatario.

[166] Citado por Apol-Lonia Martínez Nadal, Ob. Cit. Pág. 51.

Y el receptor del mensaje teniendo el mensaje completo (el mensaje inicial y la huella digital o hash), debe de proceder a la verificación de la firma. La verificación de la firma del mensaje original y una clave pública verificara si el mensaje no ha sido alterado por ninguna persona, y esto lo hace con su firma privada. Por lo que descifra con su clave privada el hash inicial y cifra todo el mensaje después añadiendo su clave privada y crea el hash final y siendo que el hash es una función irreversible, al tener los dos hash deben de coincidir perfectamente para su utilización y así que las partes no repudien dicho mensaje y dar esa autenticidad al mensaje producido electrónicamente.

La función hash podemos concluir que es un algoritmo matemático que ayuda a cifrar y descifrar la información para crear una huella digital única la cual no se puede reproducir otra computacionalmente, lo que la convierte en única. Asegurando que el documento no ha sido alterado.

3.4 Firma Digital

Realizar un contrato con una compañía al otro lado del mundo, ya no significa tener que hacer todo el viaje hasta el lugar donde se encuentra la empresa con la queremos contratar, ahora se puede hacer con el solo hecho de conectarse a Internet, con la llamada contratación electrónica. Pero como sabemos el contrato se rige por el consentimiento de las partes y en nuestro país el consentimiento se brinda por medio de la firma, que los contratantes estampan en el documento. Pero esto es cuando se trata de contratos tradicionales impresos en papel, pero que pasa con la firma en los contratos electrónicos, como se hace entonces para el consentimiento (por medio de la firma) en los contratos que se realizan por medio de Internet. A continuación

vamos a abordar lo referente a la firma electrónica y su utilización en la contratación electrónica.

Hoy en día se puede decir que existe una idea más clara sobre lo que es firma electrónica y firma digital o avanzada, ya que antes se tomaron como un solo tipo de firma y así lo refleja la Ley de Simplificación Aduanera en el articulo 8 inciso tercero, lo cual es un error asimilar los dos tipos de firma como una misma, por lo que a continuación vamos a desarrollar los diferentes tipos de firmas que se establecen en la doctrina, como la firma autógrafa o manuscrita, la firma electrónica, la firma digital o avanzada y la firma certificada por notario.

3.4.1 Firma Autógrafa o Manuscrita.

Por mucho tiempo la firma autógrafa ha sido la base para la identificación de la autoría de los documentos, pero desde que se creó ha tenido muchos defectos, uno de ellos es la falsificación a la que ha sido objeto y también el proceso para su verificación. Sin embargo ha servido mucho como el método más aceptado para la verificación de la identidad de una persona.

La doctrina remonta el origen de la firma manuscrita o autógrafa al Derecho Romano. En Roma no se firmaban los documentos, ni por costumbre, ni tampoco era necesario, pero después se empezó a utilizar creándose la *manufirmatio*, que consistía en una ceremonia en que leído el documento por su autor o el notario se le colocaba desenrollado y extendido sobre la mesa del escribano y luego de pasar la mano abierta sobre el pergamino en actitud de jurar, pero sin hacerlo, se estampaba el nombre,

signo o una o tres cruces (una por cada una de las personas de la santísima trinidad), por el autor o el notario en su nombre, después lo hacían los testigos.

La firma la podemos definir como el nombre, apellido o titulo que se pone al pie de un escrito para acreditar que procede de quien lo escribe para autorizar ahí lo manifestado u obligarse a lo declarado en el documento.[167]

La firma tradicional tiene varias características entre ellas el hecho de que es aceptada legalmente, esto quiere decir que si una persona ha firmado un documento el cual tiene efectos jurídicos, el firmante adquiere entonces tanto los derechos como las obligaciones que del mismo se generen. Además es declarativa, lo que significa la aceptación del contenido del documento por el autor de la firma. Y es probatoria, lo que significa que permite identificar si verdaderamente el autor es quien dice ser.

Esta firma implica dos acciones, en primer lugar la acción de firmar, es decir la acción de otorgar el consentimiento en un determinado documento, la cual un individuo escribe su nombre o rubrica o algún conjunto de caracteres particulares, y no es necesaria ningún tipo de autorización para utilizarla y así tiene la validez legal. En segundo lugar la acción de verificación de la firma, que es un proceso más complicado se realiza de forma visual, comparando la firma con otra que se encuentra en un documento de identificación, y con esto acepta o rechaza la firma, o la verificación por medio de perito.

Es importante hacer notar que la firma comprueba la identidad de una persona, de tal manera que así se sabe quién es la persona que firmó, y que

[167] Cabanellas de Torres, Guillermo. Diccionario Jurídico Elemental, Editorial Heliasta S.R.L, Buenos Aires, 1994. página 115

ésta persona no puede negar responsabilidades que adquiere en un documento firmado. Con la firma manuscrita queda resuelto legalmente el problema de la autenticidad o el de comprobar la identidad de una persona.[168]

3.4.1.1 Elementos de la Firma Autógrafa o Manuscrita.

La firma manuscrita tiene ciertos elementos de los que se desprenden, los elementos formales y los elementos funcionales de la misma:

- ✓ ***Elementos Formales***

Son aquellos elementos materiales de la firma que están relacionados con los procedimientos utilizados para firmar y el grafismo mismo de la firma.[169]

1. La Firma como Signo Personal: la firma está representada por un signo que cada persona elige, ya que debe ser puesta de su puño y letra.

2. El Animus Signando: que se refiere a la intención, a la voluntad que tiene la persona de asumir el contenido del acto o contrato o cualquier otro documento.

- ✓ ***Elementos Funcionales***

Estos son las funciones de la firma, de donde se distingue una doble función:

[168] Ídem. Pagina. 15
[169] Gutiérrez Molina, Fausto Antonio y Miranda Novoa, Carmen Elena. Tesis Universidad Politécnica de El Salvador, "Factibilidad para la Creación de la Ley de Firma Digital a Fin de Garantizar la Seguridad Jurídica, en las Transacciones Electrónicas". Junio 2007, Pág. 68

1. La Función Identificadora: como lo mencionamos la firma desde hace tiempo ha servido para identificar a la persona, asegura la relación jurídica que tienen los contratantes, es en donde se determinan los deberes y derechos que tiene la persona en el acto o contrato celebrado.

2. La Función De Autenticación: la función autenticadora es aquella en que se establece que el autor de un documento ha expresado su consentimiento y el cual se le da la autoría de este documento. Por lo cual este tiene que ser dado en una forma activa por lo que no se acepta un acto por omisión porque la persona debe ser consciente de las consecuencias que va a producir dicho acto.

3.4.2 Firma Digital

Definir la firma digital no es tarea fácil, y más difícil aun cuando no se tiene una noción clara completamente de lo que es, por eso Apol-Lonia Martínez Nadal dice que firma digital es la que se crea en un sistema de criptografía asimétrica o de calve pública basada en el uso de un par de claves asociadas; una clave privada, que se mantiene en secreto y una clave pública libremente accesible para cualquier persona. [170]

Otras definiciones de firma digital las encontramos en Internet, que exponemos a continuación:

"La firma digital está formada por una serie de caracteres de lo más variado –letras, números, signos, etc.- elaborados con un programa

[170] Martínez Nadal, Apol-Lonia. Comercio Electrónico, firma Digital y Autoridades de Certificación. Obra citada. Pág. 42

informático, los cuales, al asociarse a otros datos, también de tipo electrónico permite entre otras cosas, identificar al firmante de los mismos."[171]

"La firma digital es una cadena de caracteres, generados mediante un algoritmo matemático que se obtiene utilizando como variables la clave privada y la huella digital del texto a firmar, de forma que permite asegurar la identidad del firmante y la integridad del mensaje"[172]

"La firma digital puede ser definida como una secuencia de datos electrónicos que se obtienen mediante la aplicación a un mensaje determinado de un algoritmo, o de cifrado asimétrico o de clave pública, y que equivale funcionalmente a la firma autógrafa en orden a la identificación del autor del que procede el mensaje."[173]

"La firma digital es un conjunto de caracteres que se añaden al mensaje que enviamos a través de Internet, con el objeto de proteger la integridad de los datos que se trasmiten, evitando que sean interceptados y falsificados. A través de esta codificación, el receptor del mensaje puede comprobar no solo el origen de los datos que se han remitido, sino su integridad y la identidad de la persona que los envió."[174]

En sí misma es un dato (secuencia de bits) y el peligro radica en que una vez divulgado, cualquiera puede utilizarlo y hacerse pasar por su titular. Para que esto no suceda, en la firma digital se utiliza lo que se denomina "criptografía de clave pública".

[171] www.tuguialegal.com/firmadigital/1.htm
[172] www.iec.csic.es/criptonomicon/seguridad
[173] www.espanol.groups.yahoo.com/groups/
[174] www.html.net/seguridad/varios/firma-certificado

La diferencia que podemos decir de la firma electrónica es que esta es como por ejemplo la firma o el nombre que se utiliza en un correo electrónico común y corriente, en cambio la firma digital es ya la que se tiene después de aplicar la función hash, es decir tiene un proceso para obtenerla en cambio la firma electrónica cada persona la escribe en su Email, como por ejemplo "Con amor, María", o "Atentamente Juan", es decir una firma electrónica, solo sirve para identificar a una persona, pero no sabemos si realmente María o Juan la han escrito, pero con una firma Digital se sabe si realmente fueron ellos quienes la hicieron ya que utiliza algoritmos de encriptación, como lo son las dos claves (pública y privada) y que son totalmente personales.

3.4.2.1 Tipos de Firma Digital

Se pueden distinguir dos tipos de firma digital, en función del formato que se utiliza para crearla: firma digital básica y firma digital avanzada.

- ✓ ***Firma Digital Básica***

Esta firma contiene un conjunto de datos que se recogen de forma electrónica, con los que se identifica formalmente al autor y son incorporados al documento.[175] Entonces con esta clase de firma únicamente se puede autenticar la identidad de una persona, podemos decir que se asemeja cuando una persona usa su documento de identidad para identificarse.

Entonces podemos estar seguros de que la identidad de la persona es la correcta, pero nos queda la duda de que el contenido del documento sea legítimo.

[175] www.ingenieroseninformatica.org/recursos/tutoriales/firmaelectronica/cap4.php

- ✓ ***Firma Digital Avanzada***

Esta firma es la que además de identificar al firmante permite garantizar la integridad del documento. Para ser creada emplea técnicas PKI[176].

Esta firma entonces además de que identifica a la persona también lo vincula de manera única al documento junto a los datos incorporados, ya que es el firmante el único que tiene el control absoluto de las claves, así mismo permite saber si los datos han sido alterados posteriormente.

Otra diferencia entre éstos tipos de firmas, es en cuanto a los efectos jurídicos que producen, ya que el Art. 3 del Real Decreto Ley 14/1999, establece que los datos consignados de forma electrónica, en una firma digital avanzada, tienen el mismo valor jurídico que la firma manuscrita y es admisible como prueba en juicio, es decir, que se le confiere plena eficacia jurídica y probatoria. También la Ley de Simplificación Aduanera, en el articulo 8 inciso tercero establece que para el intercambio de la información, el usuario previamente autorizado, contara con una pareja de llaves y correspondientes entre sí, una pública y una privada, y cuya vinculación constituye la Firma Digital, y que para todos los efectos legales constituye un sustituto de la firma manuscrita. Es decir que en nuestro país la actual firma digital[177] constituye una firma digital avanzada por que le brinda total efecto jurídico y probatorio al hacer la comparación con la firma manuscrita.

[176] Infraestructura de claves públicas (PKI, public key infrastucture): Infraestructura capaz de soportar la gestión de claves públicas para los servicios de autenticación, criptación, integridad, o no repudio. Recomendación UIT-T X.509

[177] Cuando decimos actual firma digital, nos referimos al hecho de que actualmente la firma digital solo es utilizada para las cuestiones aduaneras, y aun no está siendo utilizada para el comercio y para cualquier otro ámbito, por no estar regulada de forma general.

- ✓ ***Firma Digital Reconocida.***

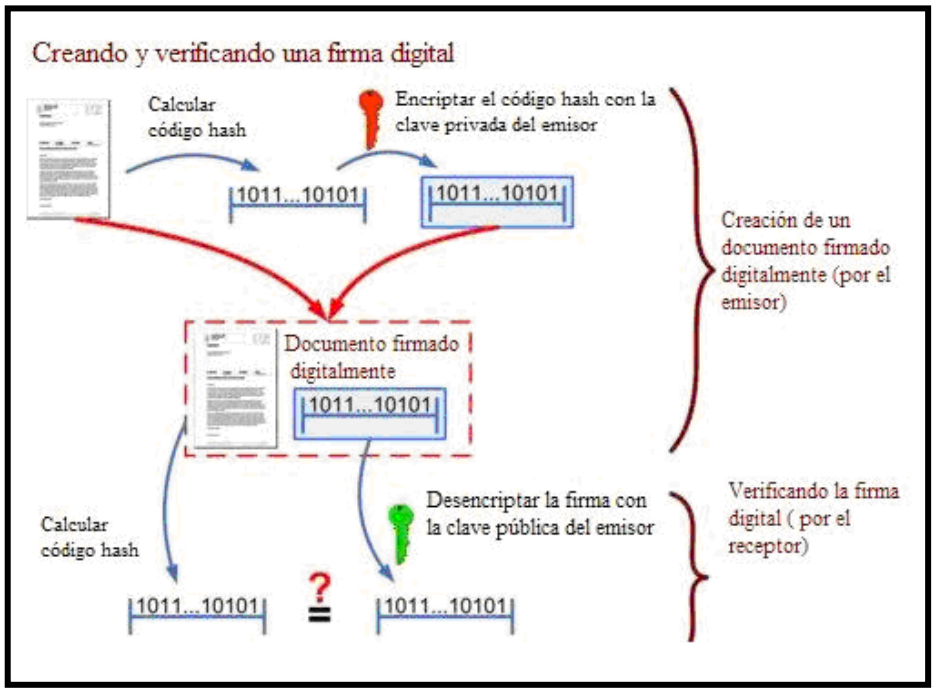
Es la firma digital avanzada ejecutada por un DSCF (Dispositivo Seguro de Creación de Firma), creada por una autoridad de certificación y amparado por un certificado reconocido o de nivel cuatro (ver tema de los tipos de certificados). En ocasiones esta firma se denomina Cualificada, por traducción del término *Qualified*, de la Directiva Europea de Firma Electrónica.

3.4.3 Funcionamiento de la Firma Digital

La firma digital es aquella que se basa en un sistema criptográfico asimétrico el cual está compuesto por dos claves (pública y privada), teniendo en cuenta esto y recapitulando lo visto anteriormente podemos decir que el funcionamiento de la firma digital es cuando al utilizar las claves se aplica una función Hash y con ello un sellamiento, y el resultado de esto es una cifra que puede variar de 128 a 160 bits que es la longitud de oscilación (hoy en día se están haciendo esfuerzo para que el rango de longitud que oscila la clave sea superior a 1024 bits para que así se pueda evitar que pueda descifrarse el mensaje más fácilmente). El cual usando la clave privada del remitente y la clave publica del destinatario se crea este código, el cual solo puede ser verificado por el destinatario del mensaje.

Todo esto usando un software en el que el firmante aplica este algoritmo sobre el texto a firmar, obteniendo un extracto de longitud fija, y absolutamente específico para ese mensaje.

Todo esto es para garantizar la seguridad de la persona a la firma. Esto se puede explicar mejor con el siguiente esquema el cual podemos tomar como base para una explicación en general de dicha firma.



En este cuadro podemos observar que el código hash encripta el mensaje enviado por el emisor, el cual se firma digitalmente y crea los algoritmos matemáticos que solo pueden ser calculados con la clave privada del destinatario, utilizando la clave pública del emisor. Si en el camino ha sido interceptado y modificado el resultado del algoritmo original ha cambiado y este al ser recibido por el receptor y utilizar su clave el resultado de desencriptación no será igual y habrá incongruencia por lo que este se percatara que ha sido alterado y no podrá ser leído.

Ahora bien lo anterior ha sido un esbozo general de cómo funciona una firma digital en un concepto doctrinario, utilizando los estándares de seguridad internacional como la directiva x.509, la w.70 entre otras; pero en El Salvador con respecto al área de aduanas, y siendo la única institución del

estado que se utiliza firma electrónica, tiene su propio funcionamiento para generar un documento firmado digitalmente. Así la dirección de aduanas de nuestro país ha generado una guía para la utilización del software proporcionado a los agentes aduanales y sus auxiliares para la utilización de la firma electrónica, estos utilizan el programa "Firma Electrónica Beta 3.0", así el procedimiento es el siguiente:

1) Colocar su login y password solicitado por el modulo[178]
2) Buscar los documentos no firmados.
3) Elegir el documento que no ha firmado.
4) Se puede como opción del sistema, consultar el detalle de la información, con el documento que se pretende firma.
5) Seleccionar los documentos que se van a firmar, seleccionándolos en el cuadro del programa y sombreándolos.
6) Colocar la contraseña del certificado digital de seguridad, previamente dado por la Dirección General de Aduanas.
7) Presionar la opción de firmar el documento el cual es firmado, por este y enviado al remitente del mismo.

3.4.4 Eficacia Jurídica de la Firma Digital

Como hemos venido diciendo en el desarrollo de este tema, la firma digital tiene los mismos efectos jurídicos que una firma manuscrita, ya que ésta tiene como función dar integridad, autenticidad y, en definitiva, el no rechazo de origen.

[178] Este login y password es dado por la Dirección General de Aduanas a los agentes aduanales que pretenden utilizar este sistema, el cual se les da un acuerdo en el que cumplen los requisitos de la ley y se eles entrega un acuerdo en el que consta este password el cual es personalísimo y solo estos pueden utilizar. Explicación de la Licda. Rubenia Moran encargada del área de atención del usuario de la Dirección General de Aduanas. Ver Cedula de Entrevista en Anexos.

Así en España y basado en las directivas europeas, establecen que la firma electrónica, tendrá respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los designados en papel y será admisible como prueba en juicio. Así también lo contempla el anteproyecto de la Ley de Comunicación y Firma Electrónica en el artículo 17 de dicho anteproyecto, asimismo el artículo 31 del Código Aduanero Uniforme Centroamericano (CAUCA), establece el principio de equivalencia funcional, pero para que surta efectos o sea jurídicamente eficaz debe cumplir con ciertos requisitos, como lo son:[179]

1. Debe tratarse de una firma electrónica avanzada, es decir. Aquella que cumple los requisitos que la Ley establece y las normas y directivas internacionales establecen.

2. Esta firma avanzada debe ser reconocida como un certificado reconocido.

3. Debe ser producido por dispositivos seguros de creación.

Así el tratamiento por medios informáticos permite la sustitución del soporte papel en otro diferente como lo es el soporte electrónico.

Al hablar de este tema, tenemos que hacer un recuento de lo que hemos estudiado, y hablar un poco del documento electrónico, el cual hemos visto que siendo un documento al igual que uno en papel, el documento electrónico se concibe como un medio de expresión de la voluntad con efectos de creación, modificación o extinción de derechos y obligaciones, por

[179] Martínez Nadal, Apol-Lonia. Comercio Electrónico, Firma Digital y Autoridades de Certificación. Obra citada. Página 332

lo que la firma digital hace eficaz este documento electrónico (contrato electrónico) y podrá ser admitido en un proceso judicial sin mayores restricciones, es mas el nuevo Código de Procedimientos Civiles y Mercantiles, en el artículo 489, establece la utilización de otros medios que no sea el escrito, por lo que abre la posibilidad del documento electrónico y la firma electrónica.

3.4.5 Firma Digital Certificada por Ciber Notarios.

Antes de profundizarnos en el siguiente tema es necesario recordar que se entiende por certificación de firma para poder dar una clara idea de lo que es la certificación de firma digital que realizara un Ciber Notario. Así se entiende certificación de firma electrónica a aquella realizada por un oficial publico notarial competente, ya sea que se asienta en el protocolo o no, de un requerimiento capaz para ese acto y de su conocimiento o que ha justificado debidamente su identificación y suscribe o estampar su firma o impresión digital, en su presencia del escribano, en el documento a certificar. La anterior definición es la certificación de firma que un notario realiza de un documento privado.

Ahora bien ¿Cuál es la importancia de la intervención del notario para que certifique las firmas digitales, si la infraestructura del sistema asimétrico permite asegurar el documento y que fue firmado con la respectiva clave privada quien figura como emisor? Es necesario, pues así como la firma ológrafa de las partes en un contrato no es suficiente para darle certeza jurídica y validez a un instrumento privado, ya que carece de autenticidad; por lo anterior para que todo documento pueda ser suficientemente eficaz jurídicamente para configurar una pretensión judicial debe de reunir los

requisitos que la ley determina, y una de ellas es que debe de ser certificada por notario en el ejercicio de su función notarial[180]. Así lo establecen los artículos Código de Procedimiento Civiles 254, 255 y 256 en el que se establece que todo documento para que pueda dar plena fe deben ser documentos públicos y auténticos, y en el caso de los documentos privados el artículo 1573 del Código Civil establece que solo tendrá el valor de escritura pública respecto de los hechos que se reputan haberlo suscrito y de las personas que se han transferido las obligaciones y derechos y todo esto en la presencia de un notario o funcionario que ejerza la función notarial así. Con respecto a la firma digital puesta en documento electrónico, rige exactamente el mismo principio; lo que cambia es el soporte[181].

Según Julia Siri García, "la autenticidad, tomada en su doble aspecto de autoría cierta y de fidelidad de la representación del acto, incluida su data correspondiente, tradicionalmente queda asegurada por la actuación notarial que registra en instrumento publico la presencia, otorgamiento y suscripción que ante él se llevan a cabo, todo lo cual refleja en papel".[182]

Por lo que en el caso de una firma digital autenticada ante notario, dicha firma digital se realizan sobre el documento electrónico en presencia de un fedatario público o funcionario especialmente cualificado.

[180] El artículo 32 de la ley de notariado establece los requisitos que debe de tener una escritura matriz y en su numeral doce nos dice que todo escritura matriz debe de ser firmado por las partes y por el mismo notario por lo que es un requisito sine quano, para que se tenga eficacia jurídica ese instrumento. El cual dice literalmente:
Art. 32.- La escritura matriz deberá reunir los requisitos siguientes:
12º- Que leído el instrumento, sea firmado por los otorgantes, por los testigos e intérpretes si los hubiere y por el Notario. Si alguno de los otorgantes no supiere o no pudiere firmar se expresará la causa de esto último y dejará la impresión digital del pulgar de la mano derecha o, en su defecto, de cualquier otro dedo que especificará el Notario o si esto no fuere posible se hará constar así y en todo caso, firmará además a su ruego, otra persona mayor de dieciocho años o uno de los testigos; pudiendo una sola persona o testigo firmar por varios otorgantes que se encontraren en alguno de dichos casos;(2)

[181] http://www.cfna.org.ar/cfna/publi/index.php?modulo=escribano&opt=verdoctrina&id=71

[182] http://www.cfna.org.ar/cfna/publi/index.php?modulo=escribano&opt=verdoctrina&id=71

En el caso de la firma digital autenticada por notario, estamos ante un supuesto donde el firmante, suscriptor del certificado asociado a su firma va a firma digitalmente el documento electrónico en presencia del fedatario (por así decirlo, ya que un notario electrónico por estar en presencia de un contrato a distancia se entiende que las partes no se encuentran presentes físicamente, pero si mediante un ordenador el cual envían toda la información para que este redacte dicho documento), previa comprobación de su identidad personal y de la validez de su clave pública.

CAPITULO IV

MARCO NORMATIVO DE LA CONTRATACIÓN ELECTRÓNICA, FIRMA DIGITAL Y CIBER NOTARIO.

SUMARIO: *Introducción. 4.1 Legislación Nacional. 4.1.1 Constitución de El Salvador de 1983. 4.1.2 Código de Comercio. 4.1.3 Ley de Bancos. 4.1.4 Ley de Simplificación Aduanera. 4.1.5 Código Tributario y Reglamento de Aplicación del Código Tributario. 4.1.6 Tratado de Libre Comercio República Dominicana – Centroamérica – Estados Unidos. (CAFTA). 4.2 Tratados Internacionales Referentes al Comercio Electrónico y a la Firma Electrónica. 4.2.1 Código Aduanero Uniforme Centroamericano (CAUCA). 4.2.2 Reglamento del Código Aduanero Uniforme Centroamericano (RECAUCA). 4.2.3 Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL por sus siglas en inglés). 4.2.4 Ley Modelo de Firma Electrónica de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. 4.2.5 La Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías. Viena 11 de abril de 1980. 4.3 Legislación Comparada Referentes al Comercio Electrónico, Firma Electrónica y Ciber Notario. 4.3.1 Real Decreto-Ley 14/1999 de 17 de Septiembre, Sobre Firma Electrónica. 4.3.2 Instrucción de 19 de Octubre de 2000, de la Dirección General de los Registros y del Notariado, sobre el Uso de la Firma Electrónica de los Fedatarios Públicos. 4.3.3 Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas. (Guatemala). 4.3.4 Ley de Certificados, Firmas Digitales y Documentos Electrónicos. (Costa Rica). 4.4 Proyecto Final de la Ley de Comunicaciones y Firma Electrónica en El Salvador.*

Introducción

En el presente capitulo se analizará la legislación tanto nacional como internacional referida a la Contratación Electrónica, la Firma Electrónica y el Ciber Notario, debemos aclarar que legislación de Ciber Notario únicamente se encuentra legislación comparada ya que en nuestro país no existe ninguna legislación del tema, tampoco existe una legislación acerca de comercio electrónico, únicamente existen disposiciones dispersas y leyes que solo regulan una parte de este fenómeno pero no como comercio sino como materia aduanera o tributaria, también existe un proyecto de Ley de Comunicación y Firma Electrónica pero que aun está siendo estudiado por el Órgano Ejecutivo para decidir si se envía a la Asamblea Legislativa para su estudio y aprobación como ley de la República.

4.1 Legislación Nacional

En nuestro país existe un ordenamiento jurídico sumamente limitado cuando se refiere a regular el comercio electrónico, y solo se encuentran ciertas disposiciones dispersas que podrían en ciertos casos ser aplicables a esta contratación o que hacen una referencia mínima, generando entonces un gran problema ya que la contratación avanza y cada vez más se adentra en nuestro país.

Este tema se dirige entonces, a analizar la normativa que existe actualmente en el país y que eso puede ser aplicable al comercio electrónico, la contratación electrónica y firma electrónica, partiendo claro, de la norma fundamental que es la Constitución de la República de 1983, hasta abarcar toda la legislación secundaria, los tratados internacionales y la legislación de otros países que regulan la materia.

4.1.1 Constitución de El Salvador de 1983

En este cuerpo legal, que constituye la base de todas las leyes y ordenamientos jurídicos de nuestro país, nos establece que el Estado de El Salvador está organizado para la consecución de la seguridad jurídica, por lo que la seguridad jurídica se tiene como un principio y garantía que goza toda persona y que el estado está obligado a cumplir para la satisfacción de la misma población, esto se encuentra en el artículo primero del mencionado cuerpo legal.

Así como en el artículo 2 se establece que toda persona tiene derecho a la seguridad jurídica, seguridad jurídica que se encuentra amenazada por el comercio electrónico, por la falta de confiabilidad de los documentos que en él se manejan, por lo que el notario como delegado del Estado y como el encargado de darle fe pública a todos los contratos y demás documentos que las personas le lleven, se hace indispensable que intervenga en la contratación electrónica para darle confiabilidad y seguridad jurídica a esos documentos para la protección de los derechos de las personas.

En el artículo 23, de la misma se establece la libre contratación, en la cual cualquier persona basada en la autonomía de la voluntad puede contratar con quien quiera, lo que quiera y adonde quiera siempre y cuando sea permitido por las leyes, tanto nacionales como extranjeras. De esto podemos decir que la Corte Suprema de Justicia ha dictado jurisprudencia:

"Sobre el contenido y los alcances de la libre contratación, la SC ha señalado que "los aspectos que ofrece el derecho a la libre contratación son: (i) el derecho a decidir si se quiere o no contratar, esto es, el derecho a decidir la celebración o no celebración de un contrato; (ii) el derecho a elegir con quién se quiere contratar; y (iii) el derecho a determinar el contenido del contrato, es decir la forma y modo en que quedarán consignados los derechos y obligaciones de las partes. Ahora, esta libertad, no obstante ser una actividad humana –y en cuanto humana, privada, es decir, librada a la iniciativa de los particulares, puede estar limitada (regulada) por razones de interés público y de distintos modos. Así, el Estado puede eventualmente alterar ex post facto los efectos de los contratos celebrados con anterioridad al pronunciamiento de una norma; puede establecer de forma obligatoria el contenido de los contratos (derechos y obligaciones), como sucede comúnmente con los servicios públicos, seguros, etc.; y puede, finalmente, imponer razonablemente a determinados individuos la celebración o no de un contrato, aún en contra de la voluntad de los interesados" (Sentencia de 13-VIII-2002, Inc. 15-99, Considerando VI 3)".

Podemos observar que constitucionalmente y vía jurisprudencialmente tenemos la facultad de elegir libremente con quien contratar y con quien hacerlo y en qué modo hacerlo, por lo que perfectamente una persona puede

elegir contratar electrónicamente y ser completamente legal, pero como expresa la Doctora Yesenia Granillo de Tobar, en la contratación electrónica los contratos que requieran de solemnidades especiales seguirán aplicando esas solemnidades especiales, ahí se encuentra el problema de la contratación electrónica que van a existir contratos en los que se requerirá la intervención de un notario (compraventa de bienes inmuebles, por ejemplo) y por no haber regulación al respecto no podrán ser ejecutados y no tendrán la suficiente seguridad jurídica que todo contrato requiere.

Podemos ver que en nuestra Constitución existen disposiciones en las que se protege la libertad y la seguridad jurídica, y por lo tanto la contratación privada, y por ende la contratación electrónica se encuentran garantizadas por el ordenamiento jurídico salvadoreño, que protege los contratos entre particulares contra el intervencionismo estatal y particular, asegurando y fomentando el ejercicio de la autonomía privada en la contratación. Pero con todo esto aun se necesita de otros cuerpos legales para fomentar totalmente el comercio electrónico y por su misma importancia que implica en el país, al abrir las puertas a nuevas oportunidades para el desarrollo económico más eficiente, tanto del comercio de sus productos o servicios en el mercado local, regional e internacional, se requiere que se regule y se brinde seguridad jurídica.

4.1.2 Código de Comercio

Ya que el comercio electrónico es un conjunto de transacciones de carácter eminentemente comercial, las relaciones que de él deriven deberán regirse por la normativa del código de comercio, ya que en las transacciones se encuentran presentes las figuras de comerciante, actos de comercio,

consumidor, empresa y demás elementos de donde podamos deducir que estamos en presencia de un acto de comercio, por lo que le serán aplicables estas disposiciones, sin dejar de lado la necesidad de una legislación específica de este tipo de comercio.

De tal forma que pueden señalarse los artículos del Código de Comercio, como lo son los artículos 1, 2, 3 y 5 que son los que expresamente regulan el objeto, los sujetos y los actos propios del comercio.

Así mismo este Código presenta indicios de la adecuación de la normativa mercantil a la contratación electrónica al hacer referencia el artículo 966 del momento en que se da el perfeccionamiento de la oferta en los contratos por correspondencia, figura que es típica de los contratos celebrados entre ausentes, de los que la contratación electrónica por Internet forma parte.

4.1.3 Ley de Bancos.

Esta ley que tiene por objeto la regulación de la función de intermediación financiera y las otras operaciones realizadas por los bancos, con lo que se propicia que estas instituciones brinden a la población un servicio transparente, que sea confiable y ágil, que contribuya al desarrollo del país, establece en su capítulo II, denominado "Operaciones Pasivas", en el artículo 56 denominado "Términos de Referencia Aplicables", en el literal "l"[183] que los bancos podrán celebrar operaciones y prestar servicios con el

[183] "Art. 56 Para la elaboración de las normas a que se refiere el artículo precedente los bancos tomarán en cuenta:…l) Que los bancos podrán celebrar operaciones y prestar servicios con el público mediante el uso de equipos y sistemas automatizados, estableciendo los contratos respectivos las bases para determinar las operaciones y servicios cuya prestación se pacte; los medios de identificación del usuario y las responsabilidades

público mediante el uso de equipos y sistemas automatizados, pudiendo establecer los contratos respectivos; es decir que el banco podrá utilizar la contratación electrónica, para el ejercicio de sus funciones, también podrá establecer "los medios de identificación del usuario y las responsabilidades correspondientes a su uso", es decir que se podrá utilizar la firma electrónica para el efecto de identificar al usuario otorgante del contrato electrónico, el uso de esta firma según este mismo literal en su inciso segundo[184] que producirá los mismos efectos que la firma autográfica, por lo que en ese caso sería factible la intervención de un notario certificador de la firma electrónica de esa persona así como del banco, para que ese contrato goce de seguridad jurídica.

Esta disposición es la única que en toda la legislación salvadoreña otorga la misma validez de la firma manuscrita a la firma digital, y a la vez permite la implementación de medios electrónicos en transacciones bancarias.

También en el capítulo III, de la misma ley que se denomina "Operaciones Activas", en el artículo 60 inciso primero[185] establece que las

---

correspondientes a su uso; y los medios por los que se hagan y obligaciones inherentes a las operaciones y servicios que se trate. (Ley de Bancos, aprobada el 10 de sep. de 1999, sancionada el 27 de sep. de 1999 y publicada en el Diario Oficial No. 181, Tomo 334, del 30 de sep. de 1999.)

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

[185] Art. 60 inc. 1º, "De los Sistemas de Pagos y las Transacciones Electrónicas", también se establece: "Las operaciones activas y pasivas que efectúen los bandos y otras instituciones a través de las cuentas que se manejan en el Banco Central, podrán realizarse mediante el intercambio electrónico de datos. Para tal efecto, tendrá validez probatoria los registros o bitácoras contenidas en los sistemas informáticos, las impresiones que reflejan las transacciones efectuadas por los mismos registros de firmas digitales o de números de identificación personal de los participantes autorizados en dichos sistemas. Las certificaciones extendidas, por el funcionario autorizado por

operaciones activas y pasivas que efectúen los bancos y otras instituciones podrán realizarse mediante el intercambio electrónico de datos, para tal efecto tendrán validez probatoria los registros o bitácoras de los sistemas informáticos así como las impresiones que reflejan las transacciones efectuadas por los mismos registros de firmas digitales o de números de identificación personal de los participantes de dichos sistemas. Por lo que este artículo establece los registros que se llevarán de firmas digitales, aunque en realidad se refiere a firmas electrónicas, confundiéndolas y por lo tanto, regulando protección solamente para las firmas y no las digitales.

4.1.4 Ley de Simplificación Aduanera

Esta ley dispone como su 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.

Constituye la base jurídica para que funcione el sistema de Teledespacho, que consiste en intercambiar información, particularmente de Declaración de Mercancías para con la Dirección General de la Renta de Aduanas, expresamente lo manifiesta en el Art. 6 al establecer: “El despacho de las mercancías podrá ser solicitado por procedimientos informáticos, mediante el intercambio de información por vía electrónica, a través del sistema conocido como Teledespacho. Entendiendo como Teledespacho el conjunto sistematizado de elementos tecnológicos de carácter informático y de comunicaciones que permiten dentro de un marco de mutuas

---

el Banco Central para llevar registros y controles de lo anteriormente referido, tendrán fuerza ejecutiva contra la parte que incumplió. Las instrucciones que dicten los bancos al Banco Central, serán de carácter irrevocable”.

responsabilidades, y mediante los procedimientos autorizados, el intercambio por vía electrónica de información de trascendencia tributaria entre la dirección general, importadores, exportadores y los operadores e instituciones contraloras del comercio exterior en general".

Podemos considerar que esto constituye el inicio de la introducción de nuevas tecnologías en nuestro medio que viene a facilitar y desarrollar las actividades que implican participación tanto de la administración pública como del sector privado.

Así mismo en el artículo 8 establece que ha 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 certificaciones de dicha información llamadas en adelante entidades certificadoras. Cuya autorización para operar, como la fiscalización y la facultad sancionatoria será ejercida por el Ministerio de Hacienda, mientras no se dicte una ley que regule el comercio electrónico. Las funciones del MINHAC[186] (importantes para nuestro tema), son: a) Autorizar la operación de las entidades certificadoras en el territorio nacional; b) Velar por el funcionamiento y la eficiente prestación del servicio por parte de las entidades certificadoras;… h) Emitir certificados en relación con las firmas digitales de las entidades certificadoras;

También establece que estas entidades certificadoras deberán ser personas jurídicas capacitadas tecnológicamente para prestar servicios de generación y certificación de firma digital, además que para la ejecución de

[186] Ministerio de Hacienda

las distintas actuaciones que conforman el sistema de Teledespacho y para el intercambio de la información general, cada usuario autorizado, contará con una pareja de claves o llaves únicas y correspondientes entre sí, 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 llaves públicas. La vinculación de ambas llaves o clases constituyen la firma digital o electrónica, que para todos 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.

Las entidades certificadoras 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. El certificado emitido por una entidad certificadora deberá ser reconocido por las demás entidades certificadoras autorizadas.

Por lo que esta ley es la primera en nuestro medio en que verdaderamente regula la firma digital.

4.1.5 Código Tributario y Reglamento de Aplicación del Código Tributario

En el Código Tributario también se menciona la utilización de medio electrónicos para presentar las declaraciones tributarias y lo menciona en el articulo 92 inciso segundo, que literalmente dice: "*La Administración Tributaria podrá autorizar mediante resolución la presentación de declaraciones mediante redes de comunicación electrónicas tales como Internet, medios magnéticos u otros medios de transmisión de datos como correo electrónico, siempre que éstas posean todos los requisitos contenidos en los formularios proporcionados por la Administración Tributaria para tal fin. El Reglamento de este Código establecerá las especificaciones de seguridad que deberán cumplir para garantizar la exactitud de la información contenida en ellas."* Esto nos demuestra que en nuestro país ya se está utilizando casi al cien por ciento los medios electrónicos para realizar varios actos jurídicos, como por ejemplo en la presentación de la declaración tributaria, no solo se ocupa en el comercio o en cuestiones aduaneras, ahora es utilizado para el pago de impuestos.

Este mismo artículo se relaciona con el artículo 35 del Reglamento de Aplicación del Código Tributario, que literalmente expresa:

*"**Presentación de Declaraciones Mediante Redes de Comunicación Electrónicos"***
***Articulo 35.-** La Administración Tributaria para efectos de garantizar la exactitud de la información contenida en las declaraciones tributarias presentadas por medios electrónicos tomara en cuenta los datos necesarios para las transferencias electrónicas, tales como: encriptado de los procesos, firma digital o electrónica, facilidades para cambios de clave por el sujeto pasivo autorizado y recibo de verificación electrónico proporcionado por la Administración como constancia de recibido."*

Con este artículo podemos ver que ya se introduce los conceptos de encriptado y firma digital o electrónica al ámbito tributario, evidenciando al igual que el anterior artículo, que no solo en el ámbito aduanal o el ámbito comercial intervienen los medios electrónicos y sus instrumentos, por lo que ya se hace necesaria una legislación más general de la firma digital o electrónica.

4.1.6 Tratado de Libre Comercio República Dominicana – Centroamérica – Estados Unidos. (CAFTA).

El Salvador fue el primer Estado en ratificar el CAFTA, que se llevo a cabo en la madrugada del 17 de diciembre de 2004 en el Salón Azul de la Asamblea Legislativa.

Tras su ratificación, se realizó el respectivo depósito en la Organización de Estados Americanos el 28 de febrero de 2006.

Este tratado tiene como objetivos el estimular la expansión y diversificación del comercio entre las partes, eliminar los obstáculos al comercio y facilitar la circulación transfronteriza de mercancías y servicios entre las partes, entre otros. Esto se establece en el artículo 1.2 del mencionado tratado.

En este tratado se regula el comercio electrónico en el capitulo catorce del mismo, en donde en los artículos del 14.1 al 14.6, se establece en primer lugar el reconocimiento de las partes del crecimiento económico y la oportunidad que el comercio electrónico genera para todos los países y la importancia de evitar los obstáculos para su utilización y desarrollo.

Se refiere también, a los productos digitales (artículo 14.3), en donde establece que ninguna parte puede imponer aranceles aduaneros, tarifas u otras cargas relacionadas con la importación o exportación de productos digitales por transmisión electrónica, y la forma en la que cada parte determinara los aranceles aduaneros aplicables.

Se menciona también, definiciones de medio electrónico, medio portador, puntos digitales, transmisión electrónica o transmitida electrónicamente.

4.2 Tratados Internacionales Referentes al Comercio Electrónico y a la Firma Electrónica.

En el presente tema se analizarán los tratados internacionales que han sido suscritos con el fin de regular el comercio electrónico, a nivel de Centroamérica o mundialmente, algunos de ellos no han sido ratificados por El Salvador como es el caso de las leyes modelo de UNCITRAL, pero que a nivel internacional son adoptados y utilizados en la contratación que se realiza a través de medios electrónicos.

4.2.1 Código Aduanero Uniforme Centroamericano (CAUCA)

El Código Aduanero Uniforme Centroamericano conocido como (CAUCA), el cual tiene como objetivo “Establecer la legislación aduanera básica de los Estados Parte conforme los requerimientos del Mercado Común Centroamericano y de los instrumentos regionales de la integración,

en particular con el Convenio sobre el Régimen Arancelario y Aduanero Centroamericano."[187].

El CAUCA es el marco legal centroamericano el cual establece criterios uniformes para el intercambio de mercadería en las fronteras centroamericanas, lo más importante que podemos decir en este punto es que el CAUCA reconoce los sistemas informáticos en cuanto a su uso en el Capitulo Tres, nos desarrolla una seria de artículos los cuales reconocen el uso de tecnologías, para el control de mercaderías en la frontera, el control de los transportistas centroamericanos entre otras funciones, y nos da una idea más desarrollada de la firma electrónica, con respecto a la Ley de Simplificación Aduanera esta ultima complementa lo establecido en el CAUCA ya que como sabemos en el Sistema Constitucional Salvadoreño en la jerarquías de las leyes tenemos a la Constitución como base y principio del ordenamiento jurídico salvadoreño y los tratados internacionales en igual rango constitucional que una ley secundaria, pero que en entrar contradicción el tratado y la ley predomina el tratado internacional. Con este orden de ideas desarrollaremos aquellos artículos que nos hablan de la firma digital, como base legal que en el país existe legislación aislada sobre a la firma digital y su posible aplicación ya no solo en aspectos de Derecho Aduanal sino que en otras áreas del derecho y en especial con respecto a los cibernotarios. Así el artículo 31 nos establece:

*"**Artículo 31. Medios equivalentes a la firma autógrafa***

Las firmas electrónicas o digitales, los códigos, claves de acceso confidenciales o de seguridad equivalen, para todos los efectos legales, a la firma autógrafa de los funcionarios y empleados aduaneros, auxiliares, declarantes y demás personas autorizadas por el Servicio Aduanero."

[187] Código Aduanero Uniforme Centroamericano (CAUCA), articulo 1.

El artículo anterior nos confirma que entre una firma autógrafa y una firma digital lo único que cambia es el soporte el cual se utiliza. Este artículo está muy relacionado al principio de equivalencia funcional. Es de notar que el artículo 31 no se limita con lo que es firma digital, sino que incluye otros dispositivos que pueden ayudar a dar esta seguridad.

Otro artículo relacionado con este tema es el artículo 32 el dice literalmente:

"Artículo 32. Firma electrónica o digital certificada

Los Servicios Aduaneros establecerán el uso de la firma electrónica o digital para verificar la integridad del documento electrónico transmitido, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico.

Una firma electrónica o digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado ante el Servicio Aduanero u organismo administrador y supervisor del sistema de certificación del Estado Parte."

Por lo que en este articulo podemos ver las funciones que la ley le da a la firma electrónica este tema ha sido tocado en capítulos anteriores, lo más importante a destacar en este artículo es que la firma digital es el único medio electrónico que es reconocido no solo en El Salvador sino que en otras partes del mundo como el único medio eficaz para confirmar la autoría de un documento electrónico. Por lo que el CAUCA es el primer instrumento internacional (a nivel centroamericano) el cual el Estado de El Salvador reconoce la Firma Digital Avanzada y es referencia para que se pueda crear otras legislaciones para regular la firma electrónica en otros rubros de la vida nacional y que se necesite tal regulación.

4.2.2 Reglamento del Código Aduanero Uniforme Centroamericano (RECAUCA)

Reglamento del Código Aduanero Uniforme Centroamericano (RECAUCA), es la herramienta que desarrolla el Código Aduanero Uniforme Centroamericano en el cual en sus artículos 175 al 185 desarrolla la firma digital, los certificados y certificadores de claves, entre otras cosas. El RECAUCA, como reglamento de ejecución del CAUCA, es una guía que nos ayudara a definir aspectos que por su complejidad son necesarios desarrollarlos en reglamentos, y directivas administrativas. Siendo la ley solo una guía que pone la base y los principios generales en los cuales descansarán sus reglamentos. Así el artículo 175 del RECAUCA nos establece los certificados digitales y la firma electrónica los que son emisión, suspensión, revocación y expiración del certificado son regulados por un ente internacional como lo es la Comisión Centroamericana de Certificados Digitales, el cual pude ser un organismo centroamericano que nos puede servir como un marco de referencia que para que en un futuro no muy lejano exista un ente parecido a nivel centroamericano y que nos ayude a controlar los certificados de cada país y dar mayor seguridad jurídica a las transacciones electrónicas. El artículo 176 y 177 nos establecen que se presumirá de derecho la autoría de una firma digital a la persona registrada y que utilizando su clave privada firmen un documento electrónico así como también el principio de equivalencia funcional que equipara al igual que la ley la firma autógrafa con la firma digital. Los siguientes artículos de la ley siguen desarrollando lo que es la firma digital, y los requisitos que necesita un certificado para quien se tenga por autentico.

Así como también podemos decir que existe mucho en legislación aduanera que ha ayudado a el tema de contratación electrónica y firma digital, las cuales sus experiencias y aportaciones con conceptos y legislación, nos da un panorama más claro de que en el país, si se puede aplicar una normativa de contratación electrónica así como también se pude llevar a cabo en otras áreas del derecho que se necesita aplicar como lo es en Derecho Penal y Procesal Penal con los delitos informáticos, en el área de derecho administrativo con los Gobiernos Cibernéticos, y en materia de contratación y económicas como lo es la contratación electrónica y el cibernotario.

4.2.3 Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL por sus siglas en inglés).

Esta ley fue aprobada por el plenario de esta comisión en su 29º período de sesiones, celebrado en New York del 28 de mayo al 14 de junio de 1996 y la Asamblea General de la ONU la aprobó mediante resolución 51/162 el 16 de diciembre de 1996.

Esta ley constituye un modelo de referencia para fomentar la armonización y unificación progresivas del derecho mercantil internacional, garantiza la seguridad jurídica y provee una legislación que facilite el uso del comercio electrónico en Estados con sistemas jurídicos diferentes. Por lo que la Ley modelo es apenas una "Ley marco" que habrá de reglamentarse, si así lo desea el Estado que incorpora, a través de un reglamento técnico.

A su vez propicia el reconocimiento jurídico de los documentos electrónicos estableciendo estándares mínimos de requisitos de forma y establece definiciones referidas al proceso de comunicación de “mensajes de datos”.

Tiene como finalidad la de ofrecer al legislador nacional un conjunto de reglas aceptables en el ámbito internacional, que le permitan eliminar ciertos obstáculos jurídicos, todo para consolidar un marco jurídico que permita el desarrollo del Comercio Electrónico. Es decir que los Estados pueden utilizarla para remediar inconvenientes que puedan surgir por marcos legales internos que sean inadecuados para el desarrollo de la contratación electrónica y en general del comercio electrónico.

La Ley Modelo tiene como objetivo, ser un instrumento internacional que sirva para interpretar ciertos convenios y otros instrumentos internacionales existentes, que impongan de hecho algunos obstáculos al empleo del Comercio Electrónico. En el supuesto que se adoptase la Ley Modelo como regla de interpretación, los Estados partes en esos instrumentos internacionales, dispondrían de un medio para reconocer la validez del Comercio Electrónico, sin necesidad de tener que negociar un protocolo para cada uno de esos instrumentos internacionales en particular.

La CNUDMI[188] busca darle validez a los documentos emitidos por medios electrónicos. Por lo tanto, desarrolla el criterio del "equivalente funcional" que consiste en darle a la documentación consignada por medios electrónicos un grado de seguridad equivalente al del papel, siempre y cuando se sigan ciertos requisitos técnicos y jurídicos.

[188] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.

Dentro de los artículo que esta ley contempla sobre comercio electrónico están los artículos 1 que nos establece su campo de aplicación, el artículo 2 que nos da las definiciones generales de lo que son mensajes de datos, intermediarios y otros, todo estos conceptos jurídico-técnicos son hoy en día la base de las definiciones de ley de muchos países suscriptores, así el ejemplo de El Salvador el anteproyecto de ley de Comunicaciones y Firma Electrónica, nos estable el marco y los conceptos que se entenderá dentro de la ley como una guía la cual se debe de seguir.

4.2.4 Ley Modelo de Firma Electrónica de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.

Aprobados por el Grupo de Trabajo de la Comisión de las Naciones Unidas sobre Comercio Electrónico en su 36º período de sesiones, celebrado del 14 al 25 de febrero de 2000 en Nueva York.

La Ley Modelo en comento, es una propuesta a los Estados para que incorporen a su derecho interno, algunas disposiciones relacionadas con estos mecanismos de seguridad tecnológica, teniendo en cuenta sus limitaciones, procedimientos y las condiciones propias de su ordenamiento jurídico. Aborda lineamientos relacionados a las técnicas denominadas firmas electrónicas y de la manera de proporcionarles a estas equivalentes funcionales de las firmas manuscritas y de otros tipos de mecanismos de autenticación empleados en el soporte de papel; así como también pautas referidas a los servicios de certificación digital, fijando criterios para evaluar la conducta de las partes involucradas, es decir, el firmante, el tercero que confía en el certificado y el prestador de servicios de certificación.

Esta al igual que La ley Modelo de comercio electrónico es una ley marco que trata de unificar los criterios de todas las naciones que integran o no las Organizaciones de las Naciones Unidas la cual en su articulado en referencia a la firma digital y comercio electrónico, y así tratar que existan menos confusiones a la hora de imponer un criterio o solucionar una litis a nivel internacional. Así los artículos que podemos citar para efectos de nuestro trabajo de investigación son: el artículo 1[189], la Comisión redactora de este instrumento estableció este articulo en base a que no restringe a los estados suscriptores o que deseen aplicar este ley marco con respecto a la protección de los consumidores y entorpecer las relaciones comerciales internacionales que tiene cada país es su régimen interno. Por lo que trata de que cada estado amplíe los derechos y las herramientas tecnológicas, así como no poder restringirlas en base a esta ley marco. Asimismo el artículo 3[190], que establece el principio de la igualdad de tratamiento de las tecnologías para la firma, este principio es la base del principio de neutralidad tecnología y equivalencia funcional que hemos venido desarrollando a lo largo de todo el trabajo y en la cual se equipara a la firma autógrafa con la firma digital en cuanto a los efectos jurídicos que produce esta. Así también lo contempla nuestra legislación en la Ley de Simplificación Aduanera en el artículo 8 inciso 3 de la ley que hace esta equiparación así como también lo confirma el CAUCA y RECAUCA las cuales son leyes de la República.

[189] **Artículo 1. Ámbito de aplicación**
El presente Régimen será aplicable en todos los casos en que se utilicen firmas electrónicas en el contexto* de actividades comerciales**. El presente Régimen no derogará ninguna norma jurídica destinada a la protección del consumidor.

[190] **Artículo 3. Igualdad de tratamiento de las tecnologías para la firma**
Ninguna de las presentes disposiciones, con la excepción del artículo 5, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla los requisitos enunciados en el párrafo 1) del artículo 6 o que cumpla de otro modo los requisitos del derecho aplicable.

En conclusión podemos decir que este marco jurídico internacional es importante para efectos de nuestro trabajo ya que el Cibernotario para poder dar fe pública de una transacción electrónica debe de firma los documentos que se le presenta y para esto la única firma en el mundo informático que reúne los requisitos de ser lo suficientemente segura y es la firma digital, por lo que debemos decir que el desarrollo de la firma digital y el cibernotario son dependientes en cuanto a que para que exista notario se necesita una ley de firma electrónica, para que este puede actuar plenamente.

4.2.5 La Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías. Viena 11 de abril de 1980

La Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías fue concertada el 11 de Abril de 1980 por una conferencia diplomática universal convocada por la Asamblea General de las Naciones Unidas y ratificada por la República de El Salvador el 18 de noviembre de 1999.

Esta Convención constituye una reglamentación de Compraventa Internacional que supera a la Convención de la Haya, pues pretende regular el contrato como un todo independientemente de cualquier legislación nacional. El juez no tiene que determinar la ley competente que rige el contrato, pues la Convención se basta en sí misma

Esta convención se aplicara a los contratos de compraventa de mercaderías entre partes que tengan sus establecimientos en Estados diferentes, cuando estos Estados sean Estados contratantes, y cuando las

normas de derecho internacional privado prevean la aplicación de la Ley de un Estado contratante.

4.3 Legislación Comparada Referentes al Comercio Electrónico, Firma Electrónica y Ciber Notario.

Ahora que se han analizado los tratados internacionales que se relacionan con el comercio electrónico y la firma electrónica, vamos a analizar la legislación que otros países como España, Costa Rica, Guatemala, Estados Unidos, que ya cuentan con la legislación que regula la contratación electrónica, y específicamente la firma electrónica.

4.3.1 Real Decreto-Ley 14/1999 de 17 de Septiembre, Sobre Firma Electrónica.

Fue creada en sesión del Consejo de Ministros de Telecomunicaciones de la Unión Europea, celebrada el 22 de abril de 1999[191], en el cual se ha informado favorablemente la adopción de una posición en común, en cuanto a firma electrónica se refiere. Así podemos decir que el primer capítulo de la Ley establecen los principios generales en los cuales se aplicara dicha normativa, así el artículo 1 nos establece el ámbito de aplicación, el artículo 2 los conceptos, el artículo 3 los efectos jurídicos de la firma electrónica y el artículo 4 los principios generales que rigen la firma electrónica, el artículo 5 nos establece el empleo de la firma electrónica. La segunda parte de la ley está compuesta por la aplicación de

[191] Gallego Higueras, Gonzalo. Código de Derecho Informático y de las nuevas tecnologías. Primera Edición. Editorial Cívitas Edición S.C. Madrid. 2002. Pág. 965.

los requisitos legales de los mensajes de datos, así como los aspectos técnicos que debe de reunir los así el articulo 6 nos establece los sistemas de acreditación de prestadores de servicio, de los artículos 8 al 15 nos establece los que es certificados electrónicos y las condiciones generales de las prestadoras de servicio. De los artículos 16 al 28 nos establece los procedimiento de cómo se utilizara la firma electrónica así como también los requisitos que se entenderá que llevara dicho dispositivo para garantizar a la firma electrónica y la parte final de procedimientos sancionatorios de dicha ley.

Y así podemos ir comentando en forma general que a la ley de firma electrónica en España ha servido de guía para otras naciones. En España podemos decir que con la ley de firma electrónica no solo se avanza en carácter de comercialización electrónica o contratación electrónica, sino también en aspectos como delitos informáticos los cuales van avanzadas con respecto a este ya que poseen una división especial de tecnología aproximadamente desde 1999, así como también en el avance del derecho administrativo electrónico, ya que en ese país con la ley de firma electrónica se introdujo en el DNI o su equivalencia en nuestro caso el DUI, un chip el cual se le proporciona una clave privada a cada ciudadano y mediante este puede firma cualquier documento o realizar cualquier trámite con la administración. Así la ley de Firma Electrónica en España abrió las puertas para que en otras áreas del derecho se pueda actuar.

4.3.2 Instrucción de 19 de Octubre de 2000, de la Dirección General de los Registros y del Notariado, sobre el Uso de la Firma Electrónica de los Fedatarios Públicos.

El Decreto-ley 14/1999 anteriormente desarrollado establece en el párrafo segundo del artículo 1.2[192]. La exclusión de la actividad de los fedatarios públicos del ámbito de la citada norma responde a una adecuada ponderación de las diferencias que separan el sistema público de garantías con la función de los notarios, de las características propias del procedimiento de firma electrónica. Así en España considerando que se deberían de reformas las leyes que en ese momento existían así como también se estima que la función de los notarios y los registradores con la firma electrónica deben de tener una aplicación práctica en lo concerniente a la recepción de documentos.

Todos los procedimientos que debe de desarrollar el notarios y los registradores deben de hacerse sobre la base del respeto mutuo a las competencias de cada uno de los prestadores de servicios de certificación que intervienen en la remisión o envío de documentos notariales a los diferentes registros y en la respuesta que éstos deben dar sobre multitud de aspectos, entre los que cabe enumerar, a título de ejemplo, los datos de inscripción, la posibilidad de notificar telemáticamente la calificación recaída y la solicitud de publicidad registral en sus diferentes manifestaciones.

---

[192] Artículo 1.2:

2. Las disposiciones contenidas en este Real Decreto-ley no alteran las normas relativas a la celebración, la formalización, la validez y la eficacia de los contratos y otros actos jurídicos ni al régimen jurídico aplicable a las obligaciones.

Las normas sobre la prestación de servicios de certificación de firma electrónica que recoge este Real Decreto-ley no sustituyen ni modifican las que regulan las funciones que corresponde realizar a las personas facultadas, con arreglo al Derecho, para dar fe de la firma en documento o para intervenir en su elevación a públicos.

Siguiendo con el desarrollo de la directiva de instrucción en España podríamos decir que El Consejo General del Notariado y el Colegio de Registradores de la Propiedad y Mercantiles de España, se constituyen, a los exclusivos efectos de la obtención de firma electrónica de Notarios y Registradores, (entidad de certificación de certificados electrónicos) en prestadores de servicios de certificación que, dentro de sus respectivas competencias, deben ofrecer la respectiva prestación de servicios de certificación de los medios técnicos precisos para que éste compruebe todos y cada uno de los atributos de la firma electrónica avanzada[193]. Así a esta institución le podríamos encontrar parecido a la Sección de Notariado de la Corte Suprema de Justicia como ente central de control de la función notarial en cada país.

4.3.3 Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas. (Guatemala).

Esta ley fue creada por el Decreto 47-2008. Del artículo 1 al artículo 7 nos establece los aspectos generales de la ley en los cuales como la ley modelo UNCITRAL los aspectos que se entenderá que es firma electrónica y los conceptos generales, otro punto que se toma en cuenta son los principios generales y los efectos jurídicos de la firma digital del artículo 8 al artículo 30 de la ley nos establece los aspectos técnicos que ha de cumplir la firma electrónica así como también el procedimiento que se ha de seguir para firmar electrónicamente un documento, otro aspecto a destacar es la presunción de envió del mensaje electrónico y en el cual se considera que una persona ha enviado un mensaje electrónico si este ha utilizado su clave

[193] http://notariosyregistradores.com/CORTOS/instrucc-firma-electr.pdf

privada. De ahí que se considera una presunción de derecho pero que si presenta pruebas de que fue utilizada su firma por un tercero ajeno a la transacción este puede iniciar un proceso de nulidad de la transacción y se siguen las reglas de las nulidades en materia civil o mercantil según sea el caso.

Ahora bien los artículos del 31 al 56 nos establecen los procedimientos que ha de seguir para revocar un certificado digital, así como también los requisitos de los prestadores de servicio y los derechos que estos poseen y las obligaciones y derechos del usuario.

Tiene como objetivo regular la actividad comercial en Guatemala, generada por medio de ese tipo de medios (e-commerce). Como dato podríamos agregar que la ley de Guatemala fue elaborada hace un poco más de siete años y que fue hasta el año 2001 que recibió el apoyo de todas las fuerzas políticas en el Parlamento de su país. Ley para la Promoción del Comercio Electrónico y Protección de la Firma Digital, presentado al Congreso el 23 de enero del año 2001; pero que no obtuvo hasta ahora el apoyo requerido de los diputados. Mariano Rayo, expresa que el anteproyecto fue sometido de inmediato a un proceso de estudio y análisis, lo cual conducirá a su posterior dictamen.

Esta nueva ley venía siendo un proyecto que al igual que en países como Costa Rica, México, Brasil entre otros solo habían mandado al archivo dichos proyectos.

Esta ley en el ámbito jurídico guatemalteco ha generado grandes expectativas entre las cuales se puede mencionar un nuevo tipo de comercio beneficiará a empresas y consumidores, así como también a entidades

gubernamentales, como el Registro de la Propiedad, Registro Mercantil, Superintendencia de Administración Tributaria, y otras dependencias.

De todo esto podemos decir que la ley de Guatemala de Firma Electrónica es una guía a seguir para los países Centroamericanos para preocuparnos por regular los actos que día a día son mayores en la Web así como también, para buscar una unificación de las legislaciones centroamericanas en la firma electrónica. Así como también la vigencia del DR-CAFTA también presiona para que esta iniciativa sea aprobada por el Legislativo, ya que se espera un fuerte crecimiento del comercio por la vía electrónica. Y así será en El Salvador ya que las empresas que contratan electrónicamente, están exigiendo más seguridad para sus transacciones así para generar confianza y así poder realizar más actos de comercio en la Web.

4.3.4 Ley de Certificados, Firmas Digitales y Documentos Electrónicos. (Costa Rica).

Esta Ley de Certificados, Firmas Digitales y Documentos Electrónicos", (Nº 8454 del 30 de agosto del 2005. La Gaceta Nº 197 del 13 de octubre del 2005), fue aprobada en esta fecha ya que se había presentado desde el año 2004 un anteproyecto el cual fue elaborado por diferentes instituciones del gobierno creando una institución multisectorial los cuales se le encargo el estudio de dicha ley y estaban conformados por el Ministerios de Ciencia y Tecnología, Justicia y Comercio Exterior, Poder Judicial, Procuraduría General de la República y el Registro Nacional General de la República Registro Nacional.

Dicha ley está estructurada por siete capítulos[194] los cuales al igual que la mayoría de legislación, la cual ha sido elaborado nuestro proyecto de ley de la firma electrónica.

Dentro de la ley existen muchas expectativas con respecto a esta ley las cuales nos ayudaran a entender mejor la ley de firma electrónica así tenemos que dentro de los aspectos más positivos que presenta esa ley son:

Los Principios rectores y que deben ser tomados en cuenta los cuales son. 1- Autonomía de la voluntad, 2- Neutralidad tecnológica, 3- Regulación del documento electrónico y 4- Produce, en general, un avance en el uso de tecnología hacia la construcción del gobierno electrónico.

4.4 Proyecto Final de la Ley de Comunicaciones y Firma Electrónica en El Salvador.

El nuevo anteproyecto de ley además de definir los conceptos básicos del comercio electrónicos, acreditación, certificado electrónico, clave privada o pública, firma electrónica y proveedor, entre otros, ha traído el nuevo borrador de Ley de Comunicaciones y Firma Electrónica[195] el cual será presentado en los próximos meses por el Ministerio de Economía y la Secretaria Técnica de la República para ser aprobado por la Asamblea Legislativa de nuestro país. Este borrador final de ley contempla cinco

[194] Capítulo I: Disposiciones generales
Capítulo II: Documentos
Capítulo III: Firmas digitales
Capítulo IV: Certificación digital
Capítulo V: Sanciones
Capítulo VI: Disposiciones finales y transitorias

[195] Ver Anexo de Borrador de Ley de Comunicaciones y Firma Electrónica.

principios legales básicos en los cuales descansara la regulación jurídica del comercio electrónico, si tenemos los principios de autenticidad[196], integridad[197], confidencialidad[198], equivalencia[199] y no repudiación[200].

Con el primer principio se garantiza a la confianza y garantía que perdura a través del tiempo así como saber quién es el que envió dicho documento. El segundo principio otorga certeza que esa información no ha sido alterada en el proceso de envió y recepción de información. En cuanto al tercer principio se garantiza al iniciador y destinatario que los mensajes que envíen no serán conocido por terceros ajenos a estos y que si desean también no se dará a conocer su identidad verdadera y solo tendrá este conocimiento la empresa certificadora y que solo podrá ser revelada por un juez que pida esta información. En cuanto a la equivalencia se garantiza que las instancias administrativas o judiciales no podrá rechazar un documento electrónico debidamente certificado. Y la no repudiación es la garantía a las persona que un mensaje ha sido suscrito con la firma electrónica, y su autor no puede aducir después desconocimiento o rechazo a este.

El abogado Ricardo Cevallos[201] opina sobre este borrador de ley diciendo “el problema básico del comercio electrónico es la jurisdicción. Si compro aquí no hay problema, pero si lo hago por Internet, en otro país, es

[196] Articulo 4 numeral a)
[197] Articulo 4 numeral b)
[198] Articulo 4 numeral c)
[199] Articulo 4 numeral d)
[200] Articulo 4 numeral e)
[201] Abogado que elaboró en el año 2000 el borrador de un anteproyecto de Ley de Comercio Electrónico, a solicitud del gobierno central. El cual tuvo este borrador como base al Ley Modelo de Comercio Electrónico de la Organización de las Naciones Unidas. Autora: Molina Tamacas, Carmen. El Comercio Electrónico Sin Regulación. El Diario de Hoy. San Salvador, 08 de febrero de 2009. Pág. 21.

difícil ubicarlo geográfica y legalmente"[202] añadiendo después que las leyes de E-comercio no buscan regular las transacciones, sino los medios.

Esta ley podemos mencionar que regularía lo que en El Salvador sabemos que ya existe como lo es el comercio electrónico. No solo porque los clientes pueden ordenar libros, artículos para bebes y de oficina entre otros, a cualquier proveedor el mundo y aun dentro del mismo país.

Este borrador final de Ley de Comunicaciones y Firma Electrónica consta de 56 artículos los cuales están distribuidos en Cuatro Títulos que son:

- ✓ Título I. Disposiciones Generales que recoge el objeto y consideraciones fundamentales de interpretación de la ley.

- ✓ Título II. Mensajes de Datos y Documentos Electrónicos. En los cuales se da las disposiciones generales del tratamiento que se le dará al documento electrónico y como se conservara este para su conservación y posible utilización más adelante. En este punto nos detendremos un poco para comentar el artículo 10 de esta ley, en el cual se reconoce los documentos auténticos y públicos emitidos en soporte electrónico[203]. En el cual vemos reflejado la posibilidad de que un notario puede en un futuro actuar en la realización de un documento público electrónico así como también la necesidad que plantea al Órgano Judicial de elaborar un

[202] Autora: Molina Tamacas, Carmen. El Comercio Electrónico Sin Regulación. El Diario de Hoy. San Salvador, 08 de febrero de 2009. Pág. 21.

[203] ***Documentos auténticos y públicos emitidos en soportes electrónicos***
Art. 10.- Los documentos auténticos podrán estar contenidos en soporte electrónico y tendrán el valor asignado por el ordenamiento legal para esta clase de documentos.
Los documentos públicos electrónicos que se refieran al ejercicio de la función notarial se regularán en una ley especial.

anteproyecto de ley y darle iniciativa de ley para que la función notarial sea regulada. Como lo vimos en las leyes de España, el cibernotario es una necesidad en la cual su intervención estaría destinada a dar seguridad y certeza jurídica a los contratos electrónicos. Además de tener en cuenta que nuestro propio Código Civil, Ley de Notariado y la Ley de Jurisdicción Voluntaria y otras Diligencias la necesaria intervención del notario en los contratos en que exija esta solemnidad y no pudiéndose omitir este requisito, sine quanon, en el cual ese instrumento que no posea este requisito seria ineficaz para ser presentado ante cualquier juzgado u otra instancia administrativa. Y en los cuales descansa nuestra afirmación en que es necesaria la intervención del notario en un contrato electrónico teniendo a la base una legislación que ampare la función notarial de este.

- ✓ Título III. Comunicación Electrónica de Datos. El cual define cuando se tendrá por recibido un mensaje y las formas de validar esta actuación por parte del receptor del mensaje, como su lugar de emisión y recepción y le acuse de recibido de los mensajes electrónicos. Así lo establece el artículo 12 de esta ley:

Verificación de la emisión del Mensaje de Datos

Art. 12- Se entenderá que un mensaje de datos proviene del iniciador, cuando éste ha sido enviado por:

a) El propio iniciador o la persona que lo representa, cuando el documento ha sido firmado electrónicamente.

b) Por un sistema de información programado por el iniciador, o bajo su autorización, para que opere automáticamente.

En el cual establece que existen dos formas para tener por verificado la emisión de un mensaje que son que se haya firmado electrónicamente y la otra que se utilice un sistema automatizado de envió de esta información.

Esto a la base del principio de no repudiación el cual hace eficaz y seguro un mensaje de dato.

- ✓ Título IV. Firma Electrónica y Certificados Electrónicos. Este es el título más extenso de la ley en el cual recoge todos los parámetros técnico-jurídicos que debe de reunir una firma electrónica para tener plena validez en El Salvador. Nos establece también este título los requisitos de un certificado electrónico, así como los deberes de y derechos que posee un proveedor de certificados electrónicos. Al final de este título podemos contemplar la parte de procedimiento administrativo para la sanción por desacatar las disposiciones de esta ley.

En conclusión este borrador final de la Ley de Comunicaciones y Firmas Electrónicas, ha venido a querer revolucionar el actual encause del derecho salvadoreño, en el cual se inicia una nueva era de investigación jurídica, por lo que los abogados salvadoreños como los notarios deben de tener en cuenta que el derecho es cambiante y que este evoluciona con la sociedad (teniendo hoy en día una era de la informática), en el cual los estudiantes de derecho, los abogados y en especial los notarios deben de adaptarse a esta nueva realidad.

CAPITULO V

INTERVENCIÓN DEL NOTARIO EN LA CONTRATACIÓN POR MEDIOS ELECTRÓNICOS.

SUMARIO: *Introducción. 5.1 Notario Salvadoreño. 5.1.1 Concepto de Notario. 5.1.2 Función Notarial. 5.1.2.1 Concepto de Función Notarial. 5.1.2.2 Fases de la Función Notarial. 5.1.2.3 Principios Rectores de la Función Notarial. 5.2 Ciber Notario o Notario Electrónico. 5.2.1 Definiciones. 5.2.2 Importancia de la Implementación de la Figura del Ciber Notario. 5.2.3 Fe Pública Informática. 5.2.4 Funciones del Ciber Notario. 5.2.5 Diferencia entre el Ciber Notario y las Autoridades de Certificación. 5.2.6 Ejemplo Práctico de la Función del Ciber Notario.*

Introducción.

En nuestro país el notario es una figura sumamente importante en la celebración de un contrato o en la celebración de cualquier acto ya que en el derecho civil para la validez de algunos contratos[204] es necesario que se realice la respectiva escritura pública, por lo que sin la participación del notario no tendrían validez y no podrían ser exigidos ante un juez los posibles incumplimientos.

Además en el mismo Código Civil se establece que en aquellos actos en los que la misma ley exija un instrumento público[205] no harán plena prueba sino se otorgan estos con las debidas solemnidades, es decir si no se otorgan en escritura pública, ante el notario autorizado para tal efecto. [206]

Por lo que en el presente capitulo se analiza el concepto de notario, su función y la incorporación del ciber notario en la contratación electrónica.

---

[204] Como por ejemplo el contrato de compraventa de inmuebles (artículos 1605 inciso segundo del Código Civil), entre otros.
[205] Artículo 1580 del Código Civil. "Deberán constar por escrito los actos o contratos que contienen la entrega o promesa de una cosa que valga más de doscientos colones".
[206] Artículo 1572 del Código Civil.

5.1 Notario Salvadoreño

El notario es un agente necesario en las distintas sociedades, desde tiempos remotos por la necesidad de los pueblos de darle seguridad jurídica y certeza a los actos que realizaban para la convivencia pacífica de la misma sociedad y así satisfacer las necesidades de los particulares que pretenden autenticar ciertos actos y hechos jurídicos. Por lo que el Estado le dota a éste de esa envestidura para dar seguridad jurídica a los actos que ante él se otorgan y así beneficiar a las personas en general, ya que según nuestro ordenamiento jurídico, específicamente nuestra Constitución establece la obligación del Estado salvadoreño de dar seguridad jurídica a los habitantes y extranjeros del país[207], y para tal efecto el Estado creo la institución del notariado para poder llevar a cabo sus fines últimos y dar seguridad jurídica y bien común al pueblo.

Otro factor que justifica la intervención del notario es la existencia de determinados actos o contratos que requieren de veracidad frente a terceros y esta autenticación solo lo pueden dar los notarios por la investidura que tiene y dar fe pública de los actos que se otorgan ante su presencia, así como también por los elementos de validez y formalidades[208] que tiene ciertos actos y que de no realizarlos este profesional del derecho, carecerían de valor ante terceros y ante la vía jurisdiccional.

---

[207] Art. 1.- El Salvador reconoce a la persona humana como el origen y el fin de la actividad del Estado, que está organizado para la consecución de la justicia, de la seguridad jurídica y del bien común.

[208] Art. 1605.- La venta se reputa perfecta, desde que las partes han convenido en la cosa que es objeto de la venta y en el precio, salvo las excepciones siguientes, y las contenidas en las leyes especiales.

La venta de los bienes raíces, y servidumbres, y la de una sucesión hereditaria, no se reputan perfectas ante la ley, mientras no se ha otorgado escritura pública.

Por lo que la existencia del notario se da de manifiesto y no existe parte en el mundo en el cual no exista un notario o una persona determinada que de fe de los actos que se celebran.

5.1.1 Concepto de Notario

Dentro de la Ley del Notariado vigente encontramos una definición de qué debemos entender por Notario y menciona que el notario es un delegado del Estado que da fe de los actos, contratos y declaraciones de voluntad que ante sus oficios se otorgan y de otras actuaciones en que personalmente intervenga[209], su misión se completa asesorando a los intervinientes; aconsejándoles con equidad sin tomar partido por ninguno, de tal forma que el notario no juzga sino que previene; ilustra y explica el Derecho por los medios normales de la convicción, sin tener en cuenta el interés particular de alguna de las partes.[210]

Según Martínez Segovia "Notario es un jurista facultado por la ley para interpretar y configurar, autenticar, autorizar y resguardar tanto el documento notarial (o medio objetivo) como el objeto material (o contenido) de la función notarial, siendo el órgano de dicha función"[211].

Muchos han sido los conceptos vertidos sobre la figura del notario, vista como la institución notarial en sus aspectos más fundamentales; pero es de hacer notar, que al hablar de Notario, enfocamos el Notariado Latino,

[209] Articulo 1 Ley de Notariado.
[210] Velasco Zelaya, Dr. Mauricio Ernesto, Magistrado de la Sala de lo Civil de la Corte Suprema de Justicia. Articulo "Del Notariado en los Países Latinos". Revista Quehacer Judicial, Enero-febrero de 2008, numero 62. página 3
[211] Citado por Córdoba Rogel, Karen Marisol, y otros. Tesis. UES "Alcances que presenta la función notarial en la ley del notariado y frente al anteproyecto de dicha ley, en lo relativo a las actuaciones notariales que se realizan en el exterior". Ciudad Universitaria. Enero 2006. 38

como una vertiente propia de nuestra región y de nuestras raíces latinas, siendo así que ha sido punto de discusión la definición del mismo en diferentes congresos internacionales a través de la historia.

En el III Congreso de Perú 1954, se dijo que "Los notarios son los profesionales del derecho más próximos a la vida por suscitación en el punto de confluencia de las leyes y de los hombres. Esta situación les impone ser un elemento vivificante en la sociedad; en sus relaciones con quienes depositan en ellos su confianza, deben humanizar las normas jurídicas y adoptar la contratación a las necesidades particulares…"[212].

Así también en el IV Congreso de Brasil 1956 se dijo que "El notario Latino por el hecho de estar encargado de aplicar la ley en los contratos que autoriza, actúa como un asesor de las partes en cuanto a ella; además, ante su oscuridad, sin contradicciones y sin omisiones, él está llamado a aclararla e interpretarla. El notario latino da vida a la ley y esta vida es la expresión tanto de la voluntad del legislador como de las partes. Debe saber adoptarse tanto a los casos particulares como a las situaciones creadas por la evolución económica y social del país en que actúa"[213].

Así muchos más congresos en los que se ha hablado de la importancia que el notario tiene para con el derecho, como un agente de la función notarial que imparte seguridad jurídica, con la dación de fe, para la protección de los derechos de las personas.

Nosotros definimos al notario como un técnico del derecho que el Estado Salvadoreño le delega parte de su poder estatal de donde se

[212] Ídem. Página 40
[213] Ídem.

desprende la facultad de dar fe a los actos, contratos o hechos jurídicos que tenga trascendencia en el ámbito jurídico otorgados ante él.

5.1.2 Función Notarial

Para el desarrollo del presente trabajo de investigación es de suma importancia el abordaje de la función notarial ya que es ahí donde radica la importancia del notario en su papel ante la sociedad y como un delegado del Estado, es por ello que con la opinión de diferentes autores se desarrollará todo lo concerniente de la función notarial, su definición, su naturaleza jurídica, abordando las fases de ésta función y los principios con los que se rige.

Por lo que con esta información se va a establecer cuál será la función del ciber notario y dar un contraste en la función que realiza el notario y la que realizará el ciber notario y demostrar que no hay diferencia notable entre una función y la otra.

5.1.2.1 Concepto de Función Notarial

El Doctor Ramírez Pérez ha definido La función notarial, como una "actividad jurídico cautelar cometida al notario, que consiste en dirigir imparcialmente a los particulares en la individualización regular de sus derechos subjetivos para dotarlos de certeza jurídica, conforme a las necesidades de tráfico y de su prueba eventual" [214].

[214] Ramírez Pérez, Benjamín. Limitaciones al Ejercicio de la Función Notarial. Tesis para optar al grado de Doctor en Jurisprudencia y Ciencias Sociales, año 1977

Podemos distinguir que esa función es de carácter estatal, que el mismo delega a una persona profesional del derecho la facultad que en su nombre brinde la función que por ley le atañe realizar brindando así la certeza jurídica a la que está obligado.

En el Primer Congreso de la Unión Internacional del Notariado, que fue celebrada en Buenos Aires en 1948 se dio un concepto de Función Notarial, estableciendo que es "recibir e interpretar la voluntad de las partes para asegurarse de que el negocio que por medio del instrumento se formalice, concuerde con la verdadera voluntad e intención de los otorgantes[215], estableciendo las tres fases de la función notarial.

Por lo anterior se puede desprender la idea que la función notarial es aquella actividad o desempeño que realiza un profesional del derecho al cual el Estado lo inviste de la potestad para impartir fe pública a todos los actos y contratos que se otorguen ante ellos, y servir a las personas en general de asesores, moldeadores y certificadores de la libre voluntad de estas y darles seguridad jurídica[216] y certeza jurídica[217] a estos actos.

---

[215] Primer congreso de la Unión Internacional del Notariado Latino, celebrado en Buenos Aires en 1948. tomado de tesis de Eva María Peña Daura y Dominga Beatriz Vásquez Molina, "Análisis de la Mala Praxis en el Ejercicio de la Función Notarial y sus Consecuencias". Universidad de El Salvador Año 2005, Pág. 55

[216] Concepción que basa en la esperanza o confianza de los ciudadanos en la función ordenadora del Derecho, por lo que es necesario darles protección. Dicha esperanza no puede, por tanto, quedar al libre albedrío del Poder o de otros particulares: el Derecho tiene que estar a disposición de los ciudadanos de manera incuestionable, segura.
En todo caso, la seguridad jurídica no se predica del conocimiento de la regulación de tal o cual norma específica o de sus consecuencias, a través fundamentalmente de su previa publicación, sino, sobre todo, por precisarse una buena estructura del Derecho, la ausencia de arbitrariedad y un grado cierto de previsibilidad, con el fin justo de dar esa confianza a los ciudadanos. A esto se le unen el poseer una cierta autonomía, objetividad y racionalidad; en definitiva, resguardar el ordenamiento jurídico de los defectos de la sociedad humana (principalmente del abuso del poder). "Seguridad jurídica." Microsoft® Student 2007 [DVD]. Microsoft Corporation, 2006.

[217] certeza. (De cierto). f. Conocimiento seguro y claro de algo. ‖ 2. Firme adhesión de la mente a algo conocible, sin temor de errar. Microsoft® Encarta® 2007. © 1993-2006 Microsoft Corporation. Reservados todos los derechos.

5.1.2.2 Fases de la Función Notarial

La función notarial, siguiendo los parámetros de las definiciones que antes planteábamos, contempla tres fases que a la vez son su contenido, de lo que se compone el trabajo del notario, fases en las que éste se encuentra sumergido por su propia función notarial las cuales son:

La *fase asesora,* la *fase formativa o legitimadora* y por último la *fase autenticadora,* estas fases son el punto central de la actividad notarial.

- ***Fase Asesora***

Es la fase en la que el notario, en el sistema notarial latino, no es un simple agente que interpone la fe notarial a aquellos actos que requieren de su intervención, sino que por la misma formación profesional que el notario posee se convierte en un asesor de las partes intervinientes en el contrato o en el acto que se realiza, proporcionándoles una orientación profesional respecto de la situación planteada.

En otras palabras el notario es un verdadero consultor jurídico, un asesor y consejero que tiene el deber de informar e instruir a las personas que le consultan de todas las posibles soluciones así como las consecuencias jurídicas de estas.

Es decir que esta fase no solo se queda en el recibimiento y la interpretación que hace el notario de la situación que le es planteada por las partes que intervienen en un determinado negocio, sino que después de la interpretación el notario asesora a las partes, brindándoles una opinión jurídica-técnica para solucionar su situación.

Esta fase también la podemos ver en el ciber notariado, ya que el ciber notario siempre es asesor de las partes, en el sentido que cuando reciba una video llamada o un correo electrónico solicitando su colaboración el deberá asesorar a las partes para que realicen el contrato esto lo pude hacer de forma directa o indirecta, cuando nos referimos a una forma directa es cuando se hace a través de un chat, o video llamada en tiempo real y en forma indirecta cuando se hace por el intercambio de mansajes por correo electrónico que si bien no se hacen al mismo tiempo pero no por ello tiene a ser menos eficaz.

- ***Fase Formativa y Legalizadora.***

Cuando se concluye la fase asesora y el notario ha terminado de explicar y asesorar a los comparecientes en una negociación o acto, entonces continua con la siguiente fase que es la fase formativa y legalizadora.

Hay ocasiones en las que las personas o clientes pueden en su momento invocar un derecho o un acto erróneo por la misma falta de formación profesional en las Ciencias Jurídicas por lo que el notario debe de encausarla en el rumbo correcto es decir el notario propone alternativas jurídicas que permiten solucionar lo planteado por las partes, además que se convierte en redactor del documento y el que califica la procedencia del acto a realizarse, es decir que el notario moldea legalmente el instrumento interpretando la voluntad de las partes. Y es legalizadora porque califica y hace una sustentación jurídica de lo que las partes le han planteado de acuerdo a sus conocimientos jurídicos, es decir que adecua la situación concreta a la norma vigente.

Es decir que en primer lugar el notario debe calificar jurídicamente la naturaleza del acto o contrato a realizarse, ya que por la falta de conocimientos jurídicos de las partes, estas pueden confundirse en la naturaleza del negocio que quieren realizar, en segundo lugar el notario debe analizar si el acto o el negocio es legal, en tercer lugar el notario deberá expresar la voluntad de las partes con sus propias palabras pero siempre reflejándola fielmente al deseo de los comparecientes, esto es la elaboración del instrumento notarial, donde después las partes dan su consentimiento por medio de las firmas.

De lo expuesto se deduce perfectamente la gran diferencia con el notario Anglosajón, ya que este puede o no ser un profesional del derecho y que solo da fe de la firma que calza al pie de un documento pero no así del contenido del mismo resultando luego en conflictos legales largos y los cuales se pueden evitar con la intervención del notario latino en asuntos judiciales.

En el caso del ciber notario, esta hará la fase formativa del contrato o acto de igual forma que un notario común con la diferencia que el contrato que envié a la parte que lo solicite llevara un sistema de seguridad el cual encriptar el mensaje con el contrato y este no podrá ser alterado por ninguna otra persona y la otra persona dará su aceptación con otro mensaje de igual manera, el cual aceptara el contrato que el ciber notario redacto. La legalización se hará con la firma digital que ayudara a dar esa autenticidad al documento que está redactado en base a las leyes del país en el cual el contrato surtirá efectos legales.

⚜ *Fase Autenticadora.*

Siguiendo la misma idea, esta fase consiste en que el notario autentica y legitima el acto que se ha celebrado ante él, realizándolo por medio de la imposición de la fe pública, redactando el instrumento.

Se puede resumir esta fase diciendo que la Fase Autenticadora, que es una de las más importantes consiste en dar fe pública a los hechos o actos jurídicos ocurridos en su presencia. La función autenticadora sobre todo en cuanto se exterioriza en las actas notariales, puede recaer sobre gran cantidad de hechos[218].

Con esta última fase concluye la función notarial y el trabajo del notario, otros llaman a estas fases como el contenido de la función notarial ya que la función notarial es lo medular de la actividad del notario, es la razón de ser, ya lo mencionaba el tratadista Rufino Larraud[219], "el notario tiene en la esfera de sus actividades, una actividad que es inherente a la institución del notariado, es la razón de ser de su existencia, su estructura y su régimen. Ya se ha dicho que la función notarial autentica, da certeza a derechos y evita contiendas, es una función de cautela, de precaución; no solamente es función autenticadora, sino que también preside, asesora a las partes en los negocios jurídicos, haciendo una verdadera labor de política jurídica, o sea una labor preventiva en la aplicación del derecho, evitando en los posible los conflictos o litigios."

En cuanto al notario electrónico, el problema de la autenticación surge precisamente del elemento que contienen las voluntades, sintetizado en un

[218] Luís Vásquez López Ob. Cit. Página 81 y 82.
[219] Citado por el Licenciado Luís Vásquez López, en su obra Derecho y Practica Notarial. Pagina 82

documento electrónico, que como se ha venido señalando es un documento sin una base en papel sino que su base es un software de computadora que contiene técnicas criptográficas así como controles tecnológicos que pueden garantizar la autenticidad.

5.1.2.3 Principios Rectores de la Función Notarial

Como sabemos los principios son la Base, el origen, o la razón fundamental sobre la cual se procede discurriendo en cualquier materia[220]. También se dice que es cada una de las primeras proposiciones o verdades fundamentales por donde se empieza a estudiar las ciencias o las artes, y también son las normas o ideas fundamentales que rigen el pensamiento o la conducta[221].

Autores como Luís Vásquez López, establecen que los principios son proposiciones necesarias de carácter universal para obtener determinados resultados[222].

Se dice que son proposiciones principales porque abarcan el ámbito de la ciencia o del arte al que pertenecen sin tener nacionalidad, se comprueban en todos lados, en todos los países. Son permanentes, su vigencia no tiene términos de donde comienzan y donde acaban, y además son racionales por ser la razón la que los descubre y los confirma, así como los explica y los hace comprensibles.

[220] Microsoft® Encarta® 2007. © 1993-2006 Microsoft Corporation. Reservados todos los derechos.
[221] Idem.
[222] Luís Vásquez López, obra citada, pagina 93

Todas las ciencias, artes, disciplinas, entre otros tienen principios de los que se basan sus estudios, y el derecho no es la excepción, como toda ciencia tiene sus principios cimentados, así como también todas sus ramas, y así el notariado y por consiguiente la función notarial tiene principios en los que se fundamenta.

En este apartado analizaremos los principios de la función notarial del notario tradicional comparándolos con los principios de la función notarial que tendría el notario electrónico o ciber notario.

- ***Principio De Conocimiento.-***

Este primer principio se manifiesta en dos planos: en primer lugar en el plano de los hechos y en segundo lugar en el plano del derecho aplicable al hecho. El notario debe conocer con exactitud cómo se debe exteriorizar la expresión de voluntad de las partes, teniendo especial cuidado en los requisitos de validez de cada una de las figuras jurídicas. Es responsabilidad de él la formalización y conocimiento de las mismas[223].

Es decir que el notario debe tener conocimiento en los hechos concretos, a las situaciones que se le presentan, que son la base del negocio jurídico que se pretende realizar, como por ejemplo la intención o voluntad de los otorgantes, los fines y los efectos que esa negociación van a generar.

Para el notario electrónico este principio no cambia, ya que éste también está obligado a tener conocimiento de en que parte del mundo se encuentran los sujetos, así como el negocio jurídico que se les presenta, la

[223] Luís Vásquez López, obra citada, pagina 93

forma de pago y las condiciones del contrato, para brindar la seguridad a ambas partes que le es requerida.

Principio De Legalidad.-

Este principio consiste en que el notario procurara siempre un perfecto ajuste al derecho, deberá analizar cuidadosamente la situación jurídica de los otorgantes, en ello su capacidad, la legitimidad para ser comparecientes, además de la competencia que tiene para intervenir en el negocio jurídico[224].

Es decir que el notario debe estar al margen de lo que las leyes le establecen, su actuación deberá ser siempre enmarcada en las disposiciones legales y en ellas deberá enmarcar la situación y las soluciones a ella.

El cumplimiento de este principio es la base de nuestra investigación, ya que éste es uno de los principios de la función notarial más importante, ya que nuestro sistema legal está basado en el *civil law*, es decir en el derecho civil, que se refiere a que todo el accionar ya sea administrativo y judicial del Estado tiene que apegarse a lo que le dicta la ley, por lo que el ciber notario y su participación en la contratación electrónica debe estar regido por una ley para su verdadera aplicación, toda su función notarial debe estar basada en una ley para dar pleno cumplimiento a este principio y veracidad a los actos y contratos realizados por medios electrónicos.

Principio De Representación.-

Este principio tiene su fundamento en la situación de que los hechos o actos son fugaces e inmateriales; existen brevemente y sin dejar rastros, es

[224] Idem.

decir pasan una vez y no vuelven a pasar y con el tiempo se olvidan, por lo que si no se materializan desaparecen en forma definitiva, entonces es necesario que se aprisione esa realidad, representándola, reconstruyéndola mentalmente para luego materializarla o darle la permanencia[225].

En este orden de ideas es entonces que entra en juego el notario que cuando le proporcionan los datos del negocio jurídico los otorgantes del mismo, dicho negocio cobra vida por medio de una estructura que no es otra que el molde una estructura adecuada a la relación del negocio celebrado, es decir que este molde no es más que la escritura matriz o más bien la idea de la escritura matriz antes de ser plasmada en el documento.

- ***Principio De Permanencia O Conservación.-***

Este principio está íntimamente relacionado con el anterior, ya que el principio de representación es la expresión sensible de la realidad percibida por el notario, este principio significa que el notario está obligado a conservar o mantener resguardados los documentos o instrumentos de los actos o contratos en los que intervenga[226], es decir para el notario tradicional este principio se cumple con el protocolo, pero para el notario electrónico debe ser un soporte electrónico, es decir un protocolo electrónico, como por ejemplo en España los notarios han creado un protocolo electrónico que le denominan “Libro Blanco del Notariado Electrónico”, de la misma manera en Holanda los notarios han creado un sistema llamado “Diginotar”, ambos tienen la finalidad de conservar los documentos electrónicos prueba de los actos o contratos electrónicos en los que han participado.

[225] Luís Vásquez López, obra citada, pagina 93
[226] http://espanol.geocities.com/notariacuartadecucuta/notarial.html#principios

⚜ *Principio De Autenticidad.-*

El instrumento auténtico[227] es aquel que está garantizado en su certeza, seguridad jurídica por haber intervenido el notario como delegado del Estado. Por tal motivo, dicho instrumento o documento tendrá presunción privilegiada de veracidad y gozará de una credibilidad que hará prueba por sí mismo de su contenido[228].

La fe pública de la cual se encuentra investido el notario hace imprimir certeza y credibilidad a los actos que autoriza.[229] Es decir que con la dación de fe pública que el notario establece hace que el documento que anteriormente, pueda no haber tenido valor legal, obtenga el valor necesario para garantizar que los derechos de las personas no sean violentados.

Este principio también puede ser aplicado en el ámbito informático, ya que los documentos electrónicos, que son la base de la contratación electrónica, deben siempre estar de acuerdo con los requisitos para los contratos que establece la ley y surtir todos los efectos jurídicos que les son atribuidos. De esta manera la intervención del notario electrónico cabe en la documentación informática y se extenderá no sólo a la legalización de firmas digitalizadas, sino también a la solemnización electrónica tanto del certificado que contiene identidad, capacidad y otros requisitos establecidos por la ley, como la autenticación del contenido del documento en sí. Ha de determinar la capacidad de una persona para realizar la transacción de que se trate, pero también ha de verificar y autenticar que la transacción misma cumple

[227] Nos referimos a la calidad que obtiene el documento cuando interviene la función notarial, es decir la calidad de ser un documento verdadero, no en si a la clasificación de instrumento autentico mencionado en el Código de Procedimientos Civiles.
[228] http://espanol.geocities.com/notariacuartadecucuta/notarial.html#principios
[229] Luís Vásquez López, obra citada. Página 96

todos los requisitos legales y formales para surtir plenos efectos en cualquier jurisdicción[230].

- ***Principio De Seguridad.-***

Este principio quiere decir el amparo a los derechos e intereses de quienes acuden ante sus oficios, es decir que el notario cuando presenta las soluciones a las situaciones planteadas por los otorgantes lo hace siempre procurando que esas soluciones sean aptas y que conlleven a obtener los fines perseguidos[231].

Este principio es uno de los más importantes para lo que es la contratación electrónica, ya que las personas buscan tener seguridad en todos los actos que deseen que permanezcan en el tiempo y mas en un contrato que no se encuentran presentes físicamente y esto ya lo estudiamos en la historia del surgimiento del notario como tal. Así el ciber notario debe de dar la seguridad jurídica a los contratos que se realizan en una base electrónica que no es tangible materialmente pero si en base a un proceso electrónico. Y todo esto lo realiza en base a que el ciber notario utiliza herramientas que dan esta seguridad como lo es con la firma digital que da esa certeza a las personas y consagra el principio de seguridad.

[230] Sánchez Muñoz, Viviana Cristina El Notario ante el Impacto Tecnológico de la Informática y las Telecomunicaciones, http://www.alfa-redi.org/rdi-articulo.shtml?x=9899
[231] http://espanol.geocities.com/notariacuartadecucuta/notarial.html#principios

Principio de Economía.-

Este principio consiste en que las soluciones que el notario presenta ante los comparecientes no deben ser excesivamente onerosos, que les causen a las partes gastos innecesarios[232].

En cuanto al ámbito notarial electrónico, este principio es también aplicable ya que uno de los propósitos de la creación de este notario es de evitar gastos a los intervinientes ya que los otorgantes están en diferentes lugares y les sería sumamente oneroso el viajar hasta el lugar donde se encuentra la otra persona, por lo que se recurre a este tipo de contratación y para darle la misma validez que a un contrato común se implementa el notario electrónico.

Principio de Rogación.-

Como se ha dicho anteriormente, la función notarial es típica del derecho privado, por tal razón no puede prestarse sin previo requerimiento de las partes, es decir que el notario solo podrá actuar por una solicitud de las partes, ya sea de ambas o de una sola de ellas, el notario por sí solo no puede ejercer sus funciones sin que se lo soliciten los interesados.

Esto lo podemos ver cuando el notario electrónico recibe un correo electrónico, una tele llamada o videoconferencia en el cual le solicitan a este la intervención en un acto por el cual debe de intervenir y realizar un contrato electrónico.

[232] Luís Vásquez López, obra citada, pagina 93

⚜ *Principio de Inmediatez.-*

Este principio expresa una relación directa de parte del notario cuando presencia hechos u actos de los que está en obligación de documentar, es decir es la presencia física en el acto en el momento en que está ocurriendo y que el notario constata.

Este principio se discute mucho cuando se trata de la comunicación del notario y los intervinientes en el comercio electrónico, ya que este principio supone la presencia física del notario y las personas que requieren sus servicios, ya sea por sí o por medio de la representación, y es en la formula "ante mi" que se demuestra, y en el comercio electrónico no existe esa presencia física y eso violentaría este principio del que se rigen todos los países con un sistema de notariado latino, como el nuestro, pero para el notario chileno Eugenio Alberto Gaete califica el documento electrónico como un documento interactivo, dinámico y de actuación a distancia y consecuentemente se produce un cambio en la formación del consentimiento del contrato electrónico, sin embargo expresa un esquema grafico de intervención notarial en los negocios perfeccionados por medios electrónicos en el que aunque no exista contacto físico directo entre los otorgantes y el notario no se vulnera la inmediatez, pues cada parte y su correspondiente notario en una sesión interactiva sellan el acuerdo de tal forma que los notarios respectivos intervienen desde cada lugar donde están los intervinientes y dan fe de lo que ocurre[233].

[233] GAETE, EUGENIO ALBERTO. Documento electrónico e instrumento público. Portal de Abogados. http://www.portaldeabogados.com.ar/noticias/derin05.htm

⚜ *Principio De La Unidad Del Acto.-*

Este principio establece la simultaneidad en el tiempo respecto de las distintas etapas de una escritura pública. La presencia del notario, de las partes, y de los testigos, en su caso, debe ser única y sin interrupción o suspensión al momento de la lectura y posterior suscripción del documento o instrumento público.[234] Es decir que cuando se redacta una escritura pública no se puede hacer parcialmente sino totalmente, el día y hora en la que se está produciendo, no puede cortarse y continuar otro día, debe hacerse en un solo acto sin tener interrupciones.

La unidad del acto es otro de los principios notariales que junto al de inmediatez y permanencia, por citar algunos, ha de tenerse en cuenta cuando de actividad notarial electrónica se trate y es que la unidad del acto supone audiencia notarial plena dada por la presencia en el mismo espacio y tiempo de los sujetos del instrumento notarial en el acto de otorgamiento y autorización del documento público. Y es porque el contrato electrónico produce importantes cambios debido a la realidad virtual en que se desarrolla, en donde al hablar de principios notariales se considera que la unidad del acto desaparece entendida como unidad temporal y espacial propia de la expresión del consentimiento contractual tanto material como formal o simultaneidad en las voluntades, pero en cuanto al acto debe ser ininterrumpida, y cuando hablamos de versión papel debe estar contenida en un solo instrumento, que si se piensa bien constituye unidad de texto de la que también goza el documento electrónico.

[234] http://espanol.geocities.com/notariacuartadecucuta/notarial.html#principios

Como lo mencionamos anteriormente estos principios son los que rigen la función notarial y son perfectamente aplicables a la función que va a realizar un notario que intervenga en la contratación electrónica. Pero no solo estos principios son los que deberá seguir sino que también los principios de la contratación electrónica y firma electrónica que los rigen, así podemos mencionar que un documento electrónico posee el principio de no repudio por ser firmado digitalmente, este postulado se aplica cuando a esta firma digital le damos un valor agregado y como lo es la figura del ciber notario.

Otro principio que podemos decir que se aplica es el de economía ya que la figura del ciber notario, ha surgido para dar respuesta a esa necesidad y preocupación de las empresas, y es la de crear un mecanismo seguro en donde pueda enviar información personal y secreta con otra empresa o institución y que esta información vaya protegida por un técnico del derecho como lo es un notario para que no se pueda divulgar, y evitar mecanismos más oneroso de protección y el tiempo para poder realizar un acto jurídico.

Por lo que un ciber notario debe de respetar los principios que rigen su profesión, y que no tienen en ningún momento contradicción ni muchos menos que no se puedan llevar a cabo solo porque pertenecen a un notario común.

5.2 Ciber Notario o Notario Electrónico

La aparición de las nuevas tecnologías han transformado la sociedad hasta tal punto que para ser un verdadero profesional en el mundo del comercio internacional o para aprovechar las muchas ventajas que brinda, ya no solo basta saber de derecho, hace falta también tener conocimientos de

informática, economía, ingeniería, matemáticas, etc. Por lo que el notariado no puede permanecer ajeno a la actual revolución tecnológica, debe estudiar y aprender esta nueva forma de tráfico comercial, ya que además de las funciones tradicionales como notario es asesor y ante una consulta sobre contrato electrónico debe tener los conocimientos necesarios sobre el tema.

Ahora bien antes de entrar a conocer una de las herramientas de la seguridad informática, que es nuestro tema central de investigación, es decir el Cibernotario, debemos saber de dónde surge este concepto y fue a finales de 1997 que la American Bar Association (ABA) siguiendo la recomendación de su Comité de Seguridad e Información (Information Security Commitee) perteneciente a la Sección de Ciencia y Tecnología de dicha Asociación, acordó la siguiente resolución: *"RESUÉLVASE que el Consejo de la Sección de Ciencia y tecnología, apoyando los esfuerzos de la EDI y de la División de tecnología e Información. Inicie los trabajos de un Comité de Especialización de la ABA y colabore con cualquier otra organización internacional o nacional que mostrara Interés en el propósito de lograr una especial certificación de los Cibernotarios"* Dicha resolución por sí misma, aunque corta y en general un poco vaga, marcó el inicio de una nueva era para la profesión notarial, ya que significó el primer acercamiento con efecto potencial hacia el conocimiento de la electrónica y hacia el intercambio de datos que se deriva de ella.

Es indiscutible la utilidad y la seguridad que presenta firmar un contrato ante un notario sin embargo tiene ciertas carencias como por ejemplo lo oneroso que a veces resulta, lo que hoy en día se puede resolver con la contratación electrónica, pero que pasa con la seguridad de esos contratos, ¿serán seguros cuando no se realizan ante un notario?, la firma digital, como vimos anteriormente, es una forma para brindar seguridad ante

un contrato electrónico, pero es un logro que fomenta la seguridad en medio de todo un proceso que por su inmensidad y rapidez apenas hemos podido asimilar, ya que en nuestro país no se ha podido utilizar al cien por ciento por la falta de legislación que la regule, ese es el problema que en muchos países se ha tratado de resolver, como por ejemplo EEUU con la creación del Cibernotario, pero el problema del notariado en Estados Unidos es que el notario anglosajón no tiene facultad de ser un intermediario porque no se han establecido los lineamientos legales que den ese efecto, sin embargo se está implementando en algunos estados como por ejemplo Florida que es el único estado que ha llevado una iniciativa a la Secretaria de Estado para que se lleve a cabo el proyecto de una legislación del ciber notario.

Pero no solo en Estados Unidos se ha querido implementar esta figura, la intervención del notario en la contratación electrónica es un área bastante explotada en los países Europeos, por ejemplo en España los notarios han implementado lo que se denomina su propio ámbito de aplicación con el llamado "*Libro Blanco del Notariado Electrónico"*, en donde recopilan las actuaciones que realizan a través de medios electrónicos[235].

Otro país en donde los notarios electrónicos han accedido al comercio jurídico electrónico es Holanda, donde los notarios han creado una organización nacional de franquicias que pone al servicio del consumidor y del comerciante un producto denominado *"diginotar",* en donde el notario actúa como un tercero de confianza, pudiendo autenticar firmas electrónicas, y actuar en el mercado de las cartas electrónicas. Según las exposiciones acerca de la organización, con ella será posible estar seguro de la persona

[235] Entrevista con la Doctora Yesenia Granillo de Tobar, docente de Derecho Civil de la Escuela de Economía y Negocios (ESEN).

que envía el mensaje y de que lo recibe la persona correcta, naturalmente junto a la firma electrónica.[236]

En la actualidad, el notariado italiano estampa aproximadamente unos tres millones de firmas digitales cada año, todos fueron dotados de un sistema de firma entre octubre del año 2002 y los primeros meses de 2003, han podido transmitir de forma telemática al Registro de Empresas todos los datos de las sociedades, y han sido más ágiles los tramites en registros y ha beneficiado la imagen del notariado italiano que se presenta como una realidad capaz de seguir el ritmo de los tiempos y de proporcionar los servicios rápidos y fiables que precisan la sociedad y la economía.

Y así en muchos países europeos ya cuentan con la suficiente legislación para la implementación total del comercio electrónico y la intervención del notario electrónico o ciber notario, incluso en países centroamericanos y suramericanos ya cuentan con la legislación para regular el comercio electrónico y las firmas digitales, como por ejemplo Costa Rica, Guatemala, Argentina, Perú, entre otros ya cuentan con sus Leyes para regular la Firma Electrónica. Ese es el reto de El Salvador empezar a preocuparse por crear una legislación acorde a las nuevas tecnologías para no quedarse atrás y poder incluirse en el tráfico comercial actual, que requiere de transacciones más rápidas pero a la vez más confiables.

[236] Perales Sanz, José Luís. Director del Seminario: "Seguridad Jurídica en las Transacciones Electrónicas", Primera Edición, Cívitas, 2002. Página 77

5.2.1 Definiciones

Por el hecho de que el concepto de cibernotario es una creación anglosajona y relativamente nueva, no hay en la doctrina muchas definiciones al respecto.

Este notario que es llamado cibernotario, es una tercera parte de confianza que podrá desempeñarse o no como Autoridad Certificante de firma digital.

Para nosotros como grupo de trabajo, nos hemos planteado una definición de ciber notario ya que aun no existen en doctrina definiciones bien estructuradas de él, así para nosotros **Ciber notario** es un profesional del derecho, con conocimientos avanzados de informática y tecnología de seguridad de la información, cuya función combina complementariamente la experiencia técnica con la legal en una sola especialización, el cual actúa como un proveedor de servicios de certificación dando fe pública electrónica, actuando como una tercero de confianza, autenticando las firmas digitales, verificando la identidad de los contratantes y verificando el contenido del contrato, todo en el ambiente de comercio electrónico.

5.2.2 Importancia de la Implementación de la Figura del Ciber Notario

Muchas de las transacciones electrónicas dan hoy problemas especiales, ya que por la velocidad y la cantidad grande de información que pueden almacenar, implica muchos riesgos que de alguna manera dan incertidumbre respecto a la identidad, autoridad y capacidad de las personas que realizan el acto de la transacción. Por tal razón en Estados Unidos se

creó el concepto de Ciber Notario que está diseñado para tener un nivel de entrenamiento y un poder de certificación con reconocimiento igual o un tanto mayor que en los sistemas de notariado latino.

La inseguridad de la naturaleza de las operaciones electrónicas nos ha llevado a pensar o a idear lo que será una tercera parte confiable en cuando a las operaciones electrónicas. Así como la utilización de una clave publica implica la intervención de una tercera persona reconocida como confiable que establezca la identidad de los poseedores de la clave publica que puede ser distribuida a las otras partes, sin esta tercera parte de confianza (ciber notario) que verifique cada parte individualmente es realmente el legitimo poseedor de esa clave sería imposible para las otras partes integrantes del negocio vía red saber a ciencia cierta si el poseedor de esa clave lo es.

5.2.3 Fe Pública Informática

Antes de entrar a conocer lo que es la fe pública informática, debemos saber que es la fe pública y por consiguiente la fe pública notarial.

La fe pública constituye el aspecto esencial de la función notarial y su origen data del antiguo Imperio Romano de Occidente, en donde los contratos eran celebrados por la declaración de los otorgantes sin más formalidad, quedando así afirmados sus derechos en las negociaciones y consecuentemente obligados por buena fe[237].

[237] De León Rodríguez, Claudia Del Carmen y otros. Tesis Instrumentos Notariales: Su Inscripción En El Centro Nacional De Registros. Universidad de El Salvador. Facultad Multidisciplinaria De Occidente, página 23

Para el Doctor Ricardo Martínez Santiago la fe pública es ese respaldo de autoridad que el Estado da de ser ciertos determinados hechos que interesan especialmente al Derecho. Y en un sentido amplio la Fe Pública viene a ser una especie de confianza general que inspiran ciertas cosas, signos, símbolos o manifestaciones emanadas de la autoridad pública, en relación con la que expresan; es una creencia o confianza general en la verdad, impuesta por las necesidades de la vida Social.[238]

La fe pública notarial es la conferida por el Estado, con la que se enviste a personas autorizadas para el ejercicio de la misma, obteniendo la facultad de autenticar en nombre y en representación del Estado, todos aquellos actos en el que el notario tiene una intervención directa, asegurando con esto una armonía social en cuanto a las relaciones privadas, evitando ambigüedades en el contenido de los actos, reflejando la voluntad expresa de las partes que intervienen, sin llegar a la intervención jurisdiccional para dilucidar conflictos derivados de estos.

El ejercicio de la función notarial conlleva intrínsecamente el elemento autenticador de todo acto o hecho que requieren ser proveído de una presunción de veracidad y autenticidad respecto de terceras personas; este elemento autenticador se materializa por medio del ejercicio de la fe pública notarial, ejercida por las personas autorizadas para tal efecto, no obstante, existen otras clases de fe pública que al igual que la anterior implican el hecho de infundir certeza y veracidad a todos aquellos actos que se encuentran fuera del ámbito del derecho notarial. Es decir que en el notariado latino, la seguridad se logra con la dación de fe, que se complementa con el asesoramiento profesional que le brinda el notario, este

[238] Martínez Santiago Ricardo. Ob. Cid. Pág. 1

a la vez analiza y controla la situación jurídica de los requirentes, ilustrándolos y determinando con precisión el comportamiento que deberá tener. Es ahí donde encontramos la importancia de la fe pública ya que sirve para acreditar un suceso, siendo el medio para evitar conflictos en el tráfico de actividades comerciales y/o contractuales, que acontecen en la realidad y que requieren de seguridad y cumplimiento.

Pero en nuestro ordenamiento jurídico cuando hablamos de ciber notariado la fe pública tradicional deviene en insuficiente cuando se trata de aplicarlo a las nuevas tendencias tecnológicas de la informática, en especial tratándose de las obligaciones surgidas a través de un ordenador que prescinde de la presencia física de las personas o un espacio de lugar-tiempo en especifico.

Ya que si nos regimos por lo que establece el artículo 1 inciso 2 de la Ley de Notariado[239] nos encontramos con dificultades al agregar la variante de los ordenadores. Los nuevos retos planteados a la fe pública exigen al derecho la creación de instituciones que sepan incorporar junto a la moderna tecnología, recursos humanos calificados e infraestructura especializada para almacenar la información necesaria.

Así Viviana Sánchez Muñoz[240] nos dice que se entenderá como **Fe pública informática**, aquella cuyo depositario cumple el rol de tercero certificador neutral, como dador de una nueva clase de fe pública, que a

[239] "La fe pública concedida al Notario es plena respecto a los hechos que, en las actuaciones notariales, personalmente ejecuta o comprueba. En los actos, contratos y declaraciones que autorice, esta fe será también plena tocante al hecho de haber sido otorgados en la forma, lugar, día y hora que en el instrumento se expresa". Ley de Notariado, D.L Nº 218, del 6 de diciembre de 1962, publicado en el D.O. Nº 225, Tomo 197, del 7 de diciembre de 1962.

[240] El Notario ante el Impacto Tecnológico de la Informática y las Telecomunicaciones. Por Viviana Cristina Sánchez Muñoz, http://www.alfa-redi.org/rdi-articulo.shtml?x=9899.

diferencia de la fe pública tradicional, no solo se otorga sobre la base de la autentificación de la capacidad de personas, del cumplimiento de formalidades en los instrumentos notariales o a los certificados de hechos, sino que se aplica también a la certificación de procesos tecnológicos, de resultados digitales, códigos y signaturas electrónicas.

Es decir que la fe pública tradicional es implementada por el notario tradicional, la fe pública informática es implementada por el ciber notario, quien como veremos más adelante el ciber notario es un profesional del derecho con una especialización en la seguridad de la información como ente certificado de esta.

Para que la fe pública produzca certeza en el ámbito informático es necesario que su integración sea eficiente con las tecnologías de la información a través de aquellas instituciones que se crearan en base al Derecho Informático existente, ya que el procesamiento, transmisión y almacenamiento de la información y el uso que de ella se está realizando masivamente enfrenta al derecho informático con el problema de encontrar soluciones prácticas y modernas para el adecuado otorgamiento de una adecuada fe pública para otorgar certeza a las operaciones electrónicas que tengan un realce jurídico.

Algunos estudiosos como Ochoa Reyes[241] han planteado los retos que la Fe Pública Informática se debe enfrentar para poder ser implementada en cualquier ordenamiento jurídico que piense utilizarla. Y estas son:

[241] http://www.rodriguezvelarde.com.pe/articulos_35.htm

- Otorgar certeza a la contratación electrónica y a la transmisión de información por medios telemáticos.

- Otorgar certeza a los procesos informáticos, dirigiendo y responsabilizándose de la adecuada utilización de las herramientas que le proporciona la informática jurídica para convertir los archivos tradicionales “pasivos” en archivos digitales “interactivos”.

- Servir de agente promotor en la reducción de costos operativos y administrativos al interior de las organizaciones económicas y propulsor de la eficiencia y competitividad empresarial.

5.2.4 Funciones del Ciber Notario

Como sabemos la iniciativa del ciber notario surgió a finales de 1997, siendo el primer país en mencionarlo Estados Unidos, cuando por el problema de las diferencias en países con un sistema de notariado latino en cuanto al procedimiento y al contenido de los documentos que se realizaban ante los notarios anglosajones, que llevo a numerosos rechazos de los documentos norteamericanos por parte de las autoridades legales de otros países en los que el sistema deriva de la ley civil, para solucionar ese problema la sección de Ciencia Y Tecnología de la American Bar Association, considero la necesidad de la existencia de una autenticación de alto nivel en donde fuera aceptada en todos los países y así fue que se creó la institución del cibernotario. Que combina de forma complementaria la experiencia técnica con la legal en una sola especialización.

Una primera función que realiza el cibernotario en EEUU es similar a la que actualmente es desarrollada por el notario latino, ya que con ello se persigue que cualquier cibernotario garantice que sus actos tengan efecto en jurisdicciones extranjeras. Una segunda función es la de poseer capacidades de certificación y autenticación extendidas, es decir que no solo dará fe sobre los documentos en papel sino que también en documentos en soporte electrónico. Esto obliga a que los notarios electrónicos posean un alto nivel de capacitación en la tecnología de seguridad de la información.

Pero surge un problema en cuanto a la implementación del ciber notario y es que toman al notario anglosajón como referencia, ya que este solo autentica las firmas que se realizan en un documento, pero no su contenido, de tal forma que solo identifica a los firmantes y solo certifica que estos han firmado el documento en su presencia en ese día y a esa hora, por lo que no se puede abarcar todo el ámbito de seguridad que se necesita en un contrato electrónico.

Por el contrario resulta más factible tomar de base al notariado latino ya que este además de autenticar las firmas e identificar a los firmantes certifica el contenido del documento. Ahora bien tomando como base el notariado latino se puede hacer una aproximación de lo que tendrían que ser las funciones de un ciber notario, para garantizar seguridad y fiabilidad a las transacciones electrónicas:

1. Autenticar a las partes;

2. Fechar los documentos electrónicos;

3. Detectar la falsificación o manipulación de mensajes por parte de usuarios no honrados;

4. Confirmar que los usuarios reciben los mensajes adecuados en los momentos adecuados;

5. Almacenar las evidencias, y

6. Registrar los sucesos.

A partir de ello se pueden establecer los siguientes servicios de notarización electrónica[242]:

1. La Autenticación de Entidades. Esta es sin duda una de las funciones más importantes del ciber notario, resulta esencial que, antes de iniciar una determinada operación, cualquier usuario involucrado en la transacción tenga plenas garantías sobre la autenticidad de las entidades con la que va a establecer la comunicación, así como de la autenticidad de los documentos firmados por esta. Además deberá tener la certeza de que cualquier identidad electrónica veraz, sino también una identidad física en el mundo real que se corresponde de forma univoca con la electrónica, es decir de que tanto la entidad real debe ser la misma que se anuncia en la Web.

Precisamente será labor preliminar del notario electrónico identificar de forma correcta, ya sea directa o indirectamente con las autoridades de los registros, a cualquier entidad que pase a formar parte del sistema y habrá de crear pruebas de su registro, las que serán usadas por otros usuarios.

2. La Certificación de Fecha y Hora. Nos encontramos con la clara necesidad de poder conocer y demostrar fehacientemente que un hecho ya sea generación, intercambio, o firma de un documento digital, ocurrió en un determinado instante de tiempo, así como poder relacionarlo frente a otros hechos. Y el uso de los documentos electrónicos hace más difícil la tarea de fecharlos por ser documentos fáciles de modificación, por lo que el notario

[242] Revista "Ágora Sic", Articulo de Javier López Muñoz, Ingeniero Informático, tema "Servicios de Notarización Electrónica". Volumen 25, Universidad de Málaga, Junio 2001. página 3

electrónico deberá utilizar un sistema o servicio de fechado de documentos electrónicos en la que le quite al autor la posibilidad de producir una fecha distinta a la del documento.

3. Certificación de Envió., Certificación de Entrega y Certificación de contenidos. Estos resultan elementos importantes a la hora de dotar de fiabilidad a las típicas transacciones de comercio electrónico. La experiencia ha demostrado de que cualquiera de las partes involucradas en el contrato puede ser una amenaza para la seguridad del mismo, ya que puede tener un comportamiento fraudulento, negando por ejemplo, el envío o la recepción del mensaje o del documento. Resulta esencial, entonces, poder enlazar a los contratantes que intervienen en la operación así como vincular su responsabilidad de autor y receptor. Aquí surge el *servicio del no-repudio,* que es procedimiento por medio del cual se protege a ambas partes de que alguna niegue intencionalmente que un determinado contrato se realizo, este servicio entonces ha de producir, validar, mantener y poner a disposición de las partes, pruebas o evidencias irrefutables respecto a la transferencia de información desde un origen a un destino, así como de la recepción y el contenido de la misma. Por lo tanto, el notario electrónico va a intervenir de una u otra forma, en la ejecución de cualquier protocolo de no-repudio.

4. Soporte de Confidencialidad. En este caso es preciso determinar que cierta información dentro del conjunto de transacciones comerciales especialmente aquellos relativos a mensajes o documentos que se comparten con el notario electrónico sean confidenciales y que además el conjunto de notarios electrónicos debe estar perfectamente definido, para

poder crear una Red Virtual Privada entre los notarios de la misma infraestructura.

5. Salvaguarda de Datos Digitales, Registro de Sucesos y Procesos. Este servicio lo deberá realizar el ciber notario, así como lo realiza un notario latino con el protocolo, es decir que el notario electrónico deberá tener un registro personal, que puede equipararse al libro de protocolo, que actualmente lleva el notario, en donde establecerá las actuaciones en las que intervenga, para tener un respaldo de los mismos.

En fin, los ciber notarios podrán ofrecer servicios profesionales relacionados con la certificación y autentificación de las transacciones internacionales vía computadora a través de registros que garanticen su consentimiento y demuestren su validez y por lo tanto su carácter como transacciones internacionales en cualquier jurisdicción. Estos especialistas garantizarán la autenticidad y credibilidad de las transacciones hechas vía computadora desde su misma existencia, incluyendo su creación, comunicación, procedimiento, retención y capacidad probatoria, porque una de las responsabilidades de estos especialistas será paralela con la de aquellos notarios que ejercen en los países del sistema latino, donde se ha establecido una profesión notarial muy sólida en que su especialidad jurídica puede llenar satisfactoriamente las necesidades de competencia profesional y seguridad que se requiere[243].

En conclusión podemos decir que no cabe duda de que los servicios de ciber notario van a resultar fundamentales durante los próximos años, el hecho de que las empresas y los ciudadanos estén familiarizados con el

[243] Revista Digital De Derecho. Colegio De Notario De Jalisco, México. www.revistanotarios.com

concepto tradicional de “notario”, así como con las funciones del mismo, va a contribuir expresamente a que el notario electrónico se convierta en un eslabón muy importante que va a conducir a un adecuado desarrollo del comercio electrónico en un ámbito global.

5.2.5 Diferencia entre el Ciber Notario y las Autoridades de Certificación

Cuando se analiza la doctrina se tiende a hacer una similitud entre el notario electrónico o ciber notario con las entidades de certificación o proveedores de servicios, en donde se encuentran que efectivamente el notario puede hacer las veces de un proveedor de servicios de certificación, lo que le brinda una ventaja al usuario porque puede optar por un notario electrónico o un empresario cualquiera que brinde el servicio de certificación, pero esta situación se da en países como España, pero surge una diferencia clara entre el notario electrónico y las entidades de certificación o proveedores de servicio de certificación, como nos mencionaba la Doctora Yesenia Granillo de Tobar, es el hecho de que en un contrato en el que la ley le exija la intervención de un notario para que le de validez al contrato, únicamente el notario puede intervenir, es decir, por ejemplo en nuestro Código Civil establece que para que sea valido un contrato de compraventa de un bien inmueble es necesario que se realice mediante escritura pública[244] y sabemos que las escrituras públicas las expiden únicamente personas que están autorizados para ejercer el notariado[245] y por excelencia la persona que está facultada para ello es el notario, por lo tanto todos aquellos contratos que pueden perfectamente realizarse mediante

[244] Articulo 1605 inciso segundo del Código Civil.
[245] Artículo 255 del Código Civil.

contratación electrónica pero que la ley le exige que se tengan que realizar en escritura pública únicamente el notario podrá intervenir.

Ahí recae la problemática para nuestro país, ya que mundialmente, específicamente en Europa donde se aplica mas esta figura, su legislación ha sido adecuada para que el notario actué de esa manera, pero en nuestro país aun no se hace ni siquiera mención del tema, siendo que la contratación electrónica cada día está avanzando mas, por lo que se hace necesaria la implementación de dicha legislación que venga a regular tanto la contratación electrónica, la firma electrónica o digital y por consiguiente la intervención del notario como la nueva figura del ciber notario.

5.2.6 Ejemplo Práctico de la Función del Ciber Notario.

En el siguiente supuesto una persona quiere comprar una inmueble en otro país y decide (por conveniencia) hacerlo por medio de contratación electrónica y se le hace necesario los servicios de certificación y notariales de un ciber notario, en el que podemos observar las funciones de Proveedor de servicios de certificación, porque el brinda al usuario los certificados digitales y la firma digital, así como las funciones ciber notariales de autenticación de identidad y certificación de fecha y hora.

1) Tony quien se encuentra residiendo en Inglaterra, realiza una compraventa de un inmueble en Orlando, Florida pero le es imposible comparecer a firmar todos los documentos personalmente, en este Estado se ha adoptado el sistema en el que la transmisión de una casa se puede hacer mediante contratación electrónica, con la formalidad de que debe ser firmados digitalmente y autenticado por un ciber notario.

2) Tony ya se ha puesto de acuerdo con los propietarios de la casa, se han hecho casi todos los trámites de pagos de impuestos y de servicios de agua, energía electrónica, y las compañías le han enviado a Tony todos los documentos por Email firmados solo electrónicamente, pensando Tony que sería suficiente.

3) Tony entonces concreta una cita con Bill, un ciber notario de Londres, y deberá ir a su oficina para firmar los documentos ante él, ya que el ciber notario solo acepta autenticar los documentos si ve a Tony personalmente, porque Bill no tiene la seguridad de que esos documentos han sido firmados por Tony, además que solo han sido firmados electrónicamente siendo necesario que sean firmados digitalmente.

4) Tony se presenta llevándole todos los documentos, por lo que Bill le asigna sus pares de claves, porque Bill tiene un programa de computadora que con el que puede generar las claves asimétricas y con ello la firma digital de Tony y a la vez le otorga los certificados digitales para comprobar la identidad de las claves. Si se diera el caso que Tony o cualquier otra persona no tiene los documentos listos o necesita del ciber notario para redactarlos éste deberá ser capaz de hacerlo porque, después de todo, es un abogado además de un ciber notario.

5) Tony firma los documentos y ya firmados Bill los autentica poniendo una razón al documento que dice que ha sido firmado por Tony y que le ha leído el documento explicándole su valor y las consecuencias legales entre otras formalidades.

6) Bill entonces firma el documento con su Firma Digital Oficial, asignada exclusivamente a él por la Asociación de Ciber Notarios, para firmar y autenticar el documento y el certificado y para encriptar el documento.

7) Una vez que han sido completados los documentos, Bill los guarda en su libro de protocolo electrónico, en el que solo el Ciber Notario tiene acceso siendo estos los documentos que son considerados como originales.

8) Bill le entrega una copia de los documentos en un CD, junto con la copia del certificado digital de las claves, para que puedan ser presentados al registro para los efectos legales correspondientes que son el de registrar el inmueble.

Otro supuesto es cuando ambas parte le solicitan al notario electrónico que participe en un determinado contrato electrónico, para darle fe al mismo, en ese caso el procedimiento sería el siguiente:

1) José y María son dos personas que quieren contratar electrónicamente, José vive en Estados Unidos y María en España. María es propietaria de un inmueble y envía la oferta por Internet para venderlo, entonces José la acepta, pero establecen que para más seguridad de ambos contrataran a un Ciber notario que es Eduardo que también vive en Estados Unidos, pero en otro estado que José.

2) Le envían a Eduardo por correo electrónico la solicitud de que participe en el contrato para darle fe, y acepta. Les pide que le envíen toda la documentación (los certificados electrónicos obtenidos por una entidad certificadora, con el que se verifica la identidad de ambos) y la relación de los hechos, es decir el contrato que desean realizar, el objeto que se desea

vender con todas las especificaciones y demás documentos que se requieren para la venta.

3) Después de que le envían los documentos, Eduardo los revisa y verifica que sean legales y que todo esté en orden y redacta el documento electrónico que servirá de contrato.

4) Cuando ha redactado el documento, Eduardo lo firma digitalmente y lo envía a José y a María, quienes lo reciben, desencriptan y lo revisan para constatar que todo está correcto, expresan su consentimiento con el documento y lo envían de regreso a Eduardo, firmado digitalmente.

5) Cuando Eduardo recibe el documento firmado por ambas partes, comprobando que las partes han aceptado el mismo, certifica la hora y el día de la realización del contrato, así como que las partes son totalmente capaces de realizar dicho contrato, también certifica todo el procedimiento que realizó (el envío y el recibimiento de ambas partes del contrato y la aceptación y reenvío del mismo). También establece una clausula de confidencialidad, es decir que el está obligado a no divulgar los datos que le fueron proporcionados.

6) Después de realizado el contrato y de la certificación que ha hecho Eduardo entonces, cierra el documento con una razón y lo envía a ambas partes a manera de testimonio. Eduardo entonces, almacena el documento electrónico en su protocolo electrónico, para su posterior consulta.

Podemos ver que estos son dos supuestos que se pueden presentar en la función de un ciber notario, en primer lugar cuando es solo una persona la que solicita sus servicios, que en ese caso podrá ir hacia la oficina del

notario o enviarle un correo electrónico, y en este caso vemos que el notario (Billy) tiene funciones de un proveedor de servicios de certificación ya que le brindo el certificado electrónico que amparaba la identidad de Tony y sus firma digital; y la segunda es cuando ambas partes le envían una solicitud por medio de correo electrónico para que participe en el contrato, donde a diferencia de la anterior el ciber notario solo tiene funciones de notario, no asi de proveedor de servicios de certificación.

Como conclusión podemos decir que en nuestro país aún falta mucho para llegar a presenciar al ciber notario, que firme los documentos. Ya que no se tiene la suficiente legislación para amparar su participación.

CAPITULO VI

ANÁLISIS DE RESULTADOS DE LA INVESTIGACIÓN DE CAMPO

SUMARIO: *Introducción. 6.1 Encuestas; 6.1.1 Procedimiento para la Obtención de la Muestra; 6.1.2 Resultado de la Investigación; 6.2 Entrevistas; 6.2.1 Entrevista con el Licenciado Elí Sigfredo Valle Flores. Asesor Jurídico del Despacho del Ministerio de Economía. Fecha 23 de enero de 2009; 6.2.2 Entrevista con la Licenciada Rubenia Moran, del Departamento de Atención al Usuario de la Aduana Terrestre de San Bartolo en Ilopango. Fecha 16 de febrero de 2009.; 6.2.3 Entrevista con la Doctora Yesenia Granillo de Tobar, Docente de la Cátedra de Derecho Civil, de la Escuela de Economía y Negocios "ESEN". De fecha 17 de Febrero de 2009.*

Introducción:

Para la investigación de campo se utilizaron dos métodos que fueron las encuestas y las entrevistas a informantes claves, para las encuestas se consultaron a 100 abogados y notarios y para las entrevistas se consultaron a tres personas, las cuales se detallan a continuación.

6.1 Encuestas

Para el desarrollo de nuestra tesis fue necesario hacer una investigación de campo que consistió en encuestas dirigidas a los abogados y notarios de la República, en la que se utilizo una muestra de 100 abogados y notarios, escogidos al azar, y los resultados de esa investigación se exponen a continuación:

6.1.1 Procedimiento para la Obtención de la Muestra.

La muestra se tomo según la fórmula:

$$N = \frac{Z^2 pq}{E^2}$$

En Donde	*Y Sustituyendo Los Valores*
N= a la muestra Z= nivel de confianza P= se refiere a la variabilidad del fenómeno estudiado Q= “”” E= la precisión con la que se generalizan los resultados	N= a la muestra Z= 0.838 (valor de curva normal 1.40) P= 0.50 Q= 0.50 E= 0.07

Procedimiento:

1. Sustitución de los valores de la formula.

N= $\underline{(1.40)^2 (0.5) (0.5)}$

$(0.07)^2$

2. Valor de 1.96 se potencio al cuadrado.

N= $\underline{(1.96) (0.5) (0.5)}$

$(0.07)^2$

3. Se multiplica con las variables.

$$N = \frac{0.98\ (0.5)}{(0.07)^2}$$

4. El resultado de Z con las variables se divide con E el cual antes se potencia al cuadrado el cual se divide para sacar el número de muestra.

$$N = \frac{0.49}{0.0049}$$

N= 100

5. N es el tamaño de la muestra de las encuestas que se pasara a los abogados y notarios de la República de El Salvador.

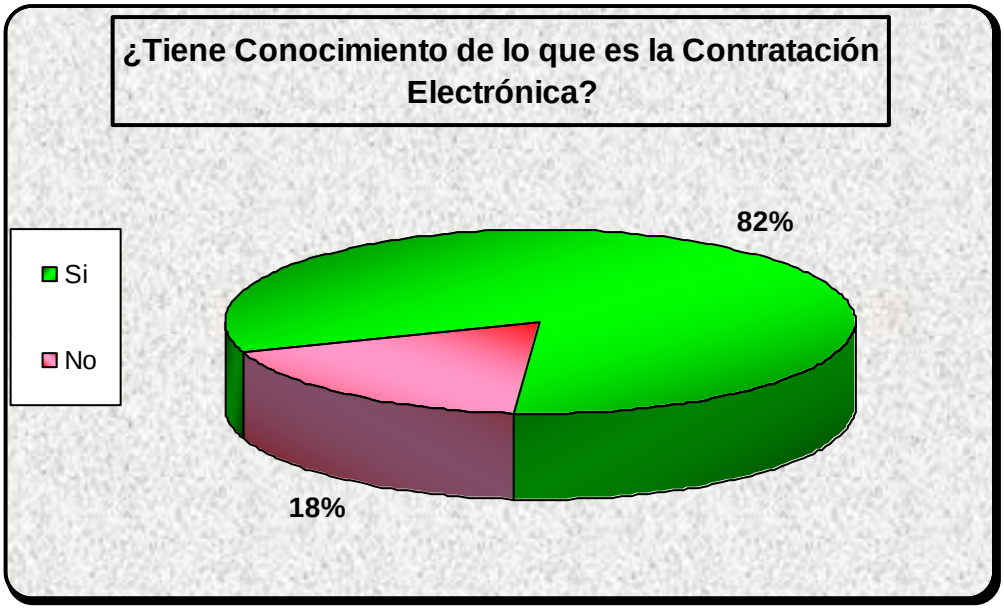
N= 100

6.1.2 Resultado de la Investigación.

A continuación se analizan los resultados de la encuesta que se realizo a cien abogados y notarios, sobre el conocimiento que tienen de la contratación electrónica, el comercio electrónico y se sometió a consideración si es necesaria la intervención del notario en la contratación electrónica en El Salvador.

1. ¿Tiene Conocimiento de lo que es la Contratación Electrónica?

Respuesta.	Nº de Encuesta	Porcentaje
Si	82	82%
No	18	18%
Total:	100	100%

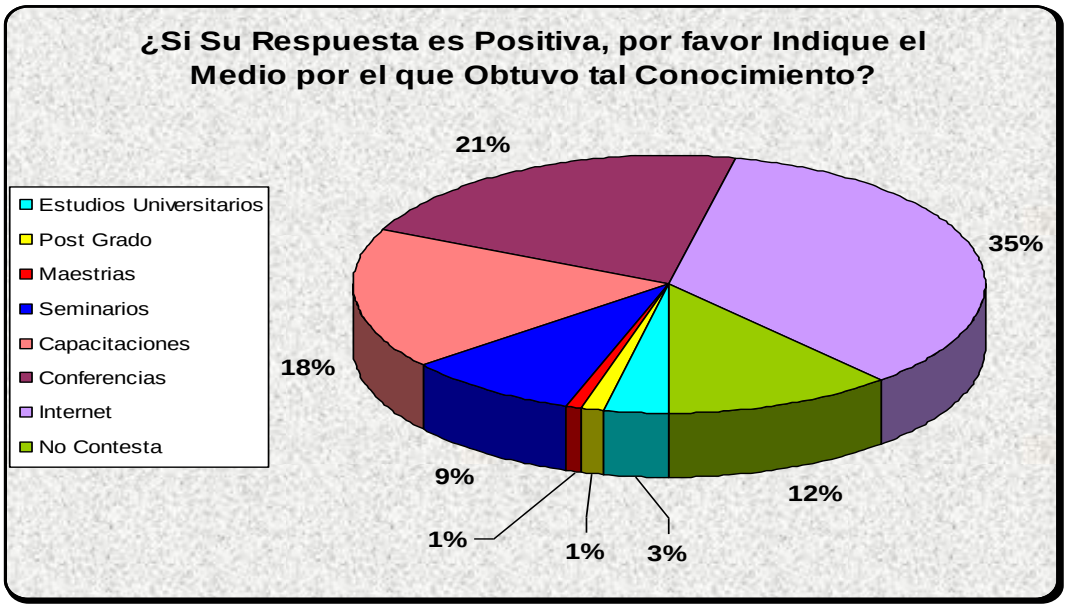


Análisis:

En el presente grafico podemos ver que la tendencia es que de los cien abogados y notarios que fueron consultados el 82 por ciento dice que tiene algún conocimiento de la Contratación Electrónica, por lo menos alguna noción de ella, en contraposición al 18 por ciento que dice desconocer totalmente del tema. Es decir que entonces la mayoría de abogados y notarios conocen ya de la contratación electrónica.

2. Si su Respuesta es Positiva por favor Indique el Medio por el que obtuvo tal Conocimiento.

Nº	Opciones	Número	Porcentaje (%)
1	Estudios Universitarios	5	3.25
2	Post Grado	2	1.30
3	Maestrías	1	0.65
4	Seminarios	14	9.09
5	Capacitaciones	27	17.53
6	Conferencias	33	21.43
7	Internet	54	35.06
8	No Contesta	18	11.69
	Total	154	100

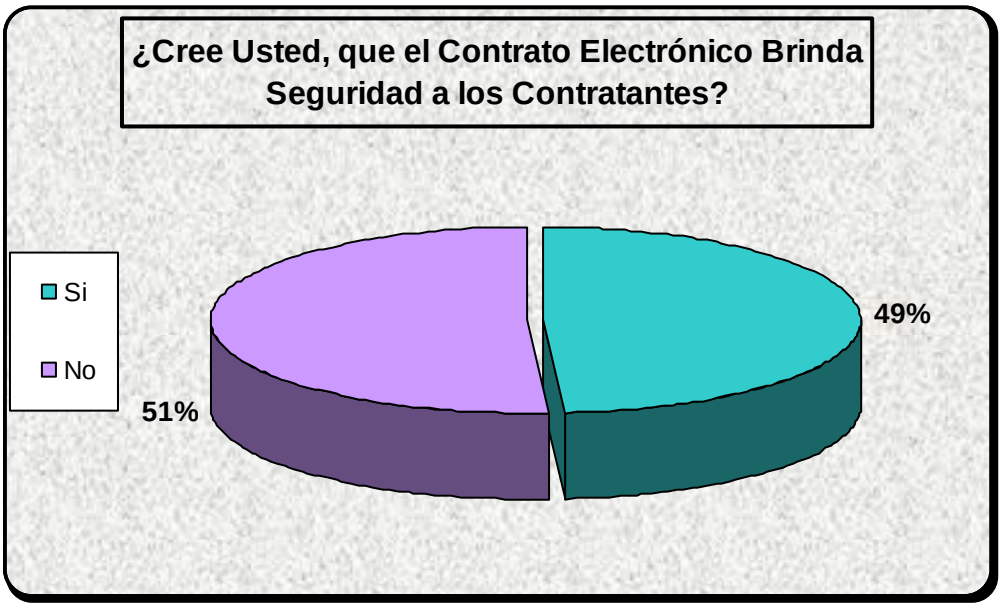


Análisis:

Podemos ver que en este grafico el porcentaje mayor de los medios es el Internet, eso demuestra que aun no existe la suficiente capacitación de los abogados y notarios, siendo ese conocimiento inseguro ya que no se puede confiar en todo lo que se carga en la Web, por lo que se debería de dar más prioridad a los estudios universitarios, maestrías, y capacitaciones.

3. ¿Cree usted que el Contrato Electrónico brinda Seguridad Jurídica a los Contratantes?

Respuesta.	*Nº de Encuesta*	*Porcentaje*
Si	49	49%
No	51	51%
Total:	100	100%

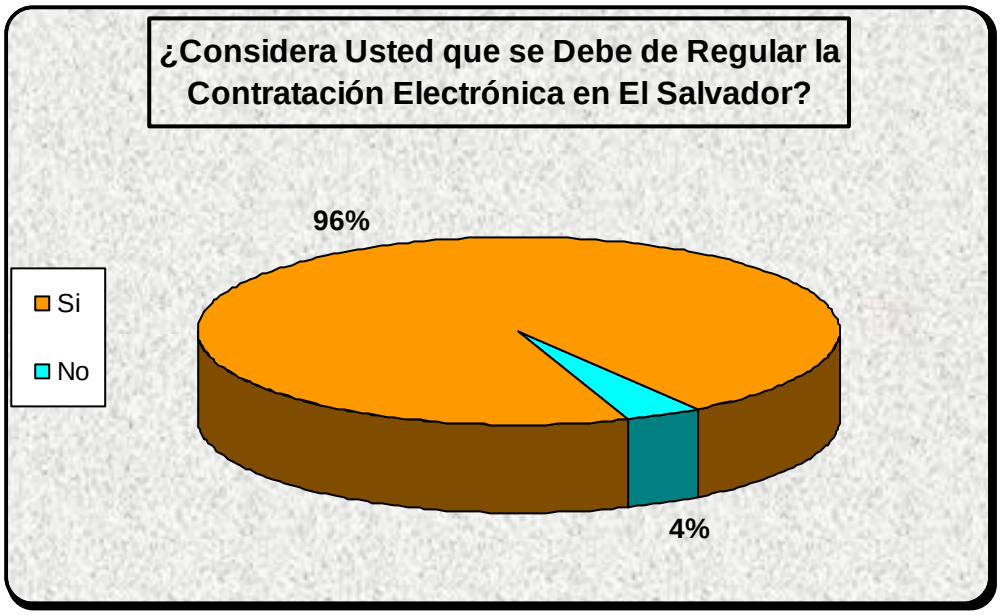


Análisis:

Podemos observar en este grafico que un 51 por ciento de los profesionales encuestados manifiestan que el contrato electrónico no brinda seguridad jurídica a los contratantes, y el 49 por ciento manifiesta que si lo hace, eso nos demuestra que el contrato electrónico en sí mismo no es suficiente para que las personas que contratan de esta forma tengan asegurados sus derechos.

4. ¿Considera usted que se debe de Regular la Contratación Electrónica en El Salvador?

Respuesta.	Nº de Encuesta	Porcentaje
Si	96	96%
No	4	4%
Total:	100	100%

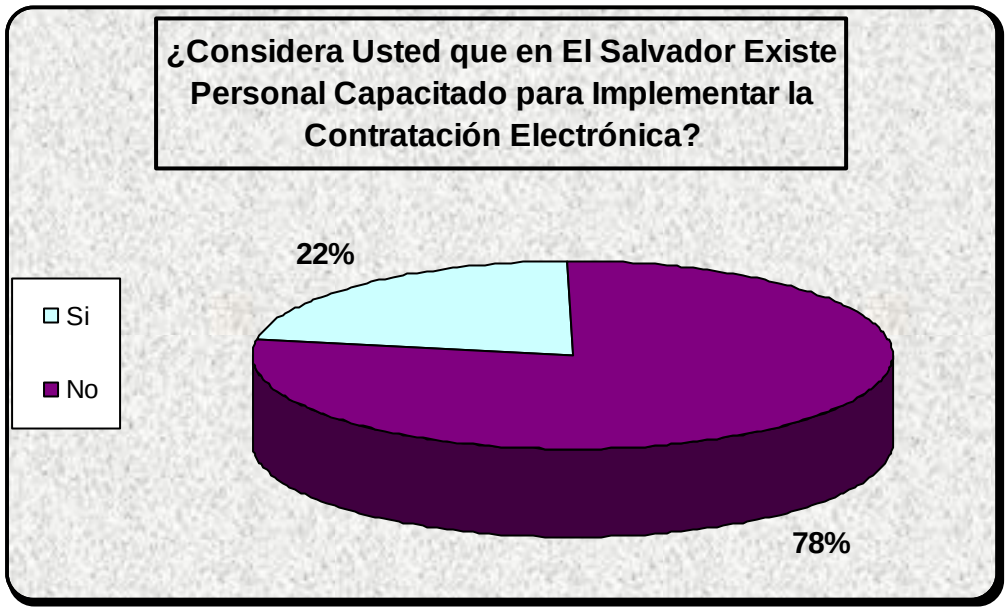


Análisis:

En este grafico se refleja la necesidad de que se regule la contratación electrónica en nuestro país, ya que un 96 por ciento de los encuestados nos respondió que si se debe regular y el 4 por ciento que no. Por lo que las institución encargadas de velar para que se cumplan las condiciones mínimas para dar seguridad en las transacciones electrónicas.

5. ¿Considera que en El Salvador existe Personal Capacitado para Implementar la Contratación Electrónica?

Respuesta.	*Nº de Encuesta*	*Porcentaje*
Si	22	22%
No	78	78%
Total:	100	100%

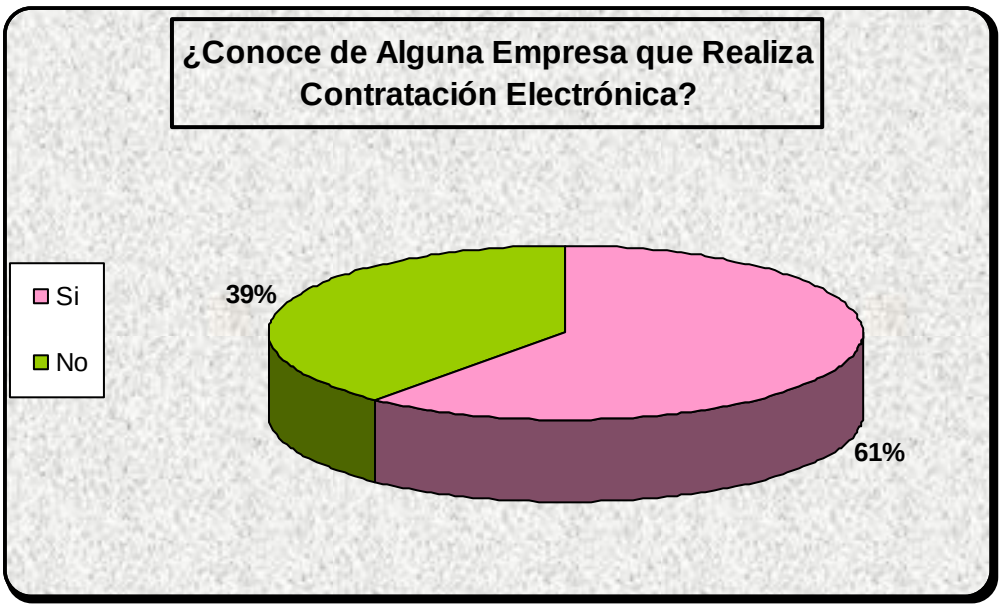


Análisis:

En esta pregunta se demuestra que el 78 por ciento de los encuestados consideran que en nuestro país no existe personal capacitado para que se implemente la contratación, es decir que no existe una capacitación de las personas sobre la contratación electrónica, y que el 22 por ciento de los encuestados opinan que si existe personal capacitado.

6. ¿Conoce de alguna Empresa que realiza Contratación Electrónica?

Respuesta.	Nº de Encuesta	Porcentaje
Si	61	61%
No	39	39%
Total:	100	100%

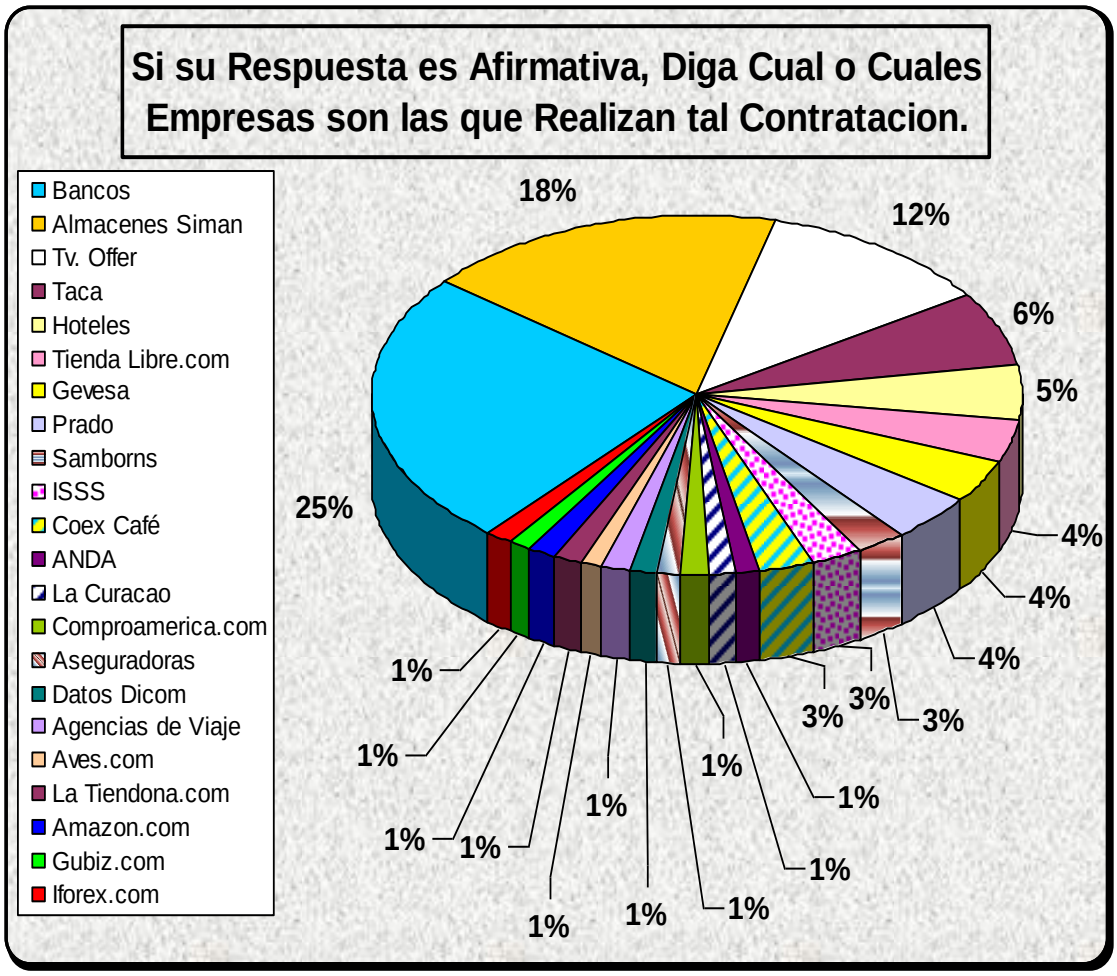


Análisis:

En la presente interrogante podemos observar que un 61 por ciento de los abogados y notarios encuestados respondió que si conoce de empresas que realizan comercio por medio de Internet, y un 39 por ciento manifestó que no conocen de ninguna empresa que realice contratación electrónica.

7. ¿Si su Respuesta es Afirmativa, diga cual o cuales Empresas son las que Realizan tal Contratación?

Empresas	Nº	Porcentaje
Bancos	19	25 %
Almacenes Simán	14	18 %
Tv Offer	9	12 %
Taca	5	6 %
Hoteles	4	5 %
Tienda Libre.com	3	4 %
Gevesa	3	4 %
Prado	3	4 %
Samborns	2	3 %
ISSS	2	3 %
Coex Café	2	3 %
ANDA	1	1 %
La Curacao	1	1 %
Comproamerica.com	1	1 %
Aseguradoras	1	1 %
Datos Dicom	1	1 %
Agencias de Viaje	1	1 %
Aves.com	1	1 %
La Tiendona.com	1	1 %
Amazon.com	1	1 %
Gubiz.com	1	1 %
Iforex.com	1	1 %
Total	77	100 %



Análisis:

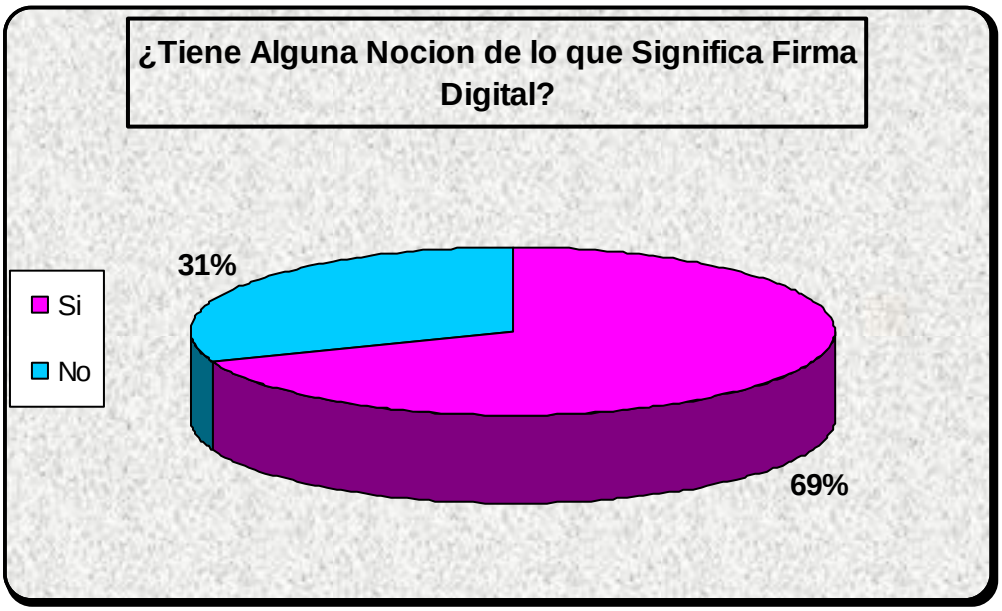
Primero debemos aclarar que 64 personas no contestaron esta pregunta aunque sabían de empresas que comercializan por medio de Internet, ya que en el momento de realizar la encuesta no recordaban cuales empresas tenían página de Internet donde se comercializa, por lo que el análisis se hace con 36 personas que si contestaron, lo que tomamos como el 100 por ciento.

Podemos observar que en este grafico el 25 por ciento de los encuestados manifestaron que los bancos son los que brindan servicios de contratación electrónica, en segundo lugar se encuentra la empresa de Almacenes Simán con el 18 por ciento, en tercer lugar se encuentra TV. Offer con un 12 por ciento, las Aerolíneas Taca se encuentra en un cuarto lugar con 6 por ciento de los encuestados, los hoteles se manifiestan con un 5 por ciento, con el 4 por ciento de los encuestados se encuentran Tienda Libre.com, Gevesa y Prado, con el 3 por ciento de los encuestados se encuentran Samborns, ISSS y Coex Café; y las empresas ANDA, La Curacao, Comproamerica.com, Empresas Aseguradoras, Datos Dicom, Agencias de Viaje, Aves.com, La Tiendona.com, Amazon.com, Gubiz.com, e Iforex.com son las menos conocidas que realizan contratación electrónica ya que todas están en un 1 por ciento de los encuestados.

Es decir que estos son los que son más conocidos por las abogados y notarios que realizan contratación electrónica, eso demuestra que hace falta más información y capacitación ya que existen muchas más empresas que realizan contratación electrónica. Podemos ver que el rubro de servicios es el más utilizado para las contrataciones electrónicas, estando como vemos los bancos realizando la mayoría de las transacciones electrónicas en el país.

8. ¿Tiene alguna Noción de lo que Significa Firma Digital?

Respuesta.	Nº de Encuesta	Porcentaje
Si	69	69%
No	31	31%
Total:	100	100%

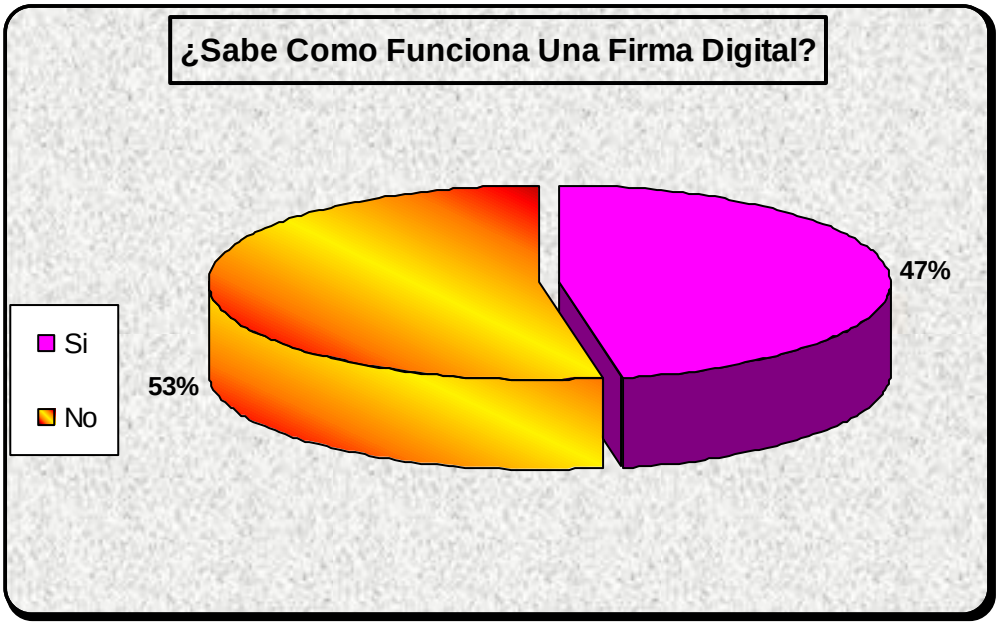


Análisis:

En esta interrogante podemos observar que de los abogados y notarios que fueron encuestados el 31 por ciento dijo no tener ninguna noción de lo que es la firma digital, y un 69 por ciento dijo que si conocía de esta firma, o por lo menos tenía alguna noción de que significa. Podemos ver que no existe un total desconocimiento de la figura de la firma electrónica necesitando una mayor capacitación para su utilización.

9. ¿Sabe cómo Funciona una Firma Digital?

Respuesta.	Nº de Encuesta	Porcentaje
Si	47	47%
No	53	53%
Total:	100	100%

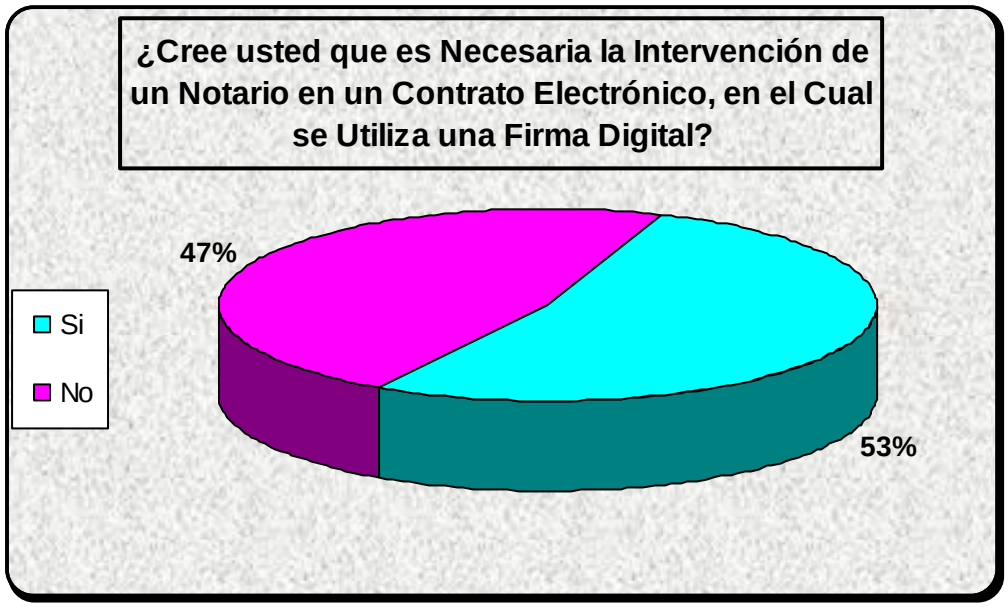


Análisis:

Esta interrogante se relaciona con la anterior, y nos demuestra que el conocimiento que los abogados tienen de la firma digital es vago ya que el 53 por ciento nos dijo que no sabe cómo funciona aunque sabe que significa, por lo que se reitera la necesidad de una mayor capacitación. Y un 47 por ciento dijo saber cómo funciona la firma digital.

10. ¿Cree usted que es Necesaria la Intervención de un Notario en un Contrato Electrónico, en el cual se utiliza una Firma Digital?

Respuesta.	Nº de Encuesta	Porcentaje
Si	53	53%
No	47	47%
Total:	100	100%

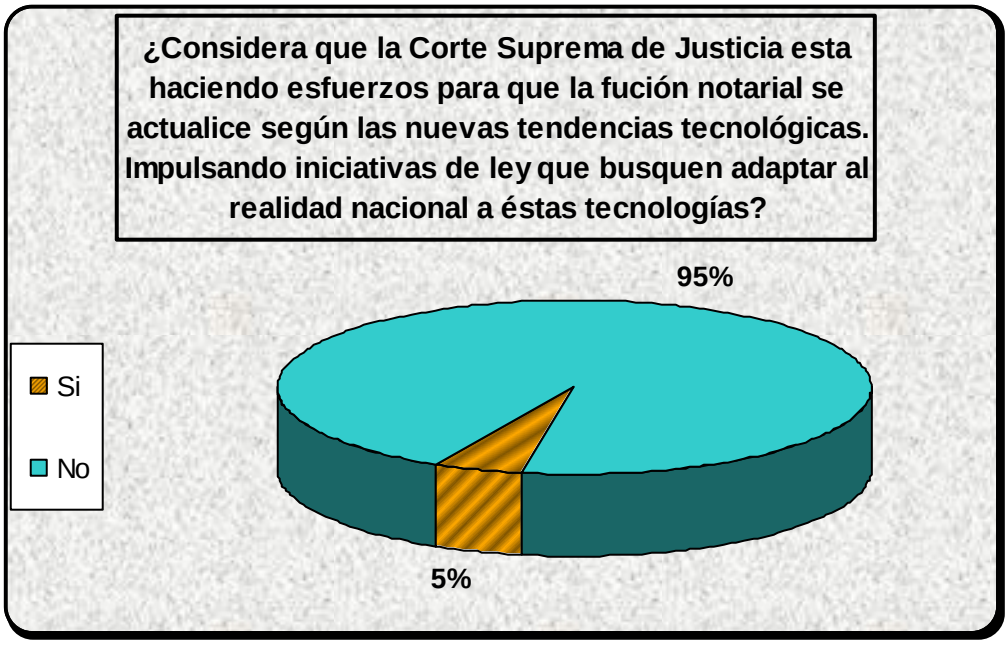


Análisis:

Esta interrogante era crucial para nuestro tema ya que establecía si es o no necesario la intervención del notario en la contratación electrónica, el 53 por ciento de los encuestados nos dijo que si sería necesaria por la falta de seguridad jurídica que brinda el mismo. Y un 47 por ciento de todos los encuestados manifiestan que no es necesaria la intervención del notario en la contratación electrónica.

11. ¿Considera que la Corte Suprema De Justicia está haciendo Esfuerzos para que la Función Notarial se actualice según las Nuevas Tendencias Tecnológicas. Impulsando iniciativas de ley que busquen adaptar la Realidad Nacional a estas Tecnologías?

Respuesta.	Nº de Encuesta	Porcentaje
Si	5	5%
No	95	95%
Total:	100	100%

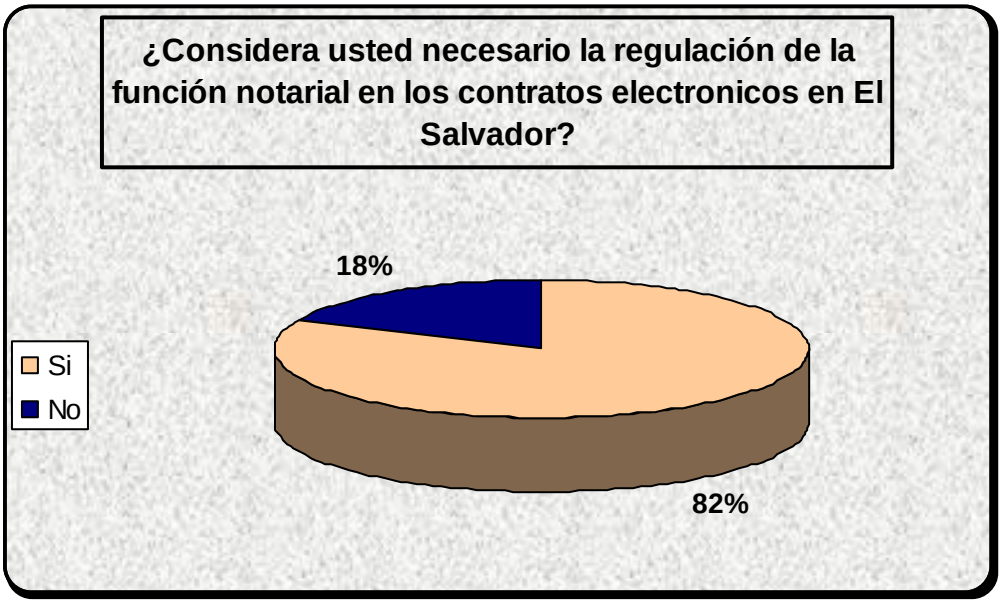


Análisis:

Podemos ver que en este grafico el 95 por ciento de los encuestados están de acuerdo en que la corte suprema de justicia, como ente encargado de la actualización de los notarios, no está realizando ninguna acción para ello en oposición al 5 por ciento que manifiestan que si lo está haciendo.

12. ¿Considera usted Necesario la Regulación de la Función Notarial en los Contratos Electrónicos en El Salvador?

Respuesta.	Nº de Encuesta	Porcentaje
Si	82	82%
No	18	18%
Total:	100	100%



Análisis:

En esta interrogante podemos observar que el 82 por ciento de los encuestados consideran que es necesario que se regule la función notarial en la contratación electrónica, ya que no puede intervenir el notario sin una buena regulación que proteja esa intervención y los derechos de los contratantes. El 18 por ciento contesto que no es necesario.

6.2 Entrevistas

Otro de los métodos que se utilizaron para el desarrollo de la investigación de campo fue el de la técnica de investigación denominada *Entrevista Estructurada O Dirigida*, la que consiste en entrevistar a ciertos informantes claves, llamados así por encontrarse en la posición de poder brindar información sobre temas que otras personas no conocen, en este sentido las entrevistas fueron dirigidas a tres instituciones, en primer lugar al Ministerio de Economía, consultando al Licenciado Elí Sigfredo Valle Flores, en segundo lugar en la Aduana Terrestre de San Bartolo, en el Departamento de Atención al Usuario, consultando a la Licenciada Rubenia Moran; y en tercer lugar a la Escuela de Economía Y Negocios "ESEN", consultando a la Doctora Yesenia Granillo de Tobar. Los resultados de dichas entrevistas se analizaran a continuación:

6.2.1 Entrevista con el Licenciado Elí Sigfredo Valle Flores. Asesor Jurídico del Despacho del Ministerio de Economía. Fecha 23 de enero de 2009

La entrevista del licenciado Elí Sigfredo Valle, fue diferente a las otras dos entrevistas, ya que al licenciado únicamente se le hicieron las interrogantes sobre la Ley de Comercio Electrónico y la Ley de Comunicación y Firma Electrónica, y no se utilizo cuestionario estructurado, sino mas bien las preguntas fueron espontáneas.

En primer lugar se le hizo la pregunta que si tenía conocimiento de la Ley de Comercio Electrónico, y el contesto que tenía conocimiento, pero que

lamentablemente esta ley solo se había quedado en primer borrador, ya que ya nunca se le volvió a dar seguimiento y no paso ni a la Secretaría Técnica de la Presidencia que es donde envían los borradores para ser estudiados y decidir si son enviados a la Asamblea Legislativa para que se discutan y puedan ser leyes de la República. También explicaba que para él la Ley de Comercio Electrónico, no es necesaria que tal vez sea útil para regular el comercio, pero que no es necesaria y seria más necesaria una ley de Firma Electrónica.

Después al licenciado Valle se le hizo la interrogante que si todos estos proyectos de leyes son producto de los tratados de libre comercio que se implementaron en nuestro país, a lo que nos respondió que no solo es el TLC, que eso también influyo pero no fue lo determinante, ya que todavía seis años antes ya existía un borrador, solo que aun no se había dado a conocer, ni mucho menos en ese entonces era necesario, solo era porque se estaba proliferando la utilización de la informática y empezando a surgir la necesidad, surgió además por la globalización, la utilización de la figura de los contratos entre ausentes y el desarrollo de la tecnología, entonces no fue el detonante el TLC, pero si fue influyente.

Se le cuestiono que si había otra ley, que se estuviera estudiando, y él respondió que sí, que era la Ley de Comunicación Y Firma Electrónica, que es la que actualmente se está impulsando en el ministerio, y que precisamente él es uno de los que la está estudiando, que es mucho más necesaria que una ley de Comercio Electrónico, por el avance de la tecnología se vuelve más necesario para darle validez a los contratos.

También se le cuestionó sobre el artículo 10 de la mencionada ley de Comunicación y Firma Electrónica, ya que menciona que la función notarial

en la contratación electrónica, se deberá regular en una ley especial[246], si se estaba estudiando o se había creado una ley para eso, y manifestó que no, que ese artículo únicamente se ha dejado así como un recordatorio, como una tarea para los que están encargados de ello, lo hagan, es decir que entonces a la Corte Suprema de Justicia, le compete crear una iniciativa de ley que regule tal situación, y es la Corte porque constitucionalmente ella es la que tiene la potestad de hacerlo, por lo tanto no se está estudiando ni si quisiera la idea de hacer una ley que regule la función notarial en el comercio electrónico.

6.2.2 Entrevista con la Licenciada Rubenia Moran, del Departamento de Atención al Usuario de la Aduana Terrestre de San Bartolo en Ilopango. Fecha 16 de febrero de 2009.

Una segunda entrevista fue la efectuada en la Aduana Terrestre de San Bartolo en Ilopango, en el Departamento de Atención al Usuario, donde se consulto a la Licenciada Rubenia Moran, personal de atención al usuario, a la que se entrevisto con un cuestionario impreso de ocho preguntas[247], a las cuales fue bastante concisa en responder. El análisis de sus respuestas se expresa a continuación:

[246] PROYECTO FINAL DE LEY DE COMUNICACIÓN Y FIRMA ELECTRÓNICA
Documentos auténticos y públicos emitidos en soportes electrónicos
Art. 10.- Los documentos auténticos podrán estar contenidos en soporte electrónico y tendrán el valor asignado por el ordenamiento legal para esta clase de documentos.
Los documentos públicos electrónicos que se refieran al ejercicio de la función notarial se regularán en una ley especial.
[247] Ver ANEXO IV

La **pregunta numero uno** era ¿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?

Su respuesta fue “que anteriormente todos los tramites se hacían manualmente, es decir que eran grandes formularios, que debían de llenarse a mano o a máquina, pero siempre iban impresos, lo que generaba dificultades como la de que los usuarios debían conocer mucho el sistema arancelario, todas se realizaban con diferente método”, es síntesis explico que todo el sistema anterior, era engorroso y bastante lento ya que como se tenía que realizar a mano, y cerciorarse de todos los aranceles y requisitos.

La **pregunta número dos,** se refiere al funcionamiento del sistema actual implementado por la Ley de Simplificación Aduanera, a lo que ella respondió que todo el procedimiento estaba en la ley y no quiso hacer alusión a ello, nos dijo que eso estaba en la legislación.

La **pregunta número tres,** se refería a si consideraba que el nuevo sistema hace más ágiles los trámites realizados en las aduanas. En síntesis la Licenciada Moran respondió que “claro que sí”, y explicaba que como lo mencionaba en la primer pregunta, antes era más lento todo el tramite, pero ahora ya no es necesario que los usuarios conocieran todo el arancel, ya que existe el arancel electrónico, y ahora todo está en línea, los requisitos, los formularios, toda la información, está en la Web, y desde la pagina Web los usuarios pueden hacer uso de su pin, y acceder a la información.

La **pregunta número cuatro,** iba dirigida al sistema que utilizan para identificar a la persona que hace uso de la declaración de mercaderías, y nos explicó que para que una persona pueda hacer uso del sistema debe tener

un password, que es una contraseña, para poder entrar, y esa contraseña se la dan después de una solicitud que presenta la persona, es decir la persona que quiere hacer uso del sistema, y se le da una resolución para ello, de parte de la Dirección General de Aduanas, entonces es en esa resolución que le dan el password, que es completamente personal, y nos ponía un ejemplo, si una empresa X tiene su password pero subcontrata a otra y quiere que realice el tramite con su password, el sistema lo bloquea y aparece como no existente, porque cada password es personal y no hay dos contraseñas iguales, por lo tanto no puede la empresa subcontratada acceder al sistema con la contraseña de la otra empresa que lo subcontrato, es así como controlan a las personas, por el password que le entregan a la persona (sea natural o jurídica) que únicamente lo puede utilizar esa persona.

La **pregunta número cinco,** se refiere a cual es el método que utilizan para asegurarse de que la información intercambiada no ha sido alterada en el proceso de envío, y explico que, así como para identificar a una persona, en el sistema cuando la persona utiliza su clave para ingresar, también utiliza ciertos códigos, (ya que todo está codificado), para llenar los formularios del sistema de Teledespacho, ahí tiene que colocar según la mercadería el código correspondiente y la cantidad que va a introducir al país, y lo envía a la aduana, pero si al llegar a la aduana, la cantidad, el peso o cualquier otra característica de la mercadería varia de la que está declarada en el sistema, entonces lo retienen y tiene que resolver el problema, y le acarrea pagos de almacenaje.

La **pregunta número seis** decía de la siguiente manera: Según su experiencia, ¿considera que la firma electrónica es un medio idóneo para asegurar la información?, a lo que la licenciada contesto que SI, pero no solo

se necesita la firma electrónica, sino que también existen proyectos de modernización y mejora del sistema, y los marcos legales que se tienen, se necesitan todo eso para asegurar toda la información.

La **pregunta número siete,** decía de la siguiente manera: Según su experiencia, ¿cree usted que sería factible que un notario electrónico sea el que de fe de esa información?, en el sistema actual, la firma electrónica y los marcos legales no se necesitan los notarios, el sistema ha trabajado así desde hace tiempo y nunca se ha necesitado de un notario para trabajar.

La **pregunta número ocho,** se refiere a la consideración de que si es necesaria una ley que regule exclusivamente la intervención de un notario y la utilización de una firma electrónica, a lo que ella respondió que no, porque en primer lugar no son necesarios los notarios en la aduana, y además que ya existe suficiente marco legal, que regule el Teledespacho y la firma electrónica, porque tenemos el CAUCA (Código Aduanero Uniforme Centroamericano) y el RECAUCA (Reglamento de Aplicación del Código Aduanero Uniforme Centroamericano), y además la Ley de Simplificación Aduanera y las demás Leyes relacionadas con las cuestiones aduaneras y las directivas, ya es un marco legal suficiente, tal vez reformarlos para modernización pero ya no es necesario que se cree más.

6.2.3 Entrevista con la Doctora Yesenia Granillo de Tobar, Docente de la Cátedra de Derecho Civil, de la Escuela de Economía y Negocios "ESEN". De fecha 17 de Febrero de 2009.

El día diecisiete de febrero de 2009, se le hizo una entrevista a la Doctora Yesenia Granillo de Tobar, dicha entrevista se llevo a cabo por

medio de una cuestionario impreso que constaba de siete preguntas[248], las cuales la doctora iba contestando, el análisis de las respuestas es el que se expresa a continuación:

La **pregunta numero** uno consistió en preguntarle si consideraba que el Tratado De Libre Comercio con Estados Unidos es un factor que incide en que se regule la contratación por medios electrónicos, a lo que la Doctora respondió que si ya que en dicho tratado existe un capitulo que se refiere al comercio electrónico, que es el capitulo catorce, agregando que este comercio es un tema amplio referente a todos los estudios y tipos de contrataciones electrónicas y esto tanto entre privados, entre dos personas particulares entre sí, o la contratación que se hace a través de páginas Web.

Agrega la doctora que "este tratado al incentivar el comercio electrónico en el capítulo 14, se incentiva, es mas se invita a que los países centroamericanos participen del Comercio Electrónico, porque Estados Unidos es el país que primero inicio con la utilización del Comercio Electrónico y ya lo tiene implementado, es una de sus formas de contratar. Es así que a través del TLC se está potenciando, se invita a los países que lo desarrollen".

La **pregunta número dos,** se trato de que si creía que el contrato electrónico, en sí mismo, brinda seguridad jurídica a los contratantes, sin la necesidad de un notario, a lo que la doctora respondió que "Si y No", ya que el contrato electrónico puede perfectamente celebrarse sin la necesidad de un notario, siempre y cuando este firmado electrónicamente, con la firma electrónica, porque en la mayoría de países del mundo, inclusive en

[248] Ver anexo V

Centroamérica, Guatemala, Costa Rica ya tienen Ley de Firma Electrónica. “Entonces el contrato electrónico puede perfectamente firmarse electrónicamente y tener la misma validez que en que interviniera el notario, entonces usted puede presidir de ello. Sin embargo los contratos aquellos en donde hay exigencia de intervención de la función notarial, (exigencia porque la ley lo exige), no son susceptibles de poderse firmar electrónicamente, por lo menos hoy por hoy no. En otros países como Europa, España en todos esos países, ya se puede, porque el notario participa del uso de la firma electrónica, entonces se debe invitar al notario a que entre en otro ámbito de aplicación de regulación”.

La **pregunta número tres,** estaba referida que si es necesario que el notario intervenga, como garante de la autenticidad de los contratantes en un contrato electrónico. A lo que la doctora contesto “si es de aquellos contratos electrónicos que el notario firmara electrónicamente, la autenticidad la da el proveedor de servicios de certificación o entidad de servicio de certificación y no el notario, incluso en la ley de firma electrónica nuestra, que es la Ley de Simplificación Aduanera, que solo sirve para cuestiones de aduanas, pero se implementan todo lo de la firma electrónica, esta misma ley tiene un artículo en donde establece que la intervención de las entidades de certificación producen fe pública, la misma que produce un notario”. Agrega que “Lo que pasa es que esta ley hoy por hoy, no está diseñada para contratos, solo para trámites aduanales, pero en la misma ley provee la aplicación de otra ley que si regiría de forma general… y es solo para trámites aduaneros porque eso era lo que urgía en su momento, en 1992 que entro en vigencia se empezó a convencer a toda el mundo que sería bueno tener una ley de firma electrónica para todo, pero ahora que todo el mundo usa el Internet como medio de comunicación ya se vuelve más necesario hacerlo…”

Agrega también que en el nuevo código civil y mercantil ya habla de los contratos electrónicos, en él hay un artículo de los procesos para las obligación de hacer, en el que se establece que hay que presentar el contrato y que ese contrato debe estar firmado y añade que puede hacerse incluso por medio de otra firma que no sea la autógrafa.

La **pregunta número cuatro,** se refiere a las funciones que debería de realizar un notario que intervenga en un contrato electrónico, a la que ella responde que en los contratos en los que sea necesaria la intervención notarial las funciones de éste van a ser exactamente las mismas, "…el contrato no va a cambiar por el hecho de que este en un soporte electrónico, eso es parte de un principio de la contratación electrónica, que es el principio del no repudio, que dice que por el hecho de que esté contenido en un documento diferente que no sea papel, no se va a rechazar,… lo único es que nosotros estamos acostumbrados al papel, nosotros no tenemos una ley de uso del papel bond, pero si vamos a tener una ley del uso de medios electrónicos y porque es necesario porque nosotros no estamos acostumbrados a eso, pero al papel bond si,… entonces la intervención del notario será lo mismo dar fe de lo que hoy por hoy da fe, no mas."

La **pregunta número cinco,** se refiere a la necesidad de que se implemente una ley que regule el comercio, la firma digital y la intervención de un notario en estos. Y la respuesta de la doctora fue la siguiente: "pues definitivamente Si". Y agrego que para el nuevo ámbito de aplicación del comercio electrónico debe haber nuevas leyes pero a la vez deben ser regulados los tres ámbitos separadamente, ya que el comercio electrónico trata de contratación en sí, de contratos, tanto entre particulares como a través de la Web, y en nuestro país ya existen bastantes empresas que tiene su propia página Web, así como todos los bancos tienen servicios a través

de la Web, "…entre nosotros es un hecho que en El Salvador ya tenemos contratación electrónica, es un hecho. Lo que pasa es que no tenemos legislación, no se han preocupado los legisladores, porque no ha habido una explosión donde evidencie un problema", explico la doctora que tampoco se puede explotar el comercio electrónico al cien por ciento porque no se tiene una ley y la gente desconfía. Esto en cuanto al comercio electrónico, en cuanto a la firma electrónica o digital, manifestó que la misma es para cualquier tipo de documento, por lo que la legislación de la firma electrónica debe necesariamente ser separada del comercio electrónico, porque si la firma se regula junto al comercio, daría la idea que la firma es solo para comercio, cosa que no es así. Agrego que la mayor área de explotación de la firma es en lo llamado Gobierno Electrónico, en donde todos los servicios del Estado son colocados en línea, de donde los particulares pueden acceder a estos servicios a través de la firma digital.

En cuanto al notario, explico que es un área que ha sido explotada en Europa, ya que los notarios en España y los demás países europeos han conformado lo que ellos llaman como "Libro Blanco del Notariado Electrónico", es decir que ya existe intervención notarial a través de los medios electrónicos, lo mismo que si fueran entidades de certificación, pero en las áreas en las que por ley es exigido la intervención únicamente de notarios, se conserva de esa manera.

La **sexta pregunta,** se refiere a que si a consideración de la entrevistada en El Salvador hay suficientes medios para aplicar la figura del ciber notario. Y su respuesta fue un rotundo No, ya que con la legislación que tenemos actualmente no, y explico que "…de hecho en el anteproyecto de Ley de Comunicación Y Firma Electrónica tiene una propuesta de no regular nada del notariado electrónico, sin embargo se propone un artículo de que la

función notarial se iba a regular con una ley especial, pero se deja como una tarea, en la que tendría que ser la Corte Suprema de Justicia el ente encargado de emitir una ley especial, porque existe una reserva de ley", explico que lo que tiene mayor importancia es la regulación inmediata del comercio electrónico, del Gobierno Electrónico, porque ya se tiene.

Y la **pregunta número siete,** y con la que concluimos la entrevista estaba dirigida a si para ella existe suficiente marco legal que regule la contratación electrónica y la firma electrónica. A lo que respondió "no de forma completa, ya de la contratación ya se tiene el procedimiento para tutelarla, con el nuevo código civil y mercantil, ya de la firma electrónica se tiene todo lo necesario, pero el área es reducida", es decir no existe todavía un marco jurídico que regule expresamente el tema, solo existen artículos dispersos, tampoco existe un marco legal que tutele los derechos de los contratantes, es decir todavía hace falta mucho para considerar que se tiene un marco jurídico amplio.

CAPITULO VII

CONCLUSIONES Y RECOMENDACIONES

7.1 Conclusiones

Como grupo de trabajo y al haber realizado toda la investigación de la necesidad de un marco legal que venga a regular la intervención del notario en la contratación electrónica, hemos llegado a las siguientes conclusiones:

1) El comercio electrónico significa una gran ventaja, para el tráfico comercial actual, ya que a través de la red sus transacciones se realizan en cuestión de segundos, lo que beneficia a los comerciantes al disminuir los costos de una contratación a distancia.

2) El documento electrónico cumple con los requisitos como un documento en soporte en papel en el sentido de que contiene un mensaje (texto alfanumérico o grafía) y lo convierte en lenguaje convencional (el texto se convierte en bits) que esta sobre un soporte que puede ser permanente o volátil, destinados a durar en el tiempo. Así el contrato que tiene su base en un documento electrónico tiene la misma validez y eficacia que tiene un documento tradicional en papel, debidamente firmado.

3) Que la firma digital cumple la misma función que realiza una firma autógrafa en legitimar a las partes que intervienen en un contrato electrónico así como su contenido y que aun la firma digital es un medio más seguro que una firma autógrafa.

4) El ciber notario será capaz de llevar a cabo la función de un notario tradicional en un sistema como el nuestro, confirmando su intervención en ciertos actos jurídicos a fin de certificar que ese acto es completamente valido entre las partes, poniendo cuidado en cumplir con las formalidades del procedimiento y de su contenido.

5) Que en nuestro país a medida que la globalización se vuelve un concepto mucho más amplio y a la par se hace más visible el desarrollo tecnológico y con ello el uso masivo del Internet, hace que el comercio electrónico sea un ámbito utilizado por muchas personas para comerciar productos de forma más rápida y ágil, lo que hace que sea necesario que se reformen la legislación actual salvadoreña y que se adecuen para la incorporación del notario en contratos electrónicos.

7.2 Recomendaciones

Como grupo de trabajo, en base a las conclusiones anteriores y a la investigación hecha, establecemos las siguientes recomendaciones:

1. Recomendamos a la Asamblea Legislativa que en conjunto con la Corte Suprema de Justicia, cumpla a brevedad posible, con la aprobación de la Ley de Comunicación y Firma Electrónica el cumplimiento del artículo diez de la misma, dando paso a una ley especial de regulación de la función notarial electrónica.

2. Recomendamos a las Universidades y en especial a la Universidad De El Salvador, para que en sus planes de estudio integren temas acerca de comercio electrónico, firma digital y cibernotario, y todo lo que

implica para que cuando los alumnos sean profesionales puedan ser más competitivos en la vida laboral por el masivo avance tecnológico actual, así como que creen programas de maestrías sobre el tema.

3. Recomendamos a la Asamblea Legislativa, hacer una reforma de ley profunda a la Corte Suprema de Justicia para que esta de capacitaciones a los notarios de la república sobre informática jurídica, seguridad jurídica en internet, firma digital reconocida. Y estos estén preparados para poder otorgar fe pública electrónica a los documentos que electrónicos que surjan de las transacciones electrónicas que se dan en el comercio electrónico.

BIBLIOGRAFÍA

LIBROS

ALESSANDRI RODRÍGUEZ, ARTURO y SOMARRIVA UNDURRAGA, MANUEL. **"Curso de Derecho Civil. Las Fuentes de las Obligaciones en Particular."** Tomo IV. Redactado y puesto al día por Antonio Vodanovic H. Santiago de Chile. Editorial Nacimiento. 1999

CABANELLAS, GUILLERMO. **"Diccionario Enciclopédico de Derecho Usual".** Tomo II. 26ª Edición. Editorial Heliasta S.R.L. 1998.

CABANELLAS, GUILLERMO. "**Diccionario Enciclopédico de Derecho Usual".** Tomo tres. 25ª Edición. Editorial Heliasta. Buenos Aires. 1997.

CARNELUTTI, FRANCESCO, **"Sistema de Derecho Procesal Civil".** Tomo II. Buenos Aires (1944).

CREMADES JAVIER, MIGUEL ÁNGEL, FERNÁNDEZ ORDÓÑEZ, RAFAEL ILLISTA. **"Régimen Jurídico de Internet".** 1ª Edición. Editorial la Ley Madrid. 2002.

CUBILLOS VELANDIA, RAMIRO y RINCÓN CÁRDENAS, ERICK. **"Introducción Jurídica al Comercio Electrónico"**. Ediciones Jurídicas Gustavo Ibáñez. 1ª Edición. Colombia. 2002.

DAVARA RODRÍGUEZ, MIGUEL ÁNGEL. **"Manual de Derecho Informático".** Ediciones Aranzandi. España. 1997.

DE SANTO, VÍCTOR. **"Diccionario de Derecho Procesal"**. Editorial Universidad. Buenos Aires. 1991

FARINA, JUAN. **"Contratos Comerciales Modernos**. **Modalidades de Contratación Empresarial"**. 3ª Edición. Editorial Astrea. Buenos Aires. 2005.

GALLEGO HIGUERAS, GONZALO. **"Código de Derecho Informático y de las Nuevas Tecnologías"**. 1ª Edición. Civitas Ediciones, S.L. Madrid. 2002

GARRONE, JOSÉ ALBERTO. **"Diccionario Enciclopédico Abeledo-Perrot".** 2ª Edición. Editorial Abeledo Perrot S.A E. e I. Buenos Aires. 1993

GIRÓN, J. EDUARDO. **"El Notario Practico o Tratado de Notaria."** 4ª Edición. Editorial Tipografía Nacional. Guatemala. 1932.

GRACIA, MEXIA PABLO. **"Principios de Derecho de Internet"**. 2ª Edición. Editorial Tirant Blanch. Valencia. 2005.

HIGHTON DE NOLASCO, ELENA INÉS y ANGÉLICA GENEROSA ELVIRA VITALE. **"La Función Notarial en la Comunidad Globalizada"**. 1ª Edición. Santa Fe. Editorial Rubinzal-Culzoni. 2005

MARTÍNEZ NADAL, APOL-LONIA. **"La Ley de Firma Electrónica"**. 2ª Edición. Civitas. Madrid. 2001

MARTÍNEZ NADAL, APOL-LONIA. **"Comercio Electrónico, Firma Digital y Autoridades de Certificación"**. 3ª Edición. Estudios de Derecho Mercantil. Civitas. Madrid. 2001.

MENDOZA ORANTEZ, RICARDO. **"Derecho Notarial Salvadoreño (comentarios)"**. Editorial Jurídico Salvadoreña. San Salvador.

NAVARRO, FRANCESC, y OTROS. **"LA ENCICLOPEDIA".** Volumen nueve. Salvat Editores. Madrid. 2004.

OSORIO, MANUEL. **"Diccionario de Ciencias Jurídicas, Políticas y Sociales".** 1ª Edición. Editorial Heliasta S.R.L. Buenos Aires. 1991.

PALÉS, MARISOL. Directora de Diccionarios, Texto y Educación. **"Diccionario Jurídico Espasa Calpe, S. A."** Editora Celia Villar. Fundación Tomás Moro. Creación y realización electrónica: Planeta Actimedia, S.A, Madrid. 2001.

PELOSI, CARLOS. **"El Documento Notarial".** 3ª Edición. Astrea.

PERALES SANZ, JOSÉ LUÍS. Director del Seminario: **"Seguridad Jurídica en las Transacciones Electrónicas"**. 1ª Edición. Cívitas. 2002.

RINCÓN CARDENAS, ERICK. **"Contratación Electrónica"**. 1ª Edición. Centro Editorial Universidad del Rosario. Bogotá. 2006.

SANTA BIBLIA. "**Versión de Reina Valera"**. 1960".

VÁSQUEZ LÓPEZ, LUÍS. **"Derecho y Práctica Notarial".** 1ª Edición. Editorial Liz. San Salvador. 2001

TESIS

AGUILAR MORAN RAÚL ARMANDO, HERNÁNDEZ NÚÑEZ EVELYN YESENIA y VARGAS CONSUEGRA FLORENCIO DE JESÚS. **"El Comercio Electrónico en El Salvador"**. Tesis de Universidad de El Salvador. San Salvador. 2002.

ARRUÉ ECHEGOYÉN, CAROLINA ESMERALDA, MASIN MASIN, NATALIA MARGARITA y VÁZQUEZ LARA, MANUEL ALEJANDRO. **"La Seguridad Jurídica que Proporciona el Estado al Utilizar la Firma Digital como Medio de Expresión del Consentimiento"**. Tesis de Universidad de El Salvador. 2004.

CALDERÓN ORELLANA, MAYRA JEANNETTE, DELGADO RAMÍREZ, JUAN CARLOS y RIVAS HERNÁNDEZ, NELSON ORLANDO. **"Técnicas y Procedimientos de Auditoría para Obtener Evidencias Virtuales en Empresas que Realizan Comercio Electrónico en El Salvador"**. Tesis de Universidad de El Salvador. San Salvador. 2005.

CASTANEDA ESPINOZA, CESAR EDGARDO, y OTROS. **"El Documento Electrónico como Medio de Prueba para Acreditar Judicialmente las Obligaciones Derivadas de Dicha Contratación"** Tesis de Universidad de El Salvador. San Salvador. 2005.

CÓRDOVA ROGEL, KAREN MARISOL y OTROS. **"Alcances que Presenta la Función Notarial en la Ley del Notariado y Frente al Anteproyecto de Dicha Ley, en lo Relativo a las Actuaciones Notariales que se Realizan en el Exterior"**. Tesis de la Universidad de El Salvador. 2006.

DELEÓN RODRÍGUEZ, CLAUDIA DEL CARMEN y OTROS. **"Instrumentos Notariales: Su Inscripción en el Centro Nacional de Registros."** Tesis Universidad de El Salvador. Facultad Multidisciplinaria de Occidente. 2004.

FLORES CÁRCAMO, ERICK ROBERTO, y OTROS**. "Efectos Jurídicos Generales por la Falta de Normativa Legal Expresa que Regula las Compraventas Mercantiles por Medios Electrónicos.** Tesis de Universidad de El Salvador. San Salvador. 2003.

FLORES CÁRCAMO, ERICK ROBERTO. y OTROS **"Efectos Jurídicos Generales por la Falta de Normativa de la Compraventa Electrónica".** Tesis de Universidad de El Salvador. 2003.

GALÁN CORTEZ, JEANNIE ELIZABETH y OTROS. **"La Firma Digital como Medio de Seguridad y Consentimiento en las Transacciones del Comercio Electrónico".** Tesis de Universidad de El Salvador. San Salvador. 2008.

GUTIÉRREZ MOLINA, FAUSTO ANTONIO y MIRANDA NOVOA, CARMEN ELENA. **"Factibilidad para la Creación de la Ley de Firma Digital a Fin de Garantizar la Seguridad Jurídica, en las Transacciones Electrónicas".** Tesis de Universidad Politécnica de El Salvador. San Salvador. 2007

MARTÍNEZ, SANTIAGO RICARDO. **"Derecho y Practica Notarial".** Tesis Doctoral. Universidad de El Salvador. 1961.

PEÑA DAURA, EVA MARÍA y VÁSQUEZ MOLINA, DOMINGA BEATRIZ. **"Análisis de la Mala Praxis en el Ejercicio de la Función Notarial y sus Consecuencias".** Tesis de Universidad de El Salvador. 2005.

RAMÍREZ PÉREZ, BENJAMÍN. **"Limitaciones al Ejercicio de la Función Notarial".** Tesis Doctoral de la Universidad de El Salvador. 1977

REYES KRAFFT, ALFREDO ALEJANDRO. **"La Firma Electrónica y las Entidades de Certificación"**. Tesis de Universidad Panamericana. México D.F. 2002.

REVISTAS

"Revista de Ciencias Jurídicas". Universidad de Costa Rica. Facultad de Derecho. Número 102. Página 39. Colegio de Abogados. San José. Costa Rica. septiembre-diciembre año 2003

LÓPEZ MUÑOZ, JAVIER. Ingeniero Informático. Revista "Ágora Sic". Articulo de tema **"Servicios de Notarización Electrónica".** Volumen 25. Universidad de Málaga. Junio 2001

UNIVERSIDAD PONTIFICIA CATÓLICA DE PUERTO RICO. Revista Jurídica. **"Revista de Derecho puertorriqueño"**. Nº 1. Volumen 39. Enero-abril de 2000.

VELASCO ZELAYA, DR. MAURICIO ERNESTO. Magistrado de la Sala de lo Civil de la Corte Suprema de Justicia. Articulo **"Del Notariado en los Países Latinos"**. Revista Quehacer Judicial. Enero-febrero de 2008. Numero 62.

PONENCIAS Y TRABAJOS DE INVESTIGACIÓN

ASOCIACIÓN DE ESCRIBANOS DEL URUGUAY. Trabajo presentado en el Curso **"Especialización en Gobierno y Administración Digital".** Organizado por Milenium 21(Rivera, 25 de julio de 2003) y en el 13º Ciclo de Encuentros Técnicos Regionales. (Rivera, 26 de julio de 2003)

BERNAL RÍOS ROBLES. Articulo Electrónica **"Firma Digital: Legalidad en las Transacciones Comerciales Electrónicas y su Entorno. Perfección de los Contratos en Línea. Incorporación del Derecho al Impulso Digital".**

CHATARA, RAÚL ANTONIO. Folleto de clases **"Sistemas Legales en el Mundo y su Práctica Contractual"**. Año 2006.

Folleto educativo de la cátedra del Curso Jurídico Filosófico Político. Área Política. Tema **"Reflexiones en Torno al Proceso de Mundialización y Globalización"**. Año 2003

PLEITEZ, RAFAEL. Ponencia presentada en el Foro del COLPROCE: **"La Doctrina Del Neoliberalismo Y El Proceso De Globalización En Los Países Subdesarrollados"**. Publicada en la Revista "Realidad". Sin edición. Distribuidora de Publicaciones de la Universidad Centroamericana José Simeón Cañas. San Salvador. 1998

VIEGA, DRA. ESC. MARÍA JOSÉ*: "***El Notariado En Tiempos De Internet**".Trabajo presentado en las Cuartas Jornadas Académicas Internacionales del Instituto de Derecho Informático. Montevideo, 21 y 22 de agosto de 2003.

PAGINAS WEB

http://diariored.com/analisis/19990926214510.html

http://entren.dgsca.unam.mx/introduccion/virus_clasif.html

http://es.wikipedia.org/wiki/criptograf%c3%ADa

http://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica

http://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica

http://espanol.geocities.com/notariacuartadecucuta/notarial.html#principios

http://personal.telefonica.terra.es/web/criptologia/tercera4.html

http://www.alfa-redi.org/rdi-articulo.shtml?x=1469

http://www.cfna.org.ar/cfna/publi/index.php?modulo=escribano&opt=verdoctrina&id=71

http://www.elnotariado.com/ver_nota.asp?idnoticias=511

http://www.monografias.com/trabajos15/virus-informatico/virus-informatico.shtml

http://www.rodriguezvelarde.com.pe/articulos_35.htm

www.aaba.org.ar-Mail:aabacoin.pccp.com.ar

www.es.wikipedia.org/wiki/Cracker

www.espanol.groups.yahoo.com/groups/

www.html.net/seguridad/varios/firma-certificado

www.iec.csic.es/criptonomicon/seguridad

www.ingenieroseninformatica.org/recursos/tutoriales/firmaelectronica/cap4.php

www.monografias.com

www.tuguialegal.com/firmadigital/1.htm

www.utem.sl/cyt/derecho/firma.html

DICCIONARIOS ELECTRÓNICOS

Microsoft ® Encarta ® 2007. © 1993-2006 Microsoft Corporation. Reservados todos los derechos.

Microsoft® Student 2007 [DVD]. Microsoft Corporation, 2006.

ARTÍCULOS DE LA WEB

DRA. LEONOR GUINI. Asesora legal de la Oficina Nacional de Tecnologías de Información (ONTI). Argentina. Tema **"Firma Digital Autenticada por Notario Electrónico. Tercero de Confianza. Autoridad Certificantes".** http://www.elnotariado.com/ver_nota.asp?id_noticia=3244

FORMENTÍN ZAYAS, MSC. YANIXET. Profesora Instructora de la Facultad de Derecho de la Universidad de Camaguey. Cuba. www.monografias.com.

Revista Digital De Derecho. Colegio De Notario De Jalisco. México. www.revistanotarios.com

GAETE, EUGENIO ALBERTO. **"Documento electrónico e instrumento público"**. Portal de Abogados. http://www.portaldeabogados.com.ar/noticias/derin05.htm

SÁNCHEZ MUÑOZ, VIVIANA CRISTINA "El Notario ante el Impacto Tecnológico de la Informática y las Telecomunicaciones" http://www.alfa-redi.org/rdi-articulo.shtml?x=9899

LEGISLACIÓN CONSULTADA

Código Aduanero Uniforme Centroamericano (CAUCA). D.L. Nº 563, del 9 de junio de 1993. Publicado en el D.O. Nº 137. Tomo 320. Del 21 de julio de 1993. Instrumento De Ratificación. Publicado en el D.O. Nº 118. Tomo Nº 327. Del 28 de junio de 1995.

Código Civil. Decreto Del Poder Ejecutivo De Fecha 23 De Agosto De 1859.

Código de Comercio. D.L. Nº 671, del 8 de mayo de 1970, publicado en el D.O. Nº 140, Tomo 228, del 31 de julio de 1970.

Código de Procedimientos Civiles, Decreto Ejecutivo de 31 de diciembre de 1881, publicado en el Diario Oficial el día 1º de enero de 1882.

Código Tributario. D.L. Nº 230, del 14 de diciembre de 2000, publicado en el D.O. Nº 241, tomo 349, del 22 de diciembre de 2000.

Constitución. D.C. Nº 38, del 15 de diciembre de 1983, publicado en el D.O. Nº 234, Tomo Nº 281, del 16 de diciembre de 1983.

Convención De Las Naciones Unidas Sobre Los Contratos De Compraventa Internacional De Mercaderías. Viena 11 de abril de 1980.

Instrucción de 19 de Octubre de 2000, de la Dirección General de los Registros y del Notariado, sobre el Uso de la Firma Electrónica de los Fedatarios Públicos.

Ley 59/2003 de Firma Electrónica de España del 19 de diciembre de 2003, BOE núm. 304, sábado 20 de diciembre de 2003.

Ley de Bancos, aprobada el 10 de sep. De 1999, sancionada el 27 de sep. De 1999 y publicada en el Diario Oficial No. 181, Tomo 334, del 30 de sep. De 1999

Ley de Certificados, Firmas Digitales y Documentos Electrónicos. (Costa Rica). Nº 8454 del 30 de agosto del 2005. La Gaceta Nº 197 del 13 de octubre del 2005

Ley de Notariado. D.L Nº 218, del 6 de diciembre de 1962, publicado en el D.O. Nº 225, Tomo 197, del 7 de diciembre de 1962.

Ley De Servicio Civil. D.LEY. Nº 507, del 24 de noviembre de 1961, publicado en el D.O. Nº 239, Tomo 193, del 27 de diciembre de 1961.

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 de Utah de 1999 de los Estados Unidos de Norteamérica.

Ley Del Instituto Nacional De Pensiones De Los Empleados Públicos. D.L. Nº 373, del 16 de octubre de 1975, publicado en el D.O. Nº 198, Tomo 249, del 24 de octubre de 1975.

Ley Modelo De Firma Electrónica De La Comisión De Las Naciones Unidas Para El Derecho Mercantil Internacional. Nueva York. 2002

Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas por el Derecho Mercantil Internacional. Aprobada en Asamblea General de la ONU por resolución 51/162, el 16 de diciembre de 1996.

Ley Orgánica Judicial. Publicada en el D.O Nº. 283 del 20 de junio de 1984.

Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas. Decreto 47-2008. Guatemala.

Proyecto Final de Ley de Comunicación y Firma Electrónica de El Salvador.

Recomendación UIT-T X.509, Unión Internacional de Telecomunicaciones.

Reglamento de Aplicación del Código Tributario. D.O. Nº. 234, Tomo 353, del 11 de diciembre de 2001.

Reglamento del Código Aduanero Uniforme Centroamericano (RECAUCA). Resolución No. 101-2002 del Consejo Arancelario y Aduanero Centroamericano, de fecha 12 de diciembre de 2002. Acuerdo 21. Órgano Ejecutivo En El Ramo De Economía. San Salvador, 9 DE ENERO DE 2003.

Tratado de Libre Comercio República Dominicana – Centroamérica – Estados Unidos. (CAFTA).

ANEXOS

ANEXO I
"Cuadro de Métodos y Herramientas de Ataque de los Hackers"

MÉTODOS Y HERRAMIENTAS DE ATAQUE DE LOS HACKERS	**EAVESDROPPING Y PACKET SNIFFING**	Muchas redes son muy vulnerables a este tipo de ataque, que se hace por medio de packet sniffers, que son programas que monitorean los paquetes de red que están diseccionado a la computadora. Este método es utilizado para capturar logins y passwords de usuarios, que generalmente viajan sin seguridad. También son utilizados para capturar números de tarjetas de crédito y direcciones de Email entrantes y salientes.
	SNOOPING Y DOWNLOADING	Estos ataques tienen el mismo objetivo que el sniffing, obtener información sin modificarla, pero son diferentes, en este tipo de ataque el hacker entra en el documento, mensajes de Email u otra información guardada, realizando en la mayoría de los casos una copia de esa información en su computadora.
	TAMPERING O DATA DIDDLING	Este ataque se refiere a la modificación desautorizada a los datos o al software instalado en el sistema, incluyendo el borrado de archivos, son particularmente serios cuando el que lo realiza tiene derechos de administrador. La manipulación que se realiza con este tipo de ataque puede hacer que todo el sistema cambie o se dañe.
	SPOOFING	Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snoofing o tampering, en este caso puede adquirir el nombre y password de un usuario legitimo e ingresar al sistema y realizar acciones en nombre de él como enviar falsos e-mails o retirar dinero de la cuenta, entre otros.
	CABALLOS DE TROYA	Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto como por ejemplo formatear el disco duro, modificar un fichero, entre otros.
	OBTENCIÓN DE PASSWORDS, CÓDIGOS Y CLAVES	Este método (usualmente denominado cracking) comprende la obtención “por fuerza bruta” de aquellas claves que permiten ingresar a servidores, aplicaciones, cuentas, etc.

ANEXO II
"Ejemplo de Certificados Digitales X.509"

Ejemplos de un Certificado X.509.

Es una decodificación (generada con openssl) de uno de los certificados viejos de www.freesoft.org. El certificado real tiene un tamaño de alrededor de 1 KB. Fue emitido (firmado) por Thawte (desde que fue adquirido por Verisign), tal como se indica en el campo Emisor. El tema contiene bastante información personal, pero la parte más importante es el nombre común (CN) de www.freesoft.org - esta es la parte que debe coincidir con la terminal que se está autenticando. A continuación viene una clave pública RSA (módulo y exponente público), seguido de la firma, computada tomando un hash MD5 de la primera parte del certificado y cifrándola con la clave privada RSA de Thawte.

```
Certificate:
   Data:
       Version: 1 (0x0)
       Serial Number: 7829 (0x1e95)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte
Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/Email=server-certs@thawte.com
       Validity
           Not Before: Jul  9 16:04:02 1998 GMT
           Not After : Jul  9 16:04:02 1999 GMT
       Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
                OU=FreeSoft,
CN=www.freesoft.org/Email=baccala@freesoft.org
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
                   33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
                   66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
                   70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
                   16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
                   c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
                   8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
                   d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                   e8:35:1c:9e:27:52:7e:41:8f
               Exponent: 65537 (0x10001)
   Signature Algorithm: md5WithRSAEncryption
       93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
       92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
       ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
       d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
       0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
       5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
       8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
       68:9f
```

Para validar este certificado, necesitamos otro certificado: uno que coincida con el Emisor (Thawte Server CA) en el primer certificado. Entonces se toma la clave pública RSA del segundo certificado (CA), se usa para decodificar la firma del primer certificado para obtener el hash MD5, el cual debe coincidir con el hash MD5 computado sobre el resto de los certificados. Éste es el certificado CA:

```
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte
Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/Email=server-certs@thawte.com
       Validity
           Not Before: Aug  1 00:00:00 1996 GMT
           Not After : Dec 31 23:59:59 2020 GMT
       Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte
Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/Email=server-certs@thawte.com
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
                   68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
                   85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
                   6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
                   6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
                   29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
                   6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
                   5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
                   3a:c2:b5:66:22:12:d6:87:0d
               Exponent: 65537 (0x10001)
       X509v3 extensions:
           X509v3 Basic Constraints: critical
               CA:TRUE
   Signature Algorithm: md5WithRSAEncryption
       07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
       a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
       3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
       4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
       8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
       e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
       b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
       70:47
```

ANEXO III
"Tabla de Usuarios de Internet. Septiembre 2007"

Cuadro de Usuarios de Internet (Sep/07)

País	*Usuarios*	*% s/ población*
Costa Rica	1,279,850	28.6%
México	14,593,136	13.4%
El Salvador	646,555	9.1%
Panamá	247,160	7.4%
Guatemala	667,200	5.0%
Honduras	246,080	3.2%
Nicaragua	102,708	1.8%

Tomado:
www.cnr.gob.sv/pi_eventos/taller_svnet/CONFERENCIA_25_ABRIL_2008.ppt

ANEXO IV
"Cedula de Entrevista
Licda. Rubenia Moran
encargada del área de atención del usuario
de la Direccion General
de Aduanas."

UNIVERSIDAD DE EL SALVADOR.

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES.

ENTREVISTA DIRIGIDA A LICENCIADA RUBENIA MORAN DEL DEPARTAMENTO DE ATENCIÓN AL USUARIO DE LA ADUANA TERRESTRE DE SAN BARTOLO EN ILOPANGO.

"NECESIDAD DE UN MARCO LEGAL QUE REGULE LA INTERVENCIÓN DEL NOTARIO EN LA CONTRATACIÓN ELECTRÓNICA EN 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. ¿Como funciona el sistema actual implementado por la ley de simplificación aduanera?

_____
_____
_____
_____.

3. ¿Considera usted que el nuevo sistema hace más ágiles los trámites realizados en las aduanas?

_____
_____
_____
_____.

4. ¿Como hacen para identificar a la persona que hace uso de la declaración de mercaderías?

_____
_____
_____
_____.

5. ¿Como hacen para asegurarse de que la información intercambiada no ha sido alterada en el proceso de envío?

_____
_____
_____
_____.

6. Según su experiencia, ¿considera que la firma electrónica es un medio idóneo para asegurar la información?

_____
_____
_____
_____.

7. Según su experiencia, ¿cree usted que sería factible que un notario electrónico sea el que de fe de esa información?

_____
_____
_____
_____.

8. ¿Considera que es necesaria una ley que regule exclusivamente la intervención de un notario y la utilización de una firma electrónica?

_____
_____
_____
_____.

Muchas Gracias.

ANEXO V
"Cedula de Entrevista dirigida a la Doctora Yesenia Granillo de Tobar. Docente de la Escuela de Economia y Negocios (ESEN)"

UNIVERSIDAD DE EL SALVADOR.
FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES.
ENTREVISTA DIRIGIDA A LA DOCTORA YESENIA GRANILLO DE TOBAR, DOCENTE DE LA ESCUELA DE ECONOMÍA Y NEGOCIOS "ESEN".

"NECESIDAD DE UN MARCO LEGAL QUE REGULE LA INTERVENCIÓN DEL NOTARIO EN LA CONTRATACIÓN ELECTRÓNICA EN EL SALVADOR".

1. ¿Consideran que el Tratado De Libre Comercio con Estados Unidos es un factor que incide en que se regule la contratación por medios electrónicos?
   _____
   _____
   _____
   _____
   _____.

2. ¿Cree usted, que el contrato electrónico, en sí mismo, brinda seguridad jurídica a los contratantes, sin la necesidad de un notario?
   _____
   _____
   _____
   _____
   _____.

3. ¿Cree usted que es necesario que el notario intervenga, como garante de la autenticidad de los contratantes en un contrato electrónico?
   _____
   _____
   _____
   _____
   _____.

4. Para usted, ¿cual seria las funciones que debería de realizar un notario que intervenga en un contrato electrónico?
   _____

_____
_____
_____
_____.

5. Cree que es necesario que se implemente una ley que regule el comercio, la firma digital y la intervención de un notario en estos.

   _____
   _____
   _____
   _____
   _____.

6. ¿Considera usted que en nuestro país hay suficientes medios para aplicar la figura del ciber notario?

   _____
   _____
   _____
   _____
   _____.

7. ¿Considera que existe suficiente marlo legal que regule la contratación electrónica y la firma electrónica?

   _____
   _____
   _____
   _____
   _____.

Muchas Gracias.

ANEXO VI
"Modelo de Encuesta"

UNIVERSIDAD DE EL SALVADOR.
FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES.
ENCUESTA DIRIGIDA A LOS ABOGADOS Y NOTARIOS AUTORIZADOS POR LA CORTE SUPREMA DE JUSTICIA.

"NECESIDAD DE UN MARCO LEGAL QUE REGULE LA INTERVENCIÓN DEL NOTARIO EN LA CONTRATACIÓN ELECTRÓNICA EN EL SALVADOR".

LA PRESENTE ENCUESTA ES PARA MEDIR EL NIVEL DE CONOCIMIENTO DE LOS ABOGADOS Y NOTARIOS SALVADOREÑOS EN EL TEMA DE LA CONTRATACIÓN ELECTRÓNICA.

EDAD_____ SEXO: F_____ M_____

TIEMPO DE EJERCER EL NOTARIADO
O LA ABOGACÍA: _____

CONDICIÓN DE TRABAJO:

SECTOR PRIVADO: _____
SECTOR PUBLICO: _____
SECTOR INDEPENDIENTE: _____

1. ¿Tiene conocimiento de lo que es la contratación electrónica?

SI_____ NO. _____

2. Si su respuesta es positiva por favor indique el medio por el que obtuvo tal conocimiento.

1. Estudios universitarios_____
2. Post grados _____
3. Maestrías _____
4. Seminarios: _____
5. Capacitaciones: _____
6. Conferencias: _____
7. INTERNET: _____

3. ¿Cree usted, que el contrato electrónico brinda seguridad jurídica a los contratantes?

SI. _____ NO. _____

4. ¿Considera usted que se debe de regular la contratación electrónica en El Salvador?

SI. _____ NO. _____

5. ¿Considera usted que en El Salvador existe personal capacitado para implementar la contratación electrónica?

SI_____ NO_____

6. ¿Conoce de alguna empresa que realiza contratación electrónica?

SI_____ NO_____

7. ¿Si su respuesta es afirmativa, diga cual (les) empresa o empresas son las que realizan tal contratación?

1. _____
2. _____
3. _____
4. _____
5. _____

8. ¿Tiene alguna noción de lo que significa Firma Digital?

SI. _____ NO. _____

9. ¿Sabe como funciona una Firma Digital?

SI _____ NO_____

10. ¿Cree usted que es necesaria la intervención de un notario en un contrato electrónico, en el cual se utiliza una firma digital?

SI. _____ NO. _____

11. ¿Considera que la Corte Suprema de Justicia está haciendo esfuerzos para que la función notarial se actualice según las nuevas tendencias tecnológicas, Impulsando iniciativas de ley que busquen adaptar la realidad nacional a éstas tecnologías?

SI_____ NO_____

12. ¿Considera usted necesario la regulación de la función notarial en los contratos electrónicos en El Salvador?

SI_____ NO_____

ANEXO VII
Instrucción de 19 de octubre de 2000, de la Direccion General de los Registros y del Notariado, sobre el Uso de la Firma Electrónica de los Fedatarios Públicos. España

I. Disposiciones generales

MINISTERIO DE JUSTICIA

20274 *INSTRUCCIÓN de 19 de octubre de 2000, de la Dirección General de los Registros y del Notariado, sobre el uso de la firma electrónica de los fedatarios públicos.*

El Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica, establece en el párrafo segundo del artículo 1.2 que sus normas «no sustituyen ni modifican las que regulan las funciones que corresponde realizar a las personas facultadas, con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en su elevación a públicos».

A su vez, este precepto está incardinado en el espíritu del artículo 1, párrafo segundo, de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, que dispone: «La presente Directiva no regula otros aspectos relacionados con la celebración y validez de los contratos u otras obligaciones legales cuando existan requisitos de forma establecidos en las legislaciones nacionales o comunitaria, ni afectan a las normas y límites, contenidos en las legislaciones nacionales o comunitarias, que rigen el uso de documentos.»

La exclusión de la actividad de los fedatarios públicos del ámbito de la citada norma responde a una adecuada ponderación de las diferencias que separan el sistema público de garantías consustanciales a la función de estos profesionales, de las características propias del procedimiento de firma electrónica y en concreto de las que se le ha dotado en nuestro ordenamiento.

Teniendo en cuenta la legalidad vigente, y sin perjuicio de que deberán emprenderse las necesarias reformas legislativas, en este momento se estima que la única faceta de la actividad de notarios y registradores en que la firma electrónica puede tener una aplicación práctica es la relativa a la remisión de comunicaciones prevista en los artículos 175 y 249 del Reglamento Notarial. En estos supuestos, lejos de suponer una apuesta caprichosa por la técnica, el uso de la firma electrónica, con los condicionamientos que se establecen, viene a introducir importantes dosis de seguridad frente a la que proporciona el telefax, en aspectos tan relevantes como la garantía de procedencia y la integridad de los mensajes.

En su virtud, al amparo del artículo 21.1 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, dispongo:

1. Los notarios y los registradores de la propiedad y mercantiles dispondrán obligatoriamente de una dirección de correo electrónico específicamente destinada a emitir y recibir comunicaciones oficiales entre ellos y con el Consejo General del Notariado y el Colegio de Registradores de la Propiedad y Mercantiles de España y con los diferentes órganos de las Administraciones Públicas. Esta dirección electrónica deberá ser comunicada al Consejo General del Notariado o al Colegio de Registradores de la Propiedad y Mercantiles de España, respectivamente, para su publicación en un directorio electrónico.

2. El Consejo General del Notariado y el Colegio de Registradores de la Propiedad y Mercantiles de España se constituirán, en el plazo máximo de nueve meses desde la publicación de la presente Instrucción, en prestadores de certificación acreditados, conforme a lo dispuesto en el Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica, a los únicos efectos de expedir certificados electrónicos mediante los que se vinculen unos datos de verificación de firma a la identidad, cualidad profesional y situación administrativa de los miembros en activo integrados en las respectivas corporaciones. Tales firmas electrónicas habrán de basarse en un dispositivo seguro de creación de firma.

3. En el plazo máximo de tres meses, a contar desde que su respectiva corporación se haya constituido en entidad de certificación, todos los notarios y registradores de la propiedad y mercantiles habrán de obtener de su corporación una firma electrónica avanzada, basada en un certificado reconocido, con un dispositivo seguro de creación de firma.

Una vez implantado el sistema, los notarios y registradores de la propiedad y mercantiles deberán obtener una nueva firma electrónica avanzada en el momento en que tomen posesión de una nueva plaza, además de cuando se produzca la revocación o caducidad de la anterior.

4. Los certificados reconocidos emitidos por el Consejo General del Notariado y el Colegio de Registradores de la Propiedad y Mercantiles de España, además de identificar a su titular, habrán de expresar su condición de notario o registrador de la propiedad o mercantil en activo y la plaza de destino, y deberán indicar que su uso se encuentra limitado a la remisión de comunicaciones entre Notarías y Registros recíprocamente y de los notarios y registradores con los órganos de sus respectivas Corporaciones.

5. Los dispositivos seguros de creación de firma habrán de ser generados con la intervención personal del signatario, auxiliado por los mecanismos técnicos correspondientes, en presencia del Decano de su Colegio, en el caso de los notarios, o del Delegado provincial, en el caso de los registradores, dejando constancia documental de ello. En ningún caso podrán ser almacenados los datos de creación de firma.

Del acto de generación del dispositivo de creación de firma y sus correspondientes datos de verificación se dejará constancia escrita en un documento suscrito con firma autógrafa por ambos asistentes. A continuación se procederá por el titular del órgano corporativo anteriormente indicado a comunicar por vía y con firma electrónica la generación del dispositivo, los datos de verificación de firma y los demás extremos precisos para que por su Corporación se emita y publique de manera inmediata el oportuno certificado con sus correspondientes datos de verificación de firma.

El Consejo General del Notariado y el Colegio de Registradores de la Propiedad y Mercantiles de España procederán a la revocación inmediata de oficio de los certificados, respecto de los notarios o registradores que dejen de servir la plaza indicada en ellos.

6. Los Notarios y los Registradores de la Propiedad y Mercantiles estarán obligados a custodiar personalmente, adoptando las medidas de seguridad adecuadas, el dispositivo seguro de creación de firma electrónica que les corresponda, no podrán ceder su uso a ninguna otra persona en ningún supuesto, y deberán denunciar de manera inmediata a la corporación emisora del certificado, por el procedimiento arbitrado por ella, su pérdida, extravío o deterioro, así como cualquier situación o acaecimiento que pueda poner en peligro el secreto o la unicidad del mecanismo, para que proceda a su suspensión o revocación.

7. El uso de la firma electrónica a que se refiere la presente Instrucción estará limitado a las solicitudes y comunicaciones contempladas en los artículos 175 y 249 del Reglamento Notarial. Podrán realizarse por vía telemática y con la firma electrónica avanzada a que se refiere la presente Instrucción.

8. Los Notarios podrán testimoniar en soporte papel, bajo su fe, las comunicaciones o notificaciones recibidas de los Registradores.

9. Queda derogada la Instrucción de esta Dirección General de 26 de abril de 2000.

Madrid, 19 de octubre de 2000.—La Directora general, Ana López-Monís Gallego.

Ilmos. Sres. Presidente del Consejo General del Notariado y Decano del Colegio de Registradores de la Propiedad y Mercantiles de España.

MINISTERIO DE HACIENDA

20275 *RESOLUCIÓN de 25 de octubre de 2000, del Departamento de Aduanas e Impuestos Especiales de la Agencia Estatal de la Administración Tributaria, por la que se actualiza el Arancel Integrado de Aplicación (TARIC).*

El Arancel Integrado de Aplicación (TARIC) fue adaptado completamente, por Resolución de 10 de diciembre de 1999 («Boletín Oficial del Estado» del 28), y parcialmente por Resolución de 27 de diciembre de 1999 («Boletín Oficial del Estado» de 5 de enero de 2000), Resolución de 14 de febrero de 2000 («Boletín Oficial del Estado» del 24), Resolución de 25 de febrero de 2000 («Boletín Oficial del Estado» de 3 de marzo), Resolución de 23 de junio de 2000 («Boletín Oficial del Estado» de 1 de julio), Resolución de 7 de agosto de 2000 («Boletín Oficial del Estado» del 17), Resolución de 28 de agosto de 2000 («Boletín Oficial del Estado» de 1 de septiembre). Habiéndose producido desde esta última Resolución la publicación de diferente normativa comunitaria que supone la variación en cuanto a los códigos puntualizables, procede actualizarlos, sustituyendo los códigos afectados, por lo que se acuerda lo siguiente:

Primero.—Actualizar la nomenclatura y codificación del Arancel Integrado de Aplicación (TARIC), reemplazándose los textos de las partidas afectadas por los incluidos como Anexo A, y aplicables desde el 1 de noviembre de 2000.

Segundo.—Incluir como Anexo B, los códigos TARIC que se suprimen a partir del 1 de noviembre de 2000.

Tercero.—Actualizar la relación de Códigos Adicionales según los contenidos en el Anexo C y aplicables a partir del 1 de noviembre de 2000.

Cuarto.—Incluir como Anexo D los Códigos Adicionales que se suprimen a partir del 1 de noviembre de 2000.

Quinto.—La presente actualización será aplicable desde el 1 de noviembre de 2000.

Lo que se dispone para su conocimiento y efectos.

Madrid, 25 de octubre de 2000.—El Director del Departamento, Javier Goizueta Sánchez.

ANEXO VIII
Proyecto Final de Ley de Comunicación y Firma Electrónica

PROYECTO FINAL DE LEY DE COMUNICACIÓN Y FIRMA ELECTRÓNICA

DECRETO No.

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE EL SALVADOR

CONSIDERANDO

I.- Que la Constitución de la República en el Art. 101 inc. 2 establece que el Estado debe promover el desarrollo económico y social mediante el incremento de la producción, productividad y racionalización de los recursos, en consecuencia, debe ofrecer los instrumentos legales que propicien las innovaciones tecnológicas que brinden oportunidad para el acceso a la información en ciencias, educación o en la realización competitiva de transacciones

II.- Que la Constitución de la República en el Art. 2 reconoce que toda persona tiene el derecho a la seguridad jurídica, por lo que el Estado debe brindar seguridad en las comunicaciones electrónicas y las transacciones autorizadas mediante las aplicaciones de la tecnología o la suscripción electrónica de las mismas, tengan validez jurídica; y,

III.- Que la Sociedad de la Información se han convertido en un factor estratégico que mejora la eficiencia de la educación y fomenta la competitividad y el crecimiento económico de los pueblos y asimismo, eleva la calidad de vida de los ciudadanos, razón por la cual nuestro país por medio de esta ley se integra al entorno mundial de comunicaciones electrónicas;

POR TANTO,
En uso de sus facultades constitucionales y a iniciativa de….

DECRETA, la siguiente:

LEY DE COMUNICACIÓN Y FIRMA ELECTRÓNICA

TITULO I
DISPOSICIONES GENERALES

CAPÍTULO I
OBJETO Y ALCANCE

Objeto

Art. 1.- La presente ley tiene por objeto brindar seguridad jurídica a los usuarios de las tecnologías de información y comunicación cuando realicen transacciones a través de comunicaciones electrónicas con o sin firma electrónica con la finalidad de que se otorgue plena validez y eficacia jurídica a las transacciones así realizadas.

Interpretación progresiva

Art. 2.- Las regulaciones de la presente ley serán aplicables a la comunicación electrónica, firma electrónica o cualquier formato electrónico, independientemente de sus características técnicas o de los desarrollos tecnológicos que se produzcan en el futuro, sus normas serán desarrolladas e interpretadas progresivamente siempre que se encuentren fundamentadas en los principios de autenticidad, integridad, confidencialidad, equivalencia y no repudiación a fin de reconocer la validez y eficacia probatoria de los mensajes de datos y firma electrónica conforme a esta ley.

CAPITULO II
DEFINICIONES Y PRINCIPIOS GENERALES

Definiciones

Art. 3.- Para los efectos de la presente ley se utilizarán las siguientes definiciones:

Acreditación: Es la autorización que otorga la Superintendencia General de Electricidad y Telecomunicaciones a los proveedores de servicios de certificación para operar y proporcionar certificados electrónicos, una vez cumplidos los requisitos y condiciones establecidas en la presente ley;

Certificado Electrónico: Documento proporcionado por un proveedor de servicios de certificación que verifica la correspondencia entre la clave pública y clave privada con su titular, otorgándole certeza y validez a la firma electrónica;

Clave privada: Es la clave generada por un proceso matemático que contiene datos únicos que el firmante utiliza para crear la firma electrónica. Su conocimiento y control es exclusivo del firmante;

Clave pública: Es aquella clave generada por un proceso matemático que contiene datos únicos que permiten verificar la firma electrónica del firmante. Su conocimiento es público;

Comunicación Electrónica: Toda información o mensajes de datos generado, enviado, recibido, archivado o comunicado por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax;

Firma Electrónica: Es la combinación de clave pública y privada que asocia a una persona con su voluntad de firmar, utilizando sistemas criptográficos asimétricos, contenida en un certificado expedido por un proveedor de servicios de certificación acreditado; y,

Proveedor de Servicios de Certificación: Persona dedicada a proporcionar certificados electrónicos y demás actividades previstas en esta ley.

Principios generales

Art. 4.- Las actividades reguladas por esta ley se regirán bajo los siguientes Principios:

a) Autenticidad, con la cual se garantiza que el mensaje es confiable y ésta garantía perdura a través del tiempo.

b) Integridad, por medio del cual se otorga certeza de que los datos recibidos por medios electrónicos no han sido modificados en su tránsito desde el iniciador hasta el destinatario

c) Confidencialidad, por medio de la cual se garantiza al iniciador y destinatario que los mensajes electrónicos no serán conocidos por terceras personas sin su expresa autorización.

d) Equivalencia, a través del cual no puede negarse la presentación de documentos electrónicos en instancias administrativas o judiciales, solo por encontrarse contenido en un soporte diferente al físico.

e) No Repudiación, por medio del cual se garantiza que cuando un mensaje ha sido suscrito con firma electrónica de conformidad a lo establecido en la presente ley, no puede ser repudiada su autoría por la persona del iniciador.

Tratamiento de datos

Art. 5.- El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad se sujetará a las siguientes reglas:

a) Para la expedición de certificados electrónicos al público, los prestadores de servicios de certificación únicamente podrán recabar datos personales directamente de los firmantes o previo consentimiento expreso de éstos. Toda cesión de datos personales también requerirá el consentimiento expreso de su titular, quien podrá solicitar la rectificación o cancelación de los datos personales cuando tales datos sean contrarios a lo previsto en este capítulo o cuando fueren inexactos o incompletos;

b) Los datos requeridos serán exclusivamente los necesarios para la expedición y el mantenimiento del certificado electrónico y la prestación de otros servicios en relación con la firma electrónica, no pudiendo tratarse con fines distintos sin el consentimiento expreso del firmante;

c) Los proveedores de servicios de certificación estarán obligados a revelar la identidad de los firmantes cuando lo solicite el juez competente o la Fiscalía General de la República en el ejercicio de sus funciones;

d) El responsable del registro de datos y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal estarán obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el responsable del registro de datos.

TITULO II
MENSAJES DE DATOS Y DOCUMENTOS ELECTRÓNICOS

CAPITULO I
DISPOSICIONES GENERALES

Equivalencia jurídica

Art. 6.- El mensaje de datos utilizando firma electrónica cualquiera sea su medio de transmisión o de almacenamiento, se tendrá por jurídicamente equivalente al contenido en documentos convencionales que se otorguen, almacenen o se transmitan por medios físicos.

Celebración por escrito

Art. 7.- En todos los casos en que se exija que una información conste por escrito o deba ser presentada en esa forma o se prevean consecuencias jurídicas si la información no consta por escrito, se entenderá que un documento contenido en un soporte electrónico, cumple con el requisito de escrituralidad, siempre y cuando la información cumpla con los principios y requisitos exigidos por esta ley.

No obstante lo anterior, el empleo del soporte electrónico para un documento determinado no dispensa en ningún caso el cumplimiento de los requisitos, formalidades o solemnidades que el ordenamiento legal exige para cada acto jurídico en particular.

Exigencia de documento original

Art. 8.- Si de acuerdo al acto jurídico o por disposiciones del ordenamiento legal se exija que la información sea conservada en su forma original, se entenderá que un documento electrónico cumple dicha exigencia si la firma electrónica demuestra que no ha sido alterado, el cual puede ser presentado en soporte diferente en caso de destrucción del soporte electrónico.

Conservación de documentos

Art. 9.- Si la ley exige que los documentos, registros, datos o información pública o privada sean conservados en archivos, se entenderá que cumple con dicha exigencia cuando permita mantener su autenticidad, integridad, confidencialidad, equivalencia, no repudiación y otros que la ley o el reglamento establezcan.

CAPITULO II
DOCUMENTOS EN SOPORTE ELECTRÓNICO

Documentos auténticos y públicos emitidos en soportes electrónicos

Art. 10.- Los documentos auténticos podrán estar contenidos en soporte electrónico y tendrán el valor asignado por el ordenamiento legal para esta clase de documentos.

Los documentos públicos electrónicos que se refieran al ejercicio de la función notarial se regularán en una ley especial.

Valor Probatorio de los documentos privados electrónicos

Art. 11. Cuando el documento privado fuera generado con firma electrónica y se refiera a actos jurídicos que no se encuentren excluidos por la presente ley, el valor del mismo será de plena prueba y tendrá fuerza ejecutiva en su caso, sin embargo, no podrá presentarse para su cobro más de una vez.

TITULO III
COMUNICACIÓN ELECTRÓNICA DE DATOS

CAPÍTULO I
DE LA EMISIÓN Y RECEPCIÓN DE LOS MENSAJES DE DATOS

Verificación de la emisión del Mensaje de Datos

Art.12.- Se entenderá que un mensaje de datos proviene del iniciador, cuando éste ha sido enviado por:

a) El propio iniciador o la persona que lo representa, cuando el documento ha sido firmado electrónicamente.

b) Por un sistema de información programado por el iniciador, o bajo su autorización, para que opere automáticamente.

Reglas para la determinación del recibo del mensaje.

Art. 13 – El recibo del mensaje, se comprobará por el sistema de la recepción y tendrá lugar cuando el mensaje de datos ingrese al repositorio destinatario, encontrándose a disposición de éste para su acceso. Las partes no podrán pactar lo contrario a esta disposición.

Lugar de emisión y recepción

Art. 14.- Salvo prueba en contrario, el mensaje de datos se tendrá por emitido en el lugar donde el iniciador tenga su domicilio y por recibido en el lugar donde el destinatario tenga el suyo. Prevalecerá el domicilio establecido por las partes; si no hubiere, se aplicará el domicilio que conste en el registro del proveedor de servicios de certificación y en su defecto, el designado por el derecho común.

Del acuse de recibo

Art. 15.- Los usuarios podrán acordar los mecanismos y métodos para el acuse de recibo de un mensaje de datos. Cuando los usuarios no hayan acordado que para el acuse de recibo se utilice un método determinado, se considerará que dicho requisito se ha cumplido cuando:

a) La comunicación dirigida al destinatario permita corroborar la recepción del mensaje de datos.

b) A través de actos del destinatario, el iniciador pueda evidenciar que ha recibido su mensaje de datos.

TITULO IV
FIRMA ELECTRONICA Y CERTIFICADOS ELECTRONICOS

CAPITULO I
DISPOSICIONES GENERALES

Requisitos y efectos de la firma electrónica

Art. 16.- La firma electrónica debe estar sustentada en un método de creación y verificación confiable y seguro, de manera que aquella sea inalterable, alertando al destinatario en caso de alteración de la información después de ser suscrita por el signatario.

La firma electrónica tiene los siguientes efectos:

a) Vincula un mensaje de datos con su titular de manera exclusiva;

b) Permite la verificación inequívoca de la autoría e identidad del signatario;

c) Asegura que los datos de la firma estén bajo control exclusivo del signatario;

Efectos jurídicos probatorios

Art. 17.- La firma electrónica tendrá igual validez y los mismos efectos jurídicos y probatorios que una firma manuscrita en relación con los datos consignados en un documento o mensaje de datos electrónicos en que fuere empleada.

Presunciones del empleo de la firma electrónica

Art. 18.- El empleo de la firma electrónica que cumpla los requisitos exigidos en la presente ley, salvo prueba en contrario, presume lo siguiente:

a) Que la firma electrónica pertenece al titular de la misma;

b) Que el mensaje de datos vinculado a la firma electrónica no ha sido modificado desde el momento de su envío, si el resultado del procedimiento de verificación así lo indica.

Uso de la firma electrónica por representantes

Art. 19.- Podrán hacer uso de la firma electrónica, los representantes legales de las personas jurídicas públicas o privadas y en tal caso, el certificado electrónico deberá contener los datos necesarios para la identificación de la persona jurídica y de su representante legal.

Para los mandatarios de las personas naturales, solo se utilizará la firma electrónica de aquel, previa verificación de tal calidad por parte del proveedor de servicios de certificación, ésta circunstancia deberá constar en el certificado que se le extienda.

No podrán hacer uso de firma electrónica los padres por sus hijos ni los tutores o curadores por sus pupilos.

CAPÍTULO II
USO DE LA FIRMA ELECTRÓNICA POR LOS ÓRGANOS DEL ESTADO

Prestación de servicios públicos mediante mensaje de datos y firma electrónica

Art. 20.- Los funcionarios y empleados públicos que presten servicios públicos, ejecuten o realicen actos o expidan cualquier documento, dentro de su ámbito de competencia, podrán suscribirlos por medio de una firma electrónica. El proveedor de servicios de certificación deberá consignar en el certificado la calidad con la que firmará electrónicamente.

Se exceptúan del uso de la firma electrónica, en aquellas actuaciones para las cuales la Constitución de la República o la ley exijan alguna solemnidad que no sea susceptible de cumplirse mediante documentos electrónicos, mensaje de datos o firmas electrónicas, o requiera la concurrencia personal de la autoridad pública que deba intervenir en ellas.

Validez de actos y contratos

Art. 21.- Los actos y documentos de las Instituciones del Estado que tengan la calidad de instrumento auténtico, podrán suscribirse mediante firma electrónica.

Interacción electrónica entre administrados y funcionarios públicos

Art. 22.- Las personas podrán relacionarse con las Instituciones del Estado, sin necesidad de firma electrónica, siempre que se ajusten a las técnicas y medios electrónicos establecidos para tal fin.

El uso de la firma electrónica del particular en la interacción con el Estado solo será necesario en casos de suscripción de contratos o cuando la ley expresamente exija firma.

Conservación, registro y archivo

Art. 23.- Las Instituciones del Estado podrán disponer la conservación, registro y archivo de cualquier actuación que esté bajo su competencia, por medio de sistemas electrónicos. Tales archivos y registros sustituirán a los registros físicos para todo efecto, sin embargo, no podrán destruirse los documentos originales sin la previa verificación y colaboración del Director del Archivo General de la Nación.

Comunicaciones electrónicas

Art. 24.- Cualquier Institución del Estado, siempre y cuando cuente con la infraestructura tecnológica adecuada podrá practicar comunicaciones por vía electrónica, utilizando firma electrónica, tales como citaciones y notificaciones, siempre y cuando el administrado o usuario de los servicios públicos haya elegido como domicilio especial una dirección de correo electrónico.

Las actuaciones de las Instituciones del Estado que sean comunicadas por medio de soporte electrónico deberán cumplir con los requisitos del ordenamiento legal de la materia y con la presente ley.

CAPITULO III
DE LA AUTORIDAD DE CONTROL Y VIGILANCIA

La Autoridad de Control y Vigilancia

Art. 25.- La Superintendencia General de Electricidad y Telecomunicaciones por medio de la Gerencia de Acreditación de Servicios de Certificación será competente para la acreditación, control y vigilancia de los proveedores de los servicios de certificación electrónica de conformidad con esta ley y su reglamento, sin perjuicio de las competencias que esta ley confiere a la Defensoría del Consumidor o a alguno de sus órganos.

De la Gerencia de Acreditación de Servicios de Certificación

Art. 26.- La SIGET organizará la Gerencia de Acreditación de Servicios de Certificación quien estará a cargo de uno de sus funcionarios, el cual será nombrado por el Superintendente.

Requisitos del Gerente de Acreditación de Servicios de Certificación

Art. 27.- El Gerente de Acreditación de Servicios de Certificación deberá reunir los requisitos exigidos en la Ley de Creación de la Superintendencia General de Electricidad y Telecomunicaciones para los gerentes de la Institución.

Competencias de la SIGET para la aplicación de la presente ley

Art. 28.- La SIGET por medio de la Gerencia de Acreditación de Servicios de Certificación, tendrá las siguientes competencias:

1. Otorgar la acreditación a los proveedores de servicios de certificación una vez cumplidas las formalidades y requisitos de esta ley, su reglamento y demás normas técnicas aplicables.

2. Validar los certificados de los diversos proveedores de servicios de certificación.

3. Imponer las sanciones establecidas en la presente ley.

4. Crear, actualizar y custodiar la Sección del Registro de los Proveedores de Servicios de Certificación, el cual dependerá del Registro de Electricidad y Telecomunicaciones y deberá estar disponible para consultas del público.

CAPÍTULO IV
DE LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN

Requisitos generales

Art. 32.- El servicio de certificación sólo podrá ser prestado por aquella persona o personas, naturales o jurídicas, públicas o privadas, que demuestren cumplir con los siguientes requisitos:

a) Tener suficiente capacidad técnica para garantizar la seguridad de las claves pública y privada así como la calidad y fiabilidad de los certificados emitidos de conformidad a los requerimientos contenidos en las Normas Técnicas.

b) Contar con el personal técnico adecuado con conocimiento especializado en la materia y experiencia en el servicio a prestar comprobable.

c) La capacidad económica y financiera suficiente para prestar los servicios autorizados como proveedor de servicios de certificación. En el caso de Instituciones del Estado, éstas deberán contar con un presupuesto de gastos y de ingresos que permitan el desarrollo de esta actividad.

d) Rendir fianza inicial por el monto de doscientos cincuenta mil dólares con el objetivo de indemnizar los daños y perjuicios que pudieren ocasionarse a los usuarios de los servicios de certificación, la cuál será revisada anualmente tomando en cuenta la variación del patrimonio social y el índice de precios al consumidor,

e) Presentar un pliego tarifario de los servicios que brindarán a los usuarios.

f) Un sistema de información de acceso libre, permanente, actualizado y eficiente en el cual se publiquen las políticas y procedimientos aplicados para la prestación de sus servicios, especialmente lo relacionado a las claves públicas otorgadas así como a los certificados electrónicos que hubiere proporcionado, revocado, suspendido o cancelado y las restricciones o limitaciones aplicables a éstos.

g) Garantiza, a solicitud del usuario, la suspensión o la cancelación de los certificados electrónicos que proporcione, de forma rápida y segura; y.

h) Satisfacer los demás requisitos previstos en esta ley

Acreditación de los Proveedores de Servicios de Certificación

Art. 33.- La acreditación de los proveedores de servicios de certificación será solicitada por el interesado que se encuentre previamente registrado como operador de redes comerciales, quien además deberá presentar un perfil técnico y económico en el que se refleje el cumplimiento de los requisitos antes relacionados, los cuáles serán verificados por la SIGET a través de una auditoría inicial cuyo costo será sufragado previamente por el solicitante. El plazo de duración de la acreditación será por tiempo indefinido, pero podrá ser revocada de conformidad con el Art. 51 lit. a).

La SIGET avalará el pliego tarifario que sea presentado por los proveedores de los servicios de certificación el cual deberá establecerse empleando un modelo basado en costos que sean razonables, no discriminatorios y transparentes.

Funcionamiento de los Proveedores de Servicios de Certificación extranjeros

Art. 34.- Los proveedores de servicios de certificación extranjeros podrán realizar actividades en el país y sus certificados tendrán validez solo sí estuviere avalado mediante un proveedor de servicios de certificación nacional debidamente acreditado.

Inicio de las actividades del Proveedores de Servicios de Certificación

Art. 35.- El proveedor de servicios de certificación acreditado que inicie sus actividades, deberá dar notificación de este hecho a la Gerencia de Acreditación de Servicios de Certificación a más tardar diez días hábiles con antelación al mismo.

Obligación de Notificación

Art. 36.- El cumplimiento de los requisitos exigidos por esta ley para prestar los servicios de certificación deberá asegurarse por todo el plazo en que el proveedor realice su actividad. Si surgen circunstancias dentro de las cuales esta garantía de cumplimiento ya no puede ser mantenida deberá notificarse de inmediato a la Gerencia de Acreditación de Servicios de Certificación.

Suspensión Temporal Voluntaria

Art. 37.-El Signatario podrá solicitar la suspensión temporal del servicio de certificación de la firma electrónica, en cuyo caso su proveedor deberá proceder a suspender el mismo durante el tiempo solicitado por el signatario, sin que por ello se reste validez a los actos jurídicos firmados con anterioridad a la suspensión.

Obligaciones de los Proveedores

Art. 38.- Los proveedores de servicios de certificación tendrán las siguientes obligaciones:

a) Inscribir el nombre de dominio en el registro correspondiente bajo el sufijo .sv.

b) Adoptar las medidas necesarias para determinar la exactitud de los certificados electrónicos que proporcionen, la identidad y la calidad del signatario.

c) Garantizar la validez, vigencia, legalidad y seguridad del certificado electrónico que proporcione.

d) Garantizar la adopción de las medidas necesarias para evitar la falsificación de certificados electrónicos y de las firmas electrónicas que proporcionen.

e) Verificar la información suministrada por el signatario.

f) Crear y mantener un archivo de certificados en medios electrónicos para su consulta por plazo indefinido.

g) Sin perjuicio de otras obligaciones establecidas en la Ley de Protección al Consumidor, deberá informar a los interesados en sus servicios de certificación, utilizando un lenguaje comprensible en su página web en la Internet y a través de cualquier otra forma de acceso público, los términos precisos y condiciones para el uso del certificado electrónico y, en particular, de cualquier limitación sobre su responsabilidad, así como de los procedimientos especiales existentes para resolver cualquier controversia.

h) Garantizar la autenticidad, integridad y confidencialidad de la información y documentos relacionados con los servicios que proporcione. A tales efectos, deberán mantener un respaldo tecnológico confiable y seguro de dicha información.

i) Efectuar las notificaciones para informar a los signatarios y personas interesadas, y las publicaciones necesarias acerca del vencimiento, revocación, suspensión o cancelación de los certificados electrónicos que proporcione, así como de cualquier otro aspecto de relevancia para el público en general, en relación con dichos certificados electrónicos.

J) Dar aviso a la Fiscalía General de la República cuando en el desarrollo de sus actividades tenga indicios del cometimiento de un delito.

k) Cooperar con las autoridades del Ministerio Público y judiciales cuando le sea requerido para la investigación de un delito o la presentación de una prueba.

l) Cumplir con las demás obligaciones establecidas en esta ley y su reglamento.

El incumplimiento de cualquiera de los requisitos anteriores dará lugar a las sanciones establecidas en la presente ley.

Pérdida de capacidad tecnológica o económica de los proveedores de servicios de certificación

Art. 39.- Cuando el proveedor de servicios de certificación pierda la capacidad técnica o económica necesaria para brindar el servicio posterior al inicio de sus actividades, determinado por auditoría o inspección, la SIGET concederá el plazo máximo de dos meses para suplir dichas deficiencias.

En caso de no suplir dichas deficiencias o de reiteración de las mismas en el lapso de tres años y en dos auditorías sucesivas, se aplicarán las sanciones previstas en esta ley.

Responsabilidad por daños y perjuicios

Art. 40.- Los proveedores de servicios de certificación serán responsables de los daños y perjuicios que ocasionen a los usuarios de sus servicios cuando deriven del incumplimiento de las obligaciones y requisitos establecidos en esta ley y su reglamento o del incumplimiento de sus obligaciones contractuales.

El proveedor de servicios de certificación también asume la obligación de resarcir por actos imputables a terceros que hayan sido encargados por él para la realización de servicios para el cumplimiento de sus funciones.

Para la responsabilidad por daños y perjuicios se observará el derecho común, sin embargo, le corresponderá al proveedor de servicios de certificación probar la debida diligencia.

Notificación del cese de actividades

Art. 41.- Cuando los proveedores de servicios de certificación decidan cesar en sus actividades, lo notificarán a la Gerencia de Acreditación de Servicios de Certificación, al menos con noventa días de anticipación a la fecha de cesación.

La Gerencia de Acreditación de Servicios de Certificación después de haber recibido la notificación , emitirá un resolución dentro de las siguientes setenta y dos horas, por medio de la cual se declare la cesación de actividades del proveedor de servicios de certificación como prestador de ese servicio, sin perjuicio, de las investigaciones que pueda realizar a fin de determinar las causas que originaron el cese de las actividades del proveedor y las medidas que fueren necesarias adoptar con el objeto de salvaguardar los derechos de los usuarios.

La Gerencia de Acreditación de Servicios de Certificación podrá ordenar al proveedor que realice los trámites que considere necesarios para hacer del conocimiento de los usuarios y del público en general, de la cesación de esas actividades, y para garantizar la conservación de la información que fuere de interés para sus usuarios y el público en general.

El proveedor de servicios de certificación trasladará sus usuarios activos a otro prestador con la finalidad de garantizar la continuidad del servicio hasta la finalización del contrato, previo consentimiento expreso del usuario, sin que signifique costo adicional para éste último. Si no existiere posibilidad de traspaso a otro proveedor o bien, deberá notificar a los usuarios, para que tomen conocimiento de la extinción de sus certificados, y a SIGET.

El proveedor de servicios de certificación deberá trasladar a SIGET el archivo de certificados en medio electrónico a que se refiere la letra f) del Art. 38.

En todo caso, el cese de las actividades de un proveedor de servicios de certificación conllevará su cancelación del registro llevado por la Gerencia de Acreditación de Servicios de Certificación así como el pago de las obligaciones económicas pendientes derivadas de sus funciones.

CAPITULO V

DE LOS CERTIFICADOS ELECTRONICOS

Garantía de la Autoría de la Firma Electrónica

Art. 42.- El certificado electrónico garantiza la autoría de la firma electrónica así como la autenticidad, integridad, confidencialidad y no repudiación del documento electrónico.

Si el certificado electrónico no garantiza la autoría y demás características antes dichas, por alteración o cualquier otra razón, el documento electrónico carecerá de validez.

Vigencia del Certificado Electrónico

Art. 43.- El proveedor de servicios de certificación y el signatario, de mutuo acuerdo, determinarán la vigencia del certificado electrónico.

Cancelación del Certificado Electrónico

Art. 44.- El certificado electrónico de la firma electrónica puede ser cancelado por resolución judicial o del Ministerio Público de conformidad con el ordenamiento legal. Asimismo puede ser cancelado por resolución razonada emitida por la SIGET por medio de la Gerencia de Acreditación de Servicios de Certificación, en cualquiera de los supuestos siguientes:

1. Que se compruebe que alguno de los datos del certificado electrónico proporcionado por el proveedor de servicios de certificación es falso.

2. Que sea violentado el sistema de seguridad del proveedor de servicios de certificación que afecte la integridad y confiabilidad del certificado.

3. Que el signatario de aviso al proveedor del hurto, destrucción o extravío del certificado electrónico.

Procedimiento para la cancelación de un certificado electrónico

Art. 45. La SIGET por medio de la Gerencia de Acreditación de Servicios de Certificación, previa denuncia del interesado o de oficio, ordenará audiencia por tres días al proveedor de servicios de certificación y con lo que conteste o no, se abrirá a pruebas por ocho días hábiles a fin de demostrar cualquiera de las situaciones consideradas en el artículo anterior, finalizado el término probatorio, la SIGET emitirá resolución razonada en la que determine si es procedente la cancelación del certificado que ampara la firma electrónica, esta resolución admitirá recurso de revisión y será resuelto en el plazo de quince días hábiles con la vista de autos.

Contenido de los Certificados Electrónicos

Art. 46.-Los certificados electrónicos deberán contener la siguiente información:

1. Identificación del proveedor de servicios de certificación que proporciona el certificado electrónico, indicando su domicilio y dirección electrónica.

2. Fecha de la acreditación y caducidad asignada al proveedor de servicios de certificación por la SIGET por medio de la Gerencia de Acreditación de Servicios de Certificación.

3. Identificación del titular del certificado electrónico, indicando su domicilio y dirección electrónica.

4. La clave pública del titular del certificado.

5. Las fechas de inicio y vencimiento del periodo de vigencia del certificado electrónico.

6. El Algoritmo empleado para la generación de la firma electrónica.

7. Un serial único de identificación del certificado electrónico.

8. Cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que esté sometido el certificado electrónico.

9. Indicación de la ruta de certificación.

Certificados Electrónicos Extranjeros

Art. 47.-Los certificados electrónicos emitidos por proveedores de servicios de certificación extranjeros tendrán la misma validez y eficacia jurídica reconocida, siempre que cumplan con lo requerido en la presente ley y su reglamento

Los certificados electrónicos extranjeros, no garantizados por un proveedor de servicios de certificación debidamente acreditado, carecerán de los efectos jurídicos que se atribuyen en la presente ley.

CAPÍTULO VII

DE LOS DERECHOS Y OBLIGACIONES DE LOS USUARIOS DE LOS SERVICIOS DE FIRMA Y CERTIFICACIÓN ELECTRÓNICOS

Derechos de los usuarios

Art. 48.- Además de los derechos reconocidos por la Ley de Protección al Consumidor y cualquier otra normativa aplicable, los usuarios o titulares de certificados o firmas electrónicas tendrán los siguientes derechos:

1. A ser informados por los proveedores de servicios de certificación, de las características generales de los procedimientos de creación y de verificación de firma electrónica, así como las reglas sobre prácticas de certificación y los demás que estos se comprometan a seguir en la prestación de los servicios, previamente a que se empiece a efectuar;

2. A la confidencialidad en la información cuando los proveedores de servicios de certificación decidan cesar en sus actividades,

3. A ser informado, antes de la emisión de un certificado, del pliego tarifario, incluyendo cargos adicionales y formas de pago, en su caso; de las condiciones precisas para la utilización del certificado y de sus limitaciones de uso, y de los procedimientos de reclamación y de resolución de litigios;

4. A que el prestador de servicios le proporcionen la información sobre sus domicilios en El Salvador;

5. A ser informado, al menos con noventa días de anticipación, por los prestadores de servicios de certificación para los efectos del artículo 41,

6. A traspasar sus datos a otro prestador de servicios de certificación si así lo solicitan,

7. A que el prestador no proporcione más servicios y de calidad inferior de los que haya pactado, y a no recibir publicidad comercial de ningún tipo por intermedio del prestador, salvo autorización expresa del usuario en todos los casos señalados;

8. A que se le respeten los principios y derechos establecidos en el artículo 5 de esta ley.

La violación a los derechos previstos en este artículo constituye infracción grave en los términos previstos en la Ley de Protección al Consumidor y será sancionada como tal.

La determinación de la infracción y la imposición de la sanción correspondiente será competencia del Tribunal Sancionador de la Defensoría del Consumidor de acuerdo con el procedimiento previsto en la Ley de Protección al Consumidor en lo que fuere aplicable.

Obligaciones de los usuarios

Art. 49.- Los usuarios o titulares de certificados o firmas electrónicas quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a brindar declaraciones veraces y completas. Además, estarán obligados a custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que le proporcione el prestador y a actualizar sus datos en la medida que éstos vayan cambiando, so pena de pagar por la indemnización de daños y perjuicios derivada del incumplimiento de estas obligaciones.

CAPÍTULO VI
DE LAS INFRACCIONES Y SANCIONES

Infracciones

Art. 50.- Las infracciones a la presente ley se clasifican en graves y menos graves.

Son infracciones graves:

a) No suplir las deficiencias económicas o técnicas que motivaren las acciones previstas en el Art. 39.

b) La reiteración al incurrir en las deficiencias económicas o técnicas referidas en el Art. 39.
c) No renovar las garantías exigidas con el objetivo de garantizar daños y perjuicios que pudieran ocasionarse a los usuarios de servicios de certificación.
d) No garantizar los servicios de suspensión, cancelación y revocación de los certificados electrónicos que proporcione.
e) Negar información requerida por la SIGET, especialmente en el desarrollo de una inspección o auditoría
f) Brindar información falsa cuando sea solicitada por la SIGET
g) Negar el acceso a las instalaciones físicas y sistemas de los proveedores de servicios de certificación.
h) Violar intencionalmente el secreto de las comunicaciones de sus usuarios.
i) Cometer tres o más infracciones tipificadas como menos graves en el lapso de tres años.
j) No cumplir las resoluciones emitidas por la SIGET de acuerdo a los procedimientos establecidos en esta ley y su reglamento.

Son infracciones menos graves:
a) No informar al usuario el tipo de servicio en el que deberá utilizarse el certificado
b) No cancelar las obligaciones económicas derivadas de la presente ley
c) La revelación culposa del secreto de las comunicaciones de sus usuarios.

Sanciones
Art. 51.- Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones graves, se impondrá al infractor hasta una multa de ochenta y un mil seiscientos treinta y siete dólares con cincuenta y siete centavos de dólar.

En el caso de las letras a) y b) del artículo anterior, se ordenará la revocación de la acreditación para operar y se aplicarán las reglas previstas para el cese de actividades contenida en el Art. 41.
b) Por la comisión de infracciones menos graves, se impondrá al infractor hasta una multa de dieciséis mil trescientos veintisiete dólares con cincuenta y un centavos de dólar.

Las infracciones graves llevarán aparejada, a costa del sancionado, la publicación de la resolución sancionadora en un periódico de circulación nacional y en el Diario Oficial, en la página de inicio del sitio web del Prestador de Servicios de Certificación y en el sitio de Internet de la SIGET, una vez que aquélla tenga carácter de firme.

El valor de las multas será ajustado con base al índice de precios al consumidor publicado por el Ministerio de Economía, el ajuste se realizará anualmente a partir del primer día hábil del mes de enero.

TITULO V
DISPOSICIONES FINALES

CAPITULO UNICO

Reglamento

Art. 52.- El Presidente de la República deberá emitir el reglamento de esta ley, en un plazo no mayor a seis meses contados a partir de su publicación.

Disposición transitoria

Art. 53.- El Ministerio de Hacienda contará con un plazo máximo de seis meses contados a partir de la vigencia de esta ley para hacer la entrega a SIGET de la base de datos y una memoria de labores de

su función como Autoridad de Control y Vigilancia de las Entidades Certificadoras en las funciones otorgadas por la Ley de Simplificación Aduanera.

Cualquier persona natural o jurídica que al momento de entrar en vigencia la presente ley se encuentre brindando servicios de certificación, contará con un plazo no mayor de seis meses para adecuarse al cumplimiento de los requerimientos establecidos por la misma.

Disposiciones Supletorias

Art. 54.- Las disposiciones y procedimientos contenidos en la Ley de Telecomunicaciones podrán aplicarse en lo que fuere pertinente.

Derogatorias

Art. 55.- Derogase los artículos 6 Inc. 3º y 4º, 7 Inc. 2º, 8, 8-A, 8-B, 8-C, 8-D, 8-E, 9 Inc. 1º, 2º y 3º de la Ley de Simplificación Aduanera contenida en el Decreto Legislativo No. 529, de fecha 13 de enero de 1999, publicada en el Diario Oficial No. 23, Tomo 342 de fecha 3 de febrero de 1999.

Vigencia

Art. 56 La presente ley entrará en vigencia ocho días después de su publicación.

DADO EN EL SALON AZUL DEL PALACIO LEGISLATIVO: San Salvador, a los….

ANEXO IX
Noticias Publicadas En Periódicos De Mayor Circulación Nacionales E Internacionales Acerca de Comercio Electrónico y Firma Electrónica.

15 al 21
DE MAIG DE 2005

SUPLEMENTO DE ECONOMÍA DEL DIARI DE TARRAGONA

Telef. 977 29 97 52
977 29 97 35
977 29 97 57
Fax. 977 22 30 13
e.mail:
economia@diaridetarragona.com
Coordinación:
Núria Pérez
Rafael Servent
Rafel Villa

ECONOMÍA y NEGOCIOS

EN EL MUNDO EXISTEN

12,3 MILLONES DE VICTIMAS DEL TRABAJO FORZOSO

12,3 millones de personas en el mundo son víctimas del trabajo forzoso y generan 31.600 millones de dólares de beneficio anual a intermediarios, empresas y multinacionales, según la Organización Internacional del Trabajo (OIT). En Europa se detecta un tráfico ilegal de mano de obra, destinado en sus dos terceras partes al abuso sexual; el resto se reparte entre el entorno doméstico y agrícola y en tareas clandestinas.

LOS NUEVOS EUROS

MOSTRARAN EL MAPA DE TODA EUROPA

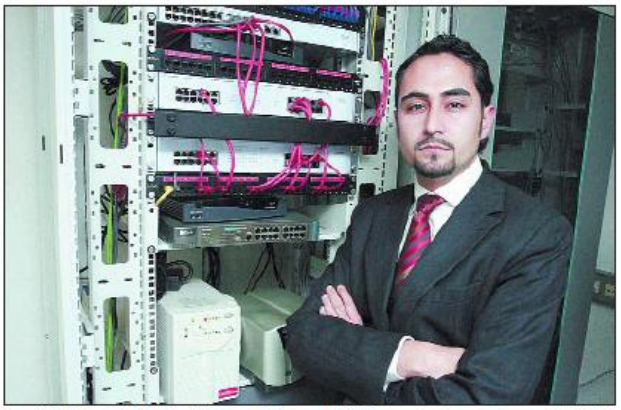
Las futuras acuñaciones del euro mostrarán un mapa de Europa más amplio que el actual, para incluir a los nuevos países miembros de la UE que aspiran a entrar en el euro.

Notarios virtuales al servicio de la red

Terceros de Confianza validan legalmente las operaciones en Internet

Si una compraventa habitual que supone un gasto importante acostumbra a ser validada por un notario, ¿qué pasa cuando esta venta se hace a través de un mercado tan virtual como es el de Internet? ¿Quién da fe de que se ha hecho la operación, y de las condiciones en que se ha efectuado? La respuesta es una figura creada recientemente y que se denomina terceros de confianza, el mismo nombre de la empresa creada por el abogado tarraconense Jaume Garrido.

RAFEL VILLA/TARRAGONA
rvilla@diaridetarragona.com



Jaume Garrido, uno de los socios fundadores de Terceros de Confianza. PERE TODA

Usted hace una compra por Internet. Va rellenando las sucesivas pantallas para adquirir un artículo y, justo en el momento antes de transmitir los datos de su tarjeta de crédito, aparece un enlace en el que se le pregunta si quiere archivar los datos de la operación. Acaba de recibir el servicio de Terceros de Confianza, empresa que, si usted lo decide, congelará la *fotografía* de ese momento en que usted ha realizado la compra y la guardará durante cinco años. Si existe algún problema con las condiciones de la compra, podrá recurrir a la *fotografía* guardada por Terceros de Confianza para reclamar sus derechos.

Ésta es la base del funcionamiento de Terceros de Confianza, que ejerce de algo parecido a un notario pero de las operaciones efectuadas a través de Internet. Su existencia está regulada por el Ministerio de Ciencia y Tecnología (actualmente de Industria, Comercio y Turismo) con el objetivo de ser una tercera parte imparcial y ajena a los contratantes, para otorgar seguridad jurídica a toda una serie de operaciones que se hacen a través de la red. Dos abogados y dos tecnólogos tuvieron la idea de lanzarse a este negocio cuando la figura estaba en proceso de gestación, así que el mismo día en que se aprobó la ley que creaba la figura del tercero de confianza, ellos pudieron registrar el nombre de la figura como el propio de su empresa. Por tanto, toda la promoción e información que se ha dado sobre esta figura legal, se ha hecho también sobre la empresa.

En realidad, la mayor parte de la promoción que se ha efectuado sobre el servicio la ha realizado la propia empresa, consciente de que se trata de unas prestaciones no conocidas hasta el momento, respecto a las cuales la administración parece haberse desmentido. Desde la creación de la figura en una ley aprobada el 17 de julio de 2002, el Ministerio no ha vuelto a preocuparse al respecto, creando una sensación de falta de cobertura legal. «Llevamos tiempo reclamando que se regule al respecto, que se dicten las condiciones como mínimo creando un registro de las entidades que pueden prestar este servicio, homologándolas, concretando los avales», explica Garrido. No se trata tan sólo de dar cobertura legal a las empresas que prestan este servicio, sino sobre todo de evitar que otras se apropien de la información con fines fraudulentos.

Garrido se muestra convencido del futuro de este negocio, ya que «todas las encuestas que se han hecho muestran que la existencia de un tercero da más seguridad a la operación, sobre todo porque nosotros no nos quedamos con los datos de la tarjeta de crédito, sino que intervenimos justo antes. Además, si existe un desacuerdo en la operación, el cliente dispone de una prueba aceptada por las dos partes que no se puede negar».

Eso sí, se paga el pecado de ser los iniciadores de un nuevo mercado, todavía poco conocido. Sí que en Estados Unidos esta figura existe y funciona regularmente, pero en España tal vez es aún demasiado pronto. «Pero estamos convencidos que cada vez habrá más transacciones en Internet y, por tanto, más problemas. Cada vez se necesitará más nuestro servicio», asegura Garrido.

El ángel del negocio

Pese a que los fundadores de Terceros de Confianza sabían desde el principio que poner en funcionamiento un negocio de este tipo requeriría paciencia hasta obtener los primeros beneficios, también es cierto que al tratarse de profesionales jóvenes no podían destinar grandes cantidades a invertir para mantener en funcionamiento el negocio. Así que la suerte estuvo en hallar un *business angel*, un economista al que le gustó la idea con independencia de la facturación alcanzada. Su inversión sirvió para poder contratar personal que se dedica a la agencia profesionalmente, liberando así a los socios fundadores.

EL COMERCIO ELECTRÓNICO SIN REGULACIÓN

» El ejecutivo elaboró una ley para la comunicación y firma electrónica. Su aprobación generaría confianza entre las empresas extranjeras

Carmen Molina Tamacas

El correo electrónico es un elemento indispensable en la comunicación contemporánea. Ahorra tiempo y dinero y es una puerta de entrada al universo infinito de la información y el intercambio.

El ir y venir de "sobrecitos virtuales" ya es utilizado en muchos países como una herramienta para hacer negocios, a pequeña y gran escala. Ahora, si usted no quiere salir de su casa para comprar un objeto -desde los insumos para su empresa hasta un lapicero- puede hacerlo por Internet: realiza una búsqueda, compara precios y características y paga con su tarjeta de crédito. Obviamente esperará recibir a vuelta de correo, desde cualquier parte del mundo, un artículo como el que tanto necesita y le prometieron.

"Es un elemento necesario, pero no ha sido indispensable, pero sería bueno tener la ley para dar confianza a las empresas de afuera"
RAFAEL IBARRA
Experto en Internet

En muchos países, esas transacciones ocurren desde hace tiempo y son considerados comercio electrónico, o e-commerce, en su forma más pura. Su desarrollo ha fomentado que existan reglas y procedimientos en caso de que algo pase y que el consumidor o el proveedor no queden satisfechos con el resultado.

En El Salvador, el comercio electrónico ya existe. No sólo porque los clientes pueden ordenar libros, artículos para bebés y de oficina, por medio de Internet, a cualquier proveedor en el mundo, sino porque pueden hacerlo aquí mismo.

Por ejemplo, algunos almacenes locales ya permiten hacer compras en línea; empresas de telefonía ofrecen recarga de saldo en sus páginas web y enviando mensajes de texto en donde autoriza el cobro de servicios como el envío de salmos, bromas, compra de ring-tones y participación en rifas y sorteos. Pero si quiere hacer un reclamo o no está satisfecho con lo que recibió, ¿quién podrá defenderlo?

Salvo la Defensoría del Consumidor, que ha establecido límites y alcances de la actuación de las empresas locales, el comercio electrónico como tal no está regulado. Si usted quisiera llevar adelante un juicio mercantil por una transacción que realizó vía electrónica, ningún juez aceptará como válidos los documentos impresos de las comunicaciones, y mucho menos de los correos enviados y recibidos.

ILUSTRACIÓN EDH OTTO HERNÁNDEZ

Esas transacciones comerciales que ya pueden realizarse, aunque son legales, "falta regularlas adecuadamente", como reconoce Sigfredo Figueroa, director ejecutivo del programa ePaís, que lleva a cabo la Secretaría Técnica de la Presidencia de la República.

Esta dependencia, con el apoyo de la Comisión Nacional para la Sociedad de la Información y consultores nacionales e internacionales, ha elaborado una Estrategia Nacional para que el país desarrolle y aproveche sus potenciales informáticos.

"Se definieron tres grandes líneas de trabajo: cómo se regulaba la comunicación y firma electrónica, la protección de datos y comercio electrónico. De todo eso, quizá lo más importante en este momento es el Anteproyecto de Ley de Comunicación y Firma Electrónica, porque eso le va a dar una legalidad a todas las operaciones electrónicas (...) Esa es la ley madre para que exista validez legal de todas las operaciones", destacó Figueroa.

En síntesis, el Gobierno considera que éste es el camino para regular el comercio electrónico en el país.

La comunicación electrónica es todo intercambio que se realiza por medio de Internet y sus múltiples herramientas: correo, video-llamadas, entre otras. La firma electrónica, la cual se utiliza en estas transacciones, no es, como muchos pudieran pensar, el facsímil de una firma: es una clave o código, producto de un proceso matemático, que permite hacer compras y ventas, con la garantía de inviolabilidad. La ley, no obstante, le confiere la misma validez que una firma de puño y letra en papel.

"Por e-commerce se conocen las transacciones que facilitan la venta de bienes y servicios por medio de Internet. Pero esa definición es angosta. Debería ser llamado e-bussines, ya que no sólo se hacen transacciones sino que se pueden vender servicios y crear redes en las cadenas de suministros más eficaces con socios y proveedores", dijo Oscar Herrera, consultor en la materia.

EL REINO DEL PAPEL

Hay empresas salvadoreñas que, desde luego, ya realizan transacciones comerciales internacionales; éstas se amparan en la legislación del país donde está establecido su contraparte y realizan todo en orden, comentó el gerente general de la Cámara de Comercio e Industria de El Salvador (CCIES), Rodrigo Ernesto Ayala.

Otras, como el asocio de Cuscatrading.com, se ha montado en la plataforma de la tienda electrónica por antonomasia, Amazon.com, para exportar. Uno de los precursores del e-commerce en El Salvador, latienda.com.sv, tiene un "Top 10" de los productos más buscados: cocina salvadoreña, comida típica, camisolas deportivas, libros de cultura e

Una ley que hace perdurar la autenticidad

El Diario de Hoy

2000

En ese año, el abogado Ricardo Cevallos elaboró el proyecto de Ley de Comercio Electrónico. Pero la propuesta no prosperó entre los sectores.

Además de definir los conceptos básicos del comercio electrónico, como acreditación, certificado electrónico, clave privada o pública, firma electrónica y proveedor, entre otros, el Anteproyecto de Ley de Comunicación y Firma Electrónica considera cinco principios legales básicos: autenticidad, integridad, confidencialidad, equivalencia y no repudiación.

Con la primera se garantiza que el mensaje es confiable, garantía que perdura a través del tiempo. La integridad, por su parte, otorga certeza de que los datos recibidos por medios electrónicos no han sido modificados en su tránsito desde el iniciador hasta el destinatario.

Asimismo, la confidencialidad, que garantiza al iniciador y destinatario que los mensajes electrónicos no serán conocidos por terceras personas que no han sido autorizadas; la equivalencia garantizará que las instancias administrativas o judiciales no podrán rechazar los documentos electrónicos debidamente certificados –ya que no estarán contenidos en un soporte distinto al papel- y la no repudiación. Éste último garantiza que cuando un mensaje ha sido suscrito con firma electrónica, su autor no puede aducir rechazo hacia él.

E-COMMERCE, OPCIÓN EN TIEMPOS DE CRISIS

¿Han aparecido en su casillero correos electrónicos ofreciéndole productos y servicios por parte de empresas que nunca ha visitado y a las cuales nunca ha requerido información? Las bases de datos de correos electrónicos son muy apetecidas en la actualidad, especialmente para hacer negocios. Por eso es que se recomienda no reenviar las famosas "cadenas".

Pero al estar inmersos en el océano infinito que e web, todos somos potenciales clientes de alguien, o algo. "Hacer mercadeo electrónico, o e-marketing, ma importancia en tiempos de crisis", indica Oscar I rrera, experto en e-commerce.

No solo se trata sólo del correo masivo –la atarr electrónica por medio de la cual las empresas quie pescar clientes-, apunta. Ya que la publicidad es uno los rubros que más sufren a la hora de los recortes p supuestarios, anunciarse en y por Internet, espec mente en lugares de mucho tráfico, puede llevar a re perar la inversión inicial con mucha rapidez, sostuv

En Internet pueden encontrarse opciones para a ratar costos, como los proveedores de códigos de rra, cuyas membresías y renovaciones no son nece rias después de la compra, recomendó.

historia salvadoreña, entre otros.

Sin embargo, ese tipo de transacciones no es "lo más fuerte" del comercio electrónico, apuntó el experto en Internet e informática Rafael Ibarra. Destacó la importancia que en El Salvador ha cobrado la banca electrónica, ya que en una misma sesión, un usuario puede pagarlos recibos de sus servicios –agua, energía eléctrica, colegios y universidades-, evitando los inconvenientes de tener que hacer fila en un banco.

¿No es contradictorio que para iniciar algunos de estos trámites virtuales le piden que llegue en persona a una oficina y firme papeles? Eso se debe a la falta de legislación.

UN PROBLEMA DE "JURISDICCIÓN"

Ya que la Ley debe ser aprobada por la Asamblea Legislativa, se espera que los diputados cuenten con la apertura y el interés para discutir un tema trascendental para el país.

Ibarra, quien forma parte de la Comisión Nacional para la Sociedad de la Información, subrayó que el país ya debería tener, como mínimo, esa ley aprobada.

"No tanto para el comercio local, es un elemento necesario pero no ha sido indispensable para hacer transacciones; pero sería bueno, positivo, que tuviéramos leyes como la firma electrónica para darle más tranquilidad y confianza especialmente a los de afuera (empresas extranjeras)", dijo.

El abogado Ricardo Cevallos elaboró, a solicitud del gobierno, el borrador de un anteproyecto de Ley de Comercio Electrónico, allá por 2000. La aprobación de este documento, que tuvo como base la Ley Modelo de Comercio Electrónico de la Organización de las Naciones Unidas (ONU) no prosperó, quizás por los momentos difíciles que enfrentaría la economía del país después de los terremotos y la negociación del Tratado de Libre Comercio con Estados Unidos.

Sin embargo, como experto en el tema, Cevallos opina que si bien las transacciones comerciales ya están reguladas, las leyes locales están desfasadas respecto a los medios por los cuales se puede comerciar, uno de ellos es Internet.

"El problema básico del comercio electrónico es la jurisdicción. Si compro aquí no hay problema, pero si lo hago por Internet, en otro país, es difícil ubicarlo geográfica y legalmente", reflexionó. Y añadió que las leyes de e-commerce no buscan regular las transacciones, sino el medio.

Figueroa lo confirma: "Lo que se hace es legislar o establecer seguridad jurídica a todos los usuarios de Tecnologías de Información y Comunicación (TIC) cuando realicen transacciones mediante comunicaciones electrónicas. Lo que se busca se da y es imposible controlar. (...) Lo que queremos con la Ley de Comunicación y Firma Electrónica es garantizar las operaciones que se realizan a través de documentos electrónicos".

Herrera afirma que una vez se cuente con legislación, uno de los servicios que debería agilizarse es el sistema de pagos, para facilitar transacciones comerciales.

CONCEPTOS DEL E-COMMERCE

ACREDITACIÓN:
Es la autorización que otorga la Superintendencia General de Electricidad y Telecomunicaciones a los proveedores de servicios electrónicos de certificación par operar y dar certificados electrónicos, una vez cumplidos los requisitos y las condiciones establecidos por la ley.

CLAVE PRIVADA:
Clave generada por un proceso matemático que contiene datos únicos que el firmante utiliza para crear la firma electrónica. Su conocimiento y control es exclusivo del firmante. Y la clave pública es generada por un proceso matemático que contien datos únicos que permiten verificar la firma del titular.

FIRMA ELECTRÓNICA:
Es la combinación de la clave pública y privada que asocia a una persona con su voluntad d firmar, utilizando sistemas criptográficos asimétricos, contenida en un certificado expedido por un proveedor de servicios acreditado .

CERTIFICADO ELECTRÓNICO:
Documento proporcionado por un proveedor de servicios de certificación que verifica la correspondencia entre la clave pública y la clave privada con su titular, otorgándole certeza y validez a la firma electrónica. Y el proveedor de servicios da l certificados electrónicos.

EL CAMINO DE LA LEY
La elaboración del Anteproyect de Ley de Comunicación y Firm Electrónica está por concluir. Pasará a revisión por la Secretaría Jurídica de la Presidencia de la República. Y e Minec deberá presentarla como iniciativa de Ley ante la Asambl

ANEXO X
Ley de Certificados, Firmas Digitales y Documentos Electrónicos de Costa Rica.

LA GACETA
Diario Oficial
GACETA ELECTRÓNICA http://www.imprenal.go.cr

La Uruca, San José, Costa Rica, jueves 13 de octubre del 2005

¢ 175,00 | AÑO CXXVII | Nº 197 - 4 Páginas

PODER LEGISLATIVO

LEYES

Nº 8454

LA ASAMBLEA LEGISLATIVA
DE LA REPÚBLICA DE COSTA RICA

DECRETA:

LEY DE CERTIFICADOS, FIRMAS DIGITALES
Y DOCUMENTOS ELECTRÓNICOS

CAPÍTULO I

Disposiciones generales

Artículo 1º—**Ámbito de aplicación.** Esta Ley se aplicará a toda clase de transacciones y actos jurídicos, públicos o privados, salvo disposición legal en contrario, o que la naturaleza o los requisitos particulares del acto o negocio concretos resulten incompatibles.

El Estado y todas las entidades públicas quedan expresamente facultados para utilizar los certificados, las firmas digitales y los documentos electrónicos, dentro de sus respectivos ámbitos de competencia.

Artículo 2º—**Principios.** En materia de certificados, firmas digitales y documentos electrónicos, la implementación, interpretación y aplicación de esta Ley deberán observar los siguientes principios:

a) Regulación legal mínima y desregulación de trámites.
b) Autonomía de la voluntad de los particulares para reglar sus relaciones.
c) Utilización, con las limitaciones legales, de reglamentos autónomos por la Administración Pública para desarrollar la organización y el servicio, interno o externo.
d) Igualdad de tratamiento para las tecnologías de generación, proceso o almacenamiento involucradas.

CAPÍTULO II

Documentos

Artículo 3º—**Reconocimiento de la equivalencia funcional.** Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos.

En cualquier norma del ordenamiento jurídico en la que se haga referencia a un documento o comunicación, se entenderán de igual manera tanto los electrónicos como los físicos. No obstante, el empleo del soporte electrónico para un documento determinado no dispensa, en ningún caso, el cumplimiento de los requisitos y las formalidades que la ley exija para cada acto o negocio jurídico en particular.

Artículo 4º—**Calificación jurídica y fuerza probatoria.** Los documentos electrónicos se calificarán como públicos o privados, y se les reconocerá fuerza probatoria en las mismas condiciones que a los documentos físicos.

Artículo 5º—**En particular y excepciones.** En particular y sin que conlleve la exclusión de otros actos, contratos o negocios jurídicos, la utilización de documentos electrónicos es válida para lo siguiente:

a) La formación, formalización y ejecución de los contratos.
b) El señalamiento para notificaciones conforme a la Ley de notificaciones, citaciones y otras comunicaciones judiciales.
c) La tramitación, gestión y conservación de expedientes judiciales y administrativos; asimismo, la recepción, práctica y conservación de prueba, incluida la recibida por archivos y medios electrónicos. De igual manera, los órganos jurisdiccionales que requieran la actualización de certificaciones y, en general, de otras piezas, podrán proceder sobre simples impresiones de los documentos en línea efectuadas por el despacho o aceptar las impresiones de dichos documentos en línea, aportadas por la parte interesada y certificadas notarialmente.
d) La emisión de certificaciones, constancias y otros documentos.
e) La presentación, tramitación e inscripción de documentos en el Registro Nacional.
f) La gestión, conservación y utilización, en general, de protocolos notariales, incluso la manifestación del consentimiento y la firma de las partes.

No se podrán consignar en documentos electrónicos:

a) Los actos o negocios en los que, por mandato legal, la fijación física resulte consustancial.
b) Las disposiciones por causa de muerte.
c) Los actos y convenios relativos al Derecho de familia.
d) Los actos personalísimos en general.

Artículo 6º—**Gestión y conservación de documentos electrónicos.** Cuando legalmente se requiera que un documento sea conservado para futura referencia, se podrá optar por hacerlo en soporte electrónico, siempre que se apliquen las medidas de seguridad necesarias para garantizar su inalterabilidad, se posibilite su acceso o consulta posterior y se preserve, además, la información relativa a su origen y otras características básicas.

La transición o migración a soporte electrónico, cuando se trate de registros, archivos o respaldos que por ley deban ser conservados, deberá contar, previamente, con la autorización de la autoridad competente.

En lo relativo al Estado y sus instituciones, se aplicará la Ley del Sistema Nacional de Archivos, Nº 7202, de 24 de octubre de 1990. La Dirección General del Archivo Nacional dictará las regulaciones necesarias para asegurar la gestión debida y conservación de los documentos, mensajes o archivos electrónicos.

Artículo 7º—**Satisfacción de los requisitos fiscales.** Cuando la emisión de un acto o la celebración de un negocio jurídico en soporte electrónico conlleve el pago de requisitos fiscales, el obligado al pago deberá conservar el comprobante respectivo y exhibirlo cuando una autoridad competente lo requiera.

CAPÍTULO III

Firmas digitales

Artículo 8º—**Alcance del concepto.** Entiéndese por firma digital cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico.

Una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado.

Artículo 9º—**Valor equivalente.** Los documentos y las comunicaciones suscritos mediante firma digital, tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito. En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera tanto la digital como la manuscrita.

Los documentos públicos electrónicos deberán llevar la firma digital certificada.

Artículo 10.—**Presunción de autoría y responsabilidad.** Todo documento, mensaje electrónico o archivo digital asociado a una firma digital certificada se presumirá, salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital, vigente en el momento de su emisión.

No obstante, esta presunción no dispensa el cumplimiento de las formalidades adicionales de autenticación, certificación o registro que, desde el punto de vista jurídico, exija la ley para un acto o negocio determinado.

CAPÍTULO IV

Certificación digital

SECCIÓN I

Los certificados

Artículo 11.—**Alcance.** Entiéndese por certificado digital el mecanismo electrónico o digital mediante el que se pueda garantizar, confirmar o validar técnicamente:

a) La vinculación jurídica entre un documento, una firma digital y una persona.
b) La integridad, autenticidad y no alteración en general del documento, así como la firma digital asociada.
c) La autenticación o certificación del documento y la firma digital asociada, únicamente en el supuesto del ejercicio de potestades públicas certificadoras.
d) Las demás que establezca esta Ley y su Reglamento.

Artículo 12.—**Mecanismos.** Con las limitaciones de este capítulo, el Estado, las instituciones públicas y las empresas públicas y privadas, las personas jurídicas y los particulares, en general, en sus diversas relaciones, estarán facultados para establecer los mecanismos de certificación o validación que convengan a sus intereses.

Para tales efectos podrán:

a) Utilizar mecanismos de certificación o validación máquina a máquina, persona a persona, programa a programa y sus interrelaciones, incluso sistemas de llave pública y llave privada, firma digital y otros mecanismos digitales que ofrezcan una óptima seguridad.
b) Establecer mecanismos de adscripción voluntaria para la emisión, la percepción y el intercambio de documentos electrónicos y firmas asociadas, en función de las competencias, los intereses y el giro comercial.
c) De consuno, instituir mecanismos de certificación para la emisión, la recepción y el intercambio de documentos electrónicos y firmas asociadas, para relaciones jurídicas concretas.
d) Instaurar, en el caso de dependencias públicas, sistemas de certificación por intermedio de particulares, quienes deberán cumplir los trámites de la Ley de contratación administrativa.
e) Fungir como un certificador respecto de sus despachos y funcionarios, o de otras dependencias públicas, en el caso del Estado y las demás instituciones públicas.
f) Ofrecer, en el caso de las empresas públicas cuyo giro lo admita, servicios comerciales de certificación en condiciones de igualdad con las empresas de carácter privado.
g) Implantar mecanismos de certificación para la tramitación, gestión y conservación de expedientes judiciales y administrativos.

Artículo 13.—**Homologación de certificados extranjeros.** Se conferirá pleno valor y eficacia jurídica a un certificado digital emitido en el extranjero, en cualesquiera de los siguientes casos:

a) Cuando esté respaldado por un certificador registrado en el país, en virtud de existir una relación de corresponsalía en los términos del artículo 20 de esta Ley.
b) Cuando cumpla todos los requisitos enunciados en el artículo 19 de esta Ley y exista un acuerdo recíproco en este sentido entre Costa Rica y el país de origen del certificador extranjero.

Artículo 14.—**Suspensión de certificados digitales.** Se podrá suspender un certificado digital en los siguientes casos:

a) Por petición del propio usuario a favor de quien se expidió.
b) Como medida cautelar, cuando el certificador que lo emitió tenga sospechas fundadas de que el propio usuario haya comprometido su confiabilidad, desatendido los lineamientos de seguridad establecidos, suplido información falsa al certificador u omitido cualquier otra información relevante, para obtener o renovar el certificado. En este caso, la suspensión podrá ser recurrida ante la Dirección de Certificadores de Firma Digital regulada en la siguiente sección, con aplicación de lo dispuesto en el artículo 148 de la Ley General de la Administración Pública.
c) Si contra el usuario se ha dictado auto de apertura a juicio, por delitos en cuya comisión se haya utilizado la firma digital.
d) Por orden judicial o de la Dirección de Certificadores de Firma Digital. En este último caso, cuando esta lo determine o cuando el Ente Costarricense de Acreditación (ECA) acredite que el usuario incumple las obligaciones que le imponen esta Ley y su Reglamento.
e) Por no cancelar oportunamente el costo del servicio.

Artículo 15.—**Revocación de certificados digitales.** El certificado digital será revocado en los siguientes supuestos:

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

Artículo 16.—**Revocación por el cese de actividades del certificador.** El cese de actividades del certificador implicará la revocatoria de todos los certificados que haya expedido, salvo que anteriormente hayan sido traspasados a otro certificador, previo consentimiento del usuario.

Artículo 17.—**Conservación de efectos.** La suspensión o revocación de un certificado digital no producirá, por sí sola, la invalidez de los actos o negocios realizados con anterioridad al amparo de dicho certificado.

SECCIÓN II

Certificadores

Artículo 18.—**Definición y reconocimiento jurídico.** Se entenderá como certificador la persona jurídica pública o privada, nacional o extranjera, que emite certificados digitales y está debidamente autorizada según esta Ley o su Reglamento; asimismo, que haya rendido la debida garantía de fidelidad. El monto de la garantía será fijado por la Dirección de Certificadores de Firma Digital y podrá ser hipoteca, fianza o póliza de fidelidad de un ente asegurador, o bien, un depósito en efectivo.

Sin perjuicio de lo dispuesto en los artículos 3º, 9º y 19 de esta Ley, los certificados digitales expedidos por certificadores registrados ante la Dirección de Certificadores de Firma Digital, solo tendrán pleno efecto legal frente a terceros, así como respecto del Estado y sus instituciones.

Artículo 19.—**Requisitos, trámites y funciones.** La Dirección de Certificadores de Firma Digital será la encargada de establecer, vía reglamento, todos los requisitos, el trámite y las funciones de las personas que soliciten su registro ante esta Dirección; para ello, el ECA, a solicitud del Ministerio de Ciencia y Tecnología, deberá fijar los requerimientos técnicos para el estudio, de acuerdo con la Ley Nº 8279, de 2 de mayo de 2002, y las prácticas y los estándares internacionales.

Artículo 20.—**Corresponsalía.** Los certificadores registrados podrán concertar relaciones de corresponsalía con entidades similares del extranjero, para efectos de homologar los certificados digitales expedidos por estas entidades o que estas hagan lo propio en el exterior con los emitidos por los certificadores registrados.

Se deberá informar a la Dirección de Certificadores de Firma Digital, acerca del establecimiento de relaciones de esta clase, de previo a ofrecer ese servicio al público.

Artículo 21.—**Auditorías.** Todo certificador registrado estará sujeto a los procedimientos de evaluación y auditoría que acuerde efectuar la Dirección de Certificadores de Firma Digital o el ECA.

Artículo 22.—**Cesación voluntaria de funciones.** Los certificadores registrados de carácter privado podrán cesar en sus funciones, siempre y cuando avisen, a los usuarios, con un mes de anticipación como mínimo, y con dos meses a la Dirección de Certificadores de Firma Digital.

SECCIÓN III

Administración del Sistema de Certificación

Artículo 23.—**Dirección.** La Dirección de Certificadores de Firma Digital, perteneciente al Ministerio de Ciencia y Tecnología, será el órgano administrador y supervisor del Sistema de Certificación.

Artículo 24.—**Funciones.** La Dirección de Certificadores de Firma Digital tendrá las siguientes funciones:

a) Recibir, tramitar y resolver las solicitudes de inscripción de los certificadores.
b) Llevar un registro de los certificadores y certificados digitales.
c) Suspender o revocar la inscripción de los certificadores y de certificados, así como ejercer el régimen disciplinario en los casos y en la forma previstos en esta Ley y su Reglamento.
d) Expedir claves y certificados a favor de los certificadores registrados, y mantener el correspondiente repositorio de acceso público, con las características técnicas que indique el Reglamento.
e) Fiscalizar el funcionamiento de los certificadores registrados, para asegurar su confiabilidad, eficiencia y el cabal cumplimiento de la normativa aplicable, imponiendo, en caso necesario, las sanciones previstas en esta Ley. La supervisión podrá ser ejercida por medio del ECA, en el ámbito de su competencia.
f) Mantener una página electrónica en la red Internet, a fin de divulgar, permanentemente, información relativa a las actividades de la Dirección de Certificadores de Firma Digital y el registro correspondiente de certificadores.
g) Señalar las medidas que estime necesarias para proteger los derechos, los intereses y la confidencialidad de los usuarios, así como la continuidad y eficiencia del servicio, y velar por la ejecución de tales disposiciones.
h) Dictar el Reglamento respectivo para el registro de certificadores.
i) Las demás funciones que esta Ley o su Reglamento le señalen.

Artículo 25.—**Jefatura.** El superior administrativo de la Dirección de Certificadores de Firma Digital será el director, quien será nombrado por el ministro de Ciencia y Tecnología y será un funcionario de confianza, de conformidad con el inciso g) del artículo 4, del Estatuto de Servicio Civil. El director deberá declarar sus bienes oportunamente, de acuerdo con la Ley contra el enriquecimiento ilícito de los servidores públicos.

CAPÍTULO V

Sanciones

Artículo 26.—**Sanciones a certificadores.** Previa oportunidad de defensa, la Dirección de Certificadores de Firma Digital podrá imponerles, a los certificadores, las siguientes sanciones:

a) Amonestación.
b) Multa hasta por el equivalente a cien salarios base; para la denominación salario base se considerará lo indicado en el artículo 2º de la Ley Nº 7337, de 5 de mayo de 1993.
c) Suspensión hasta por un año.
d) Revocatoria de la inscripción.

El certificador a quien se le haya revocado su inscripción, no podrá volver a registrarse durante los siguientes cinco años, ya sea como tal o por medio de otra persona jurídica en la que figuren las mismas personas como representantes legales, propietarias o dueñas de más de un veinticinco por ciento (25%) del capital.

Artículo 27.—**Amonestación.** Se aplicará la amonestación, a los certificadores, en los siguientes casos:

a) Por la emisión de certificados digitales que no incluyan la totalidad de los datos requeridos por esta Ley o su Reglamento, cuando la infracción no requiera una sanción mayor.
b) Por no suministrar a tiempo los datos requeridos por la Dirección de Certificadores de Firma Digital, en ejercicio de sus funciones.
c) Por cualquier otra infracción a la presente Ley que no tenga prevista una sanción mayor.

Artículo 28.—**Multa.** Se aplicará la multa, a los certificadores, en los siguientes casos:

a) Cuando se emita un certificado y no se observen las políticas de seguridad o de certificación previamente divulgadas, de modo que cause perjuicio a los usuarios o a terceros.
b) Cuando no se suspenda o revoque, oportunamente, un certificado, estando obligados a hacerlo.
c) Por cualquier impedimento u obstrucción a las inspecciones o auditorías por parte de la Dirección de Certificadores de Firma Digital o del ECA.
d) Por el incumplimiento de los lineamientos técnicos o de seguridad impartidos por la Dirección de Certificadores de Firma Digital.
e) Por la reincidencia en la comisión de infracciones, que hayan dado lugar a la sanción de amonestación, dentro de los dos años siguientes.

Artículo 29º—**Suspensión.** Se suspenderá al certificador que:

a) No renueve oportunamente la caución que respalde su funcionamiento o la rinda en forma indebida.
b) Reincida en cualesquiera de las infracciones que le hayan merecido una sanción de multa, dentro de los siguientes dos años.

Artículo 30.—**Revocatoria de la inscripción.** Se podrá revocar la inscripción de un certificador cuando:

a) Se compruebe la expedición de certificados falsos.
b) Se compruebe que el certificador suministró información o presentó documentos falsos, con el fin de obtener el registro.
c) Reincida en cualesquiera de las infracciones que le hayan merecido una sanción de suspensión, dentro de los cinco años siguientes.

Artículo 31.—**Procedimiento.** Todas las sanciones serán impuestas mediante el procedimiento administrativo ordinario, previsto en la Ley General de la Administración Pública, salvo en el caso de amonestación, en que podrá aplicarse el procedimiento sumario.

Artículo 32.—**Publicidad.** Excepto el caso de amonestación, todas las sanciones administrativas impuestas serán publicadas por medio de reseña o trascripción íntegra en *La Gaceta*, sin perjuicio de que, en atención al caso concreto, se disponga, además, publicarlas en uno o más medios de circulación o difusión nacional.

Asimismo, la Dirección de Certificadores de Firma Digital dispondrá la publicación electrónica en su página de información en Internet.

CAPÍTULO VI

Disposiciones finales y transitorias

Artículo 33.—**Reglamentación.** El Poder Ejecutivo reglamentará esta Ley dentro de los seis meses siguientes a su publicación.

Además, para el trámite eficiente de sus asuntos, cada dependencia pública podrá adoptar las medidas particulares de aplicación de esta Ley de acuerdo con sus necesidades.

Transitorio único.—Los rubros presupuestarios requeridos para que la Dirección de Certificadores de Firma Digital entre en funcionamiento, deberán ser incluidos por el Ministerio de Hacienda, a propuesta del Ministerio de Ciencia y Tecnología, en el primer presupuesto remitido a la Asamblea Legislativa, después de promulgada esta Ley.

Rige a partir de su publicación.

Comuníquese al Poder Ejecutivo

Asamblea Legislativa.—San José, a los veintitrés días del mes de agosto de dos mil cinco.—Gerardo González Esquivel, Presidente.—Daysi Serrano Vargas, Primera Secretaria.—Luis Paulino Rodríguez Mena, Segundo Secretario.

Dado en la Presidencia de la República.—San José, a los treinta días del mes de agosto del dos mil cinco.

Ejecútese y publíquese

ABEL PACHECO DE LA ESPRIELLA.—El Ministro de Ciencia y Tecnología, Fernando Gutiérrez Ortiz.—1 vez.—(Solicitud Nº 063).—C-160200.—(L8454-83130).

ANEXO XI
Ley para el Reconocimiento de las Comunicaciones y Firmas Digitales de Guatemala.

Fundado en 1880

Diario de Centro América

DECANO DE LA PRENSA CENTROAMERICANA I ÓRGANO OFICIAL DE LA REPÚBLICA DE GUATEMALA, C. A.

MARTES 23 de septiembre de 2008 No. 23 Tomo CCLXXXV Directora General: Ana María Rodas www.dca.gob.gt

Sumario

ATENCIÓN ANUNCIANTES:

IMPRESIÓN SE HACE CONFORME ORIGINAL

Toda impresión en la parte legal del Diario de Centro América, se hace respetando el original. Por lo anterior, esta administración ruega al público tomar nota.

ORGANISMO LEGISLATIVO

CONGRESO DE LA REPÚBLICA DE GUATEMALA

DECRETO NÚMERO 47-2008

EL CONGRESO DE LA REPÚBLICA DE GUATEMALA

CONSIDERANDO:

Que el Estado como responsable del bien común debe mantener, reforzar y aplicar políticas y acciones que permitan una mayor participación en la dinámica y beneficios del desarrollo económico y social libre, la modernización, los procesos económicos sin trabas ni obstáculos artificiales, así como la inserción del país en las corrientes del progreso mundial de manera sostenible y equitativa.

CONSIDERANDO:

Que la inmersión masiva de la tecnología en nuestra sociedad es una realidad que no podemos ignorar y por ende se debe revisar los conceptos y visiones tradicionales del mundo físico para adaptarlos al actual contexto del mundo digital.

CONSIDERANDO:

Que la promoción del comercio electrónico en todos sus aspectos requiere de una legislación cuyo fundamento sea, entre otros, la facilitación del comercio electrónico en el interior y mas allá de las fronteras nacionales, la validación, fomento y estímulo de las operaciones efectuadas por medio de las nuevas tecnologías de la información sobre la base de la autonomía de la voluntad y el apoyo a las nuevas prácticas comerciales, tomando en cuenta en todo momento la neutralidad tecnológica.

CONSIDERANDO:

Que la integración al comercio electrónico global requiere que sean adoptados instrumentos técnicos y legales basados en los modelos de legislación internacional que buscan la uniformización de esta rama del derecho tan especializada, y que debe dársele seguridad jurídica y técnica a las contrataciones, comunicaciones y firmas electrónicas mediante el señalamiento de la equivalencia funcional a estas últimas con respecto a los documentos en papel y las firmas manuscritas.

POR TANTO:

En ejercicio de las atribuciones que le confiere la literal a) del artículo 171 de la Constitución Política de la República,

DECRETA:

La siguiente:

LEY PARA EL RECONOCIMIENTO DE LAS COMUNICACIONES Y FIRMAS ELECTRÓNICAS

TÍTULO I
COMERCIO ELECTRÓNICO EN GENERAL

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Ámbito de aplicación. La presente ley será aplicable a todo tipo de comunicación electrónica, transacción o acto jurídico, público o privado, nacional o internacional, salvo en los casos siguientes:

a) En las obligaciones contraídas por el Estado en virtud de Convenios o Tratados Internacionales.

b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.

El Estado y sus instituciones quedan expresamente facultados para la utilización de las comunicaciones y firmas electrónicas.

En las transacciones y actos realizados exclusivamente entre sujetos privados y que no afecten derechos de terceros, las partes podrán convenir en la aplicación de los mecanismos previstos en esta ley o bien de cualesquiera otras alternativas que deseen para asegurar la autenticidad e integridad de sus comunicaciones electrónicas.

Las disposiciones contenidas en esta ley se aplicarán sin perjuicio de las normas relativas a la celebración, la formalización, la validez y la eficacia de los contratos y otros actos jurídicos; el régimen jurídico aplicable a las obligaciones; y de las obligaciones que para los comerciantes les establece la legislación vigente.

Las normas sobre la presentación de servicios de certificación de firma electrónica que recoge esta ley, no sustituyen ni modifican las que regulan las funciones que corresponde realizar a las personas facultadas, con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en su elevación a públicos.

Artículo 2. Definiciones. Para los efectos de la presente ley, se entenderá por:

Certificado: Todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma, usualmente emitido por un tercero diferente del originador y el destinatario.

Comercio Electrónico: Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de una o más comunicaciones electrónicas o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, incluyendo el factoraje y el arrendamiento de bienes de equipo con opción a compra; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; de inversión; de financiación; de banca; de seguros; de todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.

Comunicación: Toda exposición, declaración, reclamación, aviso o solicitud, incluida una oferta y la aceptación de una oferta, que las partes hayan de hacer o decidan hacer en relación con la formación o el cumplimiento de un contrato.

Comunicación Electrónica: Toda comunicación que las partes hagan por medio de mensajes de datos.

Datos de creación de firma: los datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

Destinatario: La parte designada por el iniciador para recibir la comunicación electrónica, pero que no esté actuando a título de intermediario con respecto a esa comunicación electrónica.

Estampado Cronológico: Comunicación electrónica firmada por una entidad de certificación que sirve para verificar que otra comunicación electrónica no ha cambiado en un período que comienza en la fecha y hora en que se presta el servicio y termina en la fecha y hora en que la firma de la comunicación electrónica generada por el prestador del servicio de estampado pierde validez.

Firma Electrónica: Los datos en forma electrónica consignados en una comunicación electrónica, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante con relación a la comunicación electrónica e indicar que el firmante aprueba la información recogida en la comunicación electrónica.

Firma Electrónica Avanzada: La firma electrónica que cumple los requisitos siguientes:

a. Estar vinculada al firmante de manera única;
b. Permitir la identificación del firmante;
c. Haber sido creada utilizando los medios que el firmante puede mantener bajo su exclusivo control;
d. Estar vinculada a los datos a que se refiere, de modo que cualquier cambio ulterior de los mismos sea detectable.

Firmante: La persona que posee los datos de creación de la firma y que actúa en nombre propio o de la persona a la que representa.

Iniciador: Toda parte que haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar una comunicación electrónica antes de ser archivada, si ese es el caso, pero que no haya actuado a título de intermediario con respecto a esa comunicación electrónica.

Intercambio Electrónico de Datos (IED): La transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto.

Intermediario: En relación con una determinada comunicación electrónica, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicha comunicación electrónica o preste algún otro servicio con respecto a él.

Mensaje de Datos: El documento o información generada, enviada, recibida o archivada por medios electrónicos, magnéticos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (IED), el correo electrónico, el telegrama, el télex o el telefax.

Parte que confía: La persona que pueda actuar sobre la base de un certificado o de una firma electrónica.

Prestador de Servicios de Certificación: Se entenderá la entidad que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas.

Sede o lugar del establecimiento comercial: Se entenderá todo lugar donde una parte mantiene un centro de operaciones no temporal para realizar una actividad económica distinta del suministro transitorio de bienes o servicios desde determinado lugar.

Sistema Automatizado de Mensajes: Todo programa informático o un medio electrónico o algún otro medio automatizado utilizado para iniciar una acción o para responder a operaciones o mensajes de datos, que actué, total o parcialmente, sin que una persona física haya de intervenir o revisar la actuación cada vez que se inicie una acción o que el sistema genere una respuesta.

Sistema de Información: Todo sistema que sirva para generar, enviar, recibir, archivar o procesar de alguna otra forma comunicaciones electrónicas.

Artículo 3. Interpretación. En la interpretación de la presente ley habrán de tenerse en cuenta su origen internacional, la necesidad de promover la uniformidad de su aplicación y de velar por la observancia de la buena fe, tanto en el comercio nacional como internacional.

Las cuestiones relativas a materias que se rijan por la presente ley y que no estén expresamente resueltas en ella, serán dirimidas de conformidad con los principios generales en que ella se inspira.

Artículo 4. Modificación mediante acuerdo mutuo. Salvo que se disponga otra cosa, la manera como se formalicen las relaciones entre las partes que generan, envían, reciban, archivan o procesan de alguna otra forma comunicaciones electrónicas, podrán ser modificadas mediante acuerdo mutuo entre las partes.

En caso de no haber acuerdo, se entenderán formalizadas conforme a lo que estipula el Capítulo III del Título I de esta Ley.

CAPÍTULO II
APLICACIÓN DE LOS REQUISITOS JURÍDICOS A LAS COMUNICACIONES ELECTRÓNICAS

Artículo 5. Reconocimiento jurídico de las comunicaciones electrónicas. No se negarán efectos jurídicos, validez o fuerza obligatoria a una comunicación o a un contrato por la sola razón de que esa comunicación o ese contrato estén en forma de comunicación electrónica.

Nada de lo dispuesto en esta ley hará que una parte esté obligada a utilizar o a aceptar información en forma de comunicación electrónica, pero su conformidad al respecto podrá inferirse de su conducta. Así mismo, nada de lo dispuesto en la presente ley obligará a que una comunicación o un contrato tengan que hacerse o probarse de alguna forma particular.

Artículo 6. Incorporación por Remisión. Salvo acuerdo en contrario entre las partes, cuando en una comunicación electrónica se haga remisión total o parcial a directrices, normas, estándares, acuerdos, cláusulas, condiciones, cualquier información o términos fácilmente accesibles con la intención de incorporarlos como parte del contenido o hacerlos vinculantes jurídicamente, se presume que esos términos están incorporados por remisión a esa comunicación electrónica. Entre las partes y conforme a la ley, esos términos serán jurídicamente válidos como si hubieran sido incorporados en su totalidad en la comunicación electrónica.

Artículo 7. Escrito. Cuando cualquier norma jurídica requiera que una información, comunicación o un contrato consten por escrito, en papel o en cualquier medio físico, o prevea consecuencias en el caso de que eso no se cumpla, una comunicación electrónica cumplirá ese requisito si la información consignada en su texto es accesible para su ulterior consulta.

Artículo 8. Firma. Cuando cualquier norma jurídica requiera que una comunicación o un contrato sea firmado por una parte, o prevea consecuencias en el caso de que no se firme, ese requisito se dará por cumplido respecto de una comunicación electrónica:

a) Si se utiliza un método para determinar la identidad de esa parte y para indicar la voluntad que tiene tal parte respecto de la información consignada en la comunicación electrónica; y,

b) Si el método empleado:

1. Es fiable y resulta apropiado para los fines para los que se generó o transmitió la comunicación electrónica, atendidas todas las circunstancias del caso, inclusive todo acuerdo aplicable; o si,

2. Se ha demostrado en la práctica que, por sí solo o con el respaldo de otras pruebas, dicho método cumple las funciones enunciadas en la literal a) del presente artículo.

Artículo 9. Original. Cuando cualquier norma jurídica requiera que una comunicación o un contrato se proporcione o conserve en su formato original, o prevea consecuencias en el caso de que eso no se cumpla, ese requisito se tendrá por cumplido respecto de una comunicación electrónica:

a) Si existe alguna garantía fiable de la integridad de la información que contiene, a partir del momento en que se generó por primera vez en su forma definitiva, tanto en comunicación electrónica como de otra índole; y,

b) Si, en los casos en que se exija proporcionar la información que contiene, ésta puede exhibirse a la persona a la que se ha de proporcionar.

Artículo 10. Integridad de una comunicación electrónica. Para efectos del artículo 9 anterior, se considerará que la información consignada en una comunicación electrónica es íntegra, si atiende a los criterios siguientes:

a) Ésta se ha mantenido completa y sin alteraciones que no sean la adición de algún endoso o algún cambio sobrevenido en el curso normal de su transmisión, archivo o presentación; y,

b) El grado de fiabilidad requerido se determinará teniendo en cuenta la finalidad para la que se generó la información, así como todas las circunstancias del caso.

Artículo 11. Admisibilidad y fuerza probatoria de las comunicaciones electrónicas. Las comunicaciones electrónicas serán admisibles como medios de prueba. No se negará eficacia, validez o fuerza obligatoria y probatoria en toda actuación administrativa, judicial o privada a todo tipo de información en forma de comunicación electrónica, por el sólo hecho que se trate de una comunicación electrónica, ni en razón de no haber sido presentado en su forma original.

Artículo 12. Criterio para valorar probatoriamente una comunicación electrónica. Toda información presentada en forma de comunicación electrónica gozará de la debida fuerza probatoria de conformidad con los criterios reconocidos por la legislación para la apreciación de la prueba. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje; la fiabilidad de la forma en la que se haya conservado la integridad de la información; la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

Artículo 13. Conservación de las comunicaciones electrónicas. Cuando cualquier norma jurídica requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho mediante la conservación de las comunicaciones electrónicas, siempre que se cumplan las condiciones siguientes:

a) Que la información que contengan sea accesible para su posterior consulta;

b) Que la comunicación electrónica sea conservada en el formato en que se haya generado, enviado o recibido o con algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida; y,

c) Que se conserve, de haber alguna, toda información o dato que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido.

No estarán sujetos a la obligación de conservación, los documentos, registros o informaciones que tenga por única finalidad facilitar el envío o recepción de la comunicación electrónica. Los libros y papeles podrán ser conservados en cualquier medio tecnológico que garantice su reproducción exacta.

Artículo 14. Conservación de mensajes de datos y archivo de documentos a través de terceros. El cumplimiento de la obligación de conservar documentos, registros o informaciones en comunicaciones electrónicas, se podrá realizar directamente o a través de terceros, siempre y cuando se cumplan las condiciones enunciadas en el artículo anterior.

CAPÍTULO III
COMUNICACIONES ELECTRÓNICAS Y FORMACIÓN DE CONTRATOS A TRAVÉS DE MEDIOS ELECTRÓNICOS

Artículo 15. Formación y validez de los contratos. En la formación de un contrato por particulares o entidades públicas, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de una comunicación electrónica. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación una o más comunicaciones electrónicas.

Artículo 16. Reconocimiento de las comunicaciones electrónicas por las partes. En las relaciones entre el iniciador y el destinatario de una comunicación electrónica, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de comunicación electrónica.

Artículo 17. Atribución de una comunicación electrónica. Se entenderá que una comunicación electrónica proviene del iniciador, si ha sido enviado por el propio iniciador.

En las relaciones entre el iniciador y el destinatario, se entenderá que una comunicación electrónica proviene del iniciador si ha sido enviado:

a) Por alguna persona facultada para actuar en nombre del iniciador respecto de esa comunicación; o,

b) Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

Artículo 18. Presunción del origen de una comunicación electrónica. En las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que una comunicación electrónica proviene del iniciador, y a actuar en consecuencia, cuando:

a) Para comprobar que la comunicación provenía del iniciador, el destinatario haya aplicado adecuadamente un procedimiento aceptado previamente por el iniciador con ese fin; o,

b) La comunicación electrónica que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar una comunicación electrónica como propia.

Lo expresado en este artículo, no se aplicará a partir del momento en que el destinatario haya sido informado por el iniciador que la comunicación electrónica no provenía del iniciador y haya dispuesto de un plazo razonable para actuar en consecuencia; o, en los casos previstos en la literal b) de este artículo, desde el momento en que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la comunicación electrónica no provenía del iniciador.

Artículo 19. Concordancia de la comunicación electrónica enviada con la comunicación electrónica recibida. Siempre que una comunicación electrónica provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, éste último tendrá derecho a considerar que la comunicación electrónica recibida corresponde a la que quería enviar el iniciador, y podrá proceder en consecuencia.

El destinatario no gozará de este derecho si sabía, o hubiera sabido, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a un error en la comunicación electrónica recibida.

El destinatario tendrá derecho a considerar que cada comunicación electrónica recibida es una comunicación electrónica separada y al actuar en consecuencia, salvo en la medida en que duplique otra comunicación electrónica, y que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la nueva comunicación electrónica era un duplicado.

Artículo 20. Acuse de recibo. Si al enviar o antes de enviar una comunicación electrónica, el iniciador solicite o acuerda con el destinatario que se acuse recibo de la comunicación electrónica, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

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

b) Todo acto del destinatario que baste para indicar al iniciador que se ha recibido la comunicación electrónica.

Cuando el iniciador haya indicado que los efectos de la comunicación electrónica estarán condicionados a la recepción de un acuse de recibo, se considerará que la comunicación electrónica no ha sido enviada en tanto que no se haya recibido el acuse de recibo.

Artículo 21. Falta de Acuse de Recibo. De conformidad con el artículo anterior, cuando el iniciador no haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, si no ha recibido acuse en el plazo fijado o convenido o no se ha fijado o convenido ningún plazo, en un plazo de cinco días el iniciador podrá:

a) Dar aviso al destinatario de que no ha recibido acuse de recibo y fijar un plazo razonable para su recepción; y,

b) De no recibir acuse dentro del plazo fijado conforme a la literal a) anterior, podrá, dando aviso de ello al destinatario, considerar que la comunicación electrónica no ha sido enviada o ejercer cualquier otro derecho que pueda tener.

Artículo 22. Presunción de recepción de una comunicación electrónica. Cuando el iniciador reciba acuse de recibo del destinatario, se presumirá que éste ha recibido la comunicación electrónica correspondiente.

Esa presunción no implicará que la comunicación electrónica corresponda al mensaje recibido. Cuando en el acuse de recibo se indique que la comunicación electrónica recibida cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que ello es así.

Artículo 23. Efectos jurídicos. Salvo en lo que se refiere al envío o recepción de comunicaciones electrónicas, los artículos 21 y 22, no obedecen al propósito de regir las consecuencias jurídicas que puedan derivarse de esa comunicación electrónica o de su acuse de recibo. Las consecuencias jurídicas de las comunicaciones electrónicas se regirán conforme a las normas aplicables al acto o negocio jurídico contenido en dicho mensaje de datos.

Artículo 24. Tiempo y lugar del envío y la recepción de las comunicaciones electrónicas. De no convenir otra cosa el iniciador y el destinatario, la comunicación electrónica se tendrá por:

a) **Expedida:** en el momento en que salga de un sistema de información que esté bajo el control del iniciador o de la parte que la envíe en nombre de éste o, si la comunicación electrónica no ha salido de un sistema de información que esté bajo el control del iniciador o de la parte que la envíe en nombre de éste, en el momento en que esa comunicación se reciba.

b) **Recibida:** en el momento en que pueda ser recuperada por el destinatario en una dirección electrónica que él haya designado. La comunicación electrónica se tendrá por recibida en otra dirección electrónica del destinatario en el momento en que pueda ser recuperada por el destinatario en esa dirección y en el momento en que el destinatario tenga conocimiento de que esa comunicación ha sido enviada a dicha dirección. Se presumirá que una comunicación electrónica puede ser obtenida por el destinatario en el momento en que llegue a la dirección electrónica de éste.

c) La comunicación electrónica se tendrá por expedida en el lugar en que el iniciador tenga su establecimiento y por recibida en el lugar en que el destinatario tenga el suyo, conforme se determine en función de lo dispuesto en esta ley.

d) La literal b) del presente artículo será aplicable aun cuando el sistema de información que sirva de soporte a la dirección electrónica esté ubicado en un lugar distinto de aquel en que se tenga por recibida la comunicación en virtud de la literal c) del presente artículo.

Artículo 25. Invitaciones para presentar ofertas. Toda propuesta de celebrar un contrato presentada por medio de una o más comunicaciones electrónicas, que no vaya dirigida a una o varias partes determinadas, sino que sea generalmente accesible para toda parte que haga uso de sistemas de información, así como toda propuesta que haga uso de aplicaciones interactivas para hacer pedidos a través de dichos sistemas, se considerará una invitación a presentar ofertas, salvo que indique claramente la intención de la parte que presenta la propuesta de quedar obligada por su oferta en caso de que sea aceptada.

Artículo 26. Empleo de sistemas automatizados de mensajes para la formación de un contrato. No se negará validez ni fuerza obligatoria a un contrato que se haya formado por la interacción entre un sistema automatizado de mensajes y una persona física, o por la interacción entre sistemas automatizados de mensajes, por la simple razón de que ninguna persona física haya revisado cada uno de los distintos actos realizados a través de los sistemas o el contrato resultante de tales actos ni haya intervenido en ellos.

Artículo 27. Disponibilidad de las condiciones contractuales. Nada de lo dispuesto en la presente ley afectará a la aplicación de regla de derecho alguna por la que se obligue a una parte que negocie algunas o todas las condiciones de un contrato mediante el intercambio de comunicaciones electrónicas a poner a disposición de la otra parte contratante, de determinada manera, las comunicaciones electrónicas que contengan las condiciones del contrato, ni eximirá a una parte que no lo haga de las consecuencias jurídicas de no haberlo hecho.

Artículo 28. Error en las comunicaciones electrónicas. Cuando una persona física cometa un error al introducir los datos de una comunicación electrónica intercambiada con el sistema automatizado de mensajes de otra parte y dicho sistema no le brinde la oportunidad de corregir el error, esa persona, o la parte en cuyo nombre ésta haya actuado, tendrá derecho a retirar la parte de la comunicación electrónica en que se produjo dicho error, si:

a) La persona, o la parte en cuyo nombre haya actuado esa persona, notifica a la otra parte el error tan pronto como sea posible después de haberse percatado de éste y le indica que lo ha cometido; y si,

b) La persona, o la parte en cuyo nombre haya actuado esa persona, no ha utilizado bienes o servicios ni ha obtenido ningún beneficio material o valor de los bienes o servicios, si los hubiere, que haya recibido de la otra parte.

Nada de lo dispuesto en el presente artículo afectara a la aplicación de regla de derecho alguna que regule las consecuencias de un error cometido, a reserva de lo dispuesto en el primer párrafo de este artículo.

Artículo 29. Ubicación de las partes. Para los fines de la presente ley, se presumirá que la sede o el lugar del establecimiento comercial de una parte está en el lugar por ella indicado, salvo que otra parte demuestre que la parte que hizo esa indicación no tiene sede o establecimiento comercial alguno en ese lugar.

Si una parte no ha indicado la sede o el lugar del establecimiento comercial, y tiene más de un establecimiento comercial, se considerará como tal, para los efectos de la presente Ley, el que tenga la relación más estrecha con el contrato pertinente, habida cuenta de las circunstancias conocidas o previstas por las partes en cualquier momento antes de la celebración del contrato o al concluirse éste.

Si una persona física no tiene establecimiento comercial, se tendrá en cuenta su lugar de residencia habitual.

Un lugar no constituye un establecimiento comercial por el solo hecho de que sea el lugar:

a) Donde estén ubicados el equipo y la tecnología que sirven de soporte para el sistema de información utilizado por una de las partes para la formación de un contrato; o,

b) Donde otras partes puedan obtener acceso a dicho sistema de información.

El hecho de que una parte haga uso de un nombre de dominio o de una dirección de correo electrónico vinculados a cierto país no crea la presunción de que su establecimiento comercial se encuentra en dicho país.

Artículo 30. Requisitos de información. Nada de lo dispuesto en la presente ley afectará a la aplicación de norma jurídica alguna en virtud de la cual las partes deban revelar su identidad, la ubicación de su establecimiento u otros datos, ni eximirá de consecuencias jurídicas a una parte que haya hecho a este respecto declaraciones inexactas, incompletas o falsas.

TÍTULO II
COMERCIO ELECTRÓNICO EN MATERIAS ESPECÍFICAS

CAPÍTULO I
TRANSPORTE DE MERCANCÍAS

Artículo 31. Actos relacionados con los contratos de transporte de mercancías. Sin perjuicio de lo dispuesto en el Título I de la presente ley, el presente capítulo será aplicable a cualquiera de los siguientes actos que guarde relación con un contrato de transporte de mercancías, o con su cumplimiento, sin que la lista sea exhaustiva:

a) Indicación de las marcas, el número, la cantidad o el peso de las mercancías; declaración de la índole o el valor de las mercancías; emisión de un recibo, factura o comprobante por las mercancías; confirmación de haberse completado la carga de las mercancías.

b) Notificación a alguna persona de las cláusulas y condiciones del contrato; comunicación de instrucciones al portador.

c) Reclamación de la entrega de las mercancías; autorización para proceder a la entrega de las mercancías; notificación de la pérdida de las mercancías o de los daños que hayan sufrido.

d) Cualquier otra notificación o declaración relativas al cumplimiento del contrato.

e) Promesa de hacer entrega de las mercancías a la persona designada o a una persona autorizada para reclamar esa entrega.

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

g) Adquisición o transferencia de derechos y obligaciones con arreglo al contrato.

Artículo 32. Documentos de transporte. Con sujeción a lo dispuesto en el tercer párrafo de este artículo, en los casos en que la ley requiera que alguno de los actos enunciados en el artículo 31 anterior se lleve a cabo por escrito o mediante un documento que conste de papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos.

El párrafo anterior será aplicable tanto si el requisito en él previsto está expresado en forma de obligación, como si la ley simplemente prevé consecuencias en el caso de que no se lleve a cabo el acto por escrito o mediante un documento.

Cuando se conceda algún derecho a una persona determinada y a ninguna otra, o ésta adquiera alguna obligación, y la ley requiera que, para que ese acto surta efecto, el derecho o la obligación hayan de transferirse a esa persona mediante el envío o la utilización de un documento, ese requisito quedará satisfecho si el derecho o la obligación se transfiere mediante la utilización de uno o más mensajes de datos, siempre que se emplee un método fiable para garantizar la singularidad de ese mensaje o esos mensajes de datos.

Para los fines del párrafo anterior, el nivel de fiabilidad requerido será determinado conforme a los fines para los que se transfirió el derecho o la obligación y de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

Cuando se utilicen uno o más mensajes de datos para llevar a cabo alguno de los actos enunciados en las literales f) y g) del artículo 31 anterior, no será válido ningún documento utilizado para llevar a cabo cualquiera de esos actos, a menos que se haya puesto fin al uso de mensajes de datos para sustituirlo por el de documentos. Todo documento que se emita en esas circunstancias deberá contener una declaración a tal efecto. La sustitución de mensajes de datos por documentos no afectará a los derechos ni a las obligaciones de las partes.

Cuando se aplique obligatoriamente una norma jurídica a un contrato de transporte de mercancías que esté consignado, o del que se haya dejado constancia en un documento, esa norma no dejará de aplicarse a un contrato de transporte de mercancías del que se haya dejado constancia en uno o más mensajes de datos por razón de que el contrato conste en ese mensaje o esos mensajes de datos en lugar de constar en un documento.

TÍTULO III
DISPOSICIONES COMPLEMENTARIAS AL COMERCIO ELECTRÓNICO

CAPÍTULO I
FIRMA ELECTRÓNICA AVANZADA Y PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Artículo 33. Efectos jurídicos de una firma electrónica o firma electrónica avanzada. La firma electrónica o la firma electrónica avanzada, la cual podrá estar certificada por una entidad prestadora de servicios de certificación, que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta, según los criterios de apreciación establecidos en las normas procesales.

Se excluye de esta normativa lo referente a las disposiciones por causa de muerte y a los actos jurídicos del derecho de familia.

Cuando una firma electrónica avanzada haya sido fijada en una comunicación electrónica se presume que el suscriptor de aquella tenía la intención de acreditar esa comunicación electrónica y de ser vinculado con el contenido del mismo. Para considerarse fiable el uso de una firma electrónica avanzada, ésta tendrá que incorporar como mínimo los atributos siguientes:

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

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

c) Que sea 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 la firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, que sea posible detectar cualquier alteración de esa información hecha después del momento de la firma.

Lo dispuesto en este artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre, de cualquier otra manera, la fiabilidad de una firma electrónica; o, que aduzca pruebas de que una firma electrónica no es fiable.

Artículo 34. Órgano competente. El Estado a través del órgano o entidad correspondiente, podrá atribuir competencia a una persona, órgano o entidad pública o privada, para determinar qué firmas electrónicas cumplen con lo dispuesto en el artículo 33 anterior. Para tal efecto, dicha determinación que se haga deberá ser compatible con las normas o criterios internacionales reconocidos.

Artículo 35. Proceder del Firmante. Cuando puedan utilizarse datos de creación de firmas para crear una firma con efectos jurídicos, cada firmante deberá:

a) Actuar con la diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma.

b) Sin dilación indebida, utilizar los medios que le proporcione el prestador de servicios de certificación conforme la presente ley, o en cualquier caso esforzarse razonablemente, para dar aviso a cualquier persona que, según pueda razonablemente prever el firmante, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen si:

1. El firmante sabe que los datos de creación de la firma han quedado en entredicho; o,

2. Las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho.

c) Cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado o que hayan de consignarse en él son exactas y cabales.

Serán a cargo del firmante las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos anteriores enunciados en éste artículo.

Artículo 36. Proceder del prestador de servicios de certificación. Cuando un prestador de servicios de certificación preste servicios para apoyar una firma electrónica que pueda utilizarse como firma con efectos jurídicos, ese prestador de servicios de certificación deberá:

a) Actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas.

b) Actuar con diligencia razonable para cerciorarse que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él son exactas y precisas.

c) Proporcionar a la parte que confía en el certificado, medios razonablemente accesibles que permitan a esta determinar mediante el certificado:

1. La identidad del prestador de servicios de certificación;
2. 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;

3. Que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella.

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

1. El método utilizado para comprobar la identidad del firmante;
2. Cualquier limitación de los fines o del valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;
3. Si los datos de creación de la firma son válidos y no están en entredicho;
4. Cualquier limitación del alcance o del grado de responsabilidad que haya establecido el prestador de servicios de certificación;
5. Si existe un medio para que el firmante de aviso de que los datos de creación de la firma están en entredicho, conforme a lo dispuesto en la literal b) del artículo 35 de la presente ley;
6. Si se ofrece un servicio de revocar oportunamente el certificado.

e) Cuando se ofrezcan servicios conforme al numeral 5 de la literal d) del presente artículo, proporcionar un medio para que el firmante de aviso conforme a la literal b) del artículo 35 de esta ley y, cuando se ofrezcan servicios en virtud del numeral 6 del inciso d) del presente artículo, cerciorarse que existe un servicio para revocar oportunamente el certificado.

f) Utilizar, al prestar servicios, sistemas, procedimientos y recursos humanos fiables.

Serán a cargo del prestador de servicios de certificación las consecuencias jurídicas que produzca el hecho de no haber cumplido los requisitos anteriores enunciados en este artículo.

Artículo 37. Fiabilidad. A los efectos de la literal f) del artículo 36 anterior, para determinar si los sistemas, procedimientos o recursos humanos utilizados por un prestador de servicios de certificación son fiables, y en qué medida lo son, podrán tenerse en cuenta los factores siguientes:

a) Los recursos humanos y financieros, incluida la existencia de activos;

b) La calidad de los sistemas de equipo y programas informáticos;

c) Los procedimientos para la transmisión del certificado y las solicitudes de certificados, y la conservación de registros;

d) La disponibilidad de la información para los firmantes nombrados en el certificado y para las partes que confíen en éste;

e) La periodicidad y el alcance de la auditoría realizada por un órgano independiente;

f) La existencia de una declaración del Estado, de un órgano de acreditación o del prestador de servicios de certificación respecto del cumplimiento o la existencia de los factores que anteceden; o,

g) Cualesquiera otros factores pertinentes.

Artículo 38. Proceder de la parte que confía en el certificado. Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que produzca el hecho que no haya tomado medidas razonables para:

a) Verificar la fiabilidad de la firma electrónica; o,

b) Cuando la firma electrónica esté refrendada por un certificado:

i. Verificar la validez, suspensión o revocación del certificado; y,
ii. Tener en cuenta cualquier limitación en relación con el certificado.

Artículo 39. Reconocimiento de certificados extranjeros y de firmas electrónicas extranjeras. Al determinar si un certificado o una firma electrónica producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración:

a) Lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica; ni,

b) El lugar en que se encuentre el establecimiento del expedidor o del firmante.

Todo certificado expedido en el extranjero producirá los mismos efectos jurídicos que el expedido dentro del territorio de la República, si se presenta un grado de fiabilidad sustancialmente equivalente.

Toda firma electrónica creada o utilizada en el extranjero producirá los mismos efectos jurídicos que la expedida dentro del territorio de la República, si presenta un grado de fiabilidad sustancialmente equivalente.

A efectos de determinar si un certificado o una firma electrónica presentan un grado de fiabilidad sustancialmente equivalente para los fines de los dos párrafos anteriores del presente artículo, se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente.

Cuando, sin perjuicio de lo dispuesto en los tres párrafos anteriores del presente artículo, las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas o certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que el acuerdo no sea válido o eficaz conforme al derecho aplicable.

Artículo 40. Características y requerimientos de los prestadores de servicios de certificación. Podrán ser prestadores de servicios de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero, que previa solicitud sean autorizadas por el Registro de Prestadores de Servicios de Certificación del Ministerio de Economía y que cumplan con los requerimientos establecidos por ésta, con base en las condiciones siguientes:

a) Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como prestadores de servicios de certificación.

b) Contar con la capacidad y elementos técnicos necesarios para la generación de firmas electrónicas avanzadas, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley.

c) Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a pena privativa de libertad, o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética o hayan sido excluidas de aquella. Esta inhabilidad estará vigente por el mismo período que la ley penal o administrativa señale para el efecto.

d) Contar con las acreditaciones necesarias por los órganos o entidades correspondientes según la normativa vigente.

El Ministerio de Economía podrá emitir los requerimientos y regulaciones que considere pertinentes, siempre sobre la base de su adecuación a las normas y principios internacionales reconocidos.

Artículo 41. Actividades de los prestadores de servicios de certificación. Los prestadores de servicios de certificación autorizados por el Ministerio de Economía para prestar sus servicios en el país, podrán realizar, entre otras, las actividades siguientes:

a) Emitir certificados en relación con las firmas electrónicas avanzadas de personas naturales o jurídicas, ya sean éstas digitales o de cualquier otra índole.

b) Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción de las comunicaciones electrónicas.

c) Ofrecer o facilitar los servicios de creación de firmas electrónicas avanzadas certificadas, ya sean estas digitales o de cualquier otra índole.

d) Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en las literales f) y g) del artículo 31 de la presente ley.

e) Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de comunicaciones electrónicas.

f) Ofrecer los servicios de archivo y conservación de comunicaciones electrónicas.

g) Certificar en los certificados que expidan, las condiciones profesionales del titular de la firma para efectos de constituir prueba frente a cualquier entidad pública o privada.

Artículo 42. Obligaciones de los prestadores de servicios de certificación. Las sociedades de certificación tendrán entre otros, los deberes siguientes:

a) Emitir certificados conforme a lo solicitado o acordado con el firmante.

b) Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas electrónicas avanzadas, 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 firmante.

d) Garantizar la prestación permanente del servicio de entidad de certificación.

e) Atender oportunamente las solicitudes y reclamaciones hechas por los firmantes.

f) Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas electrónicas y certificados emitidos y en general sobre cualquier comunicación electrónica que se encuentre bajo su custodia y administración.

g) Permitir y facilitar la realización de las auditorías por parte del Registro de Prestadores de Servicios de Certificación.

h) Elaborar los reglamentos que definen las relaciones con el firmante y la forma de prestación del servicio.

i) Llevar un registro de los certificados.

Artículo 43. Remuneración por la prestación de servicios. La remuneración por los servicios de los prestadores de servicios de certificación será establecida libremente por éstos.

Artículo 44. Terminación unilateral. Salvo acuerdo entre las partes, el prestador de servicios de certificación podrá dar por terminado el acuerdo de vinculación con el firmante dando un preaviso no menor al plazo de noventa (90) días. Vencido este término, el prestador de servicio de certificación revocará los certificados que se encuentren pendientes de expiración.

Igualmente, el firmante podrá dar por terminado el acuerdo de vinculación con la sociedad de certificación dando un preaviso no inferior al plazo de treinta (30) días.

Artículo 45. Terminación de actividades por parte de los prestadores de servicios de certificación. Las sociedades de certificación autorizadas pueden cesar en el ejercicio de actividades, siempre y cuando hayan recibido autorización por parte del Registro de Prestadores de Servicios de Certificación.

Artículo 46. Contenido de los certificados. Un certificado emitido por un prestador de servicios de certificación autorizada, además de estar firmado electrónicamente por éste, debe contener por lo menos lo siguiente:

a) Nombre, dirección y domicilio del firmante.

b) Identificación del firmante nombrado en el certificado.

c) El nombre, la dirección y el lugar donde realiza actividades la prestadora de servicios de certificación.

d) La clave pública del usuario en los casos de la tecnología de criptografía asimétrica.

e) La metodología para verificar la firma electrónica del firmante impuesta en la comunicación electrónica.

f) El número de serie del certificado.

g) Fecha de emisión y expiración del certificado.

Artículo 47. Revocación de certificados. Los certificados podrán revocarse por:

a) El firmante de una firma electrónica avanzada certificada, podrá solicitar a la prestadora de servicios de certificación que expidió un certificado, la revocación del mismo. En todo caso, estará obligado a solicitar la revocación en los eventos siguientes:

i. Por pérdida de la clave privada, en el caso de la tecnología de criptografía asimétrica;

ii. La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido, en el caso de la tecnología de criptografía asimétrica.

b) Si el firmante no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exenta de culpa que confiaron en el contenido del certificado.

c) Una prestadora de servicios de certificación revocará un certificado emitido por las razones siguientes:

1. A petición del firmante o un tercero en su nombre y representación;
2. Por muerte del firmante;
3. Por liquidación del firmante en el caso de las personas jurídicas;
4. Por la confirmación de que alguna información o hecho contenido en el certificado es falso;
5. La clave privada de la prestadora de servicios de certificación o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado;
6. Por el cese de actividades de la prestadora de servicios de certificación; y,
7. Por orden judicial o de entidad administrativa competente.

Artículo 48. Término de conservación de los registros. La información y registros de certificados expedidos por una prestadora de servicios de certificación deben ser conservados por el término exigido en la ley que regule el acto o negocio jurídico en particular, o por diez años en caso de no existir dicho término.

CAPÍTULO II
REGISTRO DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Artículo 49. Funciones del Registro de Prestadores de Servicios de Certificación. El Registro de Prestadores de Servicios de Certificación, adscrito al Ministerio de Economía, ejercerá las facultades que legalmente le han sido asignadas respecto de las entidades prestadoras de servicios de certificación, y adicionalmente tendrá las funciones siguientes:

a) Autorizar la actividad de las entidades prestadoras de servicios de certificación.

b) Velar por el funcionamiento y la eficiente prestación del servicio por parte de las prestadoras de servicios de certificación.

c) Realizar visitas de auditoria a las prestadoras de servicios de certificación.

d) Revocar o suspender la autorización para operar como prestador de servicios de certificación.

e) Solicitar la información pertinente para el ejercicio de sus funciones.

f) Imponer sanciones a las prestadoras de servicios de certificación en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio.

g) Ordenar la revocación de certificados cuando la prestadora de servicios de certificación los emita sin el cumplimiento de las formalidades legales.

h) Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y prácticas comerciales restrictivas, competencia desleal y protección del consumidor, en los mercados atendidos por las prestadoras de servicios de certificación, debiéndose coordinar, según el caso, con las autoridades específicas.

i) Impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las prestadoras de servicios de certificación.

j) Emitir las regulaciones que considere basadas en las normas, regulaciones, criterios o principios internacionales reconocidos.

Artículo 50. Sanciones. El Registro de Prestadores de Servicios de Certificación del Ministerio de Economía, de acuerdo con el debido proceso y el derecho de defensa, podrá imponer, por intermedio del despacho ministerial de economía, según la naturaleza y la gravedad de la falta, las sanciones a las sociedades de certificación siguientes:

a) Amonestación.

b) Multas institucionales hasta por el equivalente a dos mil quinientos (2500) salarios mínimos no agrícolas legales mensuales vigentes, y personales a los administradores y representantes legales de las entidades prestadoras de servicios de certificación, hasta por quinientos (500) salarios mínimos no agrícolas legales mensuales vigentes, cuando se compruebe que han autorizado, ejecutado o tolerado conductas violatorias de la ley.

c) Suspender de inmediato todas o algunas de las actividades de la entidad infractora.

d) Prohibir a la entidad infractora prestar directa o indirectamente los servicios de certificación hasta por el término de cinco (5) años.

e) Revocar definitivamente la autorización para operar como entidad prestadora de servicios de certificación.

CAPÍTULO III
DISPOSICIONES VARIAS

Artículo 51. Prevalencia de las leyes de protección al consumidor. La presente Ley se aplicará sin perjuicio de las normas vigentes en materia de protección al consumidor.

Las entidades o empresas involucradas en el comercio electrónico deben respetar los intereses de los consumidores y actuar de acuerdo a prácticas equitativas en el ejercicio de sus actividades empresariales, publicitarias y de mercadotecnia. Así mismo, las entidades o empresas no deben realizar ninguna declaración, incurrir en alguna omisión, o comprometerse en alguna práctica que resulte falsa, engañosa, fraudulenta o desleal.

Siempre que las entidades o empresas publiquen información sobre ellas mismas o sobre los bienes o servicios que ofrecen, deben presentarla de manera clara, visible, precisa y fácilmente accesible. Así mismo, deben cumplir con cualquier declaración que hagan respecto a sus políticas y prácticas relacionadas con sus transacciones con consumidores.

Las empresas no deben aprovecharse de las características especiales del comercio electrónico para ocultar su verdadera identidad o ubicación, o para evadir el cumplimiento de las normas de protección al consumidor o los mecanismos de aplicación de dichas normas.

Las empresas deben desarrollar e implementar procedimientos efectivos y fáciles de usar, que permitan a los consumidores manifestar su decisión de recibir o rehusar mensajes comerciales no solicitados por medio del correo electrónico. Cuando los consumidores manifiesten que no desean recibir mensajes comerciales por correo electrónico, tal decisión debe ser respetada.

Artículo 52. Información en Línea. Sin perjuicio de cumplir con la legislación vigente para comerciantes y empresas mercantiles, las empresas que realicen comercio electrónico deberán proveer la siguiente información:

a) Información sobre la empresa: Las empresas que realicen transacciones con los consumidores por medio del comercio electrónico deben proporcionar de manera precisa, clara y fácilmente accesible, información suficiente sobre ellas mismas, que permita al menos:

1. La identificación de la empresa – incluyendo la denominación legal y el nombre o marca de comercialización; el principal domicilio geográfico de la empresa; correo electrónico u otros medios electrónicos de contacto, o el número telefónico; y, cuando sea aplicable, una dirección para propósitos de registro, y cualquier número relevante de licencia o registro gubernamental;
2. Una comunicación rápida, fácil y efectiva con la empresa;
3. Apropiados y efectivos mecanismos de solución de disputas;
4. Servicios de atención a procedimientos legales; y,
5. Ubicación del domicilio legal de la empresa y de sus directivos, para uso de las autoridades encargadas de la reglamentación y de la aplicación de la ley.

Cuando una empresa de a conocer su membresía o afiliación en algún esquema relevante de autorregulación, asociación empresarial, organización para resolución de disputas u otro organismo de certificación, debe proporcionar a los consumidores un método sencillo para verificar dicha información, así como detalles apropiados para contactar con dichos organismos, y en su caso, tener acceso a los códigos y prácticas relevantes aplicados por el organismo de certificación.

b) Información sobre los bienes o servicios: Las empresas que realicen transacciones con consumidores por medio del comercio electrónico deben proporcionar información precisa y fácilmente accesible que describa los bienes o servicios ofrecidos, de manera que permita a los consumidores tomar una decisión informada antes de participar en la transacción y en términos que les permita mantener un adecuado registro de dicha información.

Artículo 53. Plazo. El Ministerio de Economía creará y organizará el Registro de Prestadores de Servicios de Certificación en un plazo no mayor a sesenta (60) días después de entrada en vigencia la presente ley.

Artículo 54. Transitorio. El Registro de Prestadores de Servicios de Certificación del Ministerio de Economía contará con un término adicional de seis (6) meses, contados a partir de la publicación de la presente ley, para organizar la función de inspección, control y vigilancia de las actividades realizadas por las entidades prestadoras de servicios de certificación, así como para emitir las normas técnicas aplicables a las firmas electrónicas avanzadas y los certificados de cualquier tipo.

Artículo 55. Reglamento. El Organismo Ejecutivo, por conducto del Ministerio de Economía, deberá emitir el reglamento de esta Ley, en un plazo no mayor a seis (6) meses contados a partir de su publicación. Así mismo, podrá emitir las reglamentaciones o disposiciones que considere para el debido desempeño del Registro de Prestadores de Servicios de Certificación.

Artículo 56. Vigencia y Derogatorias. La presente ley entra en vigencia ocho (8) días después de su publicación y deroga las disposiciones que le sean contrarias.

REMÍTASE AL ORGANISMO EJECUTIVO PARA SU SANCIÓN, PROMULGACIÓN Y PUBLICACIÓN.

EMITIDO EN EL PALACIO DEL ORGANISMO LEGISLATIVO, EN LA CIUDAD DE GUATEMALA, EL DIECINUEVE DE AGOSTO DE DOS MIL OCHO.

ARÍSTIDES BALDOMERO CRESPO VILLEGAS
PRESIDENTE

CONGRESO DE LA REPÚBLICA - GUATEMALA, C. A.

JOSÉ ROBERTO ALEJOS CÁMBARA
SECRETARIO

ROSA ELVIRA ZAPETA OSORIO
SECRETARIA

PALACIO NACIONAL: Guatemala, dieciséis de septiembre del año dos mil ocho.

PUBLÍQUESE Y CUMPLASE

COLOM CABALLEROS

Rómulo Caballeros Otero
MINISTRO DE ECONOMÍA

Lic. Carlos Larios Ochaita
SECRETARIO GENERAL DE LA PRESIDENCIA DE LA REPÚBLICA

(E-709-2008)-23-septiembre

CONGRESO DE LA REPÚBLICA DE GUATEMALA

DECRETO NÚMERO 48-2008

EL CONGRESO DE LA REPÚBLICA DE GUATEMALA

CONSIDERANDO:

Que durante el enfrentamiento armado interno ocurrido en el país, la población guatemalteca sufrió graves violaciones a sus derechos humanos.

CONSIDERANDO:

Que la Comisión para el Esclarecimiento Histórico, presentó el 25 de febrero del año 1999 su informe final, conteniendo entre sus recomendaciones las siguientes: "Que el Estado asuma el contenido del presente informe y apoye iniciativas para su difusión y promoción.", "En la currícula de educación primaria, secundaria y universitaria se incluyan las enseñanzas del enfrentamiento armado y del contenido de los Acuerdos de Paz".

CONSIDERANDO:

Que con fecha 25 de febrero de 2004, el Congreso de la República aprobó el Decreto Número 06-04, Ley que Conmemora el 25 de febrero de cada año como el Día Nacional de la Dignidad de las Víctimas del Conflicto Armado Interno, sin establecer un procedimiento y contenido que hagan operativa dicha conmemoración y que cumpla con los objetivos para lo cual la Comisión del Esclarecimiento Histórico recomendó tal conmemoración.

POR TANTO:

En ejercicio de las atribuciones que le confiere el artículo 171 literal a) de la Constitución Política de la República,

DECRETA:

Las siguientes:

REFORMAS AL DECRETO NÚMERO 06-04 DEL CONGRESO DE LA REPÚBLICA, LEY QUE CONMEMORA EL 25 DE FEBRERO DE CADA AÑO COMO EL DÍA NACIONAL DE LA DIGNIDAD DE LAS VÍCTIMAS DEL CONFLICTO ARMADO INTERNO

Artículo 1. Se reforma el artículo 1 del Decreto Número 06-04 del Congreso de la República, para que quede de la siguiente manera:

"**Artículo 1.** Se establece el 25 de febrero de cada año, como el "Día Nacional de la Dignidad de las Víctimas del Conflicto Armado Interno", debiéndose conmemorar tal fecha en instituciones autónomas y descentralizadas, establecimientos educativos y oficinas públicas y privadas, en la forma que se honre de mejor manera la memoria de las víctimas del conflicto armado interno. Los Ministerios de Cultura y Deportes y de Educación, en coordinación, deberán promover dichas actividades conmemorativas para que cumplan su cometido.

El Ministerio de Educación deberá incluir en la currícula de educación primaria y secundaria las enseñanzas sobre las causas y consecuencias del enfrentamiento armado y del contenido de los Acuerdos de Paz."

Artículo 2. El presente Decreto entrará en vigencia el día de su publicación en el Diario Oficial.

REMÍTASE AL ORGANISMO EJECUTIVO PARA SU SANCIÓN, PROMULGACIÓN Y PUBLICACIÓN.

EMITIDO EN EL PALACIO DEL ORGANISMO LEGISLATIVO, EN LA CIUDAD DE GUATEMALA, EL VEINTE DE AGOSTO DE DOS MIL OCHO.

ARÍSTIDES BALDOMERO CRESPO VILLEGAS
PRESIDENTE

JOSÉ ROBERTO ALEJOS CÁMBARA
SECRETARIO

ROSA ELVIRA ZAPETA OSORIO
SECRETARIA

PALACIO NACIONAL: Guatemala, dieciséis de septiembre del año dos mil ocho.

PUBLÍQUESE Y CUMPLASE

COLOM CABALLEROS

Lic. Carlos Larios Ochaita
SECRETARIO GENERAL DE LA PRESIDENCIA DE LA REPÚBLICA

Jerónimo Lancerio Chingo
MINISTERIO DE CULTURA Y DEPORTES

Licda. Ana Ordóñez de Molina
MINISTRA DE EDUCACIÓN

(E-708-2008)-23-septiembre

ORGANISMO EJECUTIVO

MINISTERIO DE RELACIONES EXTERIORES

SEGUNDO PROTOCOLO AL TRATADO MARCO DEL MERCADO ELÉCTRICO DE AMÉRICA CENTRAL.

YO, ÁLVARO COLOM CABALLEROS
Presidente de la República de Guatemala

D E C L A R O:

Que el Gobierno de la República de Guatemala, habiendo suscrito en la ciudad de Campeche, de los Estados Unidos Mexicanos, con fecha 10 de abril de dos mil siete el **SEGUNDO PROTOCOLO AL TRATADO MARCO DEL MERCADO ELÉCTRICO DE AMÉRICA CENTRAL**, ratifica por el presente dicho Protocolo y se compromete a cumplir y aplicar fielmente las disposiciones que en él figuran.

EN TESTIMONIO DE LO CUAL, firmo el presente Instrumento.

Hecho en la Ciudad de Guatemala, a los veintiún días del mes de abril de dos mil ocho.

ANEXO XII
Real Decreto - Ley 14/1999, de 17 de Septiembre, sobre Firma Electrónica de España.

I. Disposiciones generales

JEFATURA DEL ESTADO

18915 *REAL DECRETO-LEY 14/1999, de 17 de septiembre, sobre firma electrónica.*

En la sesión del Consejo de Ministros de Telecomunicaciones de la Unión Europea, celebrada el 22 de abril de 1999, se ha informado favorablemente la adopción de una posición común, respecto del proyecto de Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para la firma electrónica.

El Estado español ha tenido una participación activa en el logro de la posición común que facilita la tramitación del texto, al recoger éste los elementos suficientes para proteger la seguridad y la integridad de las comunicaciones telemáticas en las que se emplee la firma electrónica. En ese sentido, existen ya en España diversas normas sobre la presentación de la declaración del Impuesto sobre la Renta de las Personas Físicas por medios telemáticos, dictadas por la Administración tributaria. La Comisión Nacional del Mercado de Valores, por su parte, ha aprobado y puesto en marcha un sistema de cifrado y firma electrónica que se emplea para la recepción de información de las entidades supervisadas. Asimismo, el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y de Orden Social, anuncia la posibilidad de prestar, por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, los servicios técnicos y administrativos necesarios para garantizar la seguridad, la validez y la eficacia de la emisión y recepción de comunicaciones, a través de técnicas y medios electrónicos, informáticos y telemáticos. La Fábrica Nacional de la Moneda y Timbre-Real Casa de la Moneda actuará en colaboración con Correos y Telégrafos.

En el proyecto de Directiva se incorpora, a solicitud del Estado español, una novedad, recogida en el apartado c) del anexo II, entre los requisitos exigibles a los prestadores de servicios de certificación que expidan certificados reconocidos. Esta novedad consiste en permitir que la certificación pueda recoger la fecha y la hora en la que se produce la actuación certificante.

Existe, además, en España un sector empresarial que podría prestar un servicio de certificación de la firma electrónica con suficiente calidad. Se considera que debe introducirse, cuanto antes, la disciplina que permita utilizar, con la adecuada seguridad jurídica, este medio tecnológico que contribuye al desarrollo de lo que se ha venido en denominar, en la Unión Europea, la sociedad de la información. La urgencia de la aprobación de esta norma deriva, también, del deseo de dar, a los usuarios de los nuevos servicios, elementos de confianza en los sistemas, permitiendo su introducción y rápida difusión.

Por ello, este Real Decreto-ley persigue, respetando el contenido de la posición común respecto de la Directiva sobre firma electrónica, establecer una regulación clara del uso de ésta, atribuyéndole eficacia jurídica y previendo el régimen aplicable a los prestadores de servicios de certificación. De igual modo, este Real Decreto-ley determina el registro en el que habrán de inscribirse los prestadores de servicios de certificación y el régimen de inspección administrativa de su actividad, regula la expedición y la pérdida de eficacia de los certificados y tipifica las infracciones y las sanciones que se prevén para garantizar su cumplimiento.

La presente disposición ha sido sometida al procedimiento de información en materia de normas y reglamentaciones técnicas previsto en la Directiva 98/34/CE, del Parlamento Europeo y del Consejo, de 22 de junio de 1998, modificada por la Directiva 98/48/CE, del Parlamento Europeo y del Consejo, de 20 de julio de 1998, y en el Real Decreto 1337/1999, de 31 de julio.

En su virtud, a propuesta del Ministro de Fomento, de la Ministra de Justicia y del Ministro de Industria y Energía, previo informe del Consejo General del Poder Judicial y de la Agencia de Protección de Datos, tras la deliberación del Consejo de Ministros, en su reunión celebrada el día 17 de septiembre de 1999, y en uso de la autorización concedida en el artículo 86 de la Constitución,

D I S P O N G O :

TÍTULO I

Disposiciones generales

CAPÍTULO ÚNICO

Disposiciones generales

Artículo 1. *Ámbito de aplicación.*

1. Este Real Decreto-ley regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación. Las normas sobre esta actividad son de aplicación a los prestadores de servicios establecidos en España.

2. Las disposiciones contenidas en este Real Decreto-ley no alteran las normas relativas a la celebración, la formalización, la validez y la eficacia de los contratos y otros actos jurídicos ni al régimen jurídico aplicable a las obligaciones.

Las normas sobre la prestación de servicios de certificación de firma electrónica que recoge este Real Decreto-ley no sustituyen ni modifican las que regulan las funciones que corresponde realizar a las personas facultadas, con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en su elevación a públicos.

Artículo 2. *Definiciones.*

A los efectos de este Real Decreto-ley, se establecen las siguientes definiciones:

a) «Firma electrónica»: Es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.

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

c) «Signatario»: Es la persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.

d) «Datos de creación de firma»: Son los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la firma electrónica.

e) «Dispositivo de creación de firma»: Es un programa o un aparato informático que sirve para aplicar los datos de creación de firma.

f) «Dispositivo seguro de creación de firma»: Es un dispositivo de creación de firma que cumple los requisitos establecidos en el artículo 19.

g) «Datos de verificación de firma»: Son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

h) «Dispositivo de verificación de firma»: Es un programa o un aparato informático que sirve para aplicar los datos de verificación de firma.

i) «Certificado»: Es la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad.

j) «Certificado reconocido»: Es el certificado que contiene la información descrita en el artículo 8 y es expedido por un prestador de servicios de certificación que cumple los requisitos enumerados en el artículo 12.

k) «Prestador de servicios de certificación»: Es la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica.

l) «Producto de firma electrónica»: Es un programa o un aparato informático o sus componentes específicos, destinados a ser utilizados para la prestación de servicios de firma electrónica por el prestador de servicios de certificación o para la creación o verificación de firma electrónica.

ll) «Acreditación voluntaria del prestador de servicios de certificación»: Resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se dicta, a petición del prestador al que le beneficie, por el organismo público encargado de su supervisión.

Artículo 3. *Efectos jurídicos de la firma electrónica.*

1. La firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales.

Se presumirá que la firma electrónica avanzada reúne las condiciones necesarias para producir los efectos indicados en este apartado, cuando el certificado reconocido en que se base haya sido expedido por un prestador de servicios de certificación acreditado y el dispositivo seguro de creación de firma con el que ésta se produzca se encuentre certificado, con arreglo a lo establecido en el artículo 21.

2. A la firma electrónica que no reúna todos los requisitos previstos en el apartado anterior, no se le negarán efectos jurídicos ni será excluida como prueba en juicio, por el mero hecho de presentarse en forma electrónica.

TÍTULO II

La prestación de servicios de certificación

CAPÍTULO I

Principios generales

Artículo 4. *Régimen de libre competencia.*

1. La prestación de servicios de certificación no está sujeta a autorización previa y se realiza en régimen de libre competencia, sin que quepa establecer restricciones para los servicios de certificación que procedan de alguno de los Estados miembros de la Unión Europea.

2. La prestación de los servicios de certificación por las Administraciones o los organismos o sociedades de ellas dependientes se realizará con la debida separación de cuentas y con arreglo a los principios de objetividad, transparencia y no discriminación.

Artículo 5. *Empleo de la firma electrónica por las Administraciones públicas.*

1. Se podrá supeditar por la normativa estatal o, en su caso, autonómica el uso de la firma electrónica en el seno de las Administraciones públicas y sus entes públicos y en las relaciones que con cualesquiera de ellos mantengan los particulares, a las condiciones adicionales que se consideren necesarias, para salvaguardar las garantías de cada procedimiento.

Las condiciones adicionales que se establezcan podrán incluir la prestación de un servicio de consignación de fecha y hora, respecto de los documentos electrónicos integrados en un expediente administrativo. El citado servicio consistirá en la acreditación por el prestador de servicios de certificación, o por un tercero, de la fecha y hora en que un documento electrónico es enviado por el signatario o recibido por el destinatario.

Las normas estatales que regulen las condiciones adicionales sobre el uso de la firma electrónica a las que se refiere este apartado sólo podrán hacer referencia a las características específicas de la aplicación de que se trate y se dictarán a propuesta del Ministerio de Administraciones Públicas y previo informe del Consejo Superior de Informática.

2. Las condiciones adicionales a las que se refiere el apartado anterior deberán garantizar el cumplimiento de lo previsto en el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, serán objetivas, razonables y no discriminatorias y no obstaculizarán la prestación de servicios al ciudadano, cuando en ella intervengan distintas Administraciones públicas nacionales o extranjeras.

3. Podrá someterse a un régimen específico, la utilización de la firma electrónica en las comunicaciones

que afecten a la información clasificada, a la seguridad pública o a la defensa. Asimismo, el Ministro de Economía y Hacienda, respetando las condiciones previstas en este Real Decreto-ley, podrá establecer un régimen normativo destinado a garantizar el cumplimiento de las obligaciones tributarias, determinando, respecto de la gestión de los tributos, la posibilidad de que el signatario sea una persona física o una persona jurídica.

Artículo 6. *Sistemas de acreditación de prestadores de servicios de certificación y de certificación de productos de firma electrónica.*

1. El Gobierno, por Real Decreto, podrá establecer sistemas voluntarios de acreditación de los prestadores de servicios de certificación de firma electrónica, determinando, para ello, un régimen que permita lograr el adecuado grado de seguridad y proteger, debidamente, los derechos de los usuarios.

2. Las funciones de certificación a las que se refiere este Real Decreto-ley serán ejercidas por los órganos, en cada caso competentes, referidos en la Ley 11/1998, de 24 de abril, General de Telecomunicaciones; en la Ley 21/1992, de 16 de julio, de Industria, y en la demás legislación vigente sobre la materia. El Real Decreto al que se refiere el apartado 1 establecerá las condiciones que permitan coordinar los sistemas de certificación.

3. Las normas que regulen los sistemas de acreditación y de certificación deberán ser objetivas, razonables y no discriminatorias. Todos los prestadores de servicios que se sometan voluntariamente a ellos, podrán obtener la correspondiente acreditación de su actividad o, en su caso, la certificación del producto de firma electrónica que empleen.

4. Los órganos competentes para el ejercicio de las funciones a que se refiere el apartado anterior valorarán los informes técnicos que emitan las entidades de evaluación sobre los prestadores de servicios que hayan solicitado su acreditación o los productos para los que se haya pedido certificación. También tomarán en cuenta el cumplimiento, por el prestador de servicios, de los requisitos que se determinen reglamentariamente para poder ser acreditado.

5. A los efectos de este Real Decreto-ley, sólo podrán actuar como entidades de evaluación aquellas que hayan sido acreditadas por el organismo independiente al que se haya atribuido esta facultad por el Real Decreto al que se refiere el apartado primero de este artículo.

Artículo 7. *Registro de Prestadores de Servicios de Certificación.*

1. Se crea, en el Ministerio de Justicia, el Registro de Prestadores de Servicios de Certificación, en el que deberán solicitar su inscripción, con carácter previo al inicio de su actividad, todos los establecidos en España. Su regulación se desarrollará por Real Decreto.

2. La solicitud de inscripción habrá de formularse, aportando la documentación que se establezca reglamentariamente, a efectos de la identificación del prestador de servicios de certificación y de justificar que éste reúne los requisitos necesarios, en cada caso, para ejercer su actividad. También será objeto de inscripción ulterior cualquier circunstancia relevante, a efectos de este Real Decreto-ley, relativa al prestador de servicios de certificación, como su acreditación o estar en condiciones de expedir certificados reconocidos.

La formulación de la solicitud de inscripción en el Registro por los citados prestadores de servicios, les permitirá iniciar o continuar su actividad, sin perjuicio de la aplicación, en su caso, del régimen sancionador correspondiente.

3. El Registro de Prestadores de Servicios de Certificación será público y deberá mantener permanentemente actualizada y a disposición de cualquier persona una relación de los inscritos, en la que figurarán su nombre o razón social, la dirección de su página en Internet o de correo electrónico, los datos de verificación de su firma electrónica y, en su caso, su condición de acreditado o de tener la posibilidad de expedir certificados reconocidos. En la citada relación figurarán, también, cualesquiera otros datos complementarios que se determinen por Real Decreto.

Los datos inscritos en el Registro podrán ser consultados por vía telemática o a través de la oportuna certificación registral. El suministro de esta información podrá sujetarse al pago de una tasa, cuyos elementos esenciales se determinarán por ley.

CAPÍTULO II

Certificados

Artículo 8. *Requisitos para la existencia de un certificado reconocido.*

1. Los certificados reconocidos, definidos en el artículo 2.j) de este Real Decreto-ley, tendrán el siguiente contenido:

a) La indicación de que se expiden como tales.

b) El código identificativo único del certificado.

c) La identificación del prestador de servicios de certificación que expide el certificado, indicando su nombre o razón social, su domicilio, su dirección de correo electrónico, su número de identificación fiscal y, en su caso, sus datos de identificación registral.

d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.

e) La identificación del signatario, por su nombre y apellidos o a través de un seudónimo que conste como tal de manera inequívoca. Se podrá consignar en el certificado cualquier otra circunstancia personal del titular, en caso de que sea significativa en función del fin propio del certificado y siempre que aquél dé su consentimiento.

f) En los supuestos de representación, la indicación del documento que acredite las facultades del signatario para actuar en nombre de la persona física o jurídica a la que represente.

g) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del signatario

h) El comienzo y el fin del período de validez del certificado.

i) Los límites de uso del certificado, si se prevén.

j) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

2. La consignación en el certificado de cualquier otra información relativa al signatario, requerirá su consentimiento expreso.

Artículo 9. *Vigencia de los certificados.*

1. Los certificados de firma electrónica quedarán sin efecto, si concurre alguna de las siguientes circunstancias:

a) Expiración del período de validez del certificado. Tratándose de certificados reconocidos, éste no podrá ser superior a cuatro años, contados desde la fecha en que se hayan expedido.

b) Revocación por el signatario, por la persona física o jurídica representada por éste o por un tercero autorizado.

c) Pérdida o inutilización por daños del soporte del certificado.

d) Utilización indebida por un tercero.

e) Resolución judicial o administrativa que lo ordene.

f) Fallecimiento del signatario o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos, terminación de la representación o extinción de la persona jurídica representada.

g) Cese en su actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del signatario, los certificados expedidos por aquél sean transferidos a otro prestador de servicios.

h) Inexactitudes graves en los datos aportados por el signatario para la obtención del certificado.

2. La pérdida de eficacia de los certificados, en los supuestos de expiración de su período de validez y de cese de actividad del prestador de servicios, tendrá lugar desde que estas circunstancias se produzcan. En los demás casos, la extinción de la eficacia de un certificado surtirá efectos desde la fecha en que el prestador de servicios tenga conocimiento cierto de cualquiera de los hechos determinantes de ella y así lo haga constar en su Registro de certificados al que se refiere el artículo 11.e).

3. En cualquiera de los supuestos indicados, el prestador de servicios de certificación, habrá de publicar la extinción de eficacia del certificado en el Registro al que se refiere el artículo 11.e), y responderá de los posibles perjuicios que se causen al signatario o a terceros de buena fe, por el retraso en la publicación. Corresponderá al prestador de servicios la prueba de que los terceros conocían las circunstancias invalidantes del certificado.

4. El prestador de servicios de certificación podrá suspender, temporalmente, la eficacia de los certificados expedidos, si así lo solicita el signatario o sus representados o lo ordena una autoridad judicial o administrativa. La suspensión surtirá efectos en la forma prevista en los dos apartados anteriores.

Artículo 10. *Equivalencia de certificados.*

Los certificados que los prestadores de servicios de certificación establecidos en un Estado que no sea miembro de la Unión Europea, de acuerdo con la legislación de éste, expidan como reconocidos, se considerarán equivalentes a los expedidos por los establecidos en España, siempre que se cumplan alguna de las siguientes condiciones:

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

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

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

CAPÍTULO III

Condiciones exigibles a los prestadores de servicios de certificación

Artículo 11. *Obligaciones de los prestadores de servicios de certificación.*

Todos los prestadores de servicios de certificación deben cumplir las siguientes obligaciones:

a) Comprobar por sí o por medio de una persona física o jurídica que actúe en nombre y por cuenta suyos, la identidad y cualesquiera circunstancias personales de los solicitantes de los certificados relevantes para el fin propio de éstos, utilizando cualquiera de los medios admitidos en derecho. Se exceptúan de esta obligación, los prestadores de servicios de certificación que, expidiendo certificados que no tengan la consideración de reconocidos, se limiten a constatar determinadas circunstancias específicas de los solicitantes de aquéllos.

b) Poner a disposición del signatario los dispositivos de creación y de verificación de firma electrónica.

c) No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo que ésta lo solicite.

d) Informar, antes de la emisión de un certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial.

e) Mantener un registro de certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión o perdida de vigencia de sus efectos. A dicho registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten, cuando así lo autorice el signatario.

f) En el caso de cesar en su actividad, los prestadores de servicios de certificación deberán comunicarlo con la antelación indicada en el apartado 1 del artículo 13, a los titulares de los certificados por ellos emitidos y, si estuvieran inscritos en él, al Registro de Prestadores de Servicios del Ministerio de Justicia.

g) Solicitar la inscripción en el Registro de Prestadores de Servicios de Certificación.

h) Cumplir las demás normas previstas, respecto de ellos, en este Real Decreto-ley y en sus normas de desarrollo.

Artículo 12. *Obligaciones exigibles a los prestadores de servicios de certificación que expidan certificados reconocidos.*

Además de cumplir las obligaciones establecidas en los artículos 7 y 11, los prestadores de servicios de certificación que expidan certificados reconocidos, han de cumplir las siguientes:

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

b) Demostrar la fiabilidad necesaria de sus servicios.

c) Garantizar la rapidez y la seguridad en la prestación del servicio. En concreto, deberán permitir la utilización de un servicio rápido y seguro de consulta del Registro de certificados emitidos y habrán de asegurar la extinción o suspensión de la eficacia de éstos de forma segura e inmediata.

d) Emplear personal cualificado y con la experiencia necesaria para la prestación de los servicios ofrecidos,

en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados.

e) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.

f) Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación.

g) Disponer de los recursos económicos suficientes para operar de conformidad con lo dispuesto en este Real Decreto-ley y, en particular, para afrontar el riesgo de la responsabilidad por daños y perjuicios. Para ello, habrán de garantizar su responsabilidad frente a los usuarios de sus servicios y terceros afectados por éstos. La garantía a constituir podrá consistir en un afianzamiento mercantil prestado por una entidad de crédito o en un seguro de caución.

Inicialmente, la garantía cubrirá, al menos, el 4 por 100 de la suma de los importes límite de las transacciones en que puedan emplearse el conjunto de los certificados que emita cada prestador de servicios de certificación. Teniendo en cuenta la evolución del mercado, el Gobierno, por Real Decreto, podrá reducir el citado porcentaje, hasta el 2 por 100.

En caso de que no se limite el importe de las transacciones en las que puedan emplearse al conjunto de los certificados que emita el prestador de servicios de certificación, la garantía a constituir, cubrirá, al menos, su responsabilidad por un importe de 1.000.000.000 de pesetas (6.010.121,04 euros). El Gobierno, por Real Decreto, podrá modificar el referido importe.

h) Conservar registrada toda la información y documentación relativa a un certificado reconocido durante quince años. Esta actividad de registro podrá realizarse por medios electrónicos.

i) Antes de expedir un certificado, informar al solicitante sobre el precio y las condiciones precisas de utilización del certificado. Dicha información, deberá incluir posibles límites de uso, la acreditación del prestador de servicios y los procedimientos de reclamación y de resolución de litigios previstos en las leyes y deberá ser fácilmente comprensible. Estará también a disposición de terceros interesados y se incorporará a un documento que se entregará a quien lo solicite. Para comunicar esta información, podrán utilizarse medios electrónicos si el signatario o los terceros interesados lo admiten.

j) Utilizar sistemas fiables para almacenar certificados, de modo tal que:

1. Sólo personas autorizadas puedan consultarlos, si éstos únicamente están disponibles para verificación de firmas electrónicas.
2. Únicamente personas autorizadas puedan hacer en ellos anotaciones y modificaciones.
3. Pueda comprobarse la autenticidad de la información.
4. El signatario o la persona autorizada para acceder a los certificados, pueda detectar todos los cambios técnicos que afecten a los requisitos de seguridad mencionados.

k) Informar a cualesquiera usuarios de sus servicios de los criterios que se comprometen a seguir, respetando este Real Decreto-ley y sus disposiciones de desarrollo, en el ejercicio de su actividad.

Artículo 13. *Cese de la actividad.*

1. El prestador de servicios de certificación que vaya a cesar en su actividad, deberá comunicarlo a los titulares de los certificados por él expedidos y transferir, con su consentimiento expreso, los que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios que los asuma o dejarlos sin efecto. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

2. Si el prestador de servicios estuviere inscrito en el Registro de Prestadores de Servicios de Certificación del Ministerio de Justicia, deberá comunicar a éste, con la antelación indicada en el anterior apartado, el cese de su actividad, y el destino que vaya a dar a los certificados especificando, en su caso, si los va a transferir y a quién o si los dejará sin efecto. Igualmente, indicará cualquier otra circunstancia relevante, que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de un procedimiento de quiebra o suspensión de pagos respecto de él.

3. La inscripción del prestador de servicios de certificación en el Registro de Prestadores de Servicios de Certificación será cancelada, de oficio, por el Ministerio de Justicia, cuando aquél cese en su actividad. El Ministerio de Justicia se hará cargo de la información relativa a los certificados que se hubieren dejado sin efecto por el prestador de servicios de certificación, a efectos de lo previsto en el artículo 12.h).

Artículo 14. *Responsabilidad de los prestadores de servicios de certificación.*

1. Los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone este Real Decreto-ley o actúen con negligencia. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia.

2. El prestador de servicios de certificación sólo responderá de los daños y perjuicios causados por el uso indebido del certificado reconocido, cuando no haya consignado en él, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo.

3. La responsabilidad será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, con las especialidades previstas en este artículo. Cuando la garantía que, en su caso, hubieran constituido los prestadores de servicios de certificación no sea suficiente para satisfacer la indemnización debida, responderán de la deuda, con todos sus bienes presentes y futuros.

4. Lo dispuesto en este artículo, se entiende sin perjuicio de lo establecido en la legislación sobre protección de los consumidores y usuarios.

Artículo 15. *Protección de los datos personales.*

1. El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y el que se realice en el Registro de Prestadores de Servicios de Certificación al que se refiere este Real Decreto-ley, se sujetan a lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y en las disposiciones dictadas en su desarrollo. El mismo régimen será de aplicación a los datos personales que se conozcan en el órgano que, en el ejercicio de sus funciones, supervisa la actuación de los prestadores de servicios de certificación y el competente en materia de acreditación.

2. Los prestadores de servicios de certificación que expidan certificados a los usuarios, únicamente pueden recabar datos personales directamente de los titulares de los mismos o con su consentimiento explícito. Los

datos requeridos serán, exclusivamente, los necesarios para la expedición y el mantenimiento del certificado.

3. Los prestadores de servicios de certificación que hayan consignado un seudónimo en el certificado, a solicitud del signatario, deberán constatar su verdadera identidad y conservar la documentación que la acredite. Dichos prestadores de servicios estarán obligados a revelar la identidad de los titulares de certificados cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica 5/1992, de 29 de octubre. Ello se entiende sin perjuicio de lo que, en la legislación específica en materia tributaria, de defensa de la competencia y de seguridad pública, se disponga sobre la identificación de las personas.

En todo caso, se estará a lo previsto en las normas sobre protección de datos indicadas en el apartado 1 de este artículo.

CAPÍTULO IV

Inspección y control de la actividad de los prestadores de servicios de certificación

Artículo 16. *Supervisión y control.*

1. El Ministerio de Fomento controlará, a través de la Secretaría General de Comunicaciones, el cumplimiento, por los prestadores de servicios de certificación que expidan al público certificados reconocidos, de las obligaciones establecidas en este Real Decreto-ley y en sus disposiciones de desarrollo. Asimismo, vigilará el cumplimiento, por los prestadores de servicios de certificación que no expidan certificados reconocidos, de las obligaciones establecidas en el artículo 11.

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

3. Cuando, como consecuencia de una actuación inspectora, se tuviera constancia de la contravención en el tratamiento de datos, de lo dispuesto en el artículo 11.c), la Secretaría General de Comunicaciones pondrá el hecho en conocimiento de la Agencia de Protección de Datos. Ésta podrá, con arreglo a la Ley Orgánica 5/1992, iniciar el oportuno procedimiento sancionador, con arreglo a la legislación que regula su actividad.

Artículo 17. *Deber de colaboración.*

Los prestadores de servicios de certificación tienen la obligación de facilitar a la Secretaría General de Comunicaciones toda la información y los medios precisos para el ejercicio de sus funciones y la de permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate, referida siempre a datos que conciernan al prestador de servicios.

Artículo 18. *Resoluciones del órgano de supervisión.*

La Secretaría General de Comunicaciones podrá ordenar a los prestadores de servicios de certificación la adopción de las medidas apropiadas para exigirles que cumplan este Real Decreto-ley y sus disposiciones de desarrollo.

TÍTULO III

Los dispositivos de firma electrónica y la evaluación de su conformidad con la normativa aplicable

CAPÍTULO ÚNICO

Los dispositivos de firma electrónica y la evaluación de su conformidad con la normativa aplicable

Artículo 19. *Dispositivos seguros de creación de firma electrónica.*

A efectos del artículo 2.f), para que se entienda que el dispositivo de creación de una firma electrónica es seguro, se exige:

1.º Que garantice que los datos utilizados para la generación de firma puedan producirse sólo una vez y que asegure, razonablemente, su secreto.

2.º Que exista seguridad razonable de que dichos datos no puedan ser derivados de los de verificación de firma o de la propia firma y de que la firma no pueda ser falsificada con la tecnología existente en cada momento.

3.º Que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros.

4.º Que el dispositivo utilizado no altere los datos o el documento que deba firmarse ni impida que éste se muestre al signatario antes del proceso de firma.

Artículo 20. *Normas técnicas.*

1. Se presumirá que los productos de firma electrónica que se ajusten a las normas técnicas cuyos números de referencia hayan sido publicados en el «Diario Oficial de las Comunidades Europeas» son conformes con lo previsto en la letra e) del artículo 12 y en el artículo 19.

2. Sin perjuicio de esta presunción, los números de referencia de esas normas se publicarán en el «Boletín Oficial del Estado».

Artículo 21. *Evaluación de la conformidad con la normativa aplicable de los dispositivos seguros de creación de firma electrónica.*

1. Los órganos de certificación a los que se refiere el artículo 6 podrán certificar los dispositivos seguros de creación de firma electrónica, previa valoración de los informes técnicos emitidos sobre los mismos, por entidades de evaluación acreditadas.

En la evaluación del cumplimiento de los requisitos previstos en el artículo 19, las entidades de evaluación podrán aplicar las normas técnicas respecto de los productos de firma electrónica a las que se refiere el artículo anterior u otras que determinen los órganos de acreditación y de certificación, y cuyas referencias se publiquen en el «Boletín Oficial del Estado».

2. Se reconocerá eficacia a los certificados sobre dispositivos seguros de creación de firma que hayan sido expedidos por los organismos designados para ello por los Estados miembros de la Unión Europea, cuando pongan de manifiesto que dichos dispositivos cumplen los requisitos contenidos en la normativa comunitaria sobre firma electrónica.

Artículo 22. *Dispositivos de verificación de firma.*

1. Los dispositivos de verificación de firma electrónica avanzada deben garantizar lo siguiente:

1. Que la firma se verifica de forma fiable y el resultado de esa verificación figura correctamente.
2. Que el verificador puede, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.
3. Que figura correctamente la identidad del signatario o, en su caso, consta claramente la utilización de un seudónimo.
4. Que se verifica de forma fiable el certificado.
5. Que puede detectarse cualquier cambio relativo a su seguridad.

2. El Real Decreto al que se refiere el artículo 6 podrá establecer los términos en los que las entidades de evaluación y los órganos de certificación podrán evaluar y certificar, respectivamente, el cumplimiento, por los dispositivos de verificación de firma electrónica avanzada, de los requisitos establecidos en este artículo.

TÍTULO IV

Tasa por el reconocimiento de acreditaciones y certificaciones

CAPÍTULO ÚNICO

Tasa por el reconocimiento de acreditaciones y certificaciones

Artículo 23. *Régimen aplicable a la tasa.*

1. La gestión precisa para el reconocimiento de las acreditaciones y de las certificaciones con arreglo a los artículos 6, 21 y 22, por los órganos públicos competentes, se grava con una tasa, a la que se aplicará el siguiente régimen:

a) Constituye el hecho imponible el reconocimiento por dichos órganos de la acreditación de los prestadores de servicios o de la certificación de los dispositivos de creación o de verificación de firma a que se refieren los artículos 6, 21 y 22.
b) Es sujeto pasivo la persona natural o jurídica que se beneficie del reconocimiento de la correspondiente acreditación o certificación.
c) Su cuota es de 47.500 pesetas (285,48 euros) por cada acreditación o certificación reconocida. Esta cantidad podrá ser actualizada por Real Decreto.
d) Se devengará cuando se presente la solicitud de reconocimiento de la correspondiente acreditación o certificación.

2. La forma de liquidación de la tasa se establecerá reglamentariamente.

TÍTULO V

Infracciones y sanciones

CAPÍTULO ÚNICO

Infracciones y sanciones

Artículo 24. *Clasificación de las infracciones.*

Las infracciones de las normas reguladoras de la firma electrónica y los servicios de certificación se clasifican en muy graves, graves y leves.

Artículo 25. *Infracciones.*

1. Son infracciones muy graves:

a) El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones establecidas en cualquiera de las letras del artículo 11, salvo la c), la g) y la h).
b) El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones impuestas en las letras c) a la j) del artículo 12, siempre que se causen daños graves a los usuarios o a terceros o se afecte gravemente a la seguridad de los servicios de certificación.
c) El incumplimiento grave y reiterado por los prestadores de servicios de certificación de las resoluciones dictadas por la Secretaría General de Comunicaciones, para asegurar el respeto a este Real Decreto-ley.

2. Son infracciones graves:

a) El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos, de las obligaciones impuestas en cualquiera de las letras del artículo 11, salvo la c), la g) y la h), siempre que se causen daños graves a los usuarios o a terceros o se afecte gravemente a la seguridad de los servicios de certificación.
b) El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones previstas en las letras a), b), y k) del artículo 12.
c) El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones contempladas en las letras c) a la j) del artículo 12, cuando no concurran las circunstancias previstas en el apartado 1.b) de este artículo.
d) La falta de comunicación por el prestador de servicios de certificación al Ministerio de Justicia, en los plazos previstos en el artículo 13, del cese de su actividad o de la iniciación, respecto de él, de un procedimiento de suspensión de pagos o de quiebra.
e) La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo, con arreglo a este Real Decreto-ley.
f) El incumplimiento de las resoluciones dictadas por la Secretaría General de Comunicaciones para asegurar que el prestador de servicios de certificación se ajuste a este Real Decreto-ley, cuando no deba considerarse como infracción muy grave, conforme al apartado 1.c) de este artículo.

3. Son infracciones leves:

a) El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones establecidas en cualquiera de las letras del artículo 11, excepto la c), cuando no deba considerarse como infracción grave, de acuerdo con lo previsto en el apartado 2.a) de este artículo.
b) La expedición de certificados reconocidos que incumplan alguno de los requisitos establecidos en el artículo 8.
c) No facilitar los datos requeridos, en el ámbito de sus respectivas funciones, por el Ministerio de Justicia o la Secretaría General de Comunicaciones para comprobar el cumplimiento de este Real Decreto-ley por los prestadores de servicios de certificación.
d) Cualquier otro incumplimiento de las obligaciones impuestas a los prestadores de servicios de certificación por este Real Decreto-ley, salvo el de la recogida en el artículo 11.c) o que deba ser considerado como infracción grave o muy grave, de acuerdo con lo dispuesto en los apartados anteriores.

Artículo 26. *Sanciones.*

1. Por la comisión de infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, se impondrá al infractor multa por importe no inferior al tanto, ni superior al quíntuplo, del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción o, en caso de que no resulte posible aplicar este criterio o de su aplicación resultare una cantidad inferior a la mayor de las que a continuación se indican, esta última constituirá el límite del importe de la sanción pecuniaria. A estos efectos, se considerarán las siguientes cantidades: El 1 por 100 de los ingresos brutos anuales obtenidos por la entidad infractora en el último ejercicio o, en caso de inexistencia de éstos, en el ejercicio actual; el 5 por 100 de los fondos totales, propios o ajenos, utilizados para la comisión de la infracción o 100.000.000 de pesetas (601.012,10 euros).

La reiteración de dos o más infracciones muy graves, en el plazo de cinco años, podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España durante un plazo máximo de dos años. Cuando la resolución de imposición de esta sanción sea firme, será comunicada al Registro de Prestadores de Servicios de Certificación para que cancele la inscripción del prestador de servicios sancionado.

b) Por la comisión de infracciones graves, se impondrá al infractor multa por importe de hasta el duplo del beneficio bruto obtenido como consecuencia de los actos u omisiones que constituyan aquéllas o, en caso de que no resulte aplicable este criterio o de su aplicación resultare una cantidad inferior a la mayor de las que a continuación se indican, esta última constituirá el límite del importe de la sanción pecuniaria. A estos efectos, se considerarán las siguientes cantidades: El 0,5 por 100 de los ingresos brutos anuales obtenidos por la entidad infractora en el último ejercicio o, en caso de inexistencia de éstos, en el ejercicio actual; el 2 por 100 de los fondos totales, propios o ajenos, utilizados para la comisión de la infracción o 50.000.000 de pesetas (300.506,04 euros).

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

2. Las infracciones graves y muy graves podrán llevar aparejada la publicación de la resolución sancionadora en el «Boletín Oficial del Estado» y en dos periódicos de difusión nacional, una vez que aquélla tenga carácter firme.

3. La cuantía de las multas que se impongan, dentro de los límites indicados, se graduará teniendo en cuenta, además de lo previsto en el artículo 131.3 de la Ley 30/1992, lo siguiente:

a) La gravedad de las infracciones cometidas anteriormente por el sujeto al que se sanciona.

b) La repercusión social de las infracciones.

c) El daño causado, siempre que no haya sido tomado en consideración para calificar la infracción como leve, grave o muy grave.

d) El beneficio que haya reportado al infractor el hecho objeto de la infracción.

4. Se anotarán en el Registro de Prestadores de Servicios de Certificación las sanciones impuestas por resolución firme a éstos por la comisión de cualquier infracción grave o muy grave. Las notas relativas a las sanciones se cancelarán una vez transcurridos los plazos de prescripción de las sanciones administrativas previstos en la Ley reguladora del procedimiento administrativo común.

5. Las cuantías señaladas en este artículo serán actualizadas periódicamente por el Gobierno, mediante Real Decreto, teniendo en cuenta la variación de los índices de precios al consumo.

Artículo 27. *Medidas cautelares.*

En los procedimientos sancionadores por infracciones graves o muy graves se podrán adoptar, con arreglo a la Ley 30/1992, de 26 de noviembre, las medidas cautelares que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte. Estas medidas podrán consistir en la orden de cese temporal de la actividad del prestador de servicios de certificación, en la suspensión de la vigencia de los certificados por él expedidos o en la adopción de otras cautelas que se estimen precisas. En todo caso, se respetará el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.

Artículo 28. *Procedimiento sancionador.*

1. El ejercicio de la potestad sancionadora atribuida por este Real Decreto-ley corresponde a la Secretaría General de Comunicaciones del Ministerio de Fomento. Para ello, la Secretaría General de Comunicaciones se sujetará al procedimiento aplicable, con carácter general, al ejercicio de la potestad sancionadora por las Administraciones públicas.

2. El Ministerio de Justicia y los demás órganos que ejercen competencias con arreglo a este Real Decreto-ley y sus normas de desarrollo podrán instar la incoación de un procedimiento sancionador, mediante petición razonada dirigida a la Secretaría General de Comunicaciones

Disposición adicional única. *Posibilidad de emisión por las entidades públicas de radiodifusión de una Comunidad Autónoma en el territorio de otras con las que aquélla tenga espacios radioeléctricos colindantes.*

Las entidades autonómicas habilitadas, con arreglo a la Ley, para prestar el servicio de radiodifusión digital terrenal, podrán emitir en el territorio de otras Comunidades Autónomas con las que aquélla tenga espacios radioeléctricos colindantes. Para ello, será preciso que exista acuerdo entre las Comunidades Autónomas afectadas y que, en cada territorio, se empleen los bloques de frecuencias planificados en el Plan Técnico Nacional de Radiodifusión Sonora Digital Terrenal, para el ámbito autonómico.

Disposición transitoria única. *Prestadores de servicios de certificación establecidos en España antes de la entrada en vigor de este Real Decreto-ley.*

Los prestadores de servicios de certificación ya establecidos en España y cuya actividad se rija por una normativa específica habrán de adaptarse a este Real Decreto-ley en el plazo de un año desde su entrada en vigor. No obstante conservarán su validez los certificados ya expedidos que hayan surtido efectos.

Disposición final primera. *Fundamento constitucional.*

Este Real Decreto-ley se dicta al amparo del artículo 149.1.8.ª, 18.ª y 21.ª de la Constitución, que atribuye competencia exclusiva al Estado en materia de legislación civil, de bases del régimen jurídico de las Administraciones Públicas y de telecomunicaciones.

Disposición final segunda. *Habilitación al Gobierno.*

Se habilita al Gobierno para desarrollar, mediante Reglamento, lo previsto en este Real Decreto-ley.

Disposición final tercera. *Entrada en vigor.*

El presente Real Decreto-ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Dado en Madrid a 17 de septiembre de 1999.

JUAN CARLOS R.

El Presidente del Gobierno,
JOSÉ MARÍA AZNAR LÓPEZ

MINISTERIO DE ASUNTOS EXTERIORES

18916 *CONVENIO sobre la Ayuda Alimentaria, 1999, hecho en Londres el 13 de abril de 1999. Aplicación provisional.*

CONVENIO SOBRE AYUDA ALIMENTARIA, 1999

CONVENIO SOBRE AYUDA ALIMENTARIA, 1999

PREÁMBULO

Las Partes en el presente Convenio

Habiendo revisado el Convenio sobre Ayuda Alimentaria, 1995 y su objetivo de asegurar como mínimo 10 millones de toneladas de ayuda alimentaria anualmente en forma de cereal adecuado para el consumo humano, y deseando confirmar su deseo de mantener la cooperación internacional en asuntos de ayuda alimentaria entre Gobiernos miembros;

Recordando la Declaración sobre Seguridad Alimentaria Mundial y el Plan de Acción de la Cumbre Alimentaria Mundial aprobado en Roma en 1996 y, en particular, el compromiso de lograr seguridad alimentaria para todos y de hacer un esfuerzo continuo por erradicar el hambre;

Deseando mejorar la capacidad de la comunidad internacional de responder a situaciones de emergencia alimentaria y de mejorar la seguridad alimentaria mundial, a través de suministros garantizados de ayuda alimentaria independientemente del precio mundial de alimentos y de las fluctuaciones de la oferta;

Recordando que, en su decisión de Marrakech de 1994 sobre medidas relativas a países menos desarrollados y países en desarrollo importadores netos de alimentos, los Ministros de países miembros de la OMC convinieron en revisar el nivel de ayuda alimentaria establecido en virtud del Convenio sobre Ayuda Alimentaria según lo desarrollado adicionalmente en la Conferencia Ministerial de Singapur de 1996;

Reconociendo que los beneficiarios y miembros tienen sus propias políticas sobre ayuda alimentaria y asuntos afines, y que el objetivo final de la ayuda alimentaria es la eliminación de la propia necesidad de ayuda alimentaria;

Deseosos de mejorar la eficacia y calidad de la ayuda alimentaria como instrumento en apoyo de la seguridad alimentaria en países en desarrollo, en particular para aliviar la pobreza y el hambre de los grupos más vulnerables, y de mejorar la coordinación y cooperación entre miembros en la esfera de la ayuda alimentaria;

Han convenido en lo siguiente:

PARTE I

Objetivos y definiciones

Artículo I. *Objetivos.*

Los objetivos del presente Convenio son contribuir a la seguridad alimentaria mundial y mejorar la capacidad de la comunidad internacional de responder a situaciones de emergencia alimentaria y otras necesidades alimentarias de países en desarrollo:

a) facilitando niveles apropiados de ayuda alimentaria en forma previsible, según lo determinado por las disposiciones del presente Convenio;

b) alentando a los miembros a asegurarse de que la ayuda alimentaria proporcionada esté destinada en particular al alivio de la pobreza y del hambre de los grupos más vulnerables, y guarde conformidad con el desarrollo agrícola en esos países;