UNIVERSIDAD DEL ISTMO

Facultad de Derecho

ANÁLISIS JURÍDICO DE LAS ENTIDADES CERTIFICADORAS DE FIRMA ELECTRÓNICA EN GUATEMALA

MARTA PAOLA DE LA CRUZ QUIÑÓNEZ

Guatemala, mayo de 2011

UNIVERSIDAD DEL ISTMO

Facultad de Derecho

ANÁLISIS JURÍDICO DE LAS ENTIDADES CERTIFICADORAS DE FIRMA ELECTRÓNICA EN GUATEMALA

TESIS
Presentada al Consejo de
Facultad de Derecho de la Universidad del Istmo

Por

MARTA PAOLA DE LA CRUZ QUIÑÓNEZ

Al conferírsele el título de

LICENCIADA EN DERECHO

Y LOS TÍTULOS PROFESIONALES DE

ABOGADA Y NOTARIO

Guatemala, mayo de 2011

UNIVERSIDAD DEL ISTMO

Facultad de Derecho

ANÁLISIS JURÍDICO DE LAS ENTIDADES CERTIFICADORAS DE FIRMA ELECTRÓNICA EN GUATEMALA

POR

MARTA PAOLA DE LA CRUZ QUIÑÓNEZ

ASESOR

ENRIQUE SÁNCHEZ USERA

GUATEMALA, MAYO DE 2011

DEDICATORIA

A DIOS

A MIS PADRES Y HERMANA: Edgar de la Cruz Vela

Esperanza Quiñónez de de la Cruz

Jeniffer Pamela de la Cruz Quiñónez

A MI ESPOSO Aldo Federico Bianchi Barreda

A MIS HIJOS Gian Paolo Bianchi de la Cruz

Alessia Bianchi de la Cruz

A MI UNIVERSIDAD Y CATEDRÁTICOS.

Guatemala 10 de enero de 2011

Señores Miembros del Consejo
Facultad de Derecho
Universidad del Istmo
Presente

Honorable Miembros del Consejo:

Me es grato dirigirme a ustedes con el objeto de manifestarles que en virtud de la disposición por medio de la cual se me nombró asesor del trabajo de tesis de la estudiante MARTA PAOLA DE LA CRUZ QUIÑÓNES, titulado ¨ANÁLISIS JURÍDICO DE LAS ENTIDADES CERTIFICADORAS DE FIRMA ELECTRÓNICA EN GUATEMALA¨, procedo a emitir DICTAMEN FAVORABLE con relación a la misma.

El trabajo realizado por la estudiante DE LA CRUZ QUIÑÓNES se apega a los requisitos establecidos en el Instructivo de Tesis de la Facultad de Derecho, constituyendo un trabajo serio y completo en relación con las entidades certificadoras de firma electrónica en Guatemala..

Sin otro particular de momento, aprovecho para suscribirme de usted.

Atentamente,

M.A. Enrique Fernando Sánchez Usera
Asesor de Tesis.

(temala, 24 de mayo de 2011.-

Miembros del Consejo
Facultad de Derecho
Universidad del Istmo
Ciudad

Estimados miembros del Consejo de la Facultad de Derecho:

De conformidad con el nombramiento que se me hiciera para realizar la revisión de fondo y forma del trabajo de tesis de la alumna MARTA PAOLA DE LA CRUZ QUIÑONEZ, titulado, **ANÁLISIS JURÍDICO DE LAS ENTIDADES CERTIFICADORAS DE FIRMA ELECTRÓNICA EN GUATEMALA,** debo manifestar que la alumna anteriormente citada realizó las correcciones y adaptaciones que se consideraron necesarias, por lo que considero que el trabajo de tesis cumple con lo establecido en el Reglamento de Tesis, y es apto para su publicación.

Con la presente doy por **evaluado y aprobado** el trámite de revisión de fondo y forma del trabajo de tesis titulado **ANÁLISIS JURÍDICO DE LAS ENTIDADES CERTIFICADORAS DE FIRMA ELECTRÓNICA EN GUATEMALA,** de la alumna MARTA PAOLA DE LA CRUZ QUIÑONEZ para los efectos correspondientes de conformidad con el respectivo Reglamento.

Sin otro particular, me suscribo,

Atentamente,

Lic. Ronald Flores García.

Ronald Estuardo Flores García
Abogado y Notario

FDER 248-11

UNIVERSIDAD DEL ISTMO

FACULTAD DE DERECHO

ORDEN DE IMPRESIÓN DE TESIS

En la ciudad de Guatemala, el treinta y uno de mayo de dos mil once, la infrascrita Secretaria del Consejo de la Facultad de Derecho de la Universidad del Istmo,

CERTIFICA:

PUNTO ÚNICO: Haber tenido a la vista el libro de actas del Consejo de la Facultad de Derecho de la Universidad del Istmo correspondiente al año dos mil once, en el que se contiene el acta número diecisiete diagonal once (17/11), correspondiente a la sesión celebrada por el Consejo de Facultad el lunes treinta de mayo de dos mil once.

Consta en el punto sexto de dicha acta la resolución que, en su parte conducente, dice textualmente:

El Consejo de Facultad conoció la propuesta de autorización de impresión del trabajo de tesis de la alumna ***Marta Paola de la Cruz Quiñonez***, con el título **"ANÁLISIS JURÍDICO DE LAS ENTIDADES CERTIFICADORAS DE FIRMA ELECTRÓNICA DE GUATEMALA".** Estudiado el punto, y considerando que se ha cumplido con todos los requisitos exigidos por el Reglamento de Tesis respectivo, el Consejo de Facultad resolvió:

> Autorizar la impresión del trabajo de tesis de la alumna ***Marta Paola de la Cruz Quiñonez***, con el título **"ANÁLISIS JURÍDICO DE LAS ENTIDADES CERTIFICADORAS DE FIRMA ELECTRÓNICA DE GUATEMALA".**

No habiendo más que hacer constar, se finaliza la presente, firmando la misma la Secretaria del Consejo de la Facultad de Derecho de la Universidad del Istmo, quien da fe.

Licda. Leticia Andrea Morales Díaz
Secretaria de Consejo de Facultad

SECRETARIA FACULTAD DE DERECHO

Ja. Avenida 3-67 zona 13
PBX (502) 2429-1400
(502) 2429-1420
Fax: (502) 2475-2192
(502) 2429-1456
E-mail: fder@unis.edu.gt
www.unis.edu.gt
Guatemala, Centroamérica

RESUMEN

La revolución de la tecnología de información, conjuntamente con el desarrollo de la infraestructura de comunicaciones, está haciendo cambiar significativamente las relaciones entre individuos y organizaciones, tanto en Guatemala como en todo el mundo. Estas nuevas formas de comunicación abren un gran abanico de posibilidades tanto para ciudadanos como para empresas y permiten comercializar productos y servicios de una forma ágil y económica.

En muchos países del mundo las distintas administraciones estatales están apostando decididamente por Internet como vía de comunicación, creando webs con información de interés público a disposición de la ciudadanía. Guatemala, por su parte, es una principiante en este tipo de situaciones debido a que los demás países le llevan una gran ventaja en cuanto tiempo y experiencia de utilización de los medios electrónicos; pero aún así está dando sus primeros pasos; esto se evidencia en la reciente aprobación de la Ley para el Reconocimiento de las Comunicaciones y Firma Electrónica Decreto 47-2008 del Congreso de la República, publicado en el Diario de Centro América el 23 de septiembre de 2008 y que entró en vigencia el 01 de octubre del mismo año.

Los países que han legislado en la materia, tales como España, Argentina, Chile, Ecuador, México, entre otros, equipararan la firma electrónica ó digital a la tradicional firma manuscrita u ológrafa, que tiene características propias, la principal de ellas es que es aceptada legalmente, esto quiere decir que si una persona firmó un documento adquiere tanto los derechos como las obligaciones que de él deriven, y si no cumple con obligaciones a su cargo, el tenedor del documento puede demandar judicialmente el cumplimiento. La autoridad

competente acepta las responsabilidades adquiridas con sólo calificar a la firma como válida.

Es en el aspecto de la verificación de la autenticidad de la firma electrónica o digital en donde se encuentra la función de las entidades certificadoras de la misma, éstas pueden ser personas jurídicas nacionales o extranjeras, públicas o privadas que otorgan los certificados de firma electrónica, así como otros servicios que la legislación vigente así les permita. Son prestadores acreditados del servicio de certificación en quienes descansa el otorgamiento de la seguridad y certeza jurídica de que debe ir impregnada la firma electrónica, a través de los certificados que emiten.

En virtud de lo anteriormente expuesto se puede decir que el objetivo principal a seguir será el de presentar un análisis jurídico de las entidades certificadoras de firma electrónica, que según la Ley para el Reconocimiento de las Comunicaciones y Firma Electrónica Decreto 47-2008 del Congreso de la República, podrán actuar libremente en el país para otorgar una mayor seguridad y certeza jurídica en la contratación electrónica tanto nacional como internacional. Analizar así las deficiencias que las mismas presentan en nuestro ámbito nacional y proponer las mejoras en base a un estudio comparativo con legislaciones que la poseen ya dentro de su normativa legal y se encuentran en funcionamiento desde hace ya bastantes años, así como estudiar si nuestra legislación se aplica a las nacientes corrientes tecnológicas ante las cuales se ven enfrentados nuestros comerciantes, y si nuestra ley en la materia los ampara lo suficiente y permite hacer a nuestro país un lugar con ventajas competitivas a nivel internacional o si existen situaciones que hacen falta regular.

ÍNDICE

INTRODUCCIÓN

Existen en la actualidad una diversidad de medios de comunicación y distintas infraestructuras tecnológicas que permiten la interacción entre individuos de distintos lugares de una forma ágil, eficaz y económica. La colocación de productos en el mercado se realiza sin la necesidad de que se encuentren físicamente presentes, de igual manera sucede en las relaciones entre individuos, ya no es necesaria la presencia de los mismos para que el encuentro se lleve a cabo. Guatemala es un país que a pesar de no encontrarse al nivel tecnológico en que se encuentran los distintos países del mundo ya está incursionando en esta nueva era tecnológica.

Existen países tales como Estados Unidos, México, Chile, Ecuador, España, entre otros muchos, que están empleando el Internet como un medio de comunicación para intereses ya no sólo privados sino también públicos. Todos estos avances han tenido la aceptación de la población que ve como lo que antes era un trámite tardado y engorroso se convierte en algo ágil y sencillo.

Estas iniciativas han tenido una gran aceptación positiva en la opinión pública lo que ha provocado que la demanda en el mundo entero por la utilización generalizada de la red sea mayor.

Guatemala, por su parte, es una principiante en este tipo de situaciones debido a que los demás países le llevan una gran ventaja en cuanto tiempo y experiencia de utilización de los medios electrónicos; pero aún así está dando sus primeros pasos; esto se evidencia con la aprobación de la Ley para el Reconocimiento de las Comunicaciones y Firma Electrónica Decreto 47-2008 del Congreso de la República, publicado en el Diario de Centro América el 23 de septiembre de 2008 y que entró en vigencia el 01 de octubre del mismo año.

Con la incorporación al Derecho vigente de esta nueva normativa se le ha abierto el paso a una figura jurídica, la firma electrónica, la cual generará grandes cambios en la conceptualización de la forma tradicional de contratación, adaptándose de esta manera a la constante necesidad de cambio y evolución que el Derecho como ciencia requiere para irse adaptando a las necesidades del hombre.

El fin de la firma digital es el mismo que el de la firma ológrafa: Prestar conformidad y responsabilizarse con el documento firmado.

Los países que han legislado en la materia equiparan la firma electrónica ó digital a la tradicional firma manuscrita u ológrafa, que tiene características propias, la principal radica en que es aceptada legalmente, es decir que en el momento en que una persona firma un documento adquiere tanto los derechos como las obligaciones que de él deriven, de tal manera que si no los cumple, la persona que posee el documento se encuentra en la capacidad de demandar judicialmente el cumplimiento del mismo, esto debido a que la autoridad competente al calificar la firma como válida acepta las responsabilidades adquiridas.

Las entidades certificadoras de firma electrónica pueden ser personas jurídicas nacionales o extranjeras, públicas o privadas que otorgan los certificados de firma electrónica, así como otros servicios que la legislación vigente así les permita[1]. Son prestadores acreditados del servicio de certificación en quienes descansa el otorgamiento de la seguridad y certeza jurídica de que debe ir impregnada la firma electrónica, a través de los certificados que emiten. El análisis jurídico de dichas entidades es el tema alrededor del cual gira el trabajo de investigación, el cual inicialmente se planteó cuando recién fue aprobada la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, que

[1] Artículo 10 del Acuerdo Gubernativo 135-2009 del Reglamento de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

presentó ciertas deficiencias que posteriormente fueron complementadas con la aprobación de su respectivo reglamento el Acuerdo Gubernativo 135-2009. No así la ley siguió presentado ciertas inconsistencias que serán objeto de análisis a lo largo de la presente investigación.

Según la normativa vigente, en el artículo 33 del Decreto 47-2008 los documentos autenticados con firma digital, por medio de un certificado emitido por una entidad certificadora legalmente constituida, produce plena prueba en un proceso judicial; este es un tema de mucha importancia pues si las entidades certificadoras no poseen una regulación integral esto se prestará a futuros problemas jurídicos, estafas y demás tergiversaciones de medios probatorios que entorpecerán el curso de los procesos, eliminando así la certeza y seguridad jurídica que esta institución debe proveer.

Por lo tanto es necesario realizar un análisis comparativo de las legislaciones que poseen ya dentro de su normativa legal la figura de la firma electrónica, para así determinar si la legislación nacional en la materia presenta deficiencias, así como determinar si la misma se aplica a las nacientes corrientes tecnológicas ante las cuales se ven enfrentados nuestros comerciantes y personas particulares y permite hacer a nuestro país un lugar con ventajas competitivas a nivel internacional o si existen situaciones que hacen falta regular.

En virtud de lo anteriormente expuesto cabe señalar que el objetivo principal del trabajo será el de presentar un análisis jurídico de las entidades certificadoras de firma electrónica que, según la Ley para el Reconocimiento de las Comunicaciones y Firma Electrónica Decreto 47-2008 del Congreso de la República, podrán actuar libremente en el país para otorgar una mayor seguridad y certeza jurídica en la contratación electrónica tanto nacional como internacional.

La legislación aplicable al presente estudio será la Constitución Política de la República de Guatemala, la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas Decreto 47-2008 del Congreso de la República de Guatemala, el Código de Comercio de Guatemala Decreto 2-70, Código Civil Decreto Ley 106, el Código Procesal Civil y Mercantil, Decreto Número 107, la Ley Modelo Ley Modelo de la CNUDMI Sobre las Firmas Electrónicas del año 2001 de Comisión de las Naciones Unidas para el Derecho Comercial Internacional y los Convenios y Tratados Internacionales aplicables.

Los instrumentos a utilizar para la realización del trabajo de campo serán por un lado entrevistas con profesionales de la materia que otorgarán sus criterios con relación a la figura de la firma electrónica en Guatemala, sus ventajas, funcionamiento en Guatemala y si la legislación nacional se apega a las normas internacionales creadas para la materia. Asimismo se realizará una comparación de las legislaciones que cinco países: España, México, Argentina, Chile y Perú, que cuentan con legislación sobre la firma electrónica dentro de su ordenamiento jurídico a modo de examinar si nuestra legislación contempla los temas suficientes para competir internacionalmente en el mercado digital.

OBJETIVOS ESPECÍFICOS

- Establecer el marco conceptual de los antecedentes históricos y jurídicos de la identificación de personas.
- Presentar los conceptos tecnológicos que se reflejan en la Ley para el Reconocimiento de las Comunicaciones y Firma Electrónica.
- Comparar la fortaleza tecnológica de las diferentes formas de identificación.
- Reconocer la importancia de los certificados digitales y la forma en que se encuadran en el texto de la Ley.

- Analizar la importancia de las entidades certificadoras y la forma en que se destacan en la Ley para el Reconocimiento de las Comunicaciones y Firma Electrónica.
- Analizar las consecuencias jurídicas que trae una regulación difusa en materia de certificación para los actos y negocios futuros que se realizarán bajo el amparo de las entidades certificadoras.

HIPÓTESIS

La nueva Ley para el Reconocimiento de la Comunicaciones y Firma Electrónica, Decreto 47-2008, posee algunas inconsistencias en cuanto a la normativa y regulación de las entidades certificadoras de firma electrónica especialmente respecto a garantizar un servicio eficiente y confiable que propicie el comercio internacional, ya que se desconocen aspectos importantes tales como quién puede realizar estos servicios, qué requisitos deben cumplir, si están o no acreditados, en qué medida la acreditación influye en la prestación del servicio y las responsabilidades que esto conlleva, entre otros aspectos que son de vital importancia para el buen funcionamiento de esta figura jurídica.

ALCANCES Y LÍMITES

El problema de estudio resulta de especial importancia debido a que se ha escrito acerca de lo que es la firma electrónica, su implicación en el sistema legal, la importancia de dar certeza y seguridad jurídica a los actos y negocios jurídicos a través de los medios electrónicos, pero poco se ha hablado acerca de qué entidades serán las encargadas de certificar la autenticidad de dichos negocios, qué requisitos deben llenar para funcionar legalmente y cómo pueden constituirse en entidades de confianza y que actúan bajo un régimen legal establecido.

La Ley para el Reconocimiento de las Comunicaciones y Firma Electrónica contempla artículos referentes a las entidades certificadoras pero con una

normativa muy inconsistente, a pesar de que de ellas depende la autenticidad de la firma electrónica y que la misma sea un medio eficiente y eficaz para los actos, negocios jurídicos y contrataciones. Conviene hacer un análisis de esta figura jurídica debido a que es un tema de actualidad que se aplica constantemente en las contrataciones tanto nacionales como internacionales por medios electrónicos, se constituye así un nuevo capítulo en la historia del Derecho que es necesario estudiar para empezar a crear documentación suficiente al respecto que servirá de base para futuras investigaciones.

El estudio de este tema presenta una propuesta importante, porque el Derecho busca siempre dar seguridad y certeza jurídica a lo que ampara y las entidades de certificación son eso, las instituciones encargadas de impregnar de seguridad y certeza jurídica a la firma electrónica para hacer de ella un sistema aplicable. El alcance que se pretende lograr con la elaboración de la presente investigación será estrictamente doctrinario y jurídico debido a que en Guatemala aún no se ha inscrito ninguna entidad prestadora de servicios de certificación, por diversas cuestiones tanto culturales como económicas, entre otras. Aunque sí se cuenta ya con una normativa compuesta por una ley y un reglamento y las guías registrales que permiten realizar un análisis jurídico bastante completo de dicha figura. Por lo tanto, el límite con el que se encuentra el estudio será que aún no se puede analizar las entidades prestadoras de servicios de certificación en su aplicación práctica en la realidad guatemalteca, pues aún no existe ninguna inscrita bajo las normas legales establecidas, por lo que la investigación no puede ir más allá del tema doctrinario.

UNIDADES DE ANÁLISIS

Leyes de Ley de Firma Electrónica de los países siguientes:

- España
- México
- Chile
- La ley de Reconocimiento de Comunicaciones y Firma Electrónica, Decreto 47-2008 del Congreso de la República de Guatemala.

TIPOS DE INVESTIGACIÓN

Según los tipos de investigación jurídica, la TESIS será:

Jurídico comparativa: Esta tesis buscará identificar las similitudes y diferencias que pudieren encontrarse en normas jurídicas e institucionales formales en los sistemas jurídicos que poseen el sistema de firma electrónica incorporado en su normativa vigente, con respecto a la Ley para el Reconocimiento de las Comunicaciones y Firma Electrónica, Decreto 47-2008 del Congreso de la República de Guatemala. A manera de comparar si realmente se ajusta a los estándares internacionales para saber si es competitiva a nivel internacional.

Jurídico descriptiva: Por medio de este análisis será posible descomponer el problema de la ausencia de requisitos necesarios para la constitución de las entidades certificadoras de Firma Electrónica en Guatemala y sus posibles consecuencias jurídicas.

Jurídico propositiva: Se cuestionará la Ley para el Reconocimiento de las Comunicaciones y Firma Electrónica, Decreto 47-2008 del Congreso de la República de Guatemala. Para evaluar las deficiencias que puede presenta con respecto al tema y proponer cambios o reformas que pudieran hacer más eficiente la misma ley.

APORTE

El estudio de este tema servirá para complementar aspectos que no se han tocado a profundidad en las tesis de Derecho que se han trabajo en otras universidades, pues como se ha mencionado anteriormente se ha escrito sobre la firma electrónica, la seguridad y certeza de los negocios electrónicos pero poco se ha hablado sobre quienes llevarán a cabo la actividad de certificar estos medios, quiénes gozarán de esta potestad de otorgar autenticidad, quién los va a facultar para hacerlo y en base a qué poder se podrá facultar.

Los instrumentos a utilizar durante el desarrollo de la investigación serán entrevistas con profesionales del Derecho relacionados con esta rama y un cuadro de cotejo de algunos de los países que han introducido en su legislación la figura de la firma electrónica.

Capítulo I: La Firma Electrónica

I.1 Antecedentes históricos

En las relaciones entre personas muchas veces se hace necesario contar con un elemento o un signo distintivo que permita otorgar información acerca de la identidad del autor de un determinado documento y al mismo tiempo que por dicho signo manifiesta su consentimiento sobre el contenido del mismo. Este elemento es generalmente conocido como firma. El empleo de la firma se da con mucha frecuencia en las distintas relaciones humanas, y aún así no existe una teoría, elementos, conceptos o consecuencias definidos en la doctrina al respecto de la misma.[2]

Existe conocimiento del uso de la firma en distintas épocas de la humanidad como lo es durante el imperio romano, en la edad media, el sistema utilizado por el sistema visigodo, entre otras.

En Roma, por ejemplo, los documentos no eran firmados, por su lado existía una ceremonia conocida como *manufirmatio,* en la cual los documentos eran leídos por su autor o el funcionario encargado y luego de ello se colocaba el pergamino desenrollado y extendido sobre la mesa del escribano para que el autor del mismo pudiera pasar la mano abierta sobre dicho documento en actitud de juramento, y se colocaba el nombre, signo o una o tres cruces por el autor y seguidamente por los testigos.[3]

Durante la Edad Media lo que se acostumbró hacer fue el inscribir en el documento una cruz a la que se le agregaban letras y rasgos los cuales eran utilizados como firma. Debido a la cultura de la época y el analfabetismo de la mayoría de la población, la nobleza reemplazó esta práctica por el uso de sellos.

---

[2] Acosta Romero, Miguel. NUEVO DERECHO MERCANTIL, capítulo XVIII: La Firma en el derecho mercantil mexicano, Primera edición, Editorial Porrúa, México 2000. pp 537 a 562.

[3] ibid

Al pasar los años el encabezamiento de la firma de algunos documentos se realizó con tinta roja.

En el caso del Imperio Bizantino en las escrituras que firmaba el rey se utilizaba tinta de color rojo mientras en las que utilizaba el heredero se empleaba el color verde. Puede decirse entonces que el origen de la palabra rúbrica o *rubrum* proviene de dicha costumbre de firmar con tinta roja para garantizar la autenticidad.

En el sistema visigótico los testigos tocaban el documento o lo firmaban, esta firma era corriente y no necesariamente imprescindible. En la época auriciana las leyes visigodas procuraron prestar más atención a las formalidades documentales regulando de otra manera las suscripciones, signos y comprobación de escritura. "La "*subscriptio",* representaba la indicación del nombre del signante y la fecha, y el "*signum"* un rasgo que la sustituye si no sabe o no puede escribir. La "*subscriptio"*, daba pleno valor probatorio al documento y el "*signum"* debía ser completado con el juramento de la veracidad por parte de uno de los testigos. Si faltaba la firma y el signo del autor del documento, éste era inoperante y debía completarse con el juramento de los testigos sobre la veracidad del contenido."[4]

En la actualidad el uso de la firma en el mundo entero está generalizado a través de estampar un signo distintivo de cada persona por medio del cual acepta el contenido del documento en el cual la coloca sin mayor formalidad que la sola impresión manuscrita de la misma hecha por el firmante; para mayor seguridad, se corrobora por medio del documento personal de identificación; en el caso de Guatemala, la cédula de vecindad que paulatinamente será sustituirá por el Documento Personal de Identificación DPI. Esta facilidad en cuanto a la colocación de la firma manuscrita que no requiere las mismas formalidades que

[4] Acosta Romero, Miguel. NUEVO DERECHO MERCANTIL, capítulo XVIII: La Firma en el derecho mercantil mexicano, Primera edición, Editorial Porrúa, México 2000. pp 537 a 562

se exigieron en las distintas cultura antiguas ha facilitado que la misma pueda ser falsificada sin mayor inconveniente, razón por la cual las modernas tecnologías han empezado a buscar mecanismos para lograr que la firma sea una figura que ofrezca un grado de certeza y seguridad mayor en cuanto a la identidad del firmante.

Elementos de la firma

La firma, en general, para poder ser considerada como tal, debe contar con una serie de elementos que la caracterizan, estos elementos son:

a) **Elementos formales:** son todos aquellos componentes materiales de la firma que se encuentran relacionados con los procedimientos empleados para firmar y el grafismo de la misma. Están compuestos por el signo distintivo y personal que en sí representa a la firma, el cual puede haber sido puesto de puño y letra del firmante o que como es el caso de la firma electrónica pudo haber sido sustituido por dicho medio.

b) **El elemento intencional o intelectual:** Este es el componente en el que se establece la voluntad del firmante de asumir el contenido de un documento, tal como lo señala Larrieu citado por Alfredo Reyes Krafft.[5]

   En el caso de la firma electrónica la firma se encuentra integrada y fielmente unida al contenido del documento, no se pueden separar, de hacerlo se desvirtuaría la razón de ser de la firma electrónica.

c) **Elementos funcionales:** según los elementos prácticos de la firma ésta puede tener dos funciones una identificadora y otra de autenticación. Según la función identificadora la firma constituye el elemento que

[5] Reyes Krafft, Alfredo, LA FIRMA ELECTRÓNICA Y LAS ENTIDADES DE CERTIFICACIÓN, Editorial Porrúa, México, 2004, pp 40

establece la relación jurídica entre el acto firmado a través de un documento y las personas que participan en el mismo. La identidad de dichas personas determina la personalidad con la que actúan y qué derechos y obligaciones pueden adquirir con dicho acto.

Por lo tanto se puede decir que la firma manuscrita expresa la identidad, aceptación y autoría del firmante. Dicha autenticación puede padecer de falencias ya que no es del todo fiable que la firma pertenezca a una persona determinada en virtud de las falsificaciones que pueden darse de dicho signo; razón por la cual ante la duda de la misma será necesario el auxilio de un estudio de caligrafía forense o peritaje caligráfico, con el fin de establecer si existió o no una falsificación.[6]

Ante esta situación la firma electrónica viene a facilitar el hecho de no ser necesario el uso de un experto forense para determinar la veracidad de una firma ya que los elementos y sistemas criptográficos empleados para crear la firma electrónica ofrecen una mayor seguridad en cuanto a la identidad, aceptación y autoría del firmante; esto no quiere decir que la firma electrónica venga a sustituir a la firma manuscrita ya que esto sería imposible ya que siempre será necesaria la firma en papel de mano del firmante para muchos actos de la vida cotidiana pero lo que sí es que facilitará ciertas relaciones, comerciales sobre todo, y las volverá mucho más eficientes y seguras.

En cuanto a la función de autenticación ésta constituye el acto por medio del cual el firmante expresa su consentimiento con respecto al contenido del documento y hace suyo el mensaje. Pueden existir dos fases en este proceso de la autenticación, por un lado una fase u operación pasiva en la cual no se requiere del consentimiento ni del conocimiento siquiera del sujeto identificado y un proceso activo, por el cual el firmante es quien se identifica conscientemente en

[6] Reyes Krafft, Alfredo, ORÍGENES DE LA FIRMA AUTÓGRAFA, Editorial Porrúa, México, 2006, pp.39

cuanto al contenido suscrito y se adhiere al mismo por medio de la firma.[7] Es así como la firma constituye el lazo entre el firmante y el documento en el cual es estampada[8].

Dicha función de autenticación no se pierde con el empleo de la firma electrónica al contrario se refuerza ya que la misma ofrece mecanismos que le permiten que dicha función sea verificada de una forma más generalizada y segura.

En cuanto al lazo que se crea para que el mismo se establezca no es necesario que la firma sea legible ni nominal, es decir no es necesario que la firma misma exprese el nombre del firmante. No es imprescindible la función identificativa de la firma a la que se ha hecho referencia en párrafos anteriores para que el nexo se cree. [9]

Esto debido a que el nexo que la firma crea no depende de la forma que la misma emplee para estamparse sino al hecho de firmar en sí, no es necesario como se estableció anteriormente que se empleen los métodos utilizados en las antigua culturas para establecer que se estaba firmando un documento ya que en la actualidad la modalidad es mucho más sencilla, sino emplear la modalidad tradicional es suficiente para que se ese nexo de consentimiento, identidad y autenticación se formen.

En los documentos notariales por ejemplo es en el inicio o encabezado de los mismos en donde se consigna el nombre completo de las partes intervinientes razón por la cual no importa si las firmas no son legibles. En el caso de la firma electrónica se da que la función identificativa de la firma es una exigencia de la

[7] idem
[8] Rodríguez Adrados, Antonio, LA FIRMA ELECTRÓNICA: comunicación discutida en sesión del pleno de académicos de número el día 5 de junio de 2000. Real Academia de Jurisprudencia y Legislación publicada en sus anales 2000.
[9] idem

contratación a distancia y no de los conceptos tradicionales de documento y firma[10]. Por otro lado, lo que sí es necesario es que la firma haya sido puesta en el documento por el firmante "en persona". Dicha idea suele expresarse como "manuscrita"[11] pero esto puede ampliarse a cualquier "grafia"[12] puesta en el documento por el mismo firmante, es decir a toda "autografía", de ahí el término de "firma autógrafa". Por lo tanto, si se puede ampliar a cualquier grafía la firma manuscrita puede ser sustituida por cualquier grafía, siempre y cuando sea obligadamente personal, como lo que ha ocurrido con la huella digital, no así por una grafía que pueda ser colocada por algún tercero o por procedimientos que permitan a terceros imponerla[13].

Al establecerse que la firma puede realizarse por cualquier grafía no se limita exclusivamente a una forma autógrafa por lo que se entiende que puede realizarse en la actualidad por medio de los mecanismos digitales que las recientes tecnologías ofrecen a nivel mundial, que no desvirtúan a la figura de la firma por sí misma.

Por consiguiente, la función primordial de la firma no será la identificativa sino la de ser el instrumento de su declaración de voluntad, por medio del cual se exige la actuación personal del firmante y declara que se trata de un documento original, en el cual el firmante declara y asume como propias las manifestaciones, declaraciones o acuerdos que el mismo contiene.[14]

---

[10] Artículo 2 de la Ley para el Reconocimiento de las comunicaciones y firmas electrónicas, Decreto 47-2008 del Congreso de la República.

[11] Escrita con la propia mano, del puño y letra del escribiente.

[12] Modo de escribir o representar los sonidos, y, en especial, empleo de tal letra o tal signo gráfico para representar un sonido dado.

[13] Reyes Krafft, Alfredo, LA FIRMA ELECTRÓNICA Y LAS ENTIDADES DE CERTIFICACIÓN, Editorial Porrúa, México, 2004, pp 56

[14] idem

Algunos autores, tales como Alfredo Reyes Krafft, consideran que "*la firma como exteriorización de la declaración de voluntad de una persona es imprescindible en los documentos comerciales, no es un mero requisito la cual precisa de una actuación personal del firmante, una actuación física, corporal del firmante mismo, porque solo así puede ser instrumento de su declaración de voluntad. En este sentido existe oposición con los seguidores de la firma electrónica, ya que se considera que si la firma es la exteriorización de la declaración de voluntad de una persona, esta exteriorización puede hacerse por otro medio, como pudiera ser el electrónico siempre que la haga el firmante o legalmente se atribuya a él. Se vuelve entonces a la función identificativa de la firma, pero ahora con el calificativo de electrónica, pues ésta sí requiere de identificación del autor para dar certeza de que es él y no un tercero quien declara su voluntad, de ahí el concepto de UNCITRAL*[15] *de "equivalente funcional de la firma*."[16]

Por lo tanto, se deduce entonces que en el caso de la firma electrónica no será exclusivamente la declaración de voluntad que la firma conlleva una característica primaria de la firma electrónica sino más bien lo será la función identificativa ya que se requiere que el autor de la misma sea plenamente identificado para dar la certeza de ser exclusivamente esa persona la que se compromete y no otra, es decir que sopesa la identificación del firmante antes de la declaración de voluntad del mismo.

I.2 Concepto

Diversos conceptos han surgido alrededor del tema de la firma electrónica. Existen tantos como legislaciones han surgido con el devenir de los años. En España, por ejemplo, en el Real Decreto – Ley 14/1999 de 17 de septiembre de

[15] Siglas en inglés de la Comisión de las Naciones Unidas para el Derecho Mercantil (CNUDMI)
[16] Reyes Krafft, Alfredo, LA FIRMA ELECTRÓNICA Y LAS ENTIDADES DE CERTIFICACIÓN, Editorial Porrúa, México, 2004

1999, derogado por la Ley de 19 de diciembre de 2003 en su artículo 3º. se define a la firma electrónica como el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante. Firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

En Chile, la ley 19.799 del 25 de marzo de 2002, en su artículo 2º. literal f), define la firma electrónica como: cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un comunicación electrónica identificar al menos formalmente a su autor; y en la literal g) define a la firma electrónica avanzada como aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.

Colombia, según la ley 527 de 18 de agosto de 1999, en su artículo 2º. literal c), define a la firma electrónica como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

En Guatemala se define a la firma electrónica en su Ley para el Reconocimiento de las Comunicaciones Electrónicas, Decreto Número 47-2008 del Congreso de la República, "*artículo 2 Definiciones. Para los efectos de la presente ley se entenderá por: …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..."

Tomando elementos de las anteriores definiciones proporcionadas por las distintas legislaciones vigentes, se puede definir a la firma electrónica como: "*un conjunto de datos adjuntos o asociados a un mensaje y utilizados como medio para identificar al autor y garantizar la integridad de los documentos digitales. Entonces, es el resultado de obtener un patrón que se asocie biunívocamente a un individuo y su voluntad de firmar, utilizando determinados mecanismos, técnicas o dispositivos electrónicos que garanticen que después no pueda negar su autoría*."[17]

Se convierte así en un conjunto de datos electrónicos que identifican a una persona en concreto que suelen unirse al documento que se envía por medio telemático, como si de la firma tradicional y manuscrita se tratara, de esta forma el receptor del mensaje está seguro de quién ha sido el emisor, así como que el mensaje no ha sido alterado o modificado.[18]

En conclusión en la legislación guatemalteca se contemplaron los aspectos mencionados anteriormente al respecto de las funciones de la firma electrónica ya que se menciona primero que la misma identifica al firmante y en segundo

[17] Banco Interamericano de Desarrollo, FIRMA ELECTRÓNICA DIGITAL Y CONTRATOS ELECTRÓNICA, Documento conceptual para la legislación en la era de la información, iniciativa Glin Américas, Noviembre 2005, pp 67,68

[18] Carrión, Hugo Daniel, ANÁLISIS COMPARATIVO DE LA LEGISLACION Y PROYECTOS A NIVEL MUNDIAL SOBRE FIRMAS Y CERTIFICADOS DIGITALES, http://www.mbc.com/legis/cu-digsig-dir.html.

lugar que por medio de la misma se aprueba la información contenida en el mensaje de datos, dos funciones primordiales de la firma electrónica que son contempladas en sentido estricto en el texto de la Ley para el Reconocimiento de las Comunicaciones y Firma Electrónica. Elementos que pueden encontrarse también en la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, norma internacional que sirvió de base para la creación de la legislación guatemalteca en relación a la firma electrónica.

I.2.1 Características

De la definición sobre firma electrónica pueden deducirse las características siguientes:

Identificativa: Jurídicamente es necesario establecer el reconocimiento de la persona que suscribe un documento. Por medio de la firma electrónica esto se logra a través del conjunto de datos adjuntos o asociados a un mensaje los cuales son utilizados como medio para identificar al autor del documento.

Puede darse al mismo tiempo dos modalidades de identificación: la identificación de origen de datos, por medio de la cual el identificado está relacionado con ciertos datos los cuales le son propios y al mismo tiempo lo vinculan al mensaje que ha enviado. Y la identificación de entidades, la cual consiste en el método por medio del cual la identificación resulta de una comparación entre los datos que han sido enviados y los datos que han sido almacenados por haber sido enviados anteriormente. Esta autenticación de la identidad se puede dar por diversos métodos dentro de los que se encuentran las pruebas de conocimiento, la solicitud de claves, la autenticación biométrica, entre otras.[19]

Es de especial importancia la función identificativa de la firma electrónica sobre todo para la formación de contratos a través de medios electrónicos que es

[19] Flores Bacca, Glenn, Características de la Firma Electrónica Avanzada, México, www.notarios.com.mx, consultado: 20 de julio de 2010.-

precisamente lo que ha contemplado la Ley para el reconocimiento de las comunicaciones y firmas electrónicas (en adelante la Ley) de Guatemala en su capítulo III, en el cual describe todo lo relacionado a la forma en que se identificará quién es el iniciador de una comunicación electrónica y quién será considerado como el receptor de la misma es decir la función identificativa característica descrita anteriormente de la firma electrónica. Por ejemplo, de conformidad con la Ley una comunicación electrónica proviene del iniciador si ha sido enviada por el propio iniciador, o por alguna persona facultada por el mismo para hacerlo o por un sistema programado para hacerlo automáticamente.

Declarativa: Identifican biunívocamente[20] a un individuo y su voluntad de firmar. Establece la voluntad de obligarse o de aceptar el contenido del documento por parte del firmante.

En el artículo 33 de la Ley guatemalteca se establece en su tercer párrafo que 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. De esta forma se reconoce en Guatemala esta característica de la firma electrónica.

Probatoria: La firma permite identificar por diversos mecanismos electrónicos si el autor de la firma es el que ha sido identificado como tal en el acto de la firma.

Seguridad: Otorga certeza jurídica en cuanto a que los documentos recibidos digitalmente se recibirán de la misma forma íntegra como cuando fueron enviados.

En relación a esta última característica el comercio electrónico se enfrenta actualmente a la búsqueda de una mayor seguridad jurídica en las relaciones contractuales a nivel nacional e internacional. En esta esfera la firma electrónica

[20] Que tiene doblemente igual naturaleza o valor que otra cosa.

aparece como un mecanismo que proporciona las características necesarias para brindar esa certeza jurídica a dichas relaciones, lo cual se lleva a cabo a través de sistemas criptográficos en los mensajes de datos que, para Correa González, se pueden clasificar se la siguiente manera:

a) Confiabilidad: éste es un elemento derivado de la seguridad que se deposita en la otra persona que envía el mensaje y cuyo principal objetivo radica en que dicho mensaje sólo pueda ser leído por su destinatario o por las personas autorizadas o con derecho a dicha información.

b) Integridad: el sistema de claves, tanto públicas como privadas, garantiza que el mensaje no pueda ser alterado en el transcurso de su envío y posterior recepción y que, por lo tanto, sea recibido íntegramente.

c) Autenticidad: se refiere la certeza jurídica sobre la legitimidad del mensaje.

d) No repudio: que el remitente no pueda negar el mensaje de datos que ha enviado.[21] Así como que el receptor del mensaje no pueda negar que ha recibido el mensaje, es decir no repudio de origen y de recepción.

Es de especial importancia la existencia de entidades certificadoras de firma electrónica que se conviertan en los entes fiscalizadores de la seguridad con la que sean empleados los distintos mecanismos de autenticación de los mensajes enviados por la vía electrónica. Su intervención garantiza la asociación entre un par de claves y una persona determinada así como la distribución efectiva de las claves que vinculen a una persona con la clave pública, que identifique al titular de la clave privada. El certificado, expedido por el prestador de servicios de

[21] Correa González, Felipe, INTRODUCCIÓN A LA LEY No. 19.799 DE FIRMA ELECTRÓNICA Y SERVICIOS DE CERTIFICACION No. 069-abril de 2004, Revista electrónica de Derecho Informático, http://www.alfaredi.org/rdi-articulo.shtml, fecha de consulta: 15 de diciembre de 2009.

certificación, podrá garantizar frente a terceros la integridad y el origen del mismo.[22]

I.2.2 Clases de firma electrónica

La firma electrónica va desde su forma más simple como puede ser el mecanismo por medio del cual se puede identificar al autor de un documento, hasta formas más complejas como la firma electrónica avanzada que utiliza un sistema de criptografía asimétrica por medio de la cual tanto la firma como el documento se encuentran formados por una serie de números que no es posible reconocer si no es con la clave correcta que permita desencriptar el mensaje, aunándole a esto el factor de la certificación por medio de la cual se convierte en una firma mucho más segura que no puede ser repudiada con facilidad.[23]

Dentro de este esquema Felipe Correa González clasifica a la firma electrónica de la siguiente manera:[24]

a) Firma electrónica alegal. La firma electrónica, en su forma más básica, constituye un mecanismo de seguridad jurídica mínimo, a la par que respeta la economía de la transacción.

b) Firma electrónica legal. Representada técnicamente por formas más complejas de firma, combinada con otros elementos, como requisitos de operación de dispositivos seguros, evaluaciones de conformidad, etc. Constituyen mecanismos de elevada seguridad jurídica, si bien supone mayores costes por transacción.

---

[22] idem

[23] Correa González, Felipe, INTRODUCCIÓN A LA LEY No. 19.799 DE FIRMA ELECTRÓNICA Y SERVICIOS DE CERTIFICACION No. 069-abril de 2004, Revista electrónica de Derecho Informático, http://www.alfaredi.org/rdi-articulo.shtml, fecha de consulta: 15 de diciembre de 2009.

[24] Idem

c) Firma electrónica legitimada. Las firmas y los requisitos de los documentos, puestos en combinación con determinados procedimientos y actuación de determinados profesionales, suponen mecanismos de muy elevada seguridad jurídica, pero la interacción de estos grupos de requisitos (requisitos, firmas y procedimientos) suponen un costo que únicamente se justifica a la luz de la realización de transacciones de costo ciertamente elevado.

d) Firma electrónica simple o avanzada. En su forma, simple o avanzada, la firma electrónica constituye uno o varios mecanismos de seguridad jurídica básica y, por lo tanto, con impacto en el costo por transacción.

La forma en que la mayoría de las legislaciones clasifican a la firma electrónica, incluyendo la legislación guatemalteca, es en esta última forma de clasificación: firma electrónica simple y firma electrónica avanzada. Si bien se diferencian en los requisitos que deben cumplir las entidades que las certifiquen y en cuanto al valor probatorio de cada una de ellas, ambas responden al principio antes descrito de la equivalencia de soportes.

En el caso de la firma simple se puede tomar como ejemplo el envío de un e-mail donde se manifiesta la intención de comprar un producto y se señala la firma con el nombre de pila. En este caso el receptor del e-mail puede identificar quién fue quien lo envió, pero lo que no puede hacer es autenticar que el mail fue enviado por la persona cuyo nombre aparece escrito al pie del documento, inclusive puede verificar si fue desde una determinada computadora, pero no puede estar completamente seguro de quien lo haya enviado. Cuestión que en el caso de la firma electrónica avanzada sí es posible verificar, ya que esta modalidad de forma utiliza medios que el titular mantiene bajo su exclusivo control, y que impiden que el documento pueda ser alterado con posterioridad a su envío. Garantizándose de esta forma la integridad, identidad y no repudio del documento enviado. Además esta modalidad de firma electrónica requiere necesariamente que haya sido certificada por una entidad certificadora de firma

electrónica a través de un certificado entregado al usuario con lo se garantiza una mayor seguridad y certeza jurídica.

Según lo expuesto, la firma electrónica propiamente tal o no avanzada, puede o no cumplir con los parámetros de seguridad que se exigen para la avanzada.

Para garantizar la seguridad de los puntos indicados, la Ley para el reconocimiento de las comunicaciones y firmas electrónicas exige que la firma electrónica avanzada sea certificada por un prestador *acreditado*, esto es aquel que ha sido certificado y autorizado por el Registro de Prestadores de Servicios de Certificación del Ministerio de Economía que cuenta con las instalaciones, sistemas, programas informáticos y recursos humanos necesarios para otorgar certificados en los términos establecidos en la Ley (Artículo 33 Decreto 47-2008).

De esta forma, y de conformidad con los requisitos de los certificados, la firma electrónica avanzada cuenta con un sistema de claves asimétricas o sistema de criptografía asimétrica. Dicho sistema cuenta con un par de claves, una pública y otra privada, las cuales son otorgadas por las empresas que prestan el servicio de certificación y las otras, que son creadas por el mismo usuario siguiendo las instrucciones del prestador. De esta forma el prestador no tiene acceso en ningún momento a la clave privada del usuario; convirtiéndose esto en una herramienta que posee el usuario bajo su exclusivo control.

De conformidad con el artículo 33 del Decreto 47-2008 del Congreso de la República tanto la firma electrónica como 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. Por otro lado el artículo 11 de la mencionada Ley establece que serán admisibles como medios de prueba las comunicaciones electrónicas, que para los efectos de la ley son los mensajes de datos que consisten en todo documento o información generada, enviada, recibida o archivada por medios electrónicos, magnéticos, ópticos o similares, el correo electrónico, el telegrama, el télex o el telefax, con esto se establece que no necesariamente deben ir firmados sino simplemente por el hecho de ser una comunicación electrónica puede gozar de fuerza probatoria, esto constituye una inconsistencia de la ley ya que el valor probatorio sobre todo lo posee la firma electrónica avanzada por la seguridad que la misma presenta al ser certificada por una entidad prestadora del servicio de certificación que es lo que establece el artículo 33 que no es lo mismo que quiere decir el artículo 11 del mismo cuerpo legal.

El sistema ha sido descrito correctamente por Pinochet Olave de la siguiente forma: *"Una de esas claves es privada y sólo podrá ser utilizada por el titular de la firma. Dicha clave podrá estar en un ordenador o en una tarjeta electrónica y para acceder a ella el usuario deberá digitar una clave secreta u otro mecanismo más avanzado de seguridad, en ese momento podrá aplicar su firma digital al comunicación electrónica que quiera firmar digitalmente. Al aplicar la firma digital sobre un documento, ésta se mezcla o confunde con los datos que son enviados a través de un proceso de encriptación de la información. Al llegar el mensaje a su destino el mensaje se desencripta con la clave pública que se asocia a la clave privada de su autor. La clave pública podrá ser accesible por cualquier persona incluso en bancos de datos que serán consultados vía Internet. Sólo utilizando la clave pública asociada a una persona determinada será posible desencriptar una comunicación electrónica que haya sido firmada con la clave*

privada de su autor. Esto quiere decir que ambas claves se encuentran asociadas"[25]

Así, la comunicación electrónica encriptada con la clave privada de su autor puede ser desencriptado sólo con la clave pública de éste. Cualquier persona puede acceder a dicha clave pública y por lo mismo desencriptar el documento, proceso que puede verificarse incluso de manera automática. Si lo que se busca es que el documento sea abierto sólo por el destinatario, dicha comunicación electrónica deberá ser encriptada no sólo con la clave privada del autor, sino que también con la clave pública del destinatario. De esta forma el destinatario de la comunicación electrónica, una vez que lo recibe, para poder abrirlo deberá emplear la clave pública del autor y la clave privada del destinatario. Con este procedimiento se asegura además la confidencialidad del instrumento electrónico[26].

Dentro del proceso de la firma de la comunicación electrónica es necesario cumplir con el paso del hash o resúmen debido a que en la actualidad aún dicho procedimiento es lento. La función hash consiste en una versión comprimida del documento que facilita la comprobación de la firma electrónica. El usuario de la firma electrónica debe obtener el resumen de dicho documento para poder aplicar la clave privada sobre el mismo y enviar a la otra parte el mensaje, la firma electrónica y el certificado de dicha firma. Por medio de estos elementos el receptor podrá entonces comprobar la autoría e integridad del mensaje.

En general el proceso es automático y resulta transparente para las partes, ya que es llevado a cabo por programas electrónicos especialmente diseñados al efecto y los usuarios simplemente ven una interface más o menos amigable que,

[25] Pinochet Rupero, Contratos electrónicos y defensa del consumidor, Marcial Pons, Ediciones Jurídicas y Sociales, S.A., Madrid, 2001. pp. 87
[26] Idem

normalmente a través de íconos, y previa solicitud de un password de seguridad, permite firmar un documento al suscriptor y verificar la firma al receptor.

Contratación entre ausentes

Es importante señalar al respecto la teoría relacionada a la contratación entre ausentes. Por regla general la firma electrónica es un contrato realizado entre dos personas a distancia, la misma puede ser geográfica o simplemente física.

Desde hace ya varios años se ha venido dando la propuesta o aceptación de contratos por la vía telefónica, en donde se considera separadamente el momento y el lugar de la celebración. En el caso de este tipo de contratación la comunicación es instantánea es decir las personas se encuentran comunicándose al mismo tiempo, razón por la cual se considera que dicho contrato es celebrado entre presentes, pero, como los mismos no se encuentran ubicados en el mismo lugar geográfico al momento de la celebración del contrato el mismo se regirá por las normas relativas a los contratos entre ausentes, ya que los mismos se encuentran físicamente distantes el uno del otro.

En el caso de la contratación vía telefónica, la comunicación se realiza, como se mencionó anteriormente, de forma instantánea, lo que no sucede necesariamente en el caso de los contratos celebrados por la vía electrónica.

En el contrato electrónico las relaciones son más complejas y diversas, por lo que se debe distinguir:

1) cuando un contrato es celebrado entre presentes y ausentes

2) criterios de distribución del riesgo entre ausentes

3) la aplicación de estos criterios en los contratos electrónicos.

Lorenzetti señala cuatro criterios[27]:

Presencia física de los contratantes: al no encontrarse las personas físicamente presentes la aceptación para la celebración del contrato no se realiza en un mismo acto, se requiere de un tiempo para que una de las partes acepte y la otra reciba la comunicación de dicha aceptación para que el contrato se considere perfeccionado, razón por la cual este contrato se regirá por las normas de la contratación a distancia similares a las normas que rigen las cartas.

La celebración instantánea o discontinua: Puede darse la situación en la que las personas se encuentran físicamente distantes pero la comunicación es instantánea, en ese caso el vínculo entre los mismos se considera que es entre presentes. En el caso de que dichas personas se encuentren en diferentes países el vínculo entre los mismos es entre ausentes aplicando las normas del derecho internacional privado.

En el caso de la contratación electrónica cuando las personas se encuentran distantes pero con una comunicación instantánea, por los diversos medios electrónicos existentes en la actualidad, el vínculo de los mismos será considerado como una celebración entre presentes.

La distribución de riesgos: Existen distintas situaciones que pueden darse en la contratación entre ausentes durante el tiempo que transcurre entre la oferta y la aceptación, estas situaciones son consideradas como riesgos, tales como la muerte, incapacidad, quiebra o retractación. Es necesario pactar sobre quien recae la responsabilidad de cubrir dichos riesgos en cada uno de los casos o establecerlo de conformidad como lo tiene contemplado la ley para cada caso particular.

El tiempo y el espacio como conceptos normativos: la importancia de establecer la presencia o ausencia física entre los contratantes radica en que

[27] Lorenzzeti, Ricardo, Tratado de los contratos, Tomo III, Editorial Lex, Argentina, 2008, pp.105

dependiendo del vínculo que se cree entre los mismos dependerá sobre quien recaerá la obligación de cubrir los riesgos que puedan ocurrir. En el caso de la contratación electrónica puede ocurrir que el lugar de contratación puede ser un lugar variable como una computadora dentro de un avión en movimiento. En este caso no puede determinarse exactamente el lugar en donde se realizó la oferta o la aceptación pero sí el dominio desde el cual trabajó esa computadora, razón por la cual el tiempo y espacio real son conceptos de base empírica que no pueden coincidir con el tiempo y el espacio jurídicos.

Guatemala regula en el Código Civil Decreto Ley 106 normas que han venido a ser complementadas por la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas Decreto 47-2008 del Congreso de la República tales como lo son las siguientes: el artículo 1521[28] del Código Civil, se complementa con el artículo 25 de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas Decreto 47-2008 del Congreso de la República la cual establece que: "*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 generada accesiblemente 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".*

En el caso del segundo párrafo del artículo 1521 del Código Civil que establece que en el caso de no haberse fijado plazo quien propone la oferta no se obliga a menos que la aceptación sea inmediata, el artículo 15 del Decreto 47-2008 establece que: "*En la formación de un contrato por particulares o entidades*

[28] Art. 521. La persona que propone a otra la celebración de un contrato fijándole un plazo para aceptar, queda ligada por su oferta hasta la expiración del plazo.
Si no se ha fijado plazo, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente.

públicas, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de una comunicación electrónica…"

El artículo 1523[29] del Código Civil que se refiere a la formación del contrato cuando la oferta ha sido hecha entre ausentes; el Decreto 47-2008 establece en su artículo 24 que: "*De no convenir otra cosa por el iniciador y el destinatario, la comunicación electrónica se tendrá por: (…) 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".*

Por lo tanto, como se puede observar la contratación entre ausentes en el Código Civil de Guatemala se encuentra regulada en los artículos 1521 a 1528. En el caso de la oferta de un contrato la misma puede hacerse a una persona que se encuentre presente o ausente, con o sin un plazo establecido para su aceptación. En el caso de que se fije plazo se queda obligado a la espera de la contestación hasta que el plazo llegue a su final; por otro lado, en el supuesto de que no se fija plazo y la persona está presente, el proponente puede retirar la oferta realizada si la contestación no es inmediata. Pero si la persona está ausente el proponente deberá esperar un tiempo para recibir la contestación, siempre y cuando se apegue a lo mismo ofertado ya que de haber modificaciones en el mismo se trataría de una contraoferta.

[29] Artículo 1523. Cuando la oferta se haga a persona ausente, el contrato se forma en el momento en que el proponente recibe la contestación de aquélla dentro del plazo de la oferta.
Si la oferta se hiciere sin fijación de plazo, el autor de ella quedará ligado durante el tiempo suficiente para que la contestación llegue a su conocimiento.

De los sistemas sobre cuando queda perfeccionado un contrato entre ausentes: el de la declaración, el de la expedición, el de la recepción y el de la información, Guatemala, en el artículo 1523 del Código Civil, demuestra acercarse al sistema de la aceptación, que de conformidad con Rojina Villegas consiste en lo siguiente: "*Se considera en este sistema (el de la aceptación) que no basta que el aceptante deposite en el correo su contestación, porque el oferente no sabe si existe o no aceptación alguna, ya que pueden existir causas ajenas a la voluntad de las partes que impiden llegar la contestación al oferente. Puede extraviarse, por ejemplo, la carta, o sufrir una demora por un trastorno en las comunicaciones, y sería entonces injusto ligar al oferente desde el momento de la expedición de la carta, si esta, por causas ajenas a su voluntad, no llega a su poder e ignora durante algún tiempo que se encuentra ya obligado a sostener ciertos precios o condiciones desde determinado momento que es el de la expedición, que desconoce en absoluto.*"[30]

De conformidad con la teoría de la recepción la única forma de que quede perfeccionado el contrato es, por lo tanto, que el oferente se encuentre en condiciones materiales de conocer la respuesta dada lo que podrá darse al recibir la contestación. No es necesario que la conozca sino que basta con que la reciba, aunque se encuentre ausente.

De conformidad con la mencionada teoría, los artículos 1525, 1527 y 1528 del mencionado Código Civil, establecen que si por alguna razón la aceptación es recibida por el proponente una vez vencido el plazo, deberá hacérselo saber al aceptante ya que éste último puede tener la creencia se haber celebrado ya el contrato, ignorando que su respuesta llegó tardía. Ya que la aceptación se considera que no existe si con ella o antes de la misma el oferente recibe la retractación del aceptante. Y tampoco es válida la oferta en el supuesto de que

[30] Villegas, Rojina, Derecho Civil Tomo V, Volumen I, México 1951, pag. 316

quien la ha propuesto fallece o pierde su capacidad de contratar antes de recibir la aceptación o si esto sucediera antes de que el aceptante haya aceptado.[31]

En conclusión la Ley para el reconocimiento de las comunicaciones y firmas electrónicas Decreto Número 47-2008 establece en su artículo primero que establece lo relativo al ámbito de aplicación de dicha ley que las disposiciones contenidas en la misma se aplicarán sin perjuicio de las normas relativas a la celebración, formalización, validez y 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. Por lo tanto, con dicha normativa se regula que las normas contenidas en el Decreto 47-2008 vienen a complementar las normas relativas a la contratación entre ausentes en este caso del código civil Decreto Ley 106, ya que regulan lo relativo a dicha contratación vía electrónica mientras que el código civil se limita a las llamadas telefónicas, cartas, telegramas, etc. viene a ampliar dicho tipo de contratación por medio de la tecnología actual.

Con relación a la teoría a seguir por el Decreto 47-2008 sigue la misma teoría que el código civil, es decir, la teoría de la aceptación, ya que no se trata de una norma ajena a las normas civiles, sino que las complementa y en su artículo 23 establece que sus normas se refieren al envío y recepción de las comunicaciones electrónicas, con relación a las consecuencias jurídicas de dichas comunicaciones electrónicas se regirán conforme a las normas aplicables al acto o negocio jurídico contenido en dicho mensaje de datos; siendo así que si

[31] Articulo 1525. Si por alguna circunstancia la aceptación llegare tardíamente a conocimiento del oferente, éste lo cumunicará sin dilación al aceptante, bajo pena de responder por los daños y perjuicios.
Art. 1527. Se considera inexistente la aceptación, si antes de ella o junto con ella, llegare a conocimiento del oferente la retractación del aceptante.
Art. 1528. No tendrá efecto la oferta si el proponente falleciere o perdiere su capacidad para contratar, antes de haber recibido la aceptación; o si falleciere o perdiere su capacidad la otra parte antes de haber aceptado.

se trata de un contrato regido por las normas del código civil, por ejemplo, se regirá por dichas normas, aceptando así la teoría que el mismo sigue.

I.2.3 El encriptamiento

La informática ocupa en la actualidad un papel preponderante al ser uno de los medios más utilizados a nivel mundial para la comunicación tanto a nivel personal como empresarial. Esto ha traído consigo un incremento de peligros para la información que circula en la red y se almacena en los sistemas informáticos, por lo que se ha visto la necesidad de crear sistemas que doten de certeza jurídica a las relaciones surgidas por dichos medios electrónicos.

Dentro de las posibles soluciones plantadas por las distintas legislaciones en atención a la cuestión de la seguridad electrónica se encuentra la encriptación. Básicamente podría definirse como el "*proceso para volver ilegible información considerada importante. La información una vez encriptada sólo puede leerse aplicándole una clave.*"[32]

"El origen de la criptografía data del año 2000 A.C., con los egipcios y sus jeroglíficos. Los jeroglíficos estaban compuestos de pictogramas complejos, donde sólo el significado completo podría ser interpretado por algunos. El primer indicio de criptografía moderna fue usado por Julio César (100 A.C. a 44 A.C.) quien no confiaba en sus mensajeros cuando se comunicaban con los gobernadores y oficiales. Por esta razón, creó un sistema en donde los caracteres eran reemplazados por el tercer carácter siguiente del alfabeto romano. No solo los romanos, sino los árabes y los vikingos hicieron uso de sistemas de cifrado.

Gabriel de Lavinde hizo de la criptografía una ciencia más formal cuando publicó su primer manual sobre criptografía en 1379. Samuel Morse con su código

[32] Lorenzzeti, Ricardo, Tratado de los contratos, Tomo III, Editorial Lex, Argentina, 2008, pp.106

Morse creado en 1832, aunque no es propiamente un código como los otros, es una forma de cifrar las letras del alfabeto dentro de sonidos largos y cortos".[33]

Esta medida de seguridad, empleada en los medios electrónicos, se encuentra compuesta por una serie de fórmulas matemáticas empleadas para encriptar o desencriptar los mensajes por medio de una serie de claves asociadas a un sujeto, una pública que es conocida por todos los sujetos que intervienen en la situación y una privada sólo conocida por el sujeto que desea encriptar el mensaje. De esta forma se asegura que las complejas fórmulas matemáticas (algoritmo) que componen el criptograma, es decir, el mensaje cifrado no pueda ser conocido por cualquier persona que no posea la clave privada. Esta medida es empleada para almacenar o transferir información confidencial, como puede ser el caso de contraseñas, números de tarjetas de crédito, conversaciones privadas entre otros muchos usos comerciales que pueda dársele.[34]

De esta forma cuando se desea establecer una comunicación segura con otra parte basta con encriptar el mensaje con la clave pública del sujeto para que a su recepción sólo el sujeto que posee la clave privada pueda leerlo.[35]

Algoritmo

"Un algoritmo en general es la serie de reglas que no pueden ser ambigüas y deben tener una meta clara. Los algoritmos pueden ser expresados en cualquier lenguaje, desde el inglés al francés, hasta lenguajes de programación de computadoras.

Los algoritmos criptográficos son la base de construir aplicaciones y protocolos de encriptación"[36].

[33] Reyes Krafft, Alfredo Alejandro, LA FIRMA ELECTRÓNICA Y LAS ENTIDADES DE CERTIFICACIÓN, Editorial Porrúa, México 2003.
[34] Curvo, José, LA FIRMA DIGITAL Y ENTIDADES DE CERTIFICACION, http://www.alfaredi.org/rdi-articulo.shtml fecha de consulta: 11 de septiembre de 2008.
[35] idem

Algoritmo de encriptación simétrico

El algoritmo de encriptación simétrico es aquel formado por un clave que encripta el mensaje, la cual puede ser calculada desde la clave para desencriptar, ya que en muchos de los algoritmos simétricos la misma clave se utiliza tanto para encriptar como para desencriptar el mensaje, para lo cual es necesario que tanto el emisor como el receptor cuenten con la misma clave antes de comunicarse. Por lo tanto la seguridad de este tipo de algoritmos se encuentran realmente en la clave a utilizar, la cual se debe conservar en secreto el tiempo que la comunicación misma deba permanecer en secreto. [37]

Algoritmo de encriptación asimétrico

Por otro lado, los algoritmos asimétricos, a diferencia de los anteriores, están diseñados para contar con una clave para encriptar el mensaje y una diferente para desencriptarlo. Son comúnmente llamados algoritmos de "clave pública" ya que la clave para encriptar puede publicarse al no ser la misma que para desencriptar, esta clave es conocida como clave privada y sólo la persona que desee desencriptar el mensaje la podrá conocer.[38]

Los propósitos de la encriptación son: mantener en secreto las comunicaciones que se desee. Por medio de la misma sólo las personas que intervienen en la relación y cuentan con sus claves podrán comunicarse a través de encriptar y desencriptar los mensajes.

---

[36] Reyes Krafft, Alfredo Alejandro, LA FIRMA ELECTRÓNICA, http://www.razonypalabra.org.mx/libros/libros/firma.pdf, fecha de consulta: 10 de enero de 2010.-

[37] Carrión, Hugo Daniel, ANÁLISIS COMPARATIVO DE LA LEGISLACION Y PROYECTOS A NIVEL MUNDIAL SOBRE FIRMAS Y CERTIFICADOS DIGITALES, http://www.mbc.com/legis/cu-digsig-dir.html.

[38] idem

Firmas digitales

En el proceso de firma electrónica se da necesariamente la función de la encriptación a través de algoritmos de clave pública con información secreta para firmar documentos e información pública para verificar las firmas.

Hashing y Digest

El algoritmo hashing consiste en una función matemática por medio de la cual se consigue una huella digital de los datos, es decir, es una manera de verificar si un archivo pertenece a una persona por medio de un algoritmo que lo convierte de una cadena de longitud variable a una cadena de longitud fija. Se utiliza sobre todo en las transacciones financieras, ya que esto genera un valor del mensaje.

El digest es la representación del texto en forma de una cadena de dígitos, creado con una fórmula de hashing de una sola dirección. El encriptar un digest de un mensaje con una clave privada, genera una firma digital.[39]

Los algoritmos criptográficos más importantes usados hoy en día para la seguridad son: [40]

a) **RSA**[41]

Propósito: Encriptación y Firma Digital
Rango de clave: 1024 bits para uso corporativo y 2048 para claves valuables.
Fecha de creación: 1977

[39] Loc. Cit. Pág. 18
[40] Reyes Krafft, Alfredo, La firma electrónica y las entidades de certificación, Editorial Porrúa, México 2004, pp. 90
[41] RSA es un sistema de encriptación y autenticación que usa un algoritmo desarrollado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman.

b) DSA[42]

Propósito: Firmas Digitales

Rango de clave: 56 bits

Fecha de creación: 1994

c) Diffie-Hellman (DH)[43]

Propósito: Firmas Digitales

Rango de clave: 1536 bits

Fecha de creación: 1976

d) DES[44]

Propósito: Encriptación

Rango de clave: 56 bits

Fecha de creación: 1976

Otros algoritmos de encriptación:[45]

---

[42] El Digital Signature Algorithm (DSA) fue publicado por el Instituto Nacional de Tecnología y Estándares (NITS) en el estándar llamado Digital Signature Standard (DSS) que es parte del gobierno de los Estados Unidos. DSS fue seleccionado por el NIST con ayuda del NSA (National Security Agency) para ser el estándar de autenticación digital del gobierno de los Estados Unidos a partir del 19 de mayo de 1994.
DSA está basado en el problema de logaritmos discretos y se deriva de sistemas criptográficos propuestos por Schnorr y ElGamal. Es únicamente para autenticación.

[43] Este fue el primer algoritmo de clave pública inventado. Tiene su seguridad en la dificultad de calcular logaritmos infinitamente. DH se usa principalmente para distribución de claves. Es usado para generar claves secretas, mas no se usa para encriptar ni desencriptar.

[44] El Data Encryption Standard (DES) conocido también como el Algoritmo de Encriptación de Datos (DEA) ha sido un estándar por más de 20 años. Aunque muestra signos de que tiene mucho tiempo, se ha desempeñado muy bien a través de años de criptoanálisis y es aún seguro contra los adversarios.
DES es un bloque cifrado, encriptando los datos en bloques de 64 bits. DES es un algoritmo simétrico, el mismo algoritmo se usa para encriptar y desencriptar.
La clave tiene un tamaño de 56 bits, la clave usa un número de 56 bits y puede ser cambiado a cualquier hora. La seguridad recae directamente en la clave.

[45] Loc cit pág. 27

a) **3DES ya se está implementando el AES (Advance Encryptation Standard)**
b) **RC2**
c) **RC4**
d) **RC5**
e) **ECC (Criptografía de Curva Elíptica)**
   Entre otros.

Según el documento de la ISO (International Standard Organization) que describe el modelo de referencia OSI, presenta en su parte 2 una Arquitectura de seguridad. ("Information Processing Sistems. OSI Reference model- Part 2: Security Architecture". ISO/IEC IS 7498-2, Jul. 1988). Según esta arquitectura de seguridad para proteger las comunicaciones de los usuarios en las redes, es necesario dotar a las mismas de los siguientes servicios de seguridad:[46]

- Autenticación de entidad.

- Control de acceso.

- Confidencialidad de los datos.

- No repudio.

Para proporcionar estos servicios de seguridad es necesario incorporar en los niveles apropiados del modelo de referencia OSI los siguientes mecanismos de seguridad:

- **Cifrado.** Utilizando sistemas criptográficos simétricos o asimétricos.

- **Control de acceso**. Mecanismo que se utiliza para autenticar las capacidades de una entidad, con el fin de asegurar los derechos de acceso a recursos que posee.

[46] International Standard Organization, Information Processing Sistems, Reference model- Part 2: Security Architecture, Julio 1988

- **Firma digital.**

I.2.4 La firma electrónica de clave asimétrica

La firma electrónica de clave asimétrica está formada por un clave privada por parte del firmante y una clave pública por parte del emisor. El firmante aplica la clave privada a una versión comprimida del texto a firmar, para verificar la firma el receptor descifra la firma con la clave pública del emisor, luego comprime el texto original recibiendo con igual función que el emisor y compara el resultado de la parte descifrada con la parte comprimida, al darse la coincidencia de ambas el emisor podrá estar seguro de que el texto se encuentra íntegro[47].

Puede darse el caso de que una tercera parte en la relación, a modo de engañar al emisor, le entregue una clave pública que será la que le permita recibir al tercero la información para que cuando llegue al receptor llegue modificada. Esta debilidad de la firma electrónica asimétrica puede contrarrestarse con una clave pública otorgada por un intermediario cuya clave pública es conocida por todos los interesados y en el cual todos confían; así cuando alguien necesita una clave pública se la solicita a este intermediario, el cual será conocido como Autoridades de Certificación[48].

I.2.5 Efectos del encriptamiento

Como se ha mencionado anteriormente el encriptamiento consiste básicamente en el proceso por medio del cual se vuelve ilegible información considerada importante, utilizando para ello mecanismos de seguridad electrónicos, tales como un algoritmo y una clave. La utilización de este tipo de instrumento trae como consecuencia los efectos siguientes:

[47] Reyes Krafft, Alfredo, La firma electrónica y las entidades de certificación, Editorial Porrúa, México 2004. pp. 98
[48] idem

Se le otorga autenticidad a la identidad del otorgante del documento, debido a que las partes intervinientes en la relación (emisor y receptor) deben utilizar la misma clave para encriptar y desencriptar (encriptación simétrica) o en el segundo caso deben utilizar el concepto de pares de claves, es decir cada una de las partes pueden encriptar información que sólo la otra componente del par puede desencriptar. De esta forma se evita la intervención de terceros ajenos a la relación que pudieran interferir, modificar o falsear la información, ya que únicamente el emisor o el receptor cuentan con la clave para poder acceder al documento.

Asimismo **se establece un control de acceso**, por medio del cual se permite únicamente el acceso a la información a aquel que posea la clave necesaria para desencriptarla, evitando así que la información sea pública.

El otro efecto que trae consigo el encriptamiento es el de **la confidencialidad de los datos**, como consecuencia de los dos anteriores, en virtud que al dotar de autenticidad a la identidad del sujeto que emite o recibe el mensaje y por lo tanto establecer un control de acceso a dicha información se está creando un sistema de confidencialidad de los datos, que permite mantener la privacidad de los mensajes enviados y recibidos.

El conjunto de estos elementos hacen que ninguna de las dos partes de la relación puedan repudiar el contenido de la información, puesto que los elementos anteriores en conjunto otorgan una validez, integridad y seguridad jurídica a la comunicación que impide que la misma pueda ser alterada de ninguna forma, razón por la cual no podrá ser rechaza ni tachada de falsedad.

Este podría ser el efecto más importante de la encriptación, la imposibilidad de repudiar la información por la integridad con la que la misma es manejada en todo el proceso de envío y recepción.

I.2.6 Análisis de la Ley Modelo de la ONU para Firma Digital

En el año de 1996, en Asamblea General celebrada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, se creó la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional CNUDMI, la cual da pie a que surja la Ley Modelo sobre Comercio Electrónico aprobada por la Comisión en su 29°. período de sesiones celebrado en 1996[49], ambos esfuerzos con el fin de unificar el comercio internacional en materia de comercio electrónico.

La Ley Modelo sobre Comercio Electrónico contempló, dentro en su artículo 7, la opción de la firma electrónica en las operaciones de comercio electrónico como un equivalente funcional de la firma manuscrita. Dicho artículo no fue suficiente para regular todo lo concerniente a la firma electrónica, pues no determinaba todas las características, elementos, requisitos, derechos u obligaciones de la misma, razón por la cual se hizo necesario, que en el año 2001, surgiera una legislación que viniera a complementar todas las cuestiones que este artículo 7 había dejado escuetas. Se crea así, en el año 2001, la Ley Modelo sobre Firmas Electrónicas con el objetivo de que los distintos Estados con diferentes ordenamientos jurídicos, sociales y económicos puedan utilizar la firma electrónica de una manera generalizada, y que la misma contribuya al fomento de las relaciones económicas armoniosas en el plano internacional.[50]

La Ley Modelo de la CNUDMI sobre Firmas Electrónicas (en adelante la Ley Modelo) está compuesta de 12 artículos que tratan los siguientes temas:

Artículo 1 Ámbito de aplicación

Artículo 2 Definiciones

[49] Documentos oficiales de la Asamblea General, quincuagésimo primer período de sesiones, Suplemento núm. 17 (A/51/17), párr. 209

[50] Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para la incorporación al derecho interno, Naciones Unidas, Nueva York, 2001.

Artículo 3 Igualdad de tratamiento de las tecnologías para la firma

Artículo 4 Interpretación

Artículo 5 Modificación mediante acuerdo

Artículo 6 Cumplimiento del requisito de firma

Artículo 7 Cumplimiento de lo dispuesto en el artículo 6

Artículo 8 Proceder del firmante

Artículo 9 Proceder del prestador de servicios de certificación

Artículo 10 Fiabilidad

Artículo 11 Proceder de la parte que confía en el certificado

Artículo 12 Reconocimiento de certificados extranjeros y de firmas electrónicas extranjeras.

La Ley Modelo sobre Firmas Electrónicas fue creada por la Comisión de las Naciones Unidas para el Derecho Mercantil con el fin de que sirviera como una guía para que los Estados firmantes pudieran implementar esta normativa en su régimen jurídico interior.

La citada ley vino a complementar las dos funciones básicas que el artículo 7[51] contempla que son: la identificación del autor y la confirmación de que el autor

[51] El artículo 7 de la Ley Modelo de la CNUMDI sobre Comercio Electrónico establece lo siguiente:

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

aprueba el contenido del documento, con la aparición de esta normativa se le dio una seguridad al funcionamiento de estos criterios.

La Ley Modelo se basa en los siguientes principios básicos: la neutralidad respecto a los medios técnicos empleados, no discriminación entre las firmas electrónicas nacionales y las extranjeras, la autonomía de las partes y el origen internacional de la expresada ley, que tiene como objetivos la facilitación del comercio electrónico entre países, la validación de las operaciones concertadas mediante distintas tecnologías de comunicación, la promoción de nuevas tecnologías, la uniformidad del derecho y el apoyo a una práctica comercial mucho más ágil y segura.

De la lectura de los doce artículos que componen la Ley Modelo se infiere que la misma fue creada como una guía para la implementación de la firma electrónica en los países firmantes y creada con un fin comercial, es decir, el intercambio de bienes y servicios, la banca, seguros, etc., no se centra específicamente en las relaciones entre usuarios de firma electrónica y autoridades públicas, aunque tampoco deja la puerta cerrada para las mismas ya que tampoco se establece taxativamente que no sean aplicables a tales relaciones. Esta es una cuestión que en la Ley de Firma Electrónica de Guatemala sí se establece en su artículo primero que establece lo relativo al ámbito de aplicación, en el texto del artículo se contempló que la ley sería aplicable a todo tipo de comunicación electrónica, transacción o acto jurídico, privado o público, con lo que se da a entender que las relaciones entre usuarios y autoridades públicas sí son aplicables en la legislación guatemalteca; asimismo en el capítulo II del Reglamento de la Ley para el Reconocimiento de las Comunicaciones y Firma Electrónica se legisló lo relacionado al uso de las firmas electrónicas por los organismos del Estado. De

3. Lo dispuesto en el presente artículo será aplicable a: (…).

esta forma se vino a complementar las normas sugeridas por la Ley Modelo de la CNUDMI al aplicar la misma en el contexto nacional.

Por otro lado la Ley Modelo al referirse de la firma electrónica se limita únicamente a definir la misma como equivalente funcional a la firma manuscrita limitándose a las características de la firma de identificación del firmante y la intención de firmar como el mínimo común denominador con la firma manuscrita en general. Hace una diferenciación entre la firma en sí como instrumento para identificar a una persona y la firma electrónica como instrumento para emitir una aprobación sobre una información determinada; ambas funciones pueden llegar a confundirse ya que podría darse la situación en que se emplee la firma electrónica para expresar la aprobación por parte del firmante de la información firmada y pudiera utilizarse asimismo para realizar funciones de identificación que sólo asociaran el nombre del firmante a la transmisión del mensaje sin indicar la aprobación de su contenido.

En este caso la Ley Modelo sólo fue creada para que la firma electrónica expresara la aprobación de la información por parte del firmante; pero si dicha firma se crea antes de su utilización el consentimiento del firmante se debe evaluar en el momento en que se adjunte la firma al documento y no en el momento en que se cree la firma.

Por su parte la legislación de Guatemala contempla ambas funciones para la firma electrónica que puede ser empleada para identificar al firmante con relación a la comunicación electrónica e indicar que el firmante aprueba la información recogida en la comunicación. No se limita exclusivamente a la función de aprobación como sí lo hace la Ley Modelo.

Por otro lado de igual manera que como se reguló en la legislación sobre firma electrónica en Guatemala la Ley Modelo no viene a modificar las normas de protección al consumidor.

Con relación al mensaje de datos el fin de la definición de la Ley Modelo es su aplicación en el caso de revocación o modificación ya que se presume que un mensaje de datos tiene un contenido fijo de información que puede ser revocado o modificado por otro mensaje de datos, en Guatemala el mensaje de datos al igual en la ley modelo comprende todos los tipos de mensajes generados y almacenados básicamente sin papel. Constituyéndose al mismo tiempo en una especie de registros generados informáticamente de las comunicaciones generadas por este medio.

En conclusión la Ley Modelo por ser derivada de la Ley Modelo para el Comercio Electrónico de la CNUDMI, ha sido creada como una norma exclusiva para el comercio entre particulares, dejando de lado las relaciones entre las entidades públicas entre sí y entre los particulares, razón por la cual al ser adoptada en Guatemala ha sido necesario regular las cuestiones específicas, no así se han incluido los doce artículos de la misma literalmente en el contexto de la ley, mismos que se han ampliado con el resto de la normativa y la creación del Reglamento del Decreto 47-2008. Constituye una normativa que contempla ampliamente los aspectos más importantes sobre la firma electrónica partiendo de sus definiciones que han servido de base para las normativas vigentes en diversos países.

Capítulo II: De las entidades certificadoras de firma electrónica

II.1 Concepto

De conformidad con el artículo 2 del Decreto Número 47-2008 del Congreso de la República de Guatemala, se define a los prestadores de servicios de certificación como: "*la entidad que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas".* Asimismo dicho concepto se complementa con lo que establece el artículo 34 del mismo cuerpo legal cuando se refiere al órgano competente ya que 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 la ley.

En tal virtud, las entidades certificadoras de firma electrónica, o como la ley guatemalteca los define, los prestadores de servicios de certificación son aquellos órganos encargados de otorgar confianza en una infraestructura de clave pública ya que desde la perspectiva de una clave pública es necesario confiar en una tercera parte solvente que pueda garantizar u otorgue la confianza necesaria para poder identificar a una persona física o jurídica con una determinada clave pública[52].

Esta tercera parte fiable que acredita la relación entre una determinada clave y su propietario real, es similar a una función notarial que extiende un certificado de claves el cual está firmado con su propia clave, para, así, garantizar la autenticidad de dicha información. Su función consiste en certificar la identidad de los participantes de un negocio o los autores de un acto o documento, emitiendo el correspondiente certificado.

[52] Decreto Número 47-2008 del Congreso de Guatemala, Ley para el Reconocimiento de las comunicaciones y firmas electrónicas.

En el desempeño de estas funciones, los prestadores se encuentran afectos al cumplimiento de las siguientes obligaciones, de conformidad con el artículo 42 del Decreto Número 47-2008 del Congreso de la República de Guatemala:

a) Emitir los certificados digitales.
b) Crear sistemas de seguridad para la firma electrónica avanzada.
c) Proteger la información dada por el firmante.
d) Garantizar la continuidad de la prestación del servicio.
e) Prestar el debido servicio al cliente.
f) Facilitar la información solicitada por las entidades gubernamentales que se encuentre bajo su custodia.
g) Elaborar los reglamentos de funcionamiento de la relación firmante y prestación de servicio de certificación.
h) Llevar un registro de los certificados digitales autorizados.

Para ejercer la labor de certificación los prestadores deben llevar a cabo una serie de pasos y cumplir una serie de etapas, las que deben estar descritas en sus prácticas de certificación. De conformidad con la ley en Guatemala, el Registro de Prestadores de Servicios de Certificación para la Firma Electrónica, por conducto del Ministerio de Economía, ha elaborado un documento denominado Guía de Evaluación, emitido el 8 de julio de 2009, el cual describe el procedimiento de evaluación en tres pasos que serán descritos a continuación:

Procedimiento de evaluación:

La autorización es el resultado de un procedimiento en virtud del cual el prestador de servicios de certificación demuestra a la entidad autorizadora que cuenta con las instalaciones, sistemas, programas informáticos y recursos humanos necesarios para otorgar los certificados en los términos que se establecen en el Decreto Número 47-2008 del Congreso de la República de Guatemala (en adelante la Ley) y el Acuerdo Gubernativo 135-2009 (en adelante

el reglamento), permitiendo su inscripción en el Registro de Prestadores de Servicios de Certificación (en adelante RPSC), (art. 23 del Reglamento).

El procedimiento de evaluación es el siguiente:

PASO 1: SOLICITUD

Para solicitar su inscripción en el RPSC, la entidad solicitante deberá presentar ante la entidad autorizadora una solicitud por escrito dirigida al director ejecutivo, individualizándose mediante los documentos indicados en el requisito 1 de la guía de evaluación emitida por dicho Registro.

Dicha solicitud deberá ir acompañada por el comprobante de pago de los costos de la autorización (Art. 24 del Reglamento y su arancel).

Además se deberán incluir todos los documentos y antecedentes específicos en el requisito 1 admisibilidad, definido en el punto 3. Ellos incluyen documentos legales y comerciales, técnicos, de seguridad física, lógica y de la plataforma tecnológica utilizada, de la operación de la autoridad certificadora y de las autoridades de registro, de los tipos de certificados y servicios prestados, etc.

PASO 2: VERIFICACIÓN DE ADMISIBILIDAD

Recibida la solicitud, la entidad autorizadora procederá a revisar y declarar la admisibilidad de la misma mediante la verificación de la integridad de los antecedentes requeridos, dentro de un plazo de 5 días hábiles.

De ser inadmisible la solicitud, dentro del plazo indicado se procederá a comunicar al interesado tal situación y que podrá completar los antecedentes dentro del plazo de 15 días hábiles, bajo apercibimiento de ser rechazada la solicitud (Art. 24 Reglamento).

PASO 3: EVALUACIÓN DE LA AUTORIZACIÓN

Si la solicitud es declarada admisible será admitida a trámite. La entidad autorizadora procederá, dentro del plazo de 90 días calendario, a un examen sobre el cumplimiento de los requisitos y obligaciones exigidas por la ley, su reglamento y la guía de evaluación, para determinar si autoriza o no la inscripción en el RPSC de la entidad solicitante. Dicho plazo será contado desde la fecha de declaración de admisibilidad de la solicitud, y podrá ser prorrogado por una vez, en igual período, y por motivos fundados.

Para llevar a cabo esta tarea, el prestador de servicios de certificación deberá facilitar el acceso de los funcionarios o expertos que la entidad autorizadora designe para realizar las evaluaciones, además de proporcionar cualquier información adicional solicitada.

La evaluación se llevará a cabo sobre criterios objetivos, y cada requisito podrá alcanzar las calificaciones indicadas en la guía de evaluación que se adjunta a la presente investigación.

Realizada la evaluación, la entidad autorizadora se pronunciará sobre el cumplimiento de los requisitos y obligaciones necesarias para ser un prestador de servicios de certificación autorizado. Dicha declaración será emitida cuando un prestador de servicios de certificación sea evaluado con una calificación C (CUMPLE) en cada uno de los requisitos evaluados. Una vez declarada la autorización, el interesado dispone de un plazo de 30 días calendario para presentar la póliza de seguros que exige el artículo 16 del Reglamento, bajo apercibimiento de ser rechazada la solicitud si no lo cumple.

Si la entidad autorizadora determina, como resultado de la evaluación de los antecedentes e inspecciones, que los incumplimientos que presenta el prestador de servicios de certificación solicitante son subsanables en tiempos razonables, y no afectan el correcto funcionamiento del sistema ni los fines previstos en la ley,

su Reglamento y la Guía de evaluación, esto es, que exista al menos un requisito que como resultado de la evaluación se califique con nota S (SUFICIENTE), procederá a comunicar al prestador de servicios de certificación por escrito el o los requisitos incumplidos que se deberán subsanar, y dará un plazo para entregar por escrito un plan de medidas correctivas.[53]

Una vez recibido el plan de medidas correctivas propuesto por el prestador de servicios de certificación, la entidad autorizadora procederá a evaluar su factibilidad, la solución propuesta, y los plazos para ello. En caso de no ser satisfactorio, la entidad autorizadora procederá a dictar una resolución en la que rechaza la solicitud de registro mencionando los requisitos que se consideran no subsanables mediante la propuesta entregada. [54]

En caso de ser favorable la evaluación del plan de medidas correctivas, la entidad autorizadora procederá a informar al interesado que dispone de un plazo de 30 días calendario para presentar la póliza de seguros que exige el artículo 16 del Reglamento, bajo apercibimiento de ser rechazada la solicitud si no lo cumple. Esta condición obliga al prestador de servicios de certificación a dar cumplimiento fiel al plan de medidas correctivas propuesto y aceptado, cuyo incumplimiento dará lugar a las sanciones que el RPSC determine en su momento.[55]

Si el prestador de servicios de certificación no cumple con los requisitos y obligaciones de autorización definidos por la Ley, su reglamento y las regulaciones asociadas incluida la Guía de evaluación, esto es, que exista al menos un requisito que como resultado de la evaluación se determine que no sea subsanable y sea calificado con una I (INSUFICIENTE), la entidad autorizadora procederá a dictar una resolución en la que rechazará la solicitud de

[53] Registro de prestadores de servicios de certificación para la firma electrónica, GUÍA DE EVALUACIÓN, Ministerio de Economía, Guatemala, julio de 2009, pp.11
[54] Idem
[55] ibidem

inscripción en el RPSC mencionado el o los requisitos que están en dicha condición[56].

II.2 Características

De conformidad con el artículo 10 del Acuerdo Gubernativo 135-2009 las características de los prestadores de servicios de certificación son:

a) Personas jurídicas
b) Nacionales o extranjeras
c) Públicas o privadas
d) Domiciliadas en la República de Guatemala
e) Que podrán prestar otros servicios además de la certificación de la firma electrónica.
f) Estar autorizados por el Registro de Prestadores de Servicios de Certificación del Ministerio de Economía.
g) Que cuenten con la capacidad económica y financiera suficiente para prestar los servicios autorizados como prestadores de servicios de certificación.
h) Que cuenten 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 la ley.
i) Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a pena privativa de la libertad, o que hayan sido suspendidas en el ejercicio de su profesión por 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.

[56] Registro de prestadores de servicios de certificación para la firma electrónica, GUÍA DE EVALUACIÓN, Ministerio de Economía, Guatemala, julio de 2009, pp.11

j) Contar con las acreditaciones necesarias por los órganos o entidades correspondientes según la normativa vigente.

II.3 Efectos

La firma electrónica autorizada por una entidad prestadora de servicios de certificación contará con los efectos jurídicos resultantes del cumplimiento de todos los requisitos establecidos en la ley para que la misma surja, la cual, de conformidad con el artículo 33 del Decreto Número 47-2008 del Congreso de la República de Guatemala, podrá estar certificada por una entidad prestadora de servicios de certificación, que haya sido producida por un dispositivo seguro de creación de firma. En este sentido 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.

Por lo tanto los efectos jurídicos de la firma electrónica avanzada certificada por una entidad prestadora de servicios de certificación serán:

a) Respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel. (artículo 8 del Decreto Número 47-2008 del Congreso de la República de Guatemala)
b) Será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales. (Artículo 11 Decreto Número 47-2008 del Congreso de la República de Guatemala)

   Se excluye de estos efectos jurídicos lo referente a las disposiciones por causa de muerte y a los actos jurídicos del derecho de familia.

A parte de fijar los efectos jurídicos, establece una presunción para la adquisición de los efectos jurídicos antes nombrados. Señala los siguientes requisitos que se

presumen necesarios para que una firma avanzada tenga efectos jurídicos: (Artículo 33 Decreto 37-2008).

Que los datos de creación de la firma sean exclusivos del firmante y que los mismos estaban al momento de crearla bajo el exclusivo control del mismo, asimismo se requiere que sea posible detectar cualquier tipo de modificación posterior a haber sido impuesta la firma electrónica y que sea emitida con un certificado reconocido emitido por una entidad prestadora de servicios de certificación debidamente acreditado de conformidad con la ley que regula la materia.

II.4 Legislación relacionada con la firma electrónica de Guatemala

a) Constitución Política de la República de Guatemala
b) Decreto Ley 47-2008 del Congreso de la República de Guatemala
c) Acuerdo Gubernativo 135-2009 Reglamento de la Ley para el reconocimiento de las comunicaciones y firma electrónica
d) Código Civil Decreto Ley 106 de Guatemala
e) Código Procesal Civil Decreto Ley 107 de Guatemala
f) Código de Comercio Decreto 2-70 de Guatemala
g) Tratados Internacionales que contemplan la firma electrónica como método de seguridad jurídica de los negocios internacionales
h) La Ley Modelo de Comercio Electrónico de la Uncitral (o CNUDMI por sus siglas en Español – Comisión de Naciones Unidas para el Derecho Mercantil Internacional) – 1996.
i) Las Directivas respectivas de la Unión Europea – 1997 (sobre Protección a Consumidores en Contratos a Distancia) 1999 (sobre Firmas Electrónicas) 2000 (sobre Comercio Electrónico).
j) La Ley Modelo de la CNUDMI sobre Firmas Electrónicas – 2001.
k) Las Normas Interamericanas Uniformes sobre Documentos y Firmas Electrónicas de la OEA – 2002.

l) El Proyecto de Convención sobre la utilización de las Comunicaciones Electrónicas en los Contratos Internacionales - 2005 (último cuerpo normativo internacional).
m) Recomendaciones de la OECD en materia de Protección al Consumidor en el Comercio Electrónico.
n) Recomendaciones de la ICC sobre Contratación Electrónica – Cámara de Comercio Internacional en Paris. (ICC eTerms 2004 "Cláusulas contractuales 2004 de la CCI para el Comercio Electrónico": dota de mayor certeza o seguridad jurídica a todo contrato que se vaya a concertar por vía Electrónica).

II.5 Autoridades certificadoras

II.5.1 Autoridades raíz y subordinadas

Las autoridades raíz son aquellas que ofrecen servicios de certificación de clave pública a las autoridades certificadoras subordinadas. Por lo general se trata de una institución pública gubernamental establecida para el desarrollo del ámbito comercial, tanto en el registro público de prestadores de servicios de certificación como para el comercio electrónico en general.

Por su parte las autoridades certificadoras subordinadas son aquellas personas físicas o jurídicas acreditadas como entidades prestadoras de servicios de certificación por el Registro de Prestadores de Servicios de Certificación, que actúan para prestar el servicio como instituciones públicas gubernamentales, direcciones generales, es decir para actuar como entidades certificadoras de las entidades gubernamentales específicamente.

Necesitarán de un agente certificador que será la autoridad certificadora raíz que será la encargada de emitir los certificados digitales de las entidades subordinadas. La autoridad registradora, en este caso el Registro de Prestadores de Servicios de Certificación, será la entidad encargada de la

autenticación de documentos e identificación de los solicitantes y titulares del certificado digital emitido por la autoridad certificadora.

II.5.2 Estructura jerárquica

Una infraestructura de clave pública suele basarse en diversos niveles jerárquicos de autoridad. Por ejemplo:

a) Una entidad principal única que certifica la tecnología y las prácticas a todas las partes autorizadas a emitir certificados o pares de claves criptográficas en relación con el empleo de dichos pares de claves, y lleva un registro de las entidades de certificación subordinadas.
b) Diversidad de entidades de certificación, situadas bajo la autoridad principal que certificará que la clave pública de un usuario corresponde en realidad a la clave privada del mismo usuario (es decir que no ha sido alterada).
c) Diversas entidades locales de registro, situadas bajo las autoridades de certificación, que reciban de los usuarios peticiones de pares de claves criptográficas o de certificados relativos al empleo de esos pares de claves, y que exijan pruebas de identidad de los posibles usuarios y las verifiquen. En ciertos países, se prevee que los notarios podrían actuar como entidades locales de registro o prestar apoyo a dichas entidades.[57]

La Ley y el Reglamento sobre Firma Electrónica en Guatemala (Decreto 47-2008 y Acuerdo Gubernativo 135-2009 respectivamente) establecen una jerarquía de certificación para el funcionamiento de esta figura jurídica en Guatemala, que involucra a varios participantes tales como:

a) **Entidad autorizadora**: Corresponde a la autoridad administrativa, o Registro de Prestadores de Servicios de Certificación adscrito al Ministerio

[57] Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación para el Derecho Interno 2001, Naciones Unidas, Nueva York, 2002.

de Economía ser el responsable del registro y autorización para operar de los prestadores de servicios de certificación. (art. 49 de la Ley)

b) **Entidad de Normalización:** A solicitud de la entidad autorizadora, la Comisión Guatemalteca de Normas (COGUANOR) actuará para la generación u homologación de normas, regulaciones, criterios o principios internacionales reconocidos (literal j del Artículo 49 de la Ley), las que pasarán a ser parte del conjunto de normas técnicas vigentes aplicables en el contexto de la ley, el reglamento y sus regulaciones.
c) **Prestadores de Servicios de Certificación**: son las personas jurídicas, nacionales o extranjeras, públicas o privadas domiciliadas en Guatemala, encargadas de emitir los certificados que autorizan las firmas electrónicas avanzadas, siempre y cuando ya hayan sido autorizados por el Registro de Prestadores de Servicios de Certificación, luego de la evaluación de requisitos.
d) **Registro de Prestadores de Servicios de Certificación**: Consiste en el registro de carácter público que mantiene la Entidad Autorizadora, en el cual están identificados los Prestadores de Servicios de Certificación.

II.6 Análisis en la legislación sobre cómo se regulan los certificados digitales en la legislación

II.6.1 Concepto

El certificado de firma electrónica es definido en la legislación guatemalteca en el artículo 2 del Decreto 47-2008 del Congreso de la República como "*todo mensaje de datos u otro registro que confirme el vínculo entre el firmante y los datos de creación de la firma, usualmente emitido por un tercero diferente del originador y el destinatario".*

Por otro lado en la doctrina es definido como *"aquel documento que otorga certeza, asegura, afirma,*[58] *mediante una certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica. Este certificado es un elemento esencial de la firma electrónica, especialmente de la avanzada, por cuanto es lo que permite asegurar la no repudiación del documento de parte del suscriptor".*[59]

De las anteriores definiciones se colige que es función de la entidad certificadora de firma electrónica el emitir dichos certificados para vincular a un posible firmante, y al mismo tiempo crea un registro electrónico que indica una clave pública junto con el nombre del suscriptor del certificado como "sujeto" del mismo y que puede confirmar que el firmante potencial que figura en el certificado posee la clave privada correspondiente.[60]

Por lo tanto, la misión fundamental del certificado de firma electrónica es permitir comprobar que la clave pública del firmante, cuyo conocimiento es imprescindible para autenticar su firma electrónica, pertenece realmente a ese usuario, es decir vincular una clave pública con un titular determinado[61]. El certificado de firma electrónica avanzada, deberá permitir que quien lo reciba pueda comprobar en forma directa o mediante consulta electrónica, que ha sido emitido por un prestador acreditado, con la finalidad de confirmar la validez del mismo. Asimismo, el certificado podrá establecer límites en cuanto a sus posibles usos, siempre y cuando dichos límites sean conocidos por terceros.

Lo que el certificado acredita es que a la fecha de la firma del documento, quien lo suscribió era el titular de dicha firma.

---

[58] Diccionario de la Real Academia Española, Vigésima primera edición, 1992.

[59] Correa González, Felipe, INTRODUCCIÓN A LA FIRMA ELECTRÓNICA Y SERVICIOS DE CERTIFICACIÓN, documento publicado número 069 de abril de 2004, disponible en www.alfa-redi.org, consultado el 15 de diciembre de 2009.-

[60] idem

[61] Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación para el Derecho Interno 2001, Naciones Unidas, Nueva York, 2002.

Los certificados, por lo tanto, son registros electrónicos que atestiguan que una clave pública pertenece a determinado individuo o entidad. Permite verificar que una clave pública pertenece a una determinada persona, intentan evitar que alguien utilice una clave falsa haciéndose pasar por otro.

Un certificado emitido por un prestador de servicios de certificación autorizada, además de estar firmado electrónicamente por éste debe contener los requisitos establecidos en el artículo 46 del Decreto Número 47-2008 del Congreso de la República de Guatemala.[62]

II.6.2 Requisitos de validez

El certificado de firma electrónica da fe del vínculo entre el firmante o titular del certificado y los datos de creación de firma electrónica. Los mismos para ser válidos deben contener por lo menos los requisitos contemplados en el Artículo 46 del Decreto Número 47-2008 del Congreso de la República y Artículo 18 del Acuerdo Gubernativo 135-2009, tales como:

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.

[62] Artículo 46 del Decreto 47-2008 del Congreso de la República de Guatemala:
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.

e) La metodología para verificar la firma electrónica del firmante impuesta en la comunicación electrónica.
f) El número de serie el certificado.
g) Fecha de emisión y expiración del certificado.
h) Un código de identificación único del certificado y/o el número de serie del certificado.
i) Identificación del prestador de servicios de certificación, con indicación de su nombre comercial y/o razón social, número de identificación tributaria, dirección de correo electrónico y, en su caso, los antecedentes de su autorización y su propia firma electrónica avanzada.
j) Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico y su número de identificación tributaria, cédula de vecindad, código único de identificación o pasaporte según corresponda, y su plazo de vigencia.

II.6.3 Período de vigencia

Los certificados emitidos por una entidad certificadora deberá contener como un requisito de validez el plazo de vigencia del mismo el cual no podrá exceder de tres años contados a partir de haber sido emitido este.

II.6.4 Reconocimiento de certificados extranjeros

Existen ciertos principios que rigen las relaciones originadas por medio electrónico consagrados en los tratados internacionales que regulan la materia, como lo es la Ley Modelo de la CNUDMI sobre Firmas Electrónicas y la Ley Modelo de la CNUDMI sobre Comercio Electrónico, así: el principio de la neutralidad respecto a los medios técnicos utilizados; el criterio de la no discriminación de todo equivalente funcional de los conceptos y prácticas que tradicionalmente funcionan sobre soporte de papel; y una amplia confianza en la

autonomía de la voluntad contractual a las partes y el principio de no discriminación de certificados extranjeros. Éste último es el que aquí interesa.

La Ley Modelo establece como principio básico que el lugar de origen en sí no debe ser en ningún caso un factor para determinar si puede reconocerse la capacidad de los certificados extranjeros o las firmas electrónicas para tener eficacia jurídica en un Estado promulgante. La determinación de si un certificado o una firma electrónica pueden tener eficacia jurídica, y hasta qué punto pueden tenerla, no debe depender del lugar en que se haya emitido el certificado o la firma electrónica, sino de su fiabilidad técnica. Este principio se desarrolla en el artículo 12 de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas.[63]

Por su parte, el Decreto 47-2008 del Congreso de la República de Guatemala, al referirse a los certificados extranjeros en el artículo 39, establece lo siguiente:

Que no se tomarán en consideración el lugar en el que se haya expedido el mismo ni tampoco el lugar en el que se encuentre el establecimiento del expedidor o del firmante, de igual forma a como lo establece la Ley Modelo.

---

[63] Artículo 12. Reconocimiento de certificados extranjeros y 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:
El lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica; ni
El lugar en que se encuentre el establecimiento del expedidor o del firmante.
Todo certificado expedido fuera (del Estado promulgante) producirá los mismos efectos jurídicos en (El Estado promulgante) que todo certificado expedido en (El Estado promulgante) si presenta un grado de fiabilidad sustancialmente equivalente.
Toda firma electrónica creada o utilizada fuera (del Estado promulgante) producirá los mismos efectos jurídicos en (El Estado promulgante) que toda firma electrónica creada o utilizada en (el Estado promulgante) si presenta un grado de fiabilidad sustancialmente equivalente.
A efectos de determinar si un certificado o una firma electrónica presentan un grado de fiabilidad sustancialmente equivalente para los fines del párrafo 2, o del párrafo 3, se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente.
Cuando, sin perjuicio de lo dispuesto en los párrafos 2, 3 y 4, las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas o certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que el acuerdo no sea válido o eficaz conforme al derecho aplicable.

Continúa dicho artículo estableciendo que todo certificado expedido en el extranjero producirá los mismos efectos jurídicos que el expedido en la República al igual que la firma electrónica, si presenta un grado de fiabilidad sustancialmente equivalente, lo que se determinará en relación a los tratados internacionales suscritos por Guatemala. Asimismo se establece que la voluntad de las partes en acordar el tipo de certificado transfronterizo o firma electrónica prevalecerá por encima de lo que establecen las normas legales al respecto.

En la actualidad cuando un documento es otorgado en el extranjero, para que éste tenga valor probatorio o valor jurídico en Guatemala se exige que sea legalizado conforme a la cadena de legalización establecida en el Código Procesal Civil y Mercantil Decreto, Ley 107 y en el caso de instrumentos públicos estos deben ser protocolizados por un notario debidamente autorizado según el Código de Notariado, Decreto Número 314. De conformidad con lo establecido, tanto en la norma internacional como en la norma nacional referente a las firmas electrónicas, estos requisitos seguirán siendo necesarios para los documentos electrónicos; asimismo de conformidad con la Ley del Organismo Judicial en el artículo 37 que establece los requisitos de documentos extranjeros para que los mismos sean admisibles y puedan surtir efectos en Guatemala, deben ser legalizados por el Ministerio de Relaciones Exteriores. Todo lo anterior sin perjuicio de que en cuanto a los efectos jurídicos de dichos documentos otorgados en el extranjero tendrán los mismos que si lo hubiesen otorgado en Guatemala como lo establece el artículo 39 del Decreto Número 47-2008 del Congreso de la República de Guatemala.

De conformidad con el artículo 33 del Decreto Número 47-2008 del Congreso de la República de Guatemala sólo será firma electrónica avanzada aquella que sea certificada por una entidad prestadora de servicios de certificación, la cual deberá contar con un domicilio; en el caso de ser éste Guatemala, se estará en presencia de una firma electrónica avanzada en aquellos casos en que el

certificado de firma electrónica emane de un prestador de servicios de certificación acreditado con domicilio en el país; así el reconocimiento de una comunicación electrónica proveniente del extranjero no está dado por el lugar en que se suscribe el documento sino por aquel en el que tiene su domicilio la entidad certificadora.

A pesar de ello, de conformidad con la norma guatemalteca transcrita en párrafos anteriores, no se tomará en consideración para los efectos jurídicos que produzcan los certificados o firma electrónicas provenientes del extranjero, el lugar en el que se haya expedido, ni el lugar en que se encuentre el firmante, se le otorga el mismo efecto jurídico independientemente de estas situaciones y se facilita su utilización en el país.

Haciendo un análisis comparativo con la legislación extranjera, en el caso de Chile, según la Ley 19.799, en su artículo 15, se establece que los certificados de firma electrónica avanzada podrán ser emitidos por entidades no establecidas en Chile y serán equivalentes a los otorgados por prestadores establecidos en el país; cuando fueren homologados por estos últimos, bajo su responsabilidad, y cumpliendo los requisitos fijados en la ley y su reglamento, o en virtud de convenio internacional ratificado por Chile y que se encuentre vigente. Se puede homologar un certificado o un grupo de ellos, pero en todo caso deberá publicarse tal situación en el registro público que debe llevar la certificadora, permitiendo su conocimiento por terceros.[64]

En el caso de la Unión Europea, se establece con respecto a la equivalencia u homologación de certificados de Estados que no sean miembros de la Unión Europea, según el artículo 10 del Real Decreto Ley 14/1999 de 17 de septiembre sobre Firma Electrónica, una serie de requisitos o condiciones:

[64] Correa González, Felipe, INTRODUCCIÓN A LA LEY No. 19.799 DE FIRMA ELECTRÓNICA Y SERVICIOS DE CERTIFICACION No. 069-abril de 2004, Revista electrónica de Derecho Informático, http://www.alfaredi.org/rdi-articulo.shtml, fecha de consulta: 15 de diciembre de 2009.

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 con 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.[65]

En comparación con la norma guatemalteca las normas de la Unión Europea son mucho más estrictas en cuanto a la homologación de certificados provenientes del extranjero, ya que los mismos deben estar acordes a las normas de dicha Unión para ser aceptados, lo que limita el uso de certificados provenientes de cualquier parte del mundo.

II.7 Certificadores licenciados-Ente licenciante

II.7.1 Concepto

Un certificador licenciado es aquella entidad prestadora de servicios de certificación que ha cumplido con los requisitos establecidos por la Ley, el Reglamento y la Guía de Evaluación emitida por el ente licenciante; en el caso de Guatemala, el Registro de Prestadores de Servicios de Certificación. Esta entidad será la encargada de prestar los servicios de emisión de certificados de firma electrónica, y otros servicios relacionados con las mismas.[66]

[65] Ramos Suárez, Fernando, Cómo aplicar la normativa sobre firma electrónica, Universidad de Jaén, segunda edición, España, 1999.
[66] Artículo 40 del Decreto 47-2008 del Congreso de la República, Ley para el reconocimiento de las comunicaciones y firmas electrónicas.

Por su parte, el ente licenciante será el Registro de Prestadores de Servicios de Certificación que es la entidad gubernamental adscrita al Ministerio de Economía que ejercerá las facultades que legalmente le han sido asignadas respecto de las entidades prestadoras de servicios de certificación, compuesta por el director ejecutivo, la secretaría general, el asesor jurídico y el asesor técnico (artículo 31 Reglamento).

II.7.2 Funciones

Las funciones de los certificadores licenciados o entidades prestadoras de servicios de certificación son: (artículo 41 Decreto Número 47-2008 del Congreso de la República).

a) Emitir certificados digitales.
b) Emitir certificados de verificación.
c) Ofrecer servicios de creación de firmas electrónicas avanzadas.
d) Emitir certificados con relación a quienes poseen certificados o firmas electrónicas.
e) Ofrecer servicios de registro de comunicaciones electrónicas.
f) Archivo de las comunicaciones electrónicas.
g) Certificar las condiciones profesionales del titular de firma para efectos probatorios.

Por su parte, las funciones del ente licenciate es decir el Registro de Prestadores de Servicios de Certificación, son: (Artículo 49 Decreto 47-2008)

a) Autorizar las actividades de las entidades prestadoras de servicios de certificación.
b) Velar por el funcionamiento y prestación de los servicios.
c) Auditar, revocar o suspender e imponer sanciones a las entidades prestadoras de servicios de certificación.
d) Revocar certificados digitales.

e) Velar por el cumplimiento de las disposiciones legales tanto constitucionales como en materia mercantil.
f) Emitir regulaciones legales acordes a los principios y normas internacionales que sustentan la normativa legal vigente.

II.7.3 Obligaciones

Las obligaciones de los prestadores de servicios de certificación serán las siguientes: (Artículo 42 Decreto 47-2008 y artículo 23 del reglamento).

a) Emitir certificados digitales
b) Implementar sistemas de seguridad electrónica tanto para creación de firmas como para el archivo de los mensajes de datos.
c) Garantizar la confidencialidad de la información proporcionada por las partes.
d) Garantizar la prestación permanente del servicio de certificación.
e) Ofrecer la información requerida por las autoridades administrativas y/o judiciales.
f) Facilitar la auditoria.
g) Llevar registro de los certificados digitales que se emiten.
h) Contar con reglas de certificación y comunicarlas al público.
i) Contar con una póliza de seguro.

II.7.4 Responsabilidad

De conformidad con el Reglamento Decreto Gubernativo 135-2009, en su artículo 15, los prestadores de servicios de certificación serán responsables de los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación u homologación de certificados de firmas electrónicas. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia.

Sin perjuicio de lo dispuesto en el inciso anterior, los prestadores no serán responsables de los daños que tengan su origen en el uso indebido o fraudulento de un certificado de firma electrónica.

Los certificados provistos por una entidad certificadora podrán establecer límites en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles en los certificados por terceros. El prestador de servicios de certificación quedará eximido de responsabilidad por los daños y perjuicios causados por el uso que exceda de los límites indicados en el certificado.

En ningún caso la responsabilidad que pueda emanar de una certificación efectuada por un prestador privado autorizado comprometerá la responsabilidad pecuniaria del Estado.

Capítulo III: Los certificados digitales

III.1 Concepto

El concepto de certificado utilizado en el contexto de ciertos tipos de firma electrónica y utilizado también en la Ley Modelo sobre Firmas Electrónicas de la CNUDMI poco difiere de su significado general de "documento mediante el cual se asegura la verdad de un hecho."[67] La única diferencia es que el certificado se presenta en forma electrónica y no sobre papel. Sin embargo, dado que no en todos los ordenamientos jurídicos existe la noción general de "*certificado",* ni siquiera en todos los idiomas, fue incluida en la Ley Modelo una definición de certificado la cual se cita textualmente como:

Artículo 2. Definiciones…. b) Por "certificado" se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma.

La legislación guatemalteca incluye dentro de sus primeros artículos una definición de lo que es un certificado que no se aparta mucho de lo que establece la Ley Modelo, el cual es definido como 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. (Artículo 2 Decreto 47-2008)

III.2 Contenido

Todo certificado emitido por una entidad prestadora de servicios de certificación, autorizada por el Registro de Prestadores de Servicios de Certificación deberá contar como mínimo con el siguiente contenido:

a) Nombre, dirección y domicilio del firmante.
b) Identificación del firmante nombrado en el certificado.

[67] Diccionario de la Real Academia Española, vigésima segunda edición.

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.
h) Un código de identificación único del certificado y/o el número de serie del certificado.
i) Identificación del prestador de servicios de certificación, con indicación de su nombre comercial y/o razón social, número de identificación tributaria, dirección de correo electrónico y, en su caso, los antecedentes de su autorización y su propia firma electrónica avanzada.
j) Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico y su número de identificación tributaria, cédula de vecindad, código único de identificación o pasaporte según corresponda, y
k) Su plazo de vigencia.

III.3 Funcionamiento

Para los usuarios de la firma electrónica la confianza que tienen en la identidad de un remitente de una comunicación firmada electrónicamente radica en la confianza que se tenga en la autoridad certificadora que firma el certificado. De ahí la importancia del trabajo de la autoridad certificadora y la responsabilidad que tiene ésta de asegurarse de la identidad de todas las personas a quienes les han expedido un certificado.

El usuario final podría validar la confianza verificando que la autoridad certificadora esté afiliada o inscrita en alguna entidad que se encargue de hacer auditorías para dar mayor confianza a los usuarios, por ejemplo en Guatemala, el Registro de Prestadores de Servicios de Certificación.

Para entender el funcionamiento de los certificados digitales podría hacerse una analogía con los certificados emitidos por el Registro Nacional de las Personas (RENAP) como autoridad certificadora, y los Documentos Personales de Identificación (DPI), como certificados de identidad. Una autoridad o tercero de confianza (RENAP) extiende un documento (DPI) que garantiza la identidad de la persona; de igual manera funciona con los certificados digitales, los cuales son emitidos a las personas (individuales o jurídicas) por una autoridad certificadora quien garantiza la validez de los mismos. Dicha autoridad es autorizada por el Registro de Prestadores de Servicios de Certificación, con lo cual se le enviste con la calidad de validez que otorga la certeza jurídica de que quien es el titular del certificado digital es realmente quien envía el mensaje por la vía electrónica.

III.4 Finalidad

La finalidad del certificado es reconocer, mostrar o confirmar un vínculo entre los datos de creación de la firma y el firmante. Ese vínculo nace cuando se generan los datos de creación de la firma.[68] El certificado es un elemento esencial de la firma electrónica, especialmente de la avanzada, por cuanto es lo que permite la no repudiación del documento por parte del suscriptor.

El certificado de firma electrónica avanzada, deberá permitir que quien lo reciba pueda comprobar, en forma directa o mediante consulta electrónica, que ha sido emitido por un prestador acreditado, con la finalidad de acreditar la validez del mismo. Además, el certificado podrá establecer límites en cuanto a sus posibles

[68] Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001, Naciones Unidas, Nueva York 2001.

usos, siempre y cuando dichos límites sean reconocibles por terceros. Lo que un certificado acredita es que a la fecha de la firma del documento, quien lo suscribió era el titular de dicha firma.[69]

III.5 Usurpación de la identidad

El problema de la usurpación de la identidad se ha venido dando desde siempre, con los documentos de identificación falsificados, las personas que se hacen pasar por representantes de una empresa determinada para realizar un cobro que la empresa desconoce, entre otros. Con la constante utilización de los medios electrónicos para realizar actividades tanto a nivel personal, como empresarial o comercial se ha ido desarrollando una serie de delitos cibernéticos que han venido a sustituir las tradicionales formas de estafas.

En la actualidad se encuentra una forma de estafa cibernética denominada *phishing*, término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, denominado phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea[70] o incluso utilizando también llamadas telefónicas.

El término phishing proviene de la palabra inglesa "*fishing*" (pesca),[71] haciendo alusión al intento de hacer que los usuarios "*piquen en el anzuelo".* A quien lo

[69] Correa González, Felipe, INTRODUCCIÓN A LA LEY No. 19.799 DE FIRMA ELECTRÓNICA Y SERVICIOS DE CERTIFICACION No. 069-abril de 2004, Revista electrónica de Derecho Informático, http://www.alfaredi.org/rdi-articulo.shtml, fecha de consulta: 15 de diciembre de 2009.
[70] Tan, Koon. Phishing and Spamming via IM (SPIM).|Internet Storm Center. 5 de diciembre de 2006
[71] Diccionario en línea, inglés – español, http://www.wordreference.com/es/translation.asp, consultado el 8 de marzo de 2010.

practica se le llama phisher.[72] La palabra phishing también puede ser una contracción de *"password harvesting fishing"* (cosecha y pesca de contraseñas), ya que la escritura ph es comúnmente utilizada por hackers para sustituir la f, como raíz de la antigua forma de hacking telefónico conocida como phreaking.

La primera mención del término phishing data de enero de 1996. Se dio en el grupo de noticias de hackers alt.2600, aunque es posible que el término ya hubiera aparecido anteriormente en la edición impresa del boletín de noticias hacker "2600 Magazine". El término phishing fue adoptado por quienes intentaban "*pescar"* cuentas de miembros de AOL[73].

Dentro de los recientes intentos de phishing que se han dado se encuentra el phishing en Messenger con la reciente aparición de las páginas quienteadmite y noadmitido destinadas a robar el nombre y contraseña de los usuarios de MSN a cambio de mostrarles a los visitantes que la utilicen, quien los ha borrado de su lista de contactos. Esta técnica consiste en pedirle al usuario final su usuario o correo electrónico y luego la contraseña, datos que son enviados luego a la base de datos del autor de la página y así almacenando la información para poder acceder a dicha cuentas. Otro intento reciente de phishing es el que ha tomado como objetivo a los clientes de bancos y pagos de servicios en línea, ya que el creador de la página de phishing la elabora de tal manera que todo parece indicar que es la página del banco, de este modo envía un correo electrónico al usuario indicándole que debe confirmar o cambiar su contraseña, para hacerlo debe seguir el link que le es enviado en el correo el cual lo lleva a la página del phisher que da la apariencia de ser la original a no ser que se observe

---

[51] Stutz, Michael AOL: A Cracker's Paradise, enero de 1998.

[52] Ollmann, Gunter. Phishing Guide: Understanding and Preventing Phishing Attacks. Technical Info. 10 de julio de 2006.

[56]Diccionario en línea, inglés – español, http://www.wordreference.com/es/translation.asp, consultado el 8 de marzo de 2010.

detalladamente y se note un pequeño cambio en el nombre de la página, de este modo al acceder a este link y entregar la contraseña y nombre de usuario se le está entregando estos datos personales directamente al phisher quien con ellas los utiliza para entrar a la cuenta original del banco y realizar estafas utilizando dichos datos.

El phishing consiste en uno de los delitos cibernéticos que se pretende aminorar con el uso generalizado en la red de los certificados digitales autorizados por entidades prestadoras de servicios de certificación para convertir a la red en un lugar mucho más seguro.

En Guatemala no se encuentra tipificado como delito en el código penal, pero se han dado casos de este tipo que se encuentran en noticias en la red que involucran a Guatemala como un país al cual ya lo afectan estos delitos; en mayo de 2007 se publicó en una página de internet denominada www.deguate.com una noticia sobre phishing de una página que decía ser del Banco Cuscatlán, en mayo del 2008 se publicó en dicha página otra noticia sobre phishing haciéndose pasar por una página electrónica de Banco Uno, y en agosto de 2010 en la página www.gt.globedia.com se publicó un reportaje donde un phisher publica una página haciéndose pasar por la aerolínea spanair. Estos son algunos ejemplos no tipificados como delitos en la ley guatemalteca pero que están empezando a afectar a nuestro país.

III.6 Clases de certificados

Se dan distintas clases de certificados digitales, dependiendo de las necesidades de los usuarios. Existen certificados para personas individuales, como los certificados de pertenencia a empresa, y los certificados de representante; y también los certificados de persona jurídica. El Decreto Número 47-2008 y su respectivo reglamento no establecen específicamente los tipos de certificados digitales que la ley guatemalteca ampara, sino que se limita únicamente a

establecer los requisitos mínimos que deben contener, los derechos y obligaciones de los propietarios de los mismos y lo relativo a la revocación o suspensión de los mismos. Por lo tanto, se puede deducir que en el momento de empezar a funcionar las entidades certificadoras de firma electrónica en Guatemala tendrán que ir surgiendo distintos tipos de certificados dependiendo de las necesidades de los usuarios. Dentro de algunos tipos de certificados que pueden darse se encuentran los siguientes:

Certificado de pertenencia a empresa

Este certificado determina la vinculación de una persona física a una entidad determinada, informando del departamento al cual pertenece y el cargo que ocupa en la misma. La ventaja de este tipo de certificado radica en que permite fijar una forma de comunicación fiable dentro de la misma empresa, estableciendo políticas que permiten identificar plenamente a sus trabajadores.

Certificado de representante

Este tipo de certificado permite identificar a una persona física como representante de una empresa. Con este tipo de certificado, su titular podrá representar telemáticamente a su empresa en aquellos trámites para los cuales esté habilitado.

Certificados de persona jurídica

Mediante este certificado la propia empresa se convierte en titular del certificado digital, si bien se delega la custodia del mismo en una persona física responsable del mismo.

III.7 Certificados de servidores

Dentro de los certificados de servidores se encuentran:

Certificados de navegador:

Este tipo de certificados permiten firmar digitalmente los documentos, garantizando la autenticidad y el no repudio de los mismos, además de la posibilidad de cifrar la información (encriptación) de tal forma que sólo el receptor pueda descifrarlos y tener acceso a su contenido, garantizando su integridad y confidencialidad. Por último también se da la facultad de brindar seguridad y autenticar la identidad en el control de acceso de los usuarios.

Certificado de servidor seguro:

El certificado de servidor seguro es el tipo de certificado que garantiza la identidad del servidor y posibilitan las comunicaciones seguras y privadas con los clientes, socios, proveedores u otras personas.

Certificado de firma de Software:

El certificado de firma de software es el tipo de certificado que garantiza la identidad del fabricante y la integridad del contenido.

III.8 Validez y revocación

El certificado de firma electrónica podrá ser usado conforme a las operaciones que han sido autorizadas a realizar en las prácticas de certificación y las políticas del prestador de servicios de certificación con quien se han contratado.

El certificado de firma electrónica avanzada deberá permitir a quien lo reciba verificar, en forma directa o mediante consulta electrónica, que ha sido emitido u homologado por un prestador autorizado de servicios de certificación, con la finalidad de comprobar la validez del mismo. (artículo 20 del Reglamento, Acuerdo Gubernativo 135-2009)

El artículo 47 del Decreto Número 37-2008 del Congreso de la República de Guatemala establece que los certificados podrán revocarse en caso de pérdida

de la clave privada o si la misma se ha expuesto o corre peligro de que se le diera un uso distinto al destinado.

Asimismo una prestadora de servicios de certificación revocará un certificado emitido a petición del firmante, por muerte del mismo o por liquidación en el caso de las personas jurídicas, en el caso de encontrarse información falsa o por el cese de las actividades de la prestadora de servicios de certificación, así como por orden judicial competente.

En el caso de la vigencia de un certificado podrá ser suspendida por solicitud del titular o por decisión del prestador de servicios de certificación

La suspensión o revocación del certificado deberá ser comunicada inmediatamente a su titular, sin perjuicio de que deba publicarse en el registro de acceso público que señala el artículo 13 del reglamento.

III.9 Usos de certificados en internet[74]

Para poder acceder a una sede Web segura que requiere una conexión SSL[75], por ejemplo, https://www.verisign.com, o si se desea codificar o firmar el correo enviado a través de Internet, se necesita un certificado de Internet. Generalmente estos certificados se almacenan en los navegadores de Web, como, por ejemplo,

[74] Ecoforo, Uso de certificados dobles para internet, http://ecoforo.cepymev.es, consultado: 4 de marzo de 2010.

[75] Secure Sockets Layer, Protocolo de Capa de Conexión Segura- (**SSL)** son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet, SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar; la autenticación mutua requiere un despliegue de infraestructura de claves públicas (o PKI) para los clientes. Los protocolos permiten a las aplicaciones cliente-servidor comunicarse de una forma diseñada para prevenir escuchas (eavesdropping), la falsificación de la identidad del remitente (phishing) y alterar la integridad del mensaje.
SSL implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación.
- Intercambio de claves públicas y autenticación basada en certificados digitales.
- Cifrado del tráfico basado en cifrado simétrico.

Netscape o Internet Explorer; sin embargo, se pueden almacenar en un ID[76] de usuario si se desea utilizarlos con el navegador de Lotus Notes o con el correo de Lotus Notes (este nombre de navegador es utilizado a modo de ejemplo). Normalmente, los certificados de Internet contienen una dirección de correo electrónico. Debido a que los nombres de estos certificados son extensos, el navegador muestra la dirección de correo electrónico en un formato abreviado para indicar a quién pertenece el certificado. Si esta dirección no está disponible, el navegador muestra la parte más significativa del nombre del certificado. Por ejemplo, el nombre de un certificado de Internet podría tener el siguiente aspecto: CN=AC Internet HyD/O=HyD/S=CART/C=ESP. La parte que mostraría el navegador sería "AC Internet HyD" El certificado de Internet designado como certificado para firmas predeterminado para el correo electrónico SMIME[77] se indica mediante una marca de verificación en el icono situado junto al nombre del certificado.

Los certificados de Internet se pueden utilizar para firmar y codificar los mensajes de correo, así como para establecer conexiones seguras a través de Internet.

Los certificados de internet son utilizados para firmar mensajes que se envían y también para que otras personas puedan utilizarlos para codificar los mensajes que le son enviados. Dentro de las empresas que emplean este tipo de certificados se encuentran IBM, Lotus Notes, entre otras. Si se cuenta con varios certificados de internet se pueden utilizar uno de ellos para firmar los mensajes y el otro para permitir que otras personas puedan codificar los mensajes de correo.

[76] Nombre de usuario

[77] **Secure / Multipurpose Internet Mail Extensions**, del inglés, *Extensiones de Correo de Internet de Propósitos Múltiples / Seguro*) es un estándar para criptografía de clave pública y firmado de correo electrónico encapsulado en MIME, S/MIME provee los siguientes servicios de seguridad criptográfica para aplicaciones de mensajería electrónica: autenticación, integridad y no repudio (mediante el uso de firma digital) privacidad y seguridad de los datos (mediante el uso de cifrado).

Algunas autoridades certificadoras expiden certificados específicos para las firmas y otros para la codificación. Por el contrario otras expiden certificados que pueden utilizarse tanto para la codificación como para las firmas.

III.10 Autenticación de extremos[78]

La autenticación de extremos es el proceso por medio del cual se les conceden permisos a los usuarios de Windows, que posean una autenticación válida, para que puedan conectarse a extremos creados por el servidor y que de esta forma se inicie la autenticación del mismo.

La autenticación se lleva a cabo utilizando la cláusula AUTHENTICATION de la institución CREATE ENDPOINT[79] o la institución ALTER ENDPOINT. Se le proporcionan al usuario las siguientes opciones de autenticación:

Basic

Digest

NTLM

Kerberos

Integrated

Existen distintos tipos de autenticación, los cuales para fines ilustrativos únicamente se enumerarán:

Autenticación básica

Autenticación implícita

Autenticación de Kerberos[80]

[78] Microsoft Windows, Autenticación de Extremos en Internet, http://msdn.microsoft.com/es-es/library/ms191264.aspx Consultado: 5 de marzo de 2010.
[79] Crea extremos y define sus propiedades, incluidos los métodos disponibles para las aplicaciones cliente.

Autenticación integrada

III.11 Mensajería segura

Uno de los objetivos principales que se pretenden lograr con el uso de la firma electrónica y los certificados digitales es el conseguir una forma de comunicación digital segura; es decir, que en el transcurso que el mensaje tome, éste se mantenga íntegro a pesar de tratarse de un medio fácil de manipular, ya que es una forma intangible de comunicación. Se trata así de una modalidad de reciente creación pero que permitirá que las relaciones comerciales se agilicen al no necesitar de la presencia directa de los contratantes en el caso de un contrato sino que estos puedan realizarlo vía internet sin la necesidad del rigorismo notarial, pero con la misma seguridad que este proporciona. Es una vía mucho más veloz pero que debe ser utilizada adecuadamente.

III.12 No repudio

El titular de un mensaje enviado con firma digital autenticada por un certificado digital debidamente emitido por una entidad certificadora de firma electrónica no podrá negar la autoría del mensaje ya que ésta es una de las finalidades de la firma electrónica, debido a que para enviarlo éste deberá contar con su clave otorgada por el certificado. Dicha clave únicamente la podrá utilizar el titular de dicho certificado por lo que al recibirse un mensaje firmado con dicha clave no se puede dudar que este haya sido emitido por dicho titular del certificado. Esta característica de los certificados digitales otorga una mayor seguridad y certeza jurídica a las relaciones originadas por medio electrónico.

III.13 Titulares de certificados digitales[81]

[80] Kerberos es un sistema de autenticación utilizado para comprobar la identidad de un usuario o máquina.
[81] Cámara de Comercio de Guatemala, Trámite ante la Cámara de Comercio de Guatemala para los titulares de certificados digitales, septiembre de 2009, http://www.ecertchile.cl/html/productos/download/CCS_CadenaCert.p7b

Los titulares de los certificados digitales pueden ser personas individuales, personas jurídicas o propietarios de empresas mercantiles; para poder ser acreditados como tales se debe seguir el procedimiento ante la Cámara de Comercio de Guatemala quien en conjunto con la Entidad Prestadora de Servicios de Certificación chilena E-CERT son los encargados de emitir los certificados digitales en la actualidad en Guatemala. (Artículo 20 Acuerdo Gubernativo 135-2009).

Por lo tanto, para adquirir una firma electrónica simple o una firma electrónica avanzada se debe llenar una solicitud de productos y servicios ITN con el que se solicita el certificado digital, llenar y firmar el "*Formulario de Autorización de Información"* mediante el cual se autoriza a la empresa "*Informes en Red S.A*." para que verifique los datos consignados y trasladarlos a la Cámara de Comercio de Guatemala; y por último llenar y firmar el "*Consentimiento / Certificado de aceptación del uso de certificado de e-comercio /sello chamber trust".* Además quienes opten para ser titulares de certificados digitales deberán cumplir los siguientes requisitos:

Para personas jurídicas:

a) Copia de cédula de vecindad completa del representante legal (o DPI en su caso).
b) Copia de patente de comercio de empresa y patente de comercio de sociedad en el caso de la sociedad anónima.
c) Constancia de inscripción en el registro tributario unificado.
d) Copia de escritura de constitución
e) Copia de nombramiento de representante legal debidamente inscrito.
f) Para propietarios de empresas mercantiles:
g) Patente de comercio de empresa.
h) Copia de cédula de vecindad completa (o DPI en su caso).

---

consultado: 03 de enero de 2010.

i) Constancia de inscripción en el registro tributario unificado.
j) Para personas individuales:
k) Copia de cédula de vecindad completa (o DPI en su caso).
l) Constancia de inscripción en el registro tributario unificado.
m) Todas las copias deben estar autenticadas por notario.

Luego de cumplir con todo esto y de esperar el tiempo necesario, la empresa E-CERTCHILE se comunica al correo otorgado por el solicitante, para hacerle saber los pasos a seguir para descargar el certificado en el servidor y poder instalarlo en la computadora.

Los pasos son los siguientes[82]:

Habiendo recibido la solicitud de certificado y dado cumplimiento a todos los requisitos exigidos, la empresa E-CERTCHILE comunica que ha sido aprobada la emisión del certificado: ya sea de firma electrónica simple o avanzada.

Para proceder a su instalación por única vez se deben seguir los pasos que se detallan a continuación:

a) Ingresar desde la computadora al sitio web de la entidad certificadora www.e-certchile.cl a la selección Productos, dentro de esta opción se debe elegir el producto firma electrónica simple o avanzada dependiendo de la que se haya adquirido.
b) Escoger la opción o imagen llamada descargar.
c) Luego se deberán ingresar los campos de identificación, password y Verificación en el mismo orden que indica la página web.
d) Se debe otorgar al certificado un nivel de seguridad ALTO (nivel medio está por defecto), en donde se le solicitará un password (este password es de seguridad y cada vez que se desee utilizar el certificado se deberá ingresar el mismo).

[82] idem

e) Una vez definida la password se deberá hacer un clic en aceptar.

f) Luego aparecerá una imagen que dirá Instalar Certificado, se debe dar clic sobre ella, para que sea instalado el certificado en el navegador.

g) El certificado será descargado por el usuario, y será responsable de la descarga durante su instalación.

h) Por último, se debe volver al home del sitio y descargar el certificado raíz a la computadora, luego se debe presionar el botón derecho del mouse sobre el archivo y seleccionar instalar certificado y continuar con la instalación por defecto.

III.14 Derechos

Los usuarios o titulares de firmas electrónicas, de conformidad con el artículo 29 del Reglamento, tendrán los siguientes derechos[83]:

a) A ser informado por el prestador de servicios de certificación, de las características generales y de los procedimientos de creación y de verificación de la certificación.

b) A la confidencialidad en la información proporcionada a los prestadores de servicios de certificación.

c) A ser informado, antes de la emisión de un certificado, del precio de los servicios de certificación.

d) A que el prestador de servicios le proporcione la información sobre el lugar en el que se le atenderá en caso de necesitar asesoría.

e) A ser informado, de todo tipo de sanción que le sea impuesta al prestador de servicios de certificación por la entidad autorizadora.

f) A ser informado, al menos con dos meses de anticipación, por los prestadores de servicios de certificación, del cese de su actividad.

g) A ser informado inmediatamente de la cancelación de la inscripción en el registro de prestadores autorizados.

[83] Artículo 29 del Acuerdo Gubernativo 135-2009

h) A traspasar sus datos a otro prestador de servicios de certificación;
i) A que el prestador no proporcione más servicios y de otra calidad que los que haya pactado.
j) A acceder, por medios electrónicos, al registro de prestadores autorizados.
k) A ser indemnizado y hacer valer los seguros comprometidos, conforme al reglamento.

III.15 Obligaciones

El poseedor de un certificado o de una firma electrónica deberá actuar con la diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma, así como también deberá actuar sin dilación indebida, utilizar los medios que le proporcione el prestador de servicios de certificación conforme lo establece la 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:

a) El firmante sabe que los datos de creación de la firma han quedado en entredicho.
b) 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[84].

Cuando se emplee un certificado para refrendar una firma electrónica, se debe actuar con diligencia razonable para cerciorarse de que todas las declaraciones que se hayan hecho en relación con el ciclo vital del certificado o que hayan de consignarse en él son exactas y cabales; ya que serán a cargo del firmante las

[84] Artículo 35 del Decreto 47-2008 del Congreso de la República de Guatemala, Ley para el reconocimiento de las comunicaciones y firmas electrónicas.

consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos establecidos en la Ley. (Artículo 35 del Decreto Número 37-2008 del Congreso de la República de Guatemala).

Asimismo los usuarios de certificados quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a brindar declaraciones exactas y completas. Además, estarán obligados a custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que les proporcione el certificador, y a actualizar sus datos en la medida que estos vayan cambiando.

Capítulo IV: Análisis comparativo de las legislaciones que contemplan la firma electrónica

IV.1 Análisis de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas de Guatemala

La Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas es el Decreto Número 47-2008 del Congreso de la República de Guatemala, emitido en el Palacio del Organismo Legislativo, en la Ciudad de Guatemala el 19 de agosto del año dos mil ocho, la cual fue publicada el 23 de septiembre de 2008 y entró en vigencia el 3 de octubre del mismo 2008.

Se encuentra basada en varios cuerpos normativos internacionales, dentro de ellos la Ley Modelo de la CNUDMI sobre Firmas Electrónicas, creada por la Comisión de las Naciones Unidas para el Comercio Internacional. Regula los siguientes aspectos: El comercio electrónico, reconocer la validez de los documentos y la contratación electrónica, certeza jurídica a medios electrónicos.

Está compuesta por 3 títulos, 7 capítulos y 56 artículos.

El ámbito de aplicación de la ley fue creado para ser aplicable a todo tipo de materias, y no sólo en el campo mercantil, para el área tanto pública como privada, nacional e internacional. Los efectos legales que contempla abarcan diversos ámbitos del derecho tanto laboral, como civil, administrativo y tributario. (Artículo 1 Decreto 47-2008)

Esta normativa no fue promulgada para crear derechos sino solamente reconocerlos, tampoco crea medios de comunicación electrónicos sino sólo busca reconocerlos y extiende a dichas comunicaciones las nociones tradicionales de los documentos contenidos en papel. Deja atrás la noción de que el documento es de papel al crear el criterio del “equivalente funcional”, al

otorgarle el mismo valor jurídico a las comunicaciones electrónicas que a las realizadas en papel.

En cuanto a la interpretación, hace referencia en su artículo 3 a que hay que tener en cuenta el origen internacional de la ley, 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. Todo aquello que no se encuentre regulado en ella se regirá por los principios generales que la inspiran tales como la neutralidad respecto a los medios técnicos empleados, no discriminación entre las firmas electrónicas nacionales y las extranjeras, la autonomía de las partes y el origen internacional de la Ley.

Un aspecto de especial importancia se encuentra en los artículos 11 y 12 de la Ley, los cuales contemplan la admisibilidad y fuerza probatoria de las comunicaciones electrónicas, ya que al amparo de esta norma 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. Es sobre este punto sobre el que radica la importancia de la validez y el registro de las entidades prestadoras del servicio de certificación, ya que las comunicaciones electrónicas tendrán el mismo valor jurídico que los documentos presentados en papel con autorización notarial. Dichas entidades ejecutan funciones de notario al autenticar la firma del emisor del mensaje con lo que se cumplen las funciones de identidad, confidencialidad, integridad y no repudio, de la firma electrónica.

Al valorar la fuerza probatoria de una comunicación electrónica 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.

Esta fuerza probatoria que le es otorgada a las comunicaciones electrónicas se asemeja a la fuerza de que gozan la formación y validez de los contratos cuya oferta y / o aceptación se hayan generado por vía electrónica (es decir entre ausentes), ya que surten los mismos efectos jurídicos que los elaborados en papel.

En cuanto a los efectos jurídicos de una firma electrónica simple o una avanzada se le otorga el mismo valor jurídico que al de la firma manuscrita, aunque excluye de esta norma general a las disposiciones por causa de muerte, como por ejemplo los testamentos, y a los actos jurídicos del derecho de familia como podría ser el matrimonio.

Crea la figura del Registro de Prestadores de Servicios de Certificación por medio del Acuerdo Gubernativo 385-2008 el cual reformó el Reglamento interno del Ministerio de Economía donde están creadas las dependencias de dicho ministerio, describiendo sus funciones básicas.

Dicho registro es el encargado de la función de inspección, control y vigilancia de las actividades realizadas por las entidades prestadoras de servicios de certificación, así como emitir las normas técnicas aplicables. Para llevar a cabo esta labor el Registro creó cuatro guías para que los prestadores de servicios de certificación puedan presentar su documentación y tengan claras las evaluaciones que debe realizar el Registro; las guías son: Solicitud, Guía de evaluación inicial, Guía de Inspecciones periódicas y Manual de operaciones.

El reglamento de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas es el Acuerdo Gubernativo número 135-2009 del 8 de mayo de 2009, el cual cuenta con 45 artículos que establecen temas como el uso de la firma electrónica por los organismos del Estado, de los prestadores de servicios

de certificación, sobre los certificados de firma electrónica, de la autorización e inspección de los prestadores de servicios de certificación, los derechos y obligaciones de los usuarios de firmas electrónicas, del Registro de Prestadores de Servicios de Certificación y el procedimiento para la imposición de sanciones a los prestadores de servicios de certificación.

IV.2 Análisis comparativo de las legislaciones de México, España y Chile que han aprobado la firma electrónica

México

La legislación mexicana en materia de firma electrónica se caracteriza por no contar con un cuerpo legal específico como es el caso de Guatemala, España, Chile, entre otros. México, por su lado publicó en su Diario Oficial de la Federación, el 29 de mayo del año 2000, el Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal (ahora Código Civil Federal), del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor[85].

Antes de regularse lo relativo a las comunicaciones electrónicas y la firma electrónica que requerían la forma escrita para su validez lo eran si estaban por escrito en papel y firmados con firma ológrafa. A partir del año 2000 en México se incorporó la modalidad por medio de la cual se le otorga la misma validez jurídica a los documentos firmados por firma electrónica que los firmados con firma ológrafa. [86] Asimismo, en materia mercantil y en la civil cuando la ley exija la forma escrita para los contratos y la firma de los mismos estos supuestos se

[85] Reyes Krafft, Alfredo, La firma electrónica y las entidades de certificación, Editorial Porrúa, México 2004.
[86] Artículo 1834 bis. Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor.

tendrán por cumplidos si se realiza por medio de mensajes de datos siempre y cuando se puedan consultar posteriormente[87]

Las reformas al código de comercio mexicano establecieron una equivalencia funcional entre la forma escrita y la forma electrónica, siempre que la información contenida en el mensaje de datos se mantenga íntegra y sea accesible para su posterior consulta, independientemente del formato en el que se encuentre.[88] De esta equivalencia funcional se desprende el hecho de que al igual que los medios escritos pueden constituir prueba en juicio. En el Código Federal de Procedimientos Civiles se reconoció como medio de prueba la información generada por medios electrónicos; para valorar la fuerza probatoria de los mismos será estimada la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada la información.[89]

Además las reformas establecen una presunción que permite pacto en contrario por medio de la cual se presume que el mensaje proviene del emisor cuando el mismo ha sido enviado usando medios de identificación tales como claves o contraseñas de él o por un sistema de información previamente programado por el supuesto original emisor de la información con su nombre que opere automáticamente, esto en materia mercantil.[90]

Dentro de las reformas tanto al código civil como al mercantil se modificó también la Ley Federal de Protección al Consumidor en el mismo Decreto de fecha 29 de mayo de 2000. Por medio de dicha reforma se reconoce la utilización de medios

[87] Artículo 93 del Decreto por el que se reforman y adicionan disposiciones del Código de Comercio en materia de Firma Electrónica, del 29 de agosto de 2003.
[88] Artículo 93 del Decreto por el que se reforman y adicionan disposiciones del Código de Comercio en materia de Firma Electrónica, del 29 de agosto de 2003.
[89] Artículo 1298 A, del Decreto Decreto por el que se reforman y adicionan disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor del 29 de mayo de 2000.
[90] Artículo 90 y 91 bis del Decreto por el que se reforman y adicionan disposiciones del Código de Comercio en materia de Firma Electrónica, del 29 de agosto de 2003.

electrónicos para las operaciones celebradas entre proveedores y consumidores con consecuencias jurídicas para quienes no cumplan con lo establecido en dichas reformas. [91]

El Decreto de Reformas al Código de Comercio en materia de Firma Electrónica fue aprobado en la Cámara de Diputados el 26 de noviembre del 2002 con el voto favorable de 422 votos y 1 abstención; el proceso legislativo fue aprobado por el Senado de la República el 8 de abril de 2003. [92]

Las reformas del Decreto del año 2000 se apega a las normas recomendadas por la Ley Modelo de las Naciones Unidas para el Derecho Mercantil Internacional (DNUDMI), así como reconoce como Autoridad Registradora Central a la Secretaría de Economía (además de Banco de México y la Secretaría de la Función Púbica) y no descuida el reconocimiento y validez de los certificados digitales[93].

España

España fue uno de los primeros países en reconocer la necesidad de un marco jurídico básico adecuado para la regulación de la firma electrónica, y publicó el 17 de septiembre el Real Decreto Ley 14/1999, en el cual se establecen las normas que deben seguirse en el uso de la firma electrónica.

Con el paso del tiempo, este decreto, presentó algunas deficiencias por lo que hoy en día ya está aprobada la nueva Ley 59-2003 que sustituye a la anterior.

Dentro de la nueva normativa se contempla que los documentos deben cumplir con cierta seguridad para ser válidos:

---

[91] Artículo cuatro por el que se reforma el párrafo primero del artículo 128, y se adiciona la fracción VIII al artículo 1o., la fracción IX bis al artículo 24 y el Capítulo VIII bis a la Ley Federal de Protección al Consumidor.

[92] Reyes Kraft, Alfredo, Comparativo entre firma electrónica México y España, consultado: catarina.udlap.mx/u_dl_a/tales/documentos/...i.../capitulo6.pdf, con fecha: 17 de septiembre de 2009.-

[93] Loc. Cit. Pág. 84

Seguridad técnica, por medio de la cual las comunicaciones privadas se mantienen auténticas e íntegras inter partes. Y garantiza la seguridad e integridad de las mismas al mantenerlas libres de hackers.

Seguridad jurídica, se refiera a una normativa por medio de la cual se asegura una responsabilidad para quienes infrinjan las normas con hechos ilícitos cometidos en la red.

Seguridad económica que agiliza las transacciones comerciales realizadas por medio electrónico.

Seguridad de los consumidores ante abusos de empresas que se aprovechen con normas contractuales que puedan perjudicar el tráfico mercantil y constituir una forma de aprovecharse del consumidor.

Para garantizar el cumplimiento de la integridad, el no rechazo, la confidencialidad y la autenticidad, en España se emplean dos grandes alternativas, el sistema de criptografía simétrica y el de criptografía asimétrica.

La actual normativa española está contemplada en la Ley 59-2003 del 19 de diciembre la cual cuanta con seis títulos que contemplan las disposiciones generales, los certificados electrónicos, el documento nacional de identidad electrónico, la prestación de servicios de certificación, en donde se incluyen las responsabilidades y obligaciones, lo relativo a los dispositivos de firma electrónica y sistemas de certificación de prestadores de servicios de certificación y de dispositivos de firma electrónica, la certificación de prestadores de servicios de certificación y de dispositivos de creación de firma electrónica, la supervisión y control y las disposiciones adicionales; para hacer un total de treinta y seis artículos.

Chile

En el caso de Chile la norma que contempla todo lo relacionado con la firma electrónica es la denominada Ley sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma No. 19.799 publicada en el Diario Oficial el 12 de abril de 2002. Dicha normativa está conformada por veinticinco artículos distribuidos en siete títulos que regulan los siguientes temas: disposiciones generales, uso de firmas electrónicas por los órganos del Estado; los prestadores de servicios de certificación; los certificados de firma electrónica; la acreditación e inspección de los prestadores de servicios de certificación; los derechos y obligaciones de los usuarios de firmas electrónicas y lo relativo a los reglamentos.

La norma chilena se encuentra fundamentada en los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalente del soporte electrónico al soporte de papel. Por lo contemplado en capítulos anteriores, se rige por los mismos principios que contempla la Ley Modelo sobre firma electrónica de la CNUDMI. Dicha normativa recoge como actos no susceptibles de firmarse electrónicamente aquellos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante comunicación electrónica, como el caso de las escrituras públicas, todo acto que requiera inscripción en un registro especial, los libros de actas de directorios de sociedades anónimas, los pagarés con mérito ejecutivo, aquellos en que la ley requiera la concurrencia personal de alguna de las partes, aquellos relativos al derecho de familia. Regula además el aspecto tributario, aunque aún se contradice con otras normas que regulan la materia específica.[94]

La norma contempla un aspecto particular, la libertad de acreditación, según la cual para prestar servicios de certificación no es necesario que la empresa que

[94] Herrera, Rodolfo, Derecho Informático, Ediciones Jurídicas la Ley, Chile 2003.

los desee proporcionar lleve a cabo el proceso de acreditación ante la Subsecretaría de Economía, Fomento y Reconstrucción. Sin embargo, para que una empresa pueda otorgar certificados de firma electrónica avanzada, sí es necesario que se acredite previamente, de manera tal que una firma electrónica avanzada sólo podrá ser certificada por un prestador acreditado. El plazo de vigencia de los certificados de firma electrónica avanzada será de tres años.[95]

Comparación

Entre la normativa de México, España y Chile existen distintos tipos de regulación, la principal razón radica en que el Real Decreto ley fue creado en 1999, y el que lo sustituyó en el año 2003 mientras que en México la regulación para medios electrónicos no fue aprobada sino hasta el 2004, la norma de Chile se encuentra intermedia entre ambas legislaciones ya que fue aprobada en el año 2002. España es un Estado pionero en este tipo de leyes pues fue uno de los primeros en mostrar su preocupación por legislar las actividades electrónicas. El uso de los medios electrónicos es cada día más fuerte y actualmente la ley española es de las más completas. Dentro de las ventajas que presenta la ley española se encuentra el hecho de tener contemplado todo el cuerpo legal en materia de firma electrónica en una ley específica, lo que no sucede con la ley mexicana que se encuentra como reformas a una norma ordinaria, a diferencia de la norma chilena que también contempla todo en un solo cuerpo legal. En México no se permite que los trámites relacionados a la firma electrónica sean realizados por representantes de personas físicas lo que sí es permitido en la norma española, además la norma de España proporciona una mejor seguridad a los usuarios al contemplar infracciones y sanciones lo que no se establece en la norma de México ni la chilena. El período de validez de los certificados digitales en España es de 4 años, en Chile es de 3 y en México es de 2 años, en

[95] Arrieta, Raúl, Los prestadores de Servicios de Certificación de Firma Electrónica en el Derecho Chileno, Revista Chilena de Derecho Informático, Chile, 2006

este caso, debido a los avances tecnológicos, es recomendable menos tiempo ya que esta ciencia se encuentra en constante movimiento y cuanto más actualizado esté este sistema será mucho más eficiente. Como último punto, con respecto a la seguridad económica, ni en México ni en Chile es necesario pedir un respaldo económico por parte de los prestadores de servicios de certificación lo que sí es exigido en la norma española.

IV.3 Comparación de las entidades certificadoras de firma electrónica que funcionan en la actualidad en los países que han aprobado su funcionamiento

A partir de la entrada en vigencia de las distintas legislaciones a nivel mundial sobre la firma electrónica han surgido una serie de instituciones que apegadas a su marco legal correspondiente han empezado a prestar los servicios de certificación a nivel mundial, emitiendo certificados con validez tanto nacional como internacional. Existen países como Italia que cuenta con un número considerable de entidades certificadoras de firma electrónica y países como Guatemala en donde la legislación, el registro y en sí la figura jurídica es de tan reciente creación que no cuenta con ninguna entidad prestadora de servicios de certificación acreditada como tal por el Registro de Prestadores de Servicios de Certificación. Por el momento en el país, de conformidad con la información otorgada por la Cámara de Comercio de Guatemala, la entidad que se encuentra prestando el servicio es una entidad chilena denomina E-CERTCHILE, a través de dicha Cámara de Comercio, hasta que el Registro se establezca del todo y de inicio a la acreditación correspondiente.

Dentro de las entidades prestadoras de servicios de certificación se enumerarán las que funcionan en la actualidad en los países anteriormente analizados, Chile, España y México.

Entidades prestadoras de servicios de certificación en Chile[96]:

Acepta: Web: http://www.acepta.com/Contactenos/Index.html

CNC-ONCE: Web: http://www.cnc-once.cl/

E-Certchile: Web: http://www.e-certchile.cl/

e-Sign: Web: https://www.e-sign.cl .

Certinet: Web: http://www.certinet.cl

Entidades prestadoras de servicios de certificación en España:[97]

En España, la fuente principal es el Censo de Prestadores de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Comercio y Turismo. Este organismo mantiene la responsabilidad de supervisión del sector de la Certificación definida en la Ley 59/2003 de Firma Electrónica. En estos momentos, los Prestadores de Servicios de Certificación que han presentado la documentación y su revisión está finalizada o en curso son los siguientes:

ANF-AC: Asociación Nacional de Fabricantes Autoridad de Certificación. CERES: Fábrica Nacional de Moneda y Timbre (FNMT-RCM)

CAMERFIRMA

FIRMAPROFESIONAL

ACCV Autoridad de Certificación de la Comunidad Valenciana.

AC ABOGACÍA Consejo General de la Abogacía Española

[96] Ministerio de Economía Fomento y Turismo de Chile, http://www.economia.cl, Chile, 2010, Consultado: 03 de abril de 2010.

[97] Censo de Prestadores de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Comercio y Turismo, www.innovoto.com, España, 2010.- Consultado: 15 de marzo de 2010.-

CICCP Colegio de Ingenieros de Caminos, Canales y Puertos

ANCERT- Agencia Notarial de Certificación Agencia Notarial de Certificación S.L.

BANESTO

IZENPE Empresa de Certificación y Servicios, Izenpe, S.A.

CATCERT Agencia Catalana de Certificación

IPSCA

TELEFONICA DATA ESPAÑA S.A.

SERVICIO DE CERTIFICACION DE LOS REGISTRADORES (SCR)

Entidades prestadoras de servicios de certificación en México:[98]

ADVANTAGE SECURITY, S. DE R.L. DE C.V.

PSC WORLD, S.A. DE C.V.

CECOBAN

EDICOMUNICACIONES MÉXICO S.A. DE C.V.

[98] Cadena Sandoval, Carlos Alberto, Sistema Integral de gestión integral México, www.firmadigital.gob.mx, Consultado: 15 de marzo de 2010.-

Capítulo V: Ventajas futuras y económicas

V.1 Propuesta de mejoras a la ley de reconocimiento de las comunicaciones y firma electrónica en Guatemala

Uno de los factores que ha impedido un mayor desarrollo del comercio electrónico en Guatemala y en el mundo en general, es la inseguridad al momento de realizar transacciones electrónicas, debido a un sistema jurídico que no está adecuado para recoger exigencias del mismo. La mayor parte de las oportunidades para los emprendedores en Internet se perderá si los consumidores temen al fraude en el comercio en Internet. Este es un tema, por lo tanto, que interesa a todos, al comercio, al gobierno y a los consumidores, el dar la más alta prioridad a preservar la seguridad en Internet.

Otro aspecto de importancia en cuanto al poco uso que se le da al comercio electrónico en Guatemala, se refiere al costo, nuestro país es un país emergente en cuando al desarrollo tecnológico se refiere, la cultura de los sistemas informáticos aún no se encuentra arraigada en la población, el comercio continúa realizándose por los sistemas tradicionales y esto debido a que, para las pequeñas y medianas empresas, el costo que les generaría incluír certificados electrónicos por cada pequeña transacción que realizaran elevaría mucho el costo final de su producto, razón por la cual el empleo de estos medios se presenta como una opción factible para empresas multinacionales o empresas que generan contratos de cifras elevadas para quienes costear un certificado electrónico para obtener una mayor seguridad en sus transacciones por via electrónica no supondría un sacrificio mayor como sí lo sería para las pequeñas y medianas empresas. En Guatemala podría ser la causa por la cual no se ha visto la necesidad de Entidades Prestadoras de Servicios de Certificación, porque el comercio en sí aún no lo ha exigido, ya que aún es un país que no cuenta con el desarrollo tanto tecnológico, cultural ni económico como para necesitar el empleo de estas tecnologías en su comercio actual.

El Decreto 47-2008 del Congreso de la República de Guatemala, Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, publicada el 23 de septiembre de 2008 cuya entrada en vigor inició el 3 de octubre de 2008 es una norma que se apega a los estándares internacionales propuestos por la Comisión de las Naciones Unidas para el Comercio Internacional en la Ley Modelo de la CNUDMI sobre Firmas Electrónicas.

Se trata de una norma que viene a regular cuestiones que no se contemplaban en ningún cuerpo normativo como lo son: el comercio electrónico en general, la seguridad jurídica y técnica en la transmisión de los mensajes electrónicos, la validez y eficacia de los documentos electrónicos y de las firmas electrónicas y el comercio electrónico en materias específicas.

Contractualmente sí se habían regulado cuestiones similares como es el caso del pago electrónico de impuestos a través de BANCASAT (Ley Orgánica de la Superintendencia de Administración Tributaria SAT, art. 7), o el caso de BANCARED como proveedor de servicios de certificación digital y firmas digitales; pero como se mencionó anteriormente fue una normativa contractual que no posee los mismos efectos de una norma positiva de generalidad, coercitividad y observancia obligatoria para toda la nación, características con las que sí cumple el Decreto 47-2008 del Congreso de la República de Guatemala.

Se trata pues de una normativa que pretende determinar el tiempo o momento, el lugar de envío y recepción de las comunicaciones electrónicas que completen las normas tradicionales sobre el envío y recepción, sólo que transponiéndolas a un entorno electrónico. Una legislación nacional que asegura que el marco legal adoptado sea compatible con las normas internacionales y no sea discriminatorio con firmas y documentos electrónicos de otros países.

Conviene recordar en este punto de la investigación las causas que originaron la misma; siendo la hipótesis inicial la siguiente:

La Ley para el Reconocimiento de la Comunicaciones y Firma Electrónica, Decreto 47-2008, posee algunas inconsistencias en cuanto a la normativa y regulación de las entidades certificadoras de firma electrónica especialmente respecto a garantizar un servicio eficiente y confiable que propicie el comercio internacional.

En el planteamiento del problema se indicaron cuestiones tales como:

¿Qué requisitos deben observar las sociedades que sean autorizadas para convertirse en entidades certificadoras? ¿Tendrán que tener un capital mínimo? ¿Pueden ser sociedades anónimas? Esto debido a que en la ley en ningún momento se especifican los requisitos que deben llenar las entidades certificadoras, quiere esto decir que ¿cualquiera puede convertirse en una entidad certificadora?, ¿cómo se calificará la idoneidad para constituir este tipo de sociedad?

A pesar de que a lo largo de la investigación fue posible responder a la mayoría de las cuestiones planteadas en la hipótesis y el planteamiento del problema con la ayuda de la legislación que entró en vigencia a lo largo del desarrollo del trabajo, aún quedan ciertos aspectos que podrían suscitar problemas futuros que en algún momento podrían recogerse en el Decreto 47-2008 del Congreso de la República de Guatemala, y que a continuación se presentan como propuesta de mejoras a la ley.

En el artículo 33 de la Ley se establecen en su párrafo segundo los documentos que no pueden firmarse electrónicamente, se especifican las disposiciones por causa de muerte y los actos jurídicos del derecho de familia. Esta normativa deja una duda con respecto a documentos tales como aquellos en los que la ley exige una solemnidad específica como las escrituras públicas, o los actos que requieran inscripción en el registro, los títulos ejecutivos, ya que da a entender que únicamente las disposiciones por causa de muerte y los actos jurídicos del

derecho de familia no se pueden firmar electrónicamente, todo lo demás sí. En este caso, por ejemplo para los títulos ejecutivos, tendrían el mismo valor jurídico si fueran electrónicos, se cumple con lo que establece el código de comercio sobre qué es un documento que incorpora un derecho. La ley para el reconocimiento de las comunicaciones y firmas electrónicas vino a complementar ciertos aspectos en relación a la contratación entre ausentes regulada en el Código Civil Decreto Ley 106, por ejemplo, pero con esto no se quiere decir que haya modificado dichas normas sino que únicamente incrementó lo relativo a la contratación electrónica entre ausentes, sin modificar ni derogar leyes para este caso específico.

Otro aspecto que no fue encontrado en el Decreto 47-2008 ni en su reglamento es sobre si los prestadores de servicios de certificación pueden entregar certificados en actos en los que ellos mismos sean parte o tengan cualquier tipo de interés económico directo o indirecto, esto debido a que de poder hacerlo se podría generar el problema del conflicto de intereses, un aspecto de especial importancia en cuanto a la facilidad que presenta para la comisión de estafas y fraudes empresariales.

Con relación al aspecto tributario, de conformidad con la ley, los actos y contratos suscritos por medio de firma electrónica serán válidos de la misma manera y producirán los mismos efectos jurídicos que los celebrados por escrito y en soporte de papel y que dichos actos y contratos se reputarán como escritos para todos los efectos legales. De tal manera que dichos documentos electrónicos pueden dar cuenta de un acto o contrato que constituya un hecho gravado por algún impuesto; en relación a este tema la Ley no reguló específicamente sobre quién recae la obligación tributaria del pago del impuesto generado; como por ejemplo en el caso de los actos notariales como las certificaciones notariales y las legalizaciones por ejemplo; que gravan impuestos

y hacen plena prueba. Es decir que en el texto de la Ley y del reglamento no se reguló la cuestión tributaria de la función notarial.

Estos tres aspectos son las propuestas de este trabajo de investigación; y a continuación se detallan los aspectos del planteamiento del problema a los cuales se les ha dado solución resultado del análisis de la distinta normativa que ha entrado en vigencia con posterioridad de la Ley del año 2008.

Dentro de las cuestiones resueltas con el Acuerdo Gubernativo Número 135-2009 que entró en vigencia el 8 de mayo del año 2009, se encuentran: la ampliación de las obligaciones de los prestadores de servicios de certificación, la determinación específica sobre quienes pueden ser entidades de certificación, lo relativo al seguro de responsabilidad civil que es un aspecto contemplado en otras legislaciones internacionales consultadas como la de Chile y España y es un aspecto que no se contempla en la Ley de Guatemala sino en su Reglamento, en el artículo 16 del Reglamento, por lo tanto, se especifica que la suma asegurada debe ser por lo menos de doscientos mil dólares de los Estados Unidos de América, y además que los prestadores autorizados deberán mantener este seguro durante todo el periodo que contemple su autorización y el año siguiente a su término, cese o revocación, cuando sea sancionado con suspensión temporal y si se hubiere iniciado procedimiento administrativo o judicial en su contra que concluya el mismo. Este es un aspecto que asegura la integridad de las entidades que presten el servicio de certificación ya que las obliga a asegurar su responsabilidad hasta por un período de un año posterior a su suspensión de actividades, con esto se consigue que no cualquiera pueda valerse de esta institución para efectuar fraudes tan fácilmente.

Otro aspecto que no se encuentra en la ley y sí en su reglamento es lo relativo al proceso de autorización e inspección de los prestadores de servicios de certificación, ya que en el artículo 23 se establece que para ser autorizado como prestador de servicios de certificación se deberá cumplir con demostrar la

habilidad necesaria de sus servicios, garantizar la existencia de un servicio seguro de consulta del registro de certificados emitidos, emplear personal calificado para la prestación de los servicios ofrecidos y los procedimientos de seguridad y de gestión adecuados, utilizar sistemas confiables que garanticen la seguridad de sus procesos de certificación, haber contratado un seguro apropiado a los términos exigidos por la norma, contar con la capacidad tecnológica necesaria para el desarrollo de la actividad de certificación y cumplir con todas las regulaciones emitidas por el Registro.

Con esta norma se responde a la pregunta de quiénes pueden realizar estos servicios, ya que aunque puede ser cualquier persona jurídica nacional o extranjera, pública o privada domiciliada en la República de Guatemala, esta serie de requisitos delimitan a la persona que lleve a cabo este tipo de actividad. Con respecto a los requisitos que debe cumplir, el Registro de Prestadores de Servicios de Certificación ha emitido una serie de guías en las cuales se especifican toda la documentación que deberán presentar las personas interesadas en realizar los servicios de certificación, (dichas guías se adjuntan a la presente investigación). De esta manera se lleva a cabo una revisión por parte de dicho Registro, revisión que se muestra en el capítulo I bajo el epígrafe de procedimiento de evaluación, por medio de la cual se determina la idoneidad del solicitante a ser entidad prestadora de servicios de certificación[99].

El establecer una guía de evaluación favorece a determinar si las obligaciones contenidas en el artículo 13 del Reglamento 135-2009 pueden ser cumplidas por las entidades solicitantes, establece un parámetro para que no cualquiera pueda ser prestador de servicios de certificación y de esta manera preserva el status

[99] El fundamento jurídico para la obligatoriedad de las guías emitidas por el Registro de Prestadores de Servicios de Certificación se encuentra en el artículo 49 inciso j) del Decreto 47-2008 el cual establece que dentro de las funciones de dicho Registro se encuentran las de impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las prestadoras de servicios de certificación lo que se ha interpretado que se realiza a través de las guías emitidas por el mismo.

jurídico de esta institución de la firma electrónica, volviéndola mucho más segura y confiable y apegada a la realidad internacional que constituye el ámbito de funcionamiento de esta institución.

Con respecto a las preguntas esbozadas en el planteamiento del problema se puede responder que:

¿Qué requisitos deben observar las sociedades que sean autorizadas para convertirse en entidades certificadoras?

Dentro de los requisitos que deben observar las sociedades que sean autorizadas para convertirse en entidades certificadoras se encuentran: se deberá cumplir con demostrar la habilidad necesaria de sus servicios, garantizar la existencia de un servicio seguro de consulta del registro de certificados emitidos, emplear personal calificado para la prestación de los servicios ofrecidos y los procedimientos de seguridad y de gestión adecuados, utilizar sistemas confiables que garanticen la seguridad de sus procesos de certificación, haber contratado un seguro apropiado a los términos exigidos por la norma, contar con la capacidad tecnológica necesaria para el desarrollo de la actividad de certificación y cumplir con todas las regulaciones emitidas por el Registro. Asimismo presentar todos los documentos relacionados en las guías de evaluación y solicitud elaboradas por el Registro de Prestadores de Servicios de Certificación que se adjuntan en los anexos.

¿Tendrán que tener un capital mínimo?

A la pregunta sobre si deberán contar con un capital mínimo, no se le puede dar una respuesta basada en la ley debido a que la misma no establece nada al respecto, por lo que sigue constituyendo una duda que se presta a diferentes interpretaciones, lo que sí establece el Reglamento es que las mismas deben cancelar un arancel al momento de inscribirse y registrarse, de acuerdo al Acuerdo Gubernativo 109-2010 de fecha 13 de abril de 2010.

¿Pueden ser sociedades anónimas?

Sobre el aspecto de si pueden ser sociedades anónimas la ley determina que deben ser personas jurídicas por lo tanto se deduce que sí se puede tratar de una sociedad anónima, al igual que de una sociedad de responsabilidad limitada o cualquiera otra de las contempladas en el Código de Comercio Decreto 2-70 de Guatemala. Asimismo pueden ser entidades públicas aunque las mismas no entrarían dentro de la denominación de sociedades contempladas en el Código de Comercio. Ya que el artículo 40 del Decreto Número 47-2008 establece que pueden ser personas jurídicas, tanto públicas como privadas. Y en el artículo 42 del mencionado Decreto se establece específicamente las obligaciones de las sociedades de certificación, cuando en el caso de las entidades públicas las mismas no son sociedades, esto representa una de las inconsistencias legislativas que se presentan a lo largo del texto de la Ley que pueden causar diversas interpretaciones, ya que al no ser las entidades gubernamentales sociedades mercantiles estarían o no obligadas a cumplir con el artículo 42 de la Ley, en este caso se entendería que no, pero al no existir una norma específica para las relaciones electrónicas entre entidades públicas se deduce que deben regirse por dicho Decreto 47-2008 por lo que deben acatar estas normas aún sin ser mencionadas específicamente en el texto del artículo.

¿Cualquiera puede convertirse en una entidad certificadora?

Este es un aspecto que se determina más que en la ley en las guías de evaluación, ya que cualquier persona jurídica puede tener el deseo de ser entidad prestadora de servicios de certificación, pero lo serán sólo aquellas que cumplan con todos los requisitos detallados en la guía de evaluación la cual contiene además de los documentos para identificar al solicitante, requisitos tales como declaración de prácticas de Certificación, políticas de certificado, manual de operaciones de la autoridad certificadora, procedimientos de seguridad, y sobre todo contar con la tecnología necesaria y adecuada para realizar dicha

actividad, por lo tanto se limita un poco la capacidad a aquellas persona que cuenten con los recursos económicos de inversión en la tecnología necesaria y en los conocimientos que esta práctica requiere ya que se trata de una combinación de aspectos jurídicos con aspectos técnicos de ingeniería en sistemas con los que hay que contar para poder prestar el servicio. El fundamento jurídico para la obligatoriedad de las guías emitidas por el Registro de Prestadores de Servicios de Certificación se encuentra en el artículo 49 inciso j) del Decreto 47-2008 el cual establece que dentro de las funciones de dicho Registro se encuentran las de impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las prestadoras de servicios de certificación lo que se ha interpretado que se realiza a través de las guías emitidas por el mismo.

¿Cómo se calificará la idoneidad para constituir este tipo de sociedad?

La idoneidad de las personas solicitantes se calificará con una nota dividida de la siguiente forma:

C Cumple Totalmente

S Posee un apego Suficiente del requisito exigido

I Insuficiente

Cada uno de los requisitos especificado en la guía de evaluación será calificado con una de las notas anteriormente descritas, realizada la evaluación, la entidad autorizadora se pronunciará sobre el cumplimiento de los requisitos y obligaciones necesarias para ser un prestador de servicios de certificación autorizado. Dicha declaración será emitida cuando un prestador de servicios de certificación cuente con una calificación C (CUMPLE) en cada uno de los requisitos evaluados. Una vez declarada la autorización, el interesado dispone de un plazo de 30 días calendario para presentar la póliza de seguros que exige el artículo 16 del reglamento, bajo apercibimiento de ser rechazada su solicitud si no lo cumple. Cubiertos todos los requisitos la entidad es inscrita en el Registro

de Prestadores de Servicios de Certificación para iniciar su labor, dando siempre debida cuenta de sus actividades a dicho Registro.

V.2 Ventajas económicas que puede proporcionar la existencia de entidades certificadoras de firma electrónica a largo plazo

La certificación digital es el único medio que permite garantizar técnica y legalmente la identidad de una persona en Internet. Se trata de un requisito indispensable para que las instituciones puedan ofrecer servicios seguros a través de Internet. Asimismo el certificado digital permite la firma electrónica de documentos en donde el receptor del mismo puede tener la seguridad de que éste es el original y no ha sido manipulado y el autor de la firma electrónica no podrá negar la autoría de esta firma. El certificado digital permite cifrar las comunicaciones. Solamente el destinatario de la información podrá acceder al contenido de la misma.

Por lo tanto la principal ventaja de la certificación radita en que el disponer de un certificado ahorrará tiempo y dinero al realizar trámites administrativos en Internet, a cualquier hora y en cualquier lugar, se evitarán los formalismos de papeleos innecesarios y los rigorismos de las horas de atención al público, ya que desde cualquier computadora con acceso a Internet se podrán enviar mensajes, documentos, ofrecer o cerrar contratos que superan la barrera del tiempo y el espacio.

Esto genera grandes beneficios para las empresas que lo utilicen, tanto del lado del emisor como del receptor. Existen ventajas futuras que van desde las puramente económicas hasta las ecológicas, ya que esto permitirá el ahorro de costos de mensajería, el papel, la impresión, la contratación de personal que realice la labor; mejora la eficacia ya que se cuenta con la completa seguridad de que el mensaje llegará a su destino en un fracción de tiempo más o menos corta, y a la persona que se desee que llegue dicho mensaje, con la seguridad de que

el mismo no será alterado y será entregado a la persona correcta. Optimiza la economía, se logra obtener información en tiempo real, ya no es necesaria la espera de horas o días enteros para obtener la información necesaria, el negocio se puede ofrecer por esta vía y cerrarse en cuestión de minutos después, contribuyendo así a la celeridad del tráfico comercial.

Se reduce el tiempo de gestión de una actividad, contribuyendo esto a que en las empresas se puedan realizar otras labores en menor tiempo, ya que algo que podría llevar días se lleva a cabo en minutos y el tiempo restante se emplea en iniciar una nueva actividad.

Contribuye a la agilidad en la toma de decisiones, esto derivado de la facilidad de obtener información en tiempo real, pues se dispone de todos los elementos necesarios a la mayor brevedad posible y con esto se podrá agilizar la discusión y toma de una decisión. Se mejora el control de acciones erróneas y se obtiene un manejo eficaz de los recursos financieros de la empresa.

El objetivo principal es la simplificación de los procesos, el uso de certificados digitales para la comunicación vía electrónica facilitará y mejorará las relaciones internacionales y nacionales al ahorrar tiempo y dinero.

Para obtener estos beneficios económicos a nivel empresa e incluso a nivel individual es necesaria la creación de entidades prestadoras de servicios de certificación debidamente acreditados ante el Registro de Prestadores de Servicios de Certificación, ya que se trata de una figura jurídica que traerá grandes beneficios a la economía del país, facilitará el comercio internacional permitiendo que las pequeñas y medianas empresas puedan comercial sin la necesidad de trámites notariales engorrosos que incrementen los costos de operación de las negociaciones, esto no quiere decir que el papel de los notarios no sea menoscabado por dicha figura jurídica, pero sí puede ser mejorado al automatizarse servicios, debido a que la ley no especifica qué tipo de profesiones

pueden dedicarse a la prestación de dicho servicio, los notarios pueden implementar dentro de los servicios que prestan el de certificación y convertirse en una especie de notario cibernético lo que contribuirá a la facilitación de la prestación de los servicios.

Las entidades prestadoras de servicios de certificación son una institución empleada ya en muchos países del mundo un breve ejemplo fue la enumeración realizada anteriormente de las que funcionan actualmente en el mundo en países como Chile, México y España. Como se puedo observar España es de los países que cuentan con un mayor número de entidades prestadoras de servicios de certificación en comparación con los otros países, esto puede deberse a diversas razones, una de ellas es el tiempo de experiencia que este país posee en materia de firma electrónica ya que es uno de los pioneros de dicha figura jurídica, otra es la legislación que las ampara ya que contempla una variedad de situaciones apegadas a la realidad actual y al ámbito internacional al que esta figura pertenece lo que trae consigo que las sociedades o personas que deseen dedicarse a esta actividad lo realicen con total transparencia y legalidad.

Asimismo Chile posee una legislación que ha permitido que la figura jurídica de la firma electrónica vaya tomando un auge bastante grande en este país, inclusive como se mencionó en capítulos anteriores es precisamente una entidad prestadora de servicios de certificación en dicho país la que se encuentran prestando sus servicios en Guatemala.

Guatemala es un país que recién acaba de ingresar a esta era informática, es un novato en este tipo de formas de negociación, su Registro es de reciente creación y aún está dando sus primeros pasos, la legislación con la que se cuenta en Guatemala es bastante completa y se apega realmente a los estándares internacionales proporcionados por la Ley Modelo de la CNUDMI sobre Firmas Electrónicas lo que permite que en el país se instalen Entidades Certificadoras nacionales que traigan consigo muchos frutos económicos

derivados de la confianza y la seguridad que constituyen la principal característica de esta institución. La inversión, importación y exportación de empresas y productos guatemaltecos se podrá realizar con una mayor facilidad si se emplean los medios electrónicos que la legislación proporciona.

ANÁLISIS DE LAS ENTREVISTAS REALIZADAS

Las preguntas presentadas en las entrevistas fueron las siguientes:

1. Con relación a las legislaciones sobre Firma Electrónica vigentes en España, Argentina y México ¿cuál considera que contempla de una mejor manera la regulación de las Entidades Certificadoras de Firma Electrónica?

A la primer pregunta los profesionales entrevistados respondieron predominantemente que la legislación Española es la que cuenta con una normativa mucho más completa y que ha ayudado como ejemplo a la legislación de Guatemala.

2. Considera que la Ley para el Reconocimiento de las Comunicaciones y Firma Electrónica, Decreto 47-2008 del Congreso de la República se ajusta a los estándares internacionales requeridos en materia de contratación electrónica?

De conformidad con las respuestas obtenidas todos los profesionales coincidieron en que Guatemala está apegada a las normas internacionales y que inclusive han tomado ya nuestra legislación como modelo para futuras legislaciones de otros lugares.

3. Considera que la legislación vigente en Guatemala con respecto a Firma Electrónica está acorde con lo legislado por la Ley Modelo de la CNUDMI Sobre las Firmas Electrónicas del año 2001 de la Comisión de las Naciones Unidas para el Derecho Comercial Internacional.

Por unanimidad la pregunta fue respondida positivamente, ya que todos afirmaron que de la lectura de la norma se logran observar los rasgos del modelo empleado para desarrollarla que fue la Ley Modelo de la CNUDMI sobre Firmas Electrónicas.

4. Considera que el Decreto 47-2008 del Congreso de la República posee deficiencias o que contemplaron todos los aspectos necesarios. ¿por qué?

Casi en su totalidad los profesionales coincidieron en resaltar el factor de la no aplicación real de la norma como un elemento determinante para no poder llegar a conocer a fondo las falencias o aciertos que esta legislación le puede traer al país.

5. Según su criterio ¿cuáles podrían ser los principales riesgos que se correrían ante un mal empleo de las normas para las Entidades Certificadoras de Firma Electrónica en la legislación vigente en Guatemala?

Dentro de los problemas futuros que resaltaron los entrevistados que pueden llegar a darse con la aplicación de esta figura jurídica se encuentra lo relativo al robo de identidad, las estafas electrónicas y diferentes tipos de crímenes cibernéticos que se han venido danto alrededor del mundo y que la legislación actual no es infalible de sufrirlos.

Por lo tanto, de los resultados obtenidos se puede concluir que la normativa guatemalteca en la materia de firma electrónica se ajusta a los estándares internacionales requeridos para la contratación internacional por la vía cibernética, lo que le brinda al país una posibilidad viable para realizar con una mayor seguridad las contrataciones por esta vía, así mismo que las normas empleadas como modelo para la realización de la misma son las consideradas como las que contemplan una mejor regulación en materia de entidades

certificadoras de firma electrónica, es decir la legislación de Argentina, México y España de las cuales España sigue obteniendo una mejor calificación por el nivel de experiencia que dicho país posee en esta materia.

Además se pudo establecer que no existe una opinión generalizada con respecto a si existen deficiencias o no en la norma ya que falta de implementación de la misma, no ha dado la oportunidad de que se presenten situaciones sin una contestación por lo que aún no se sabe a ciencia cierta qué tipo de situaciones se pueden presentar con la operatividad de la misma. No así, sí existe una opinión generalizada en relación a la posibilidad de vulnerabilidad que la norma presenta; que como toda situación legislada no es infalible de ser tergiversada para la comisión de algún delito en este caso delitos cibernéticos con los cuales se ha venido luchando a nivel mundial desde hace ya varios años.

ANALISIS DEL CUADRO DE COTEJO

En el cuadro de cotejo fueron comparados seis países que poseen vigente la normativa en relación a la firma electrónica: España, México, Chile, Argentina, Perú y Ecuador; a lo largo del análisis se encontraron diversidad de formas de regular la materia, en el caso de España por ejemplo su Ley 59/2003 del 19 de diciembre de 2003 es una reforma ya de la primer ley promulgada en 1999, pionera en la materia. La normativa española regula una seguridad técnica por medio de la cual las comunicaciones privadas se mantienen auténticas e íntegras entre las partes, garantiza la seguridad jurídica al establecer responsabilidades para quienes pretendan infringir las normas con actos ilícitos, y constituye una forma de garantizar la seguridad económica en las transacciones comerciales realizadas por la vía electrónica. Los consumidores se encuentran protegidos también a fin de evitar perjuicios en el tráfico mercantil. Además posee una particularidad que no presentan las demás legislaciones y es el que contempla dentro de la normativa de la firma electrónica lo relacionado al documento nacional de identificación. El registro está a cargo del Ministerio de Ciencia y Tecnología.

Por su lado en el caso de México la normativa no se encuentra regulada en un solo cuerpo legal como se ha mencionado como anterioridad sino que constituye una serie de reformas a los códigos civil, código de comercio y de la Ley Federal de Protección al consumidor. Las reformas a estas leyes son del 29 de mayo del año 2000, un año después de que España promulgara el Real Decreto reformado por el 59/2003. Es así como a partir del año 2000 en México se incorpora la modalidad de otorgarse igual validez jurídica a los documentos firmados por medio de firma electrónica y ológrafa. Se reconoce como prueba la información contenida en los medios electrónicos y se establece la obligación de guardar durante diez años los originales de las comunicaciones, asimismo se establece la presunción en materia mercantil de que salvo pacto en contrario, el mensaje

proviene del emisor. La legislación en relación a los prestadores de servicios de certificación y los certificados digitales no es amplia debido a que no se trata de una ley específica en la materia; y a diferencia de los otros países poseen tres entidades de registro: a) la autoridad Registradora Central a la Secretaría de Economía, b) Banco de México, c) Secretaría de la Función Pública. Asimismo posee una particularidad que no presentan las demás legislaciones y es que según la normativa mexicana pueden ser prestadores de servicios de certificación los notarios, los corredores públicos, las empresas privadas y las instituciones públicas.

En el caso de Chile la Ley No. 19.799 del 12 de abril del año 2002, en cuanto a su regulación sobre las entidades prestadoras de servicios de certificación contempla únicamente las responsabilidades por daños y perjuicios de los acreedores por el mal uso de sus funciones, no establece los requisitos que deben llenar, las sanciones, ni otros aspectos que sí se encuentran contenidos en otras legislaciones. En cuanto a los certificados digitales únicamente establecen cuales son los requisitos de los mismos y cuando quedan sin uso, no se establece un plazo para los mismos. Y pueden ser entidades prestadoras de servicios de certificación cualquier persona nacional o extranjera, pública o privada, registrada en la Subsecretaría de Economía, Fomento y Reconstrucción.

Argentina es de los países que poseen al igual que España una legislación bastante amplia en materia de entidades certificadoras y certificados digitales, su Ley es la 25.506 del 11 de diciembre del año 2001 y establece además un sistema de auditoría a las entidades cuestión que la legislación guatemalteca no posee, así como una comisión asesora para la infraestructura de la firma digital, lo que demuestra que es una materia que se encuentra en constante estudio y análisis para su mejoramiento. Pueden ser entidades prestadoras de servicios de certificación toda persona de existencia ideal, registro público de contratos y organismo público registrados en la Jefatura de Gobierno de Ministros.

Perú y Ecuador con sus leyes del año 2000 una y la otra del año 2002 son las legislaciones que poseen una regulación bastante escueta y con deficiencias de las seis analizadas, ya que en el caso de Perú en tan solo tres artículos contempla lo relacionado a las entidades certificadoras de firma electrónica, no contempla los requisitos de las mismas ni las obligaciones, ni sanciones al incumplimiento. En cuanto a los certificados digitales no establece los requisitos que deben llenar los mismos para su validez legal. Tampoco es clara la legislación con respecto a quienes pueden ser entidades certificadoras de firma electrónica y aún no cuentan con un registro de las mismas. Por su lado Ecuador con su ley del 10 de abril de 2002, no establece obligaciones para los usuarios ni requisitos para las entidades certificadoras de firma electrónica, la regulación de los certificados digitales es más amplia que la de Perú y según su normativa pueden ser entidades prestadoras de servicios de certificación las empresas unipersonales o personas jurídicas inscritas en la Superintendencia de Telecomunicaciones.

En conclusión de las anteriores legislaciones analizadas, España, México, Chile y Argentina constituyen los países que poseen una legislación apegada a las normas internacionales de la materia y que no dan lugar a diversidad de interpretaciones, a diferencia de las normas de Perú y Ecuador que cuentan aún con deficiencias.

CONCLUSIONES

1. La Ley para el reconocimiento de las comunicaciones y firmas electrónicas entró en vigencia el 3 de octubre de 2008, conformada por 56 artículos que regularon las cuestiones recomendadas por la Ley modelo sobre firmas electrónicas de la CNUMDI del año 2002, así como otras relacionadas a las necesidades específicas del país en materia electrónica. Lo relativo al comercio electrónico en general, el comercio electrónico en materias específicas y ciertas disposiciones complementarias al comercio electrónico tales como los efectos jurídicos de la firma electrónica avanzada, las obligaciones y derechos de los prestadores del servicio y de la parte que confía en el mismo y la creación del Registro de Entidades Prestadoras de Servicios de Certificación, entre otras cuestiones. Dicha normativa dejó ciertas dudas como por ejemplo los requisitos que debían observar las sociedades autorizadas para ser entidades prestadoras de servicios de certificación, si debían tener un capital mínimo, si podían ser sociedades anónimas entre otras, cuestiones que posteriormente fueron resueltas con la entrada en vigencia el 8 de mayo de 2009 del Acuerdo Gubernativo Número 135-2009 Reglamento de la ley para el reconocimiento de las comunicaciones y firmas electrónicas. Dicho reglamento complementó aspectos contenidos en la Ley en cuanto a procedimientos, plazos y situaciones como determinar qué sucede en el caso de que una entidad certificadora deje de actuar como tal mientras los certificados aún se encuentren vigentes, de conformidad con las normas contenidas en el Reglamento en este caso la entidad prestadora de servicios de certificación debe comunicarlo previamente a cada uno de los titulares de firmas electrónicas certificados por ellos, con antelación de por lo menos quince días hábiles que dichos certificados serán transferidos a otro prestador de servicios de certificación dentro del plazo de quince días hábiles contados a partir de la fecha de la comunicación. En este caso al

ser autorizado dichos certificados son transferidos y continúan siendo válidos y gozando de vigencia, de lo contrario quedarán sin efectos jurídicos por disposición legal. Este es un ejemplo de los aspectos que no queda resuelto de la lectura de la Ley pero que el Reglamento vino a complementar.

2. El Decreto 47-2008 del Congreso de la República (en adelante la Ley), a pesar de haberse complementado con la entrada en vigor de su respectivo reglamento sigue mostrando ciertas inconsistencias en el texto de sus artículos que no permiten que los mismos sean del todo claros y den lugar a diversas interpretaciones, por ejemplo, en el artículo 1 de la Ley que se refiere al ámbito de aplicación establece, que la misma será aplicable a todo tipo de comunicación electrónica, transacción o acto jurídico, público o privado, nacional o internacional; mientras que en el artículo 5 de la mencionada Ley, que se refiere al reconocimiento jurídico de las comunicaciones electrónicas establece, que no se negarán efectos jurídicos, validez o fuerza obligatoria a una comunicación o a un contrato; cuando en el ámbito de aplicación de la Ley establece comunicación electrónica, transacción y acto jurídico no menciona la comunicación por sí sola ni el contrato. De igual manera regula en el artículo 8 y 9 en lo relativo a la firma y el original, que estas se aplicarán para una comunicación o para un contrato, cuestiones que no se mencionan en el ámbito de aplicación de la Ley. Por otro lado, en el artículo 11 de la Ley con relación a la admisibilidad y fuerza probatoria de las comunicaciones electrónicas establece que serán admisibles como medios de prueba las comunicaciones electrónicas, las cuales son definidas en el artículo 2 de la misma ley como toda comunicación que las partes hagan por medio de mensaje de datos, es decir por medio de documento o información generada, enviada, recibida o archivada por medios electrónicos,

magnéticos, ópticos o similares, como pudieran ser entre otros, el intercambio de datos electrónicos, el correo electrónico, el telegrama, el télex o telefax. Mientras que en el artículo 3 de Reglamento, Acuerdo Gubernativo Número 135-2009 establece que la fuerza probatoria se le otorga a los actos y contratos otorgados o celebrados por personas naturales o jurídicas, públicas o privadas suscritos por medio de firma electrónica, y el artículo 33 de la Ley establece que la firma electrónica por sí sola tendrá la fuerza probatoria, así como cuando haya sido fijada en una comunicación electrónica. Estas son algunas de las inconsistencias que la Ley y el Reglamento presentan que pueden dar lugar a interpretaciones diversas.

3. El Decreto 47-2008, Ley para el reconocimiento de las comunicaciones y firmas electrónicas, vino a complementar normas del Código Civil Decreto Ley 106, por ejemplo, en lo relativo a la contratación entre ausentes, al incrementar en la legislación nacional las contrataciones electrónicas. En el mismo artículo 1 del ámbito de aplicación establece que las disposiciones contenidas en la 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; con esto se demuestra que no viene a modificar las cuestiones establecidas ya en las leyes vigentes tanto civiles como mercantiles sino que simplemente las complementa con las nuevas opciones que la tecnología electrónica ofrece. Asimismo en el artículo 23 de la mencionada ley establece que la misma regula lo relativo al envío y recepción de las comunicaciones electrónicas pero que los efectos jurídicos seguirán siendo regidas conforme a las normas aplicables al acto o negocio jurídico contenido en dicho mensaje de datos. Estos son dos

ejemplos de cómo la Ley para el reconocimiento de las comunicaciones y firmas electrónicas complemento la legislación nacional en materia civil y mercantil.

4. Al hacer una comparación de la Ley Modelo sobre Firmas Electrónicas de la CNUDMI, norma que sirvió de guía a los países que incorporaron la firma electrónica dentro de su normativa, y la Ley para el reconocimiento de las comunicaciones y firmas electrónicas Decreto 47-2008 del Congreso de la República de Guatemala se puede observar que la ley guatemalteca contempla en el conjunto de sus normas las doce normas de la Ley Modelo literales, no así las complementa con aspectos tales como la regulación de esta materia para el caso de las entidades públicas, los derechos y obligaciones de las partes y todo lo relativo a procedimientos que establece su reglamento, por lo que se considera que sí se encuentra apegada a lo recomendado por la normativa internacional y contiene los elementos necesarios para poder aplicar esta figura jurídica ya que cumple con los estándares necesarios para el comercio tanto nacional como internacional.

5. El decreto 47-2008 a pesar de cumplir con los estándares internacionales necesarios para lograr el funcionamiento de la figura jurídica en Guatemala, la realidad nacional en Guatemala se muestra aún incipiente en esta materia, ya que en cuanto a materia de contratación electrónica se refiere el país cuenta con un desarrollo tecnológico emergente que se demuestra en la poca posibilidad de estar en la cultura informática; la incipiente utilización de dichos medios que se maneja en materia de comercio y en la poca exigencia o necesidad de Entidades Prestadoras de Servicios de Certificación, esto debido a que los empresarios a pesar de contar con los medios aún no han necesitado utilizar las seguridades que

la figura de la firma electrónica les ofrece por lo que se presenta como una opción viable para las empresas que generan contratos de cifras altas y no así para las pequeñas y medianas empresas. Esto genera el hecho del retraso en la inscripción de Entidades Prestadoras de Servicios de Certificación en Guatemala, debido a que las responsabilidades y exigencias que la ley les impone generan un costo elevado de operaciones que no se logra cubrir por no existir una demanda fuerte en el mercado de dichas entidades por lo que resulta desmotivante y poco rentable el tema para quienes deseen emprender este negocio, ya que además los centros nacionales competirían con los internaciones que exigirá una competencia en cuanto a servicios y tarifas que será un reto para un país como Guatemala. Por lo tanto, se concluye que ésta puede ser una de las causas por las que ha sido difícil la inscripción en el Registro de Prestadores de Servicios de Certificación de las entidades aún cuando la Ley fue aprobada en el año 2008.

6. Como conclusión final derivado de las respuestas obtenidas en las entrevistas realizadas a distintas personalidades especialistas en la materia se puede decir que la Ley para el Reconocimiento de la Comunicaciones y Firmas Electrónicas en conjunto con su Reglamento y las guías elaboradas por el Registro de Prestadores de Servicios de Certificación constituyen una base legal que se apega a la realidad jurídica internacional, que contempla aspectos que inclusive otras legislaciones de otros países no han contemplado y que constituye una herramienta que permite que nuestro país esté al nivel de países como España, México y Chile en cuanto a materia electrónica se refiere, no así esto no significa que no tenga la necesidad de perfeccionarse conforme se vaya implementando la Ley en el país, ya que en teoría no de fácil

vulnerabilidad lo que permite brindar la certeza y seguridad jurídicas que persigue desde su entrada en vigencia en el país.

RECOMENDACIONES

1. Como primera recomendación es necesario que para que la firma electrónica pueda llegar a aplicarse en el ámbito nacional hay que cambiar las concepciones culturales que se tienen en relación al comercio electrónico. Ya que por el poco conocimiento y confianza en las

transacciones de este tipo la población guatemalteca sigue prefiriendo realizar las transacciones físicas y no por medios electrónicos. Debido a que en la cultura guatemalteca el acceso a internet aún no es generalizado no así el acceso a una computadora, para el caso de las transacciones de personas comunes no necesariamente las de las grandes corporaciones, quienes sí tienen acceso a estos medios. Esta se considera que es una de las causas por las que aún no se ha generalizado el uso de la firma electrónica y se desconfía aún de la misma.

2. El desconocimiento y la poca cultura de los comerciantes en buscar las seguridades que el internet les ofrece hace necesario que se promueva la figura de la firma electrónica a efecto de cambiar la visión hacia los beneficios del comercio electrónico, para ello se recomienda además de la promoción que las entidades que empiecen su funcionamiento en el país busquen tarifas y soluciones competitivas y razonables en relación a las entidades internacionales que no vayan a desmotivar el costo del producto final que ofrecerán.

3. A pesar de que el reglamento vino a complementar las situaciones dudosas de la Ley aún siguen habiendo inconsistencias legislativas que es necesario corregir para poder hacer de la firma electrónica una figura competitiva a nivel tanto nacional como internacional. Es importante que se siga estudiando la materia y mejorando las normas que actualmente se encuentran ya vigentes en el país, así como realizar efectivamente los pasos establecidos en las guías de solicitud, evaluación y revisiones periódicas para evitar la aparición de los fraudes y delitos electrónicos de tanto apogeo en esta materia.

4. Como última recomendación se debería promover o incentivar a las empresas transnacionales o grandes empresas el empleo de las seguridades jurídicas que la firma electrónica ofrece ya que serán estas empresas las que podrán costear los certificados electrónicos sin mayor problema y darle vida y funcionamiento a esta figura jurídica en Guatemala.

REFERENCIAS

BIBLIOGRÁFICAS:

1. Acosta Romero, Miguel. NUEVO DERECHO MERCANTIL, capítulo XVIII: La Firma en el derecho mercantil mexicano, Primera edición, Editorial Porrúa, México 2000.

2. Arrieta, Raúl, Los prestadores de Servicios de Certificación de Firma Electrónica en el Derecho Chileno, Revista Chilena de Derecho Informático, Chile, 2006

3. Banco Interamericano de Desarrollo, FIRMA DIGITAL Y CONTRATOS ELECTRÓNICOS, Documentos conceptual para la legislación en la era de la información, Iniciativa Glin Américas, Noviembre, 2005.-

4. Blassetti, Roxana C., Cabanellas, Guillermo, DERECHO DEL COMERCIO INTERNACIONAL, Buenos Aires, Argentina, 2004.

5. Cámara de Comercio de Guatemala, Trámite ante la Cámara de Comercio de Guatemala para los titulares de certificados digitales, septiembre de 2009.

6. Devoto, Mauricio, COMERCIO ELECTRÓNICO Y FIRMA DIGITAL: La regulación del ciber espacio y las estrategias globales, Buenos Aires Argentina, 2001.

7. García Más, Francisco Javier, COMERCIO ELECTRÓNICO Y FIRMA ELECTRÓNICA, Editorial Cervantes, Guatemala, 2007.

8. Guisado Moreno, Angela, Porfirio Carpio, Leopoldo J., FORMACIÓN Y PERFECCIONAMIENTO DEL CONTRATO EN INTERNET, Marcial Pons, Ediciones Jurídicas, Madrid, España, 2004.-

9. Herrera, Rodolfo, Derecho Informático, Ediciones Jurídicas la Ley, Chile 2003.

10. Lessing, Lawrence, El código y otras leyes del ciberespacio, Editorial Taurus es digital, España, 2001.

11. Lorenzzeti, Ricardo, Tratado de los contratos, Tomo III, Editorial Lex, Argentina, 2008.

12. Miguel Ascencio, Pedro, DERECHO PRIVADO EN INTERNET, Tercera Edición actualizada, Editorial Civitas, Madrid España, 2002.-

13. Ollmann, Gunter. Phishing Guide: Understanding and Preventing Phishing Attacks. Technical Info. 10 de julio de 2006.

14. Pinochet Rupero, Contratos electrónicos y defensa del consumidor, Marcial Pons, Ediciones Jurídicas y Sociales, S.A., Madrid, 2001

15. Ramos Suárez, Fernando, Cómo aplicar la normativa sobre firma electrónica, Universidad de Jaén, segunda edición, España, 1999.

16. Real Academia Española, DICCIONARIO DE LA LENGUA ESPAÑOLA, Veigésima primera edición, Editorial Espasa-Calpe, S.A. Madrid, España, 1992.

17. Reyes Krafft, Alfredo Alejandro, LA FIRMA ELECTRÓNICA Y LAS ENTIDADES DE CERTIFICACIÓN, Editorial Porrúa, México 2003.

18. Rodríguez Adrados, Antonio, LA FIRMA ELECTRÓNICA: comunicación discutida en sesión del pleno de académicos de número el día 5 de junio de 2000. Real Academia de Jurisprudencia y Legislación publicada en sus anales 2000.

19. Villegas, Rojina, Derecho Civil Tomo V, Volumen I, México 1951

20. Sagui, María Mercedes, ENTIDAD CERTIFICADORA DE FIRMA ELECTRÓNICA, Editorial Tecnos, Chile, 2007.-

21. Stutz, Michael AOL: A Cracker's Paradise, enero de 1998.

22. Tan, Koon. Phishing and Spamming via IM (SPIM).|Internet Storm Center. 5 de diciembre de 2006

NORMATIVAS:

1. Constitución Política de la República de Guatemala.
2. Código Civil de Guatemala, Decreto Ley 106.
3. Código Procesal Civil de Guatemala, Decreto Ley 107.
4. Código de Comercio de Guatemala, Decreto Número 2-70
5. Decreto Número 47-2008 del Congreso de Guatemala, Ley para el Reconocimiento de las comunicaciones y firmas electrónicas.
6. Acuerdo Gubernativo No. 135-2009 Reglamento de la Ley para el reconocimiento de las comunicaciones y firmas electrónicas.
7. Convención de las Naciones Unidas sobre la utilización de las comunicaciones electrónicas en los contratos internacionales.
8. Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación para el Derecho Interno 2001, Naciones Unidas, Nueva York, 2002.
9. Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma No. 19.799 Chile.
10. Real Decreto Ley 14/1999 España.
11. Real Decreto 59/2003 España.
12. Ley 25.506 Firma Digital, Argentina.
13. Ley No. 27269 Ley de Firmas y Certificados Digitales, Perú.
14. Ley de comercio electrónico, firmas electrónicas y mensajes de datos, Ecuador.

ELECTRÓNICAS:

1. Diccionario en línea, inglés – español http://www.wordreference.com/es/translation.asp.
2. Cadena Sandoval, Carlos Alberto, Sistema Integral de gestión integral México, www.firmadigital.gob.mx
3. Cámara Oficial de Comercio e Industria de Jerez de la Frontera http://www.camarajerez.es/index.php?id=61
4. Carrión, Hugo Daniel, ANALISIS COMPARATIVO DE LA LEGISLACION Y PROYECTOS A NIVEL MUNDIAL SOBRE FIRMAS Y CERTIFICADOS DIGITALES, http://www.mbc.com/legis/eu-digsig-dir.html, y http://www.cnv.gov.ar/FirmasDig/Internacional/DirectivaFirmaDigitalComEurop_Esp.htm)
5. Carrión, Hugo Daniel, ANÁLISIS COMPARATIVO DE LA LEGISLACION Y PROYECTOS A NIVEL MUNDIAL SOBRE FIRMAS Y CERTIFICADOS DIGITALES, http://www.mbc.com/legis/cu-digsig-dir.html.
6. Censo de Prestadores de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Comercio y Turismo, www.innovoto.com, España, 2010.-
7. Correa González, Felipe, INTRODUCCIÓN A LA LEY No. 19.799 DE FIRMA ELECTRÓNICA Y SERVICIOS DE CERTIFICACION No. 069-abril de 2004, Revista electrónica de Derecho Informático, http://www.alfaredi.org/rdi-articulo.shtml
8. Curvo, José, LA FIRMA DIGITAL Y ENTIDADES DE CERTIFICACION, http://www.alfaredi.org/rdi-articulo.shtml
9. Ecoforo, Uso de certificados dobles para internet, http://ecoforo.cepymev.es
10. Espinoza Cèspedes, Josè Francisco, RÉGIMEN JURÍDICO DE LA FIRMA ELECTRÓNICA EN PERÚ http://www.ieid.org/congreso/ponencias/Espinoza%20Cespedes,%20JF.pdf
11. http://www.ecertchile.cl/html/productos/download/CCS_CadenaCert.p7b

12. Microsoft Windows, Autenticación de Extremos en Internet, http://msdn.microsoft.com/es-es/library/ms191264.aspx
13. Ministerio de Economía Fomento y Turismo de Chile, http://www.economia.cl, Chile, 2010
14. Ramos Suárez, Fernando, La firma digital: aspectos técnicos y legales, Revista Electrónica de Derecho Informático No. 35 http//publicaciones.derecho.org/redi

ANEXOS

ENTREVISTA

A CONTINUACIÓN ENCONTRARÁ UNA SERIE DE PREGUNTAS CUYAS RESPUESTAS SERÁN UTILIZADAS COMO COMPLEMENTO DE LA INVESTIGACIÓN DEL TRABAJO DE TESIS DENOMINADA "ANÁLISIS JURÍDICO DE LAS ENTIDADES CERTIFICADORAS DE FIRMA ELECTRÓNICA EN GUATEMALA". SE LE SOLICITA SEAN CONTESTADAS LO MÁS APLIAMENTE POSIBLE.

1. Con relación a las legislaciones sobre Firma Electrónica vigentes en España, Argentina y México ¿cuál considera que contempla de una mejor manera la regulación de las Entidades Certificadoras de Firma Electrónica?

2. Considera que la Ley para el Reconocimiento de las Comunicaciones y Firma Electrónica, Decreto 47-2008 del Congreso de la República se ajusta a los estándares internacionales requeridos en materia de contratación electrónica?

3. Considera que la legislación vigente en Guatemala con respecto a Firma Electrónica está acorde con lo legislado por la Ley Modelo de la CNUDMI Sobre las Firmas Electrónicas del año 2001 de la Comisión de las Naciones Unidas para el Derecho Comercial Internacional.

4. Considera que el Decreto 47-2008 del Congreso de la República posee deficiencias o que contemplaron todos los aspectos necesarios. ¿por qué?

5. Según su criterio ¿cuáles podrían ser los principales riesgos que se correrían ante un mal empleo de las normas para las Entidades Certificadoras de Firma Electrónica en la legislación vigente en Guatemala?

Entrevista No. 1: Licenciado Mariano Rayo

Diputado del Congreso de la República quien propuso el Decreto 47-2008 del Congreso de la República.

Guatemala, 16 de marzo de 2010.-

1. Cuando emitimos la ley en Guatemala, procuramos introducir la normativa mas reciente y adecuada vigente para ese momento. por lo anterior, realizamos un estudio de derecho comparado que no solo incluyó los países en la pregunta citados, sino otros más. Lo que puedo decir es que como ley, la de Guatemala es de las más avanzadas e incluye las mejores prácticas a nivel internacional. El verdadero problema ha sido la implementación de la ley, acá si tenemos un problema serio por la especialidad de la ley, la incapacidad del Ministerio de Economía, y el poco uso de los usuarios.

2. Sin lugar a dudas que es así, tengo conocimiento que otros países han utilizado nuestra legislación como referencia para emitir las propias o reformas las vigentes en sus territorios.

3. Si así es, la ley modelo fue referencia para la nuestra.

4. Considero que si contempla todos los aspectos necesarios, pero la no aplicación completa de la ley, y lo corto del tiempo, impide realizar una evaluación completa, y determinar si hay correcciones necesarias.

5. No me cabe la duda que se aumentaría exponencialmente todo lo referente a cibercrimen.

Entrevista No. 2: Licenciada Skarlette Anthone

Directora Ejecutiva del Registro de Prestadores de Servicios de Certificación de Guatemala.

Guatemala, 12 de marzo de 2010.

1. Considero que de los países mencionados la legislación española es que la contempla una mejor forma de legislar las entidades certificadoras.

2. No tengo dudas con respecto a que la norma guatemalteca se apega a los estándares internacionales, debido a que para su elaboración fue tomada en cuenta la Ley Modelo de las Naciones Unidas y en sus normas de interpretación se consideró el origen internacional de la misma.

3. Sí, considero que nuestra norma está apegada a la normativa internacional y las recomendaciones emanadas por las Naciones Unidas en la Ley Modelo.

4. Considero que sí es bastante completa, pero que aún le queda un camino muy largo por recorrer y en con el transcurso del tiempo pueda ser necesario incluir nuevas cuestiones.

5. Puede dar lugar a estafas y crímenes como los que se han venido dando con el uso de Internet, pero de la buena utilización de los recursos legales depende que esto no suceda.

Entrevista No. 3: Licenciado Hugo Bran

Jefe de Servicios al Consumidor de la Dirección de Atención al Consumidor DIACO.

Guatemala, 04 de abril de 2010

1. A mi criterio estas tres legislaciones son las que más se apegan a una buena legislación sobre la materia.

2. Sí considero que Guatemala con su nueva legislación se apega a los estándares internacionales requeridos para la contratación a nivel internacional.

3. Por lo que tengo entendido sí está acorde a la legislación de las Naciones Unidas.

4. Creo que contempla los aspectos suficientes para empezar a funcionar en Guatemala.

5. Como toda norma puede dar lugar a malas interpretaciones y a crímenes que ya se están dando como los de robo de identidad.

Entrevista No. 4: Licenciada Fanny Estrada

Directora de Competitividad AGEXPORT Guatemala

Guatemala, 06 de abril de 2010.

1. Considero que la legislación de España representa un modelo a seguir en cuanto a contratación electrónica se refiere, asimismo la legislación de Chile representa otro ejemplo de legislaciones vanguardistas en este tema.

2. Guatemala con la aparición de esta nueva norma se ha colocado en la lista de países vanguardistas que esperan superar las barreras económicas.

3. Sí, la actual legislación de Guatemala sobre la firma electrónica se apega a la creada por las Naciones Unidas en muchos aspectos.

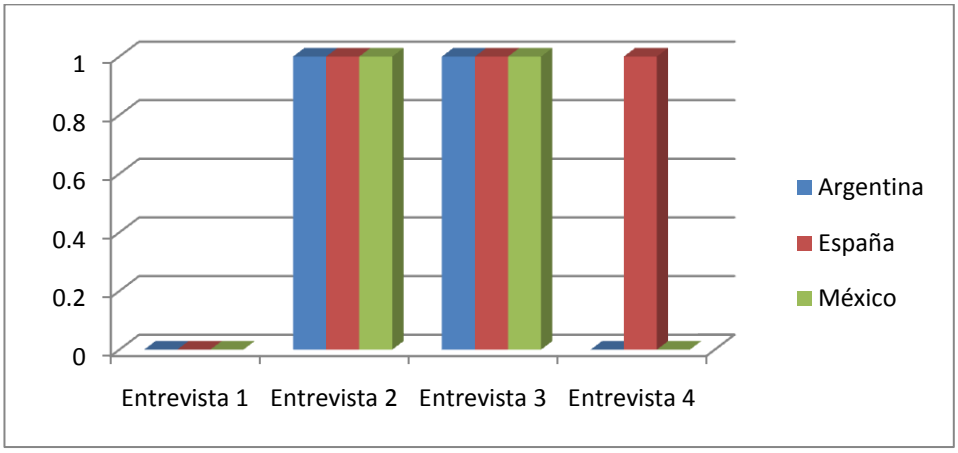
4. Aún es muy temprano para poder hablar de deficiencias propiamente dichas ya que la aplicación de la ley no se ha iniciado del todo.

5. Es muy probable que se preste para delitos por lo que la labor de las autoridades encargadas será de mucha importancia en la aplicación de la ley.

Análisis de los resultados obtenidos en las entrevistas:

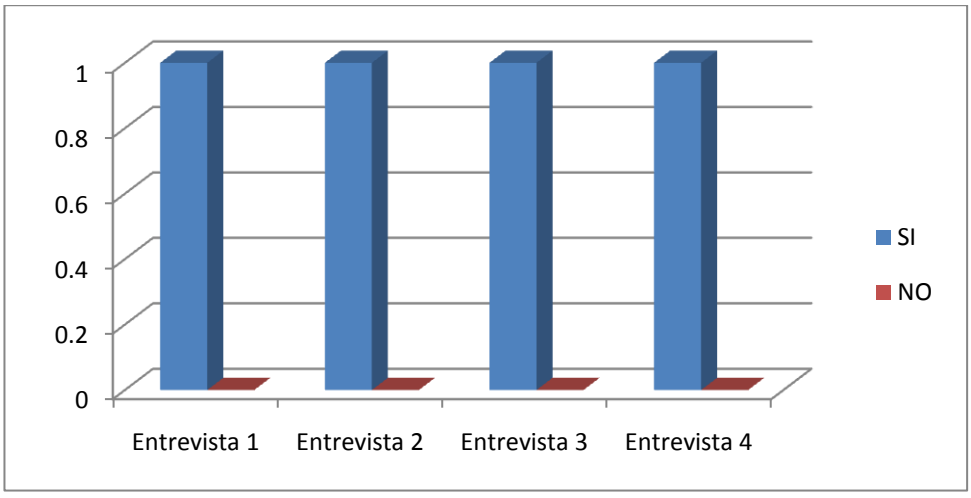
Pregunta No. 1

Con relación a las legislaciones sobre Firma Electrónica vigentes en España, Argentina y México ¿cuál considera que contempla de una mejor manera la regulación de las Entidades Certificadoras de Firma Electrónica?



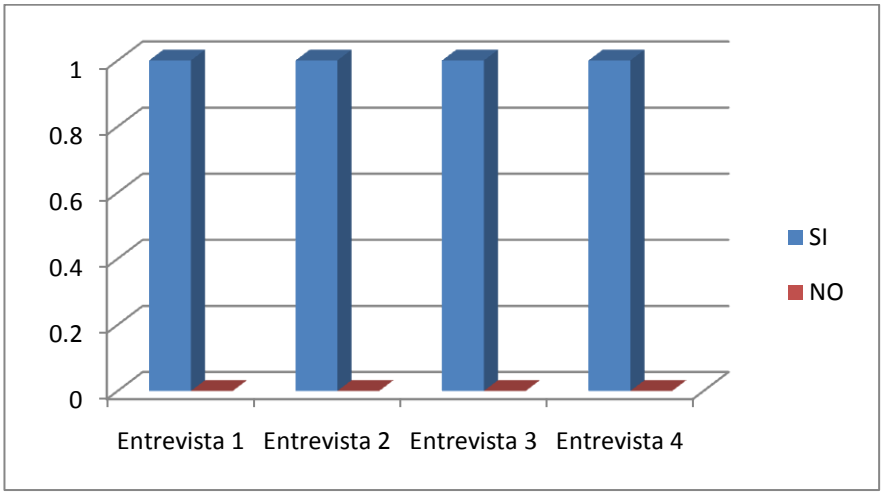
Pregunta No. 2

Considera que la Ley para el Reconocimiento de las Comunicaciones y Firma Electrónica, Decreto 47-2008 del Congreso de la República se ajusta a los estándares internacionales requeridos en materia de contratación electrónica?



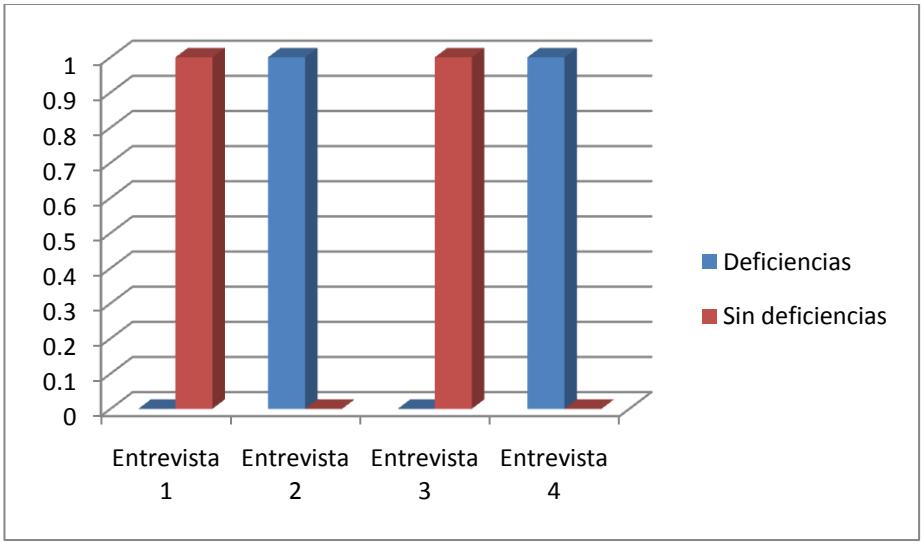
Pregunta No. 3

Considera que la legislación vigente en Guatemala con respecto a Firma Electrónica está acorde con lo legislado por la Ley Modelo de la CNUDMI Sobre las Firmas Electrónicas del año 2001 de la Comisión de las Naciones Unidas para el Derecho Comercial Internacional.



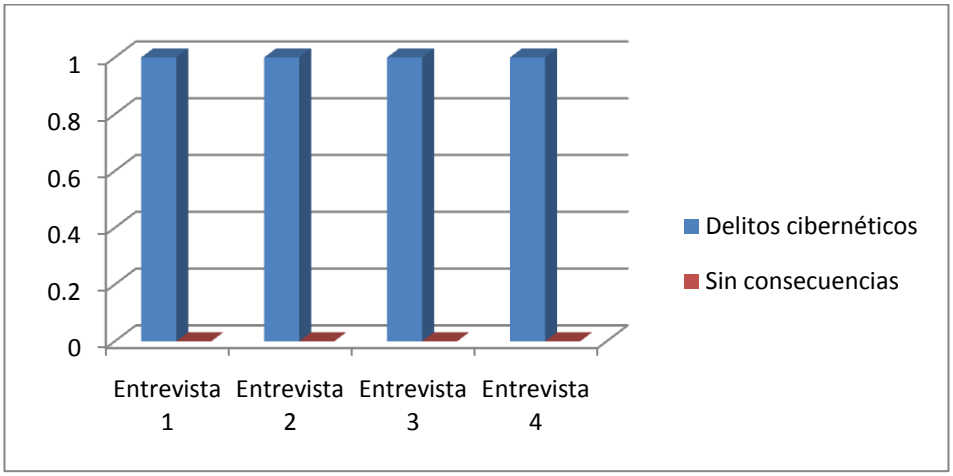
Pregunta No. 4

Considera que el Decreto 47-2008 del Congreso de la República posee deficiencias o que contemplaron todos los aspectos necesarios. ¿por qué?



Pregunta No. 5

Según su criterio ¿cuáles podrían ser los principales riesgos que se correrían ante un mal empleo de las normas para las Entidades Certificadoras de Firma Electrónica en la legislación vigente en Guatemala?



PAIS	Número de Ley o Decreto	Fecha de su entrada en vigor	Temas contemplados en la ley	Conceptos	Regulación sobre Entidades Certificadoras de Firma Electrónica	Regulación sobre Certificados Digitales	Registro	Quiénes pueden ser Entidades Certificadoras
ESPAÑA	Ley 59/2003	19 de diciembre de 2003	Disposiciones generales, certificados electrónicos, certificados reconocidos, el documento nacional de identidad electrónico, prestación de servicios de certificación, responsabilidad, dispositivos de firma electrónica y sistemas de certificación de prestadores de servicios de certificación y de dispositivos de firma electrónica, certificación de servicios de certificación y de dispositivos de creación de firma electrónica, supervisión y control, infracciones y sanciones,	Prestador de servicios de certificación: se le denomina a la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica. Firma electrónica: es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante. La firma electrónica avanzada: es la firma electrónica que permite identificar al firmante para detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.	Lo contempla en el Título III Prestación de servicios de certificación, con los siguientes temas: Obligaciones, declaración de prácticas de certificación, obligaciones de los prestadores de servicios de certificación que expidan certificados reconocidos, cese de la actividad de un prestador de servicios de certificación, la responsabilidad de los prestadores de servicios de certificación y las limitaciones de responsabilidad de los prestadores de servicios de certificación.	Del artículo 6 al 14. Regula el concepto de certificado electrónico y de firmante, los certificados electrónicos de personas jurídicas, la suspensión de la vigencia de los certificados electrónicos, los certificados reconocidos, concepto y contenido de dichos certificados, la comprobación de la identidad y otras circunstancias personales de los solicitantes de un certificado reconocido y la equivalencia internacional de certificados.	El encargado de la supervisión y control de las entidades prestadoras de servicios de certificación es el Ministerio de Ciencia y Tecnología.	Cualquier persona física o jurídica.

ESPAÑA				Firma electrónica reconocida: la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. Documento electrónico: el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente. Certificado electrónico: es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad. Firmante: es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.				
MÉXICO	Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en	29 de mayo de 2000	Se reconoció como prueba la información contenida en los medios electrónicos, ópticos o de cualquier tecnología, la obligación de conservar por un plazo mínimo de 10	Mensaje de datos: la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología.	Contempla la figura del Prestador de Servicios de Certificación quien como tercero confiable estará investido de la facultad de validar por su probidad y su tecnología (no fe	Regula el reconocimiento de certificados provenientes del extranjero.	Autoridad Registradora Central a la Secretaría de Economía además del Banco de México y la Secretaría de la	Pueden ser prestadores de servicios de certificación: Los notarios o corredores púbicos, las empresas privadas y las instituciones públicas.

MÉXICO	Materia común y para toda la República en Materia Federal, del Código Federal de Procedimientos civiles del código de comercio y de la Ley Federal de Protección al Consumidor.		años los originales de las cartas, telegramas, mensajes de datos o cualesquiera documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derecho y obligaciones. Se estableció la presunción en materia mercantil de que salvo pacto en contrario el mensaje proviene del emisor. Tanto en materia mercantil y civil cuando la ley exija la forma escrita para los contratos y la firma de los documentos relativos, esos supuestos se tendrán por cumplidos tratándose de mensajes de datos siempre que éste sea atribuible a las personas obligadas y accesible para su ulterior consulta. Se reconoce como prueba los mensajes de datos. Con respecto a la ley de protección al consumidor se reformó para reconocer la		pública) el proceso de emisión, identificación, y atribución de firmas electrónicas.		Función Pública.	

			utilización de medios electrónicos, ópticos o cualquier otra tecnología en la instrumentación de las operaciones que celebren proveedores con los consumidores.					
CHILE	Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma No. 19.799	Publicada en el Diario Oficial el 12 de abril de 2002	Disposiciones generales, uso de firmas electrónicas por los órganos del Estado, los prestadores de servicios de certificación, los certificados de firma electrónica, de la acreditación e inspección de los prestadores de servicios de certificación, derechos y obligaciones de los usuarios de firmas electrónicas y reglamentos.	Electrónico: Característica de la tecnología que tiene capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares. Certificado de firma electrónica: certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica. Certificador o Prestador de Servicios de Certificación: entidad prestadora de servicios de certificación de firmas electrónicas. Documento electrónico: toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.	Lo contempla en el Título III de los Prestadores de Servicios de Certificación, del artículo 11 al 14 y de artículo 17 al 22 Establece las obligaciones y la responsabilidad de daños y perjuicios de que son acreedores los prestadores de servicios de certificación por el mal empleo de sus funciones.	Lo contempla en Título IV de los Certificados de Firma Electrónica, artículos 15 al 16. Contiene los requisitos que deben llenar los certificados digitales, y en qué situaciones quedan sin efecto los mismos.	La Subsecretaría de Economía, Fomento y Reconstrucción	Las personas nacionales o extranjeras, públicas o privadas que otorguen certificados de firma electrónica sin perjuicio de los demás servicios que puedan realizar.

CHILE				Entidad acreditadora: la subsecretaría de Economía, Fomento y Reconstrucción. Firma Electrónica: cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor. Firma electrónica avanzada: aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a lo que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría y Usuario o titular: la persona que utiliza bajo su exclusivo control un certificado de firma electrónica.				

CHILE								
ARGENTINA	Ley 25.506	Sancionada el 14 de noviembre de 2001. Promulgada el 11 de diciembre de 2001.	Consideraciones generales, los certificados digitales, del certificador licenciado, del titular de un certificado digital, de la organización institucional, de la autoridad de aplicación, del sistema de auditoría, de la comisión asesora para la infraestructura de firma digital, responsabilidad, sanciones, disposiciones complementarias.	Firma digital: se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma. Firma Electrónica: el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. Documento digital: la representación digital de	Capítulo III del certificador licenciado artículos del 17 al 23, define lo que es un certificador licenciado, los certificados por profesión, las funciones de los mismos, licencia, las obligaciones, el cese de su actividad y el desconocimiento de la validez de un certificado digital.	Capítulo II del artículo 13 al 25. Contempla los temas de los requisitos de validez de los certificados digitales, el período de vigencia, el reconocimiento de certificados extranjeros, el certificador licenciado, los certificados profesionales, las funciones del certificador licenciado, la licencia, obligaciones, cese del certificador, desconocimiento de la validez de un certificado digital, de los titulares de un certificado digital,	La Jefatura de Gobierno de Ministros.	Toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados y/o presta otros servicios en relación con la firma digital y cuanta con licencia para ello.

ARGENTINA **ARGENTINA**				actos o hechos con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Original: los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte. Certificado digital: el documento digital firma digitalmente por un certificador, que vincula los datos de verificación de firma a su titular. Certificador licenciado: toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante.				
	Ley No. 27269 Ley de Firmas y Certificados Digitales	Promulgada el 26 de mayo de 2000 y Publicada el 28 de mayo de 2000	Objeto de la ley, la firma digital, el titular de la firma digital, los certificados digitales, de las entidades de certificación y de registro, y la reglamentación.	Firma digital: es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una a una clave privada y una clave pública	Del artículo 12 al 15, establece lo relativo a la entidad de certificación, la entidad de registro o verificación, el depósito de certificados digitales, la inscripción del	Del artículo 6 al 11 contempla lo relativo a los certificados digitales, la confidencialidad de la información, la cancelación del	Aún no cuenta con el registro respectivo aunque la ley sí contempla la obligación de su	La norma no es clara con respecto a quienes pueden ser prestadores del servicio de certificación.

PERU **PERÚ**				relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada. Certificado digital: es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad. Entidad de Certificación: cumple con la función de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado o aquellos que brinden seguridad al sistema de certificados en particular o del comercio electrónico en general.	entidades de certificación y de registro o verificación.	certificado digital, la revocación del certificado digital, el reconocimiento de certificados emitidos por entidades extranjeras.	creación.	
	Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de datos	10 de abril de 2002	Los mensajes de datos, las firmas electrónicas, certificados de firma electrónica, entidades de certificación de información, organismos de promoción de los servicios electrónicos y de regulación y control de las	Firma electrónica: son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y	Capítulo III de las Entidades de Certificación de Información, del artículo 29 al 35. Regula los temas de qué son las entidades de certificación de información, las obligaciones de las entidades de certificación de	Capítulo II de los Certificados de Firma Electrónica, del artículo 20 al 28 contempla los temas de qué es un certificado de firma electrónica, el uso del certificado de firma	La Superintendencia de Telecomunicaciones	Las empresas unipersonales o personas jurídicas.

ECUADOR **ECUADOR**			entidades de certificación acreditadas, de los organismos de promoción y difusión de los servicios electrónicos, y de regulación y control de las entidades de certificación acreditadas, de los servicios electrónicos, la contratación electrónica y telemática, los derechos de los usuarios e instrumentos públicos, de la prueba y notificaciones electrónicas, de las infracciones informáticas,	reconoce la información contenida en el mensaje de datos. Certificado de firma electrónica: es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma la identidad. Entidades de certificación de información: son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones.	información, las responsabilidades de las entidades de certificación de información acreditadas, la protección de datos por parte de las entidades, prestación de servicios de certificación por parte de terceros, la terminación contractual y la notificación de cesación de actividades.	electrónica, requisitos del certificado de firma electrónica, duración del certificado, extinción, suspensión, revocatoria y reconocimiento internacional de certificados de firma electrónica.		