



Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

IMPLEMENTACIÓN Y ADOPCIÓN DE LA FIRMA ELECTRÓNICA EN GUATEMALA

Julio René Santizo Ochoa

Asesorado por el Ing. Manuel Fernando López Fernández

Guatemala, noviembre de 2010

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

**IMPLEMENTACIÓN Y ADOPCIÓN DE LA FIRMA ELECTRÓNICA EN
GUATEMALA**

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA

FACULTAD DE INGENIERÍA

POR

JULIO RENÉ SANTIZO OCHOA

ASESORADO POR EL INGENIERO MANUEL FERNANDO LÓPEZ FERNÁNDEZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, NOVIEMBRE DE 2010

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing.	Murphy Olympo Paiz Recinos
VOCAL I	Inga.	Glenda Patricia García Soria
VOCAL II	Inga.	Alba Maritza Guerrero Spínola de López
VOCAL III	Ing.	Miguel Ángel Dávila Calderón
VOCAL IV	Br.	Luis Pedro Ortíz de León
VOCAL V	P.A.	José Alfredo Ortíz Herincx
SECRETARIO	Ing.	Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing.	Murphy Olympo Paiz Recinos
EXAMINADOR	Ing.	Pedro Pablo Hernández Ramírez
EXAMINADOR	Ing.	Ludwing Federico Altan Sac
EXAMINADOR	Ing.	Oscar Alejandro Paz Campos
SECRETARIO	Ing.	Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

IMPLEMENTACIÓN Y ADOPCIÓN DE LA FIRMA ELECTRÓNICA EN GUATEMALA,

tema que me fuera asignado por la dirección de la Escuela de Ingeniería en Ciencias y Sistemas, en noviembre del 2009.

A handwritten signature in blue ink, consisting of a large, stylized initial 'J' followed by several loops and a long horizontal stroke at the bottom.

Julio René Santizo Ochoa




Guatemala 21 de junio de 2010

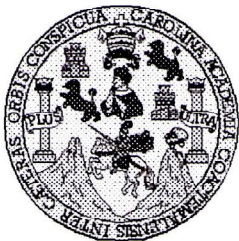
Ingeniero
Carlos Alfredo Azurdia Morales
Coordinador de Privados y Revisión de Trabajos de Graduación
Escuela de Ciencias y Sistemas
Facultad de Ingeniería
Universidad de San Carlos de Guatemala
Su despacho

Estimado Ingeniero

Atentamente me dirijo a usted para manifestarle que en los últimos meses he asesorado el trabajo de tesis del estudiante **JULIO RENÉ SANTIZO OCHOA** con carnet **200511763**; titulado **"IMPLEMENTACIÓN Y ADOCIÓN DE LA FIRMA ELECTRÓNICA EN GUATEMALA"**. Y a mi criterio el mismo se encuentra finalizado y cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Sin otro particular


Ing. Manuel Fernando López
Colegiado No. 5080



Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 21 de Julio de 2010


Ingeniero
Marlon Antonio Pérez Turk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **JULIO RENE SANTIZO OCHOA** carné **2005-11763**, titulado: **"IMPLEMENTACION Y ADOPCION DE LA FIRMA ELECTRONICA EN GUATEMALA"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,


Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación



E
S
C
U
E
L
A

D
E

C
I
E
N
C
I
A
S

Y

S
I
S
T
E
M
A
S

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA



FACULTAD DE INGENIERÍA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

*El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, de trabajo de graduación titulado **“IMPLEMENTACIÓN Y ADOPCIÓN DE LA FIRMA ELECTRÓNICA EN GUATEMALA”**, presentado por el estudiante JULIO RENÉ SANTIZO OCHOA, aprueba el presente trabajo y solicita la autorización del mismo.*

“ID Y ENSEÑAD A TODOS”


Ing. Migdon Antonio Pérez Turk
Director, Escuela de Ingeniería Ciencias y Sistemas



Guatemala, 03 de noviembre 2010



El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado; **IMPLEMENTACIÓN Y ADOPCIÓN DE LA FIRMA ELECTRÓNICA EN GUATEMALA**, presentado por el estudiante universitario **Julio René Santizo Ochoa**, autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympto Paiz Récinos
DECANO



Guatemala, noviembre de 2010

/cc
c.c. archivo.

A mis padres, artífices de mi vida.

AGRADECIMIENTOS

A Dios por la infinita bondad de sus bendiciones. ¡Gracias Padre por lo que has hecho conmigo!

De manera especial, a mi madre Judith y a mi padre Julio, por la inmensidad de su amor, su apoyo sin condiciones y sus sabios consejos. De igual manera agradezco a mi hermana Lucia por su amor y alegría.

Al ingeniero Manuel Fernando López catedrático, jefe, asesor de tesis, amigo y ejemplo.

Al doctor Byron Molina Klee por sus consejos y cuidados.

A la ingeniera María Mercedes Zaghi por su guía en la elaboración de esta tesis.

A mis amigos, en especial a Ricardo González, Jaime Molina, Javier Hernández, Héctor Villatoro, Enio De León, Gerardo García y Jenniffer Ramírez por su apoyo oportuno.

Muchas otras personas han sido importantes en este camino recorrido y me han ayudado directa o indirectamente a llegar hasta aquí, es por eso que aunque no las puedo mencionar una por una, les extiendo un agradecimiento sincero.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES.....	VII
GLOSARIO.....	IX
SINÓNIMOS.....	XI
RESUMEN.....	XIII
PALABRAS CLAVE.....	XV
OBJETIVOS.....	XVII
INTRODUCCIÓN.....	XIX
1. CONTEXTO PROPÓSITO Y METODOLOGÍA DE LA INVESTIGACIÓN.....	1
1.1 Antecedentes.....	1
1.2 Resultados esperados.....	2
1.3 Alcances y límites.....	3
1.4 Metodología.....	3
1.5 Estructura de la tesis.....	4
2. CRIPTOGRAFÍA Y CIFRADO.....	7
2.1 Criptografía.....	7
2.2 Criptoanálisis.....	10
2.3 Historia de la criptografía.....	11
2.4 Algoritmos de cifrado.....	14

2.4.1	<i>Data Encryption Standard (DES)</i>	14
2.4.2	Triple DES (TDES).....	15
2.4.3	<i>Advanced Encryption System (AES)</i>	15
2.4.4	<i>International Data Encryption Algorithm (IDEA)</i>	16
2.4.5	<i>Digital Signature Algorithm</i>	17
2.4.6	<i>RSA</i>	17
2.5	Función de <i>hash</i>	18
2.5.1	Algoritmos para calcular la función de <i>hash</i>	18
2.6	Tipos de sistemas criptográficos.....	20
2.6.1	Sistemas criptográficos de clave simétrica.....	21
2.6.2	Sistemas criptográficos de clave pública.....	22
3.	FIRMA ELECTRÓNICA Y PKI.....	25
3.1	Firma electrónica.....	26
3.3	¿Qué asegura la firma electrónica?.....	29
3.3.1	Autenticación.....	29
3.3.2	Integridad.....	29
3.3.3	No repudio.....	30
3.3.4	Confidencialidad.....	31
3.4	Certificado digital.....	31
3.4.1	Información que contiene un certificado digital.....	32
3.5	Autoridad certificadora.....	33
3.5.1	Servicios que provee una autoridad certificadora.....	34

3.5.2	Diferencias entre la firma electrónica simple y la firma electrónica avanzada	36
3.6	Infraestructura de clave pública (<i>PKI</i>)	37
3.6.1	Componentes de una <i>PKI</i>	39
4.	ANÁLISIS JURÍDICO DE LA FIRMA ELECTRÓNICA	41
4.1	Antecedentes de la Ley	43
4.2	Puntos clave de la ley	44
4.2.1	Elemento probatorio ante la ley	45
4.2.2	Aplicable a todo tipo de contratación, compra o trámite	46
4.2.3	Misma validez ante la ley que el papel	47
4.2.4	No válida para celebraciones de compromiso de familia.....	50
4.2.5	Información contenida en los certificados digitales	50
4.3	Equiparación de medios electrónicos con medios físicos.....	51
4.3.1	Escrito.....	52
4.3.2	Firma	52
4.3.3	Original	54
4.4	Obligaciones de los usuarios de firma electrónica.....	55
4.4.1	Firmante	55
4.4.2	Receptor	56
4.5	Creación del Registro de Prestadores de Servicios de Certificación (RPSC)	57
5.	GUÍAS DE USO DE LA FIRMA ELECTRÓNICA.....	61
5.1	Trámite ante la CCG e instalación del certificado	63
5.2	Firmando un correo electrónico.....	71

5.3	Verificación de una firma electrónica.....	80
6.	RECOMENDACIONES A LOS USUARIOS DE FIRMA ELECTRÓNICA	83
6.1	Base en la confianza	83
6.2	Descargar el certificado	84
6.3	Tramitar una firma electrónica.....	85
6.4	Validación de firmas electrónicas.....	85
6.5	Firmar comunicaciones electrónicas	86
6.6	Recomendaciones a las empresas e instituciones	87
6.6.1	Utilizar certificados en sus servidores para seguridad de los clientes.....	88
6.6.2	Obligatoriedad de la firma electrónica para todas las comunicaciones. ..	88
6.6.3	Obligatoriedad de cifrado mediante certificado para las comunicaciones confidenciales.....	89
6.6.4	Infraestructura de clave pública propia	90
7.	OBSTÁCULOS PARA LA ACEPTACIÓN Y UTILIZACIÓN DE LA FIRMA ELECTRÓNICA POR LOS GUATEMALTECOS.....	91
7.1	Principales obstáculos	92
7.1.1	Falta de confianza en métodos electrónicos.....	92
7.1.2	Desconocimiento de la tecnología y su uso	93
7.1.3	Falta de percepción de beneficios de su uso	94
7.2	Principales beneficios de la firma electrónica	94
8.	LA FIRMA ELECTRÓNICA COMO INSTRUMENTO DE E-GOBIERNO	97
8.1	Casos de éxito	97
8.2	Uso de la firma electrónica en los organismos del Estado.....	101

CONCLUSIONES	107
RECOMENDACIONES	111
REFERENCIAS.....	115
BIBLIOGRAFÍA.....	119
APÉNDICES	121
Apéndice A – Construcción del sitio informativo	121
ANEXOS	125
Anexo 1 – Ley para el reconocimiento de las comunicaciones y firmas electrónicas	125
Anexo 2 – Reglamento de la ley para el reconocimiento de las comunicaciones y firmas electrónicas.	135

ÍNDICE DE ILUSTRACIONES

Figuras

1. Clasificación de la criptografía	8
2. Ejemplo de cifrado	9
3. Escítala.....	12
4. Fórmula Triple DES.....	15
5. En Internet nadie sabe que eres un perro	25
6. Generación y verificación de una firma electrónica	27
7. Sitio de e-certchile	66
8. Generación de certificado en e-certchile.....	67
9. Confirmación opciones clave privada	68
10. Advertencia instalación certificado.....	68
11. Establecer nivel de seguridad	69
12. Instalación de certificado raíz	70
13. Configuración de cuenta de correo en <i>Mozilla Thunderbird</i>	71
14. Verificación de configuración de cuenta de correo	72
15. Firmar correo electrónico en <i>Mozilla Thunderbird</i>	73
16. Instalación de certificado en <i>Mozilla Thunderbird</i>	74
17. Opciones de seguridad en <i>Mozilla Thunderbird</i>	74
18. Instalación de certificado raíz en <i>Mozilla Thunderbird</i>	75

19. Agregar autoridad confiable en <i>Mozilla Thunderbird</i>	76
20. Agregar certificado digital en <i>Mozilla Thunderbird</i>	77
21. Confirmación de instalación del certificado digital.....	78
22. Información del certificado digital	78
23. Enviando correo electrónico firmado	79
24. Verificación de correo electrónico firmado	80
25. Información de firma electrónica de un correo	81
26. Sitio http://firmaelectronicagt.com/	123
27. Sitio http://firmaelectronicagt.com/	124

GLOSARIO

Algoritmo	Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema. [1]
CCG	Cámara de Comercio de Guatemala.
Comunicación electrónica	Información generada, enviada, recibida o archivada por medios electrónicos, magnéticos, ópticos o similares. [2]
Confidencialidad	Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. [3]
Correspondencia unívoca	Es una correspondencia matemática donde cada elemento del conjunto origen se corresponde con solo un elemento del conjunto imagen. [4]

Integridad

Se entiende que cuando se envíe un mensaje de una persona a otra o bien de una máquina a otra, este mensaje no sea modificado, sin que el destinatario pueda comprobarlo. La modificación se refiere tanto a una modificación explícita por alguien como a una modificación debido a un error. **[5]**

Request For Comment (RFC)

Documento cuyo contenido es una propuesta oficial para un nuevo protocolo de Internet que lo explica con todo detalle para que, en caso de ser aceptado, pueda ser implementado sin ambigüedades. **[6]**

RPSC

Registro de Prestadores de Servicios de Certificación.

SINÓNIMOS

Firma electrónica - firma digital

Los términos “firma electrónica” y “firma digital” se utilizan indistintamente y se consideran sinónimos, debido a la traducción del término en inglés “*Digital signature*”, pero en el decreto 47-2008 del congreso de la República de Guatemala, se utiliza el exclusivamente el término “firma electrónica” por lo que en el presente trabajo de investigación, se utilizara este término.

Clave - llave

Los términos “clave” y “llave” también se consideran sinónimos y se utilizan indistintamente, por ejemplo para referirse a la “clave pública” también se entiende si se dice “llave pública”, pero según el diccionario de la lengua española vigésima segunda edición de la RAE la definición de clave es: “Código de signos convenidos para la transmisión de mensajes secretos o privados” mientras que las definiciones de llave no tienen sentido para esta aplicación por lo que en este trabajo de investigación se utilizara el término “clave”.

Cifrar – encriptar

Los términos “cifrar” y “encriptar” se utilizan indistintamente, incluso se utiliza más el término “encriptar”, debido a la traducción del inglés “*encrypt*” pero la traducción correcta es “cifrar” además que la palabra “encriptar” no aparece en el diccionario de la lengua española vigésima segunda edición de la RAE por lo que en este trabajo de investigación se utilizará el término “cifrar”.

Cifrar – codificar

Estos dos términos se utilizan indistintamente, incluso es más común el término “codificar” pero éste hace referencia a la emisión de un mensaje mediante algún código, no necesariamente oculto, secreto o ininteligible, entonces en este trabajo no se utilizará ese término para evitar tergiversaciones en los conceptos.

RESUMEN

La criptografía es una ciencia antigua, bastante utilizada a lo largo de la historia. En la actualidad existen muchas aplicaciones de la criptografía, especialmente en el ámbito electrónico. Los primeros capítulos de esta tesis explican detalladamente qué es la criptografía; se revisa su evolución en la historia, se menciona algunos de los algoritmos más importantes que ha habido. Esto es base para su aplicación: la firma electrónica.

La firma electrónica es sólo un componente de la Infraestructura de Clave Pública (PKI), que incluye hardware, software y políticas de seguridad para que funcione la firma electrónica; además de otros procedimientos como el cifrado de información, el estampado cronológico, la custodia de documentos, que garantizan la integridad, la confidencialidad, la disponibilidad, la autenticación y el no repudio de la información.

Debido que la firma electrónica y la Infraestructura de Clave Pública (PKI) representan una alternativa eficiente y confiable para las comunicaciones, en muchos países del mundo, se le ha dado la misma validez jurídica que a los métodos tradicionales de comunicación basados en el papel. Guatemala no es la excepción y por medio de la “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” ha equiparado los medios físicos de comunicación, con los medios electrónicos de comunicación, así como la firma manuscrita, con la firma electrónica.

La “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” fue publicada en el diario oficial el 23 de septiembre de 2008 y a partir de esa fecha, empezó la implementación de ciertas entidades necesarias. La Cámara de Comercio de Guatemala quedó constituida como la primera entidad prestadora de servicios de certificación. El Ministerio de Economía fue el encargado de desarrollar el reglamento respectivo, publicado el 13 de mayo de 2009 y también fue el encargado de crear el Registro de Prestadores de Certificación, entidad en la cual se deben registrar todos los prestadores de servicios de certificación. El RPSC abrió sus puertas el 17 de junio de 2009. Según las indagaciones, no se ha registrado ningún prestador de servicios de certificación.

La Cámara de Comercio de Guatemala autoriza la emisión de certificados de firma electrónica, que en realidad emite e-certchile, por medio de un convenio con la Cámara de Comercio de Santiago, Chile. A pesar de esto, no existe una demanda de certificados de firma electrónica por parte de los guatemaltecos, debido a la falta de promoción y divulgación. Además, existen obstáculos o barreras que enfrentan los potenciales usuarios de la firma electrónica, por ejemplo: falta de confianza en los medios electrónicos, falta de información sobre los beneficios de su uso, y aparente dificultad de aprender a utilizarla.

La presente tesis presenta unas guías de uso que explican como firmar, verificar una firma e instalar un certificado; además recomendaciones para que esta tecnología se utilice adecuadamente y no se ponga en riesgo la información.

PALABRAS CLAVE

Firma electrónica, firma digital, criptografía, Criptología, criptoanálisis, sistemas criptográficos, clave pública, clave privada, clave simétrica, infraestructura de clave pública, algoritmo, función de hash, estampado cronológico, custodia de documentos, certificado, confidencialidad, integridad, no repudio, disponibilidad, autenticación, seguridad de la información, cifrar, correo electrónico, autoridad certificadora, prestador de servicios de certificación, Cámara de Comercio de Guatemala, Registro de Prestadores de Servicios de Certificación, USAC.

OBJETIVOS

General

Analizar el contexto de la implementación de la firma electrónica en Guatemala e identificar los principales obstáculos que enfrentan los guatemaltecos al utilizarla.

Específicos

- Conocer e interpretar la “ley para el reconocimiento de las comunicaciones electrónicas y firmas electrónicas”.
- Generar material informativo accesible para los potenciales usuarios de la firma electrónica en Guatemala.

- Impulsar la utilización de la firma electrónica en Guatemala a través de un sitio web.
- Resaltar los beneficios de la utilización de firma electrónica.

INTRODUCCIÓN

La firma electrónica es un procedimiento, que se ha utilizado en varios países del mundo desde hace varios años. En Guatemala es poco conocido, pero en septiembre de 2008 se publicó el decreto 47-2008, el cual contiene la “Ley para el reconocimiento de las comunicaciones y firmas electrónicas”; ley que otorga validez legal a la información firmada electrónicamente. Esto abre oportunidades por ser más segura que la firma manuscrita. Los medios electrónicos de almacenar información son más eficientes que los medios físicos basados en papel; además se economiza recursos económicos y naturales.

Este trabajo de graduación pretende aportar una base teórica informática para explicar el origen y el funcionamiento de la firma electrónica, y un análisis del respaldo jurídico que tiene actualmente en Guatemala.

Técnicamente, la firma electrónica tiene base en la criptografía, además forma parte de lo que se conoce como Infraestructura de Clave Pública. Se dedica un capítulo para hacer una revisión de los conceptos sobre criptografía y su historia. También se explica el funcionamiento de la Infraestructura de Clave Pública, de qué manera protege la información y cómo asegura ciertas características de la información: confidencialidad, autenticación, integridad, no repudio y disponibilidad.

Se pretende que la población guatemalteca conozca esta alternativa y tenga confianza en ella. También se explican sus beneficios y se redactan recomendaciones a los usuarios, para que utilicen adecuadamente esta tecnología y manipulen de una forma segura su información.

El hecho de tener que aprender a utilizar una nueva tecnología provoca cierta resistencia de aceptación, previendo esto se desarrollaron unas guías de uso. Otro factor que influye para la aceptación de una tecnología, es la percepción de beneficios que proporciona, por lo que se elaboró una descripción de cada beneficio. También se presenta un análisis de los obstáculos que enfrentan los guatemaltecos, al empezar a utilizar esta nueva tecnología.

Para que toda esta información sea accesible a un mayor número de personas, se diseñó una página web donde se publicará información importante sobre la teoría de la firma electrónica. También se publicarán guías de uso para apoyar a quienes deseen empezar a utilizar la firma electrónica. La dirección es la siguiente: <http://firmaelectronicagt.com/>.

1. CONTEXTO PROPÓSITO Y METODOLOGÍA DE LA INVESTIGACIÓN

1.1 Antecedentes

A lo largo del tiempo, la mayoría de países del mundo ha enfrentado una tendencia a la globalización. Esta globalización es más factible con la ayuda de herramientas tecnológicas, como Internet. A raíz de esto en Guatemala ha existido la iniciativa de modernización del Estado. Modernización necesaria debido a tratados internacionales como el TLC.

Sin embargo, en la actualidad en Guatemala, los métodos de aseguramiento de las comunicaciones electrónicas son poco conocidos. Antes del decreto 47-2008 no existía ninguna ley que diera respaldo jurídico a las comunicaciones y firmas electrónicas en general, sino que únicamente para el servicio aduanero a través de un acuerdo del directorio de la SAT.

En junio de 2009 se realizó el lanzamiento oficial de la firma electrónica por parte de la Cámara de comercio de Guatemala, única autoridad certificadora del país actualmente, pero no se ha hecho la suficiente promoción y divulgación de sus beneficios. En ese mismo mes, también quedó habilitado el Registro de Prestadores de Servicios de Certificación en el Ministerio de Economía. Publicaron el reglamento correspondiente, además de algunas guías para las empresas que deseen prestar servicios de certificación en el país.

1.2 Resultados esperados

1) Material informativo, detallando los beneficios a corto y mediano plazo de la utilización de la firma electrónica. Documentación que sirva de guía a los potenciales usuarios.

2) Análisis de la aceptación de la firma electrónica y de los obstáculos para su uso, así como recomendaciones para superarlos.

3) Interpretación en lenguaje coloquial de la “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” y su correspondiente reglamento.

4) Sitio web fácil de usar, que contenga todos los resultados de este proyecto para que estén al alcance de todos y realmente sea de beneficio para los guatemaltecos.

1.3 Alcances y límites

Esta investigación pretende contribuir de cierta manera al desarrollo tecnológico de Guatemala, describiendo a los guatemaltecos los beneficios de la firma electrónica, así como su validez legal y seguridad técnica, pero está limitada a analizar la situación desde la perspectiva de usuario y dar las recomendaciones pertinentes.

La información se encontrará disponible en el sitio Web, pero esta será conocida por los usuarios interesados, en la medida en que las instituciones competentes que tienen comunicación directa con ellos (CCG, RPSC) les informen sobre la disponibilidad de dicho material, mientras se difunde por otros medios.

1.4 Metodología

La metodología a utilizar en la investigación, será **estudio de casos** que incluye entrevistas, encuestas y observación, para poder analizar adecuadamente la situación actual de la implementación de la firma electrónica en Guatemala.

CONTEXTO, PROPÓSITO Y METODOLOGÍA DE LA INVESTIGACIÓN

Para construir el sitio web se utilizará la metodología de **desarrollo incremental**, diseñando y construyendo en iteraciones de corta duración. El uso de esta metodología permitirá evaluar constantemente los avances, así como hacer correcciones, si fuera necesario.

El análisis de la aceptación y de los mayores obstáculos para el uso de la firma electrónica se hará a la luz del modelo de aceptación de tecnología o ***Technology acceptance model (TAM)*** el cual propone que la facilidad de uso y la percepción de utilidad de un nuevo sistema o tecnología, determinan la intención de uso de los individuos.

1.5 Estructura de la tesis

La presente tesis se inicia con una introducción que describe el contexto en que se enmarca este estudio, posteriormente se presenta toda la base teórica en que se fundamenta y también el desarrollo de la investigación, así como, los resultados y conclusiones.

CONTEXTO, PROPÓSITO Y METODOLOGÍA DE LA INVESTIGACIÓN

Esta tesis está constituida por ocho capítulos, este primer capítulo, llamado: Contexto, propósito y metodología de la investigación, pretende que el lector conozca las condiciones en que se realizó la investigación. Posteriormente se encuentra el estudio teórico y fundamento jurídico que comprende los capítulos 2, 3 y 4 que contienen la base informática teórica en la que se fundamenta la firma electrónica y un análisis de las leyes aplicables en Guatemala para la firma electrónica. El desarrollo de la investigación y el aporte se encuentran en los capítulos 5, 6, 7 y 8. Seguidamente se encuentran las conclusiones y recomendaciones, concluyendo con la bibliografía y los apéndices.

2. CRIPTOGRAFÍA Y CIFRADO

La necesidad de enviar información secreta o confidencial a otras personas con la garantía de que no sea vista por nadie más que el destinatario, ha llevado al hombre a inventar métodos para ocultar esta información mientras viaja en el medio; proveyendo al receptor de tecnicismos necesarios para que él si tenga acceso a la información. Así nació la criptografía.

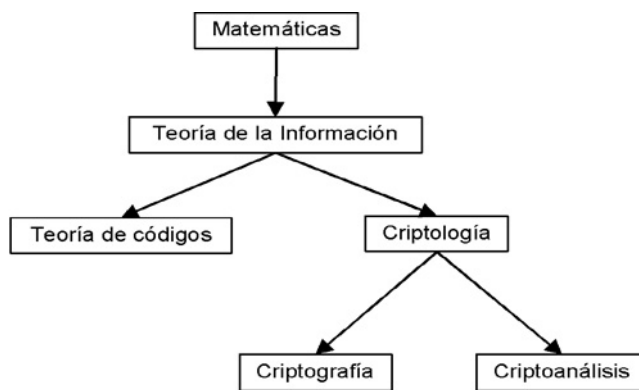
2.1 Criptografía

La palabra criptografía proviene del griego *kryptos*, que significa "ocultar", y *graphos*, que significa "escritura", la traducción literal entonces sería "escritura oculta".

[7]

En la clasificación dentro de las ciencias, la criptografía tuvo su origen en una rama de las matemáticas llamada “Teoría de la información” que fue iniciada por el matemático *Claude Elwood Shannon* en 1948. Esta rama de la ciencia a su vez, se subdivide en: “Teoría de Códigos” y en “Criptología”. La Criptología se subdivide en Criptoanálisis y Criptografía. [7]

Figura 1: Clasificación de la criptografía



Fuente: Revista Digital UNAM

Criptografía es la técnica para convertir un mensaje o información en cifrado utilizando algoritmos, de manera que solo el destinatario pueda leerlo, por ser el único que sabe como descifrarlo (conoce la clave) y así se asegura que aunque el mensaje viaje por un medio inseguro y sea interceptado no podrá ser entendido.

Un algoritmo de cifrado es una función matemática para “desordenar” una información de manera que ésta se transforme en incomprensible. Estos algoritmos hacen uso de una o más claves. A la entrada de esta función, es decir el mensaje que se quiere proteger, se llama información plana, y a la salida después de aplicar el algoritmo con la clave para cifrar, se le llama información cifrada o **criptograma**.

En algunos casos al resultado del cifrado puede aplicársele un algoritmo de descifrado para regresar del criptograma a la entrada que dio lugar al criptograma, si es así, el sistema criptográfico se llama de **dos vías**, en otros casos es imposible volver a reproducir la entrada que dio lugar a un criptograma, en estos casos el sistema criptográfico se llama de **una vía**.

Una clave de cifrado es un conjunto de caracteres con los cuales se puede cifrar una información aplicando un algoritmo de cifrado. Algunos algoritmos de dos vías, utilizan la misma clave para cifrar y descifrar y otros utilizan un par de claves, una para cifrar y otra para descifrar, ese par de claves tiene una correspondencia única entre sí.

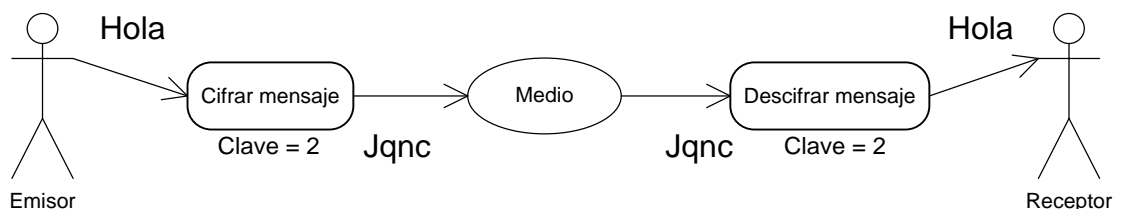
Ejemplo

El emisor desea enviar el mensaje “Hola” pero por seguridad antes de enviarlo lo cifra utilizando el algoritmo de sustituir cada letra por la que esté 2 lugares a la derecha en el alfabeto, o sea la A por la C, la B por la D y así sucesivamente. En este caso la clave sería 2 y el receptor debe conocerla para poder descifrar el mensaje.

En resumen:

- Sistema criptográfico de dos vías.
- Sistema criptográfico de una sola clave.
- Algoritmo: Sustituir cada letra por la que se encuentre N espacios a la derecha en el alfabeto.
- Clave: 2 (Número de espacios a la derecha en el alfabeto).

Figura 2: Ejemplo de cifrado



Como se puede ver, no importa que el mensaje sea visto por un tercero en el medio, porque no lo entendería, entonces el mensaje viaja seguro. **Nótese que la seguridad de los métodos criptográficos, radica en la clave y no en el algoritmo, porque de nada sirve saber con qué algoritmo fue cifrada una información si no tenemos la clave para poder descifrarla.**

2.2 Criptoanálisis

Se dedica a estudiar los métodos para obtener el sentido de una información cifrada, es decir descifrarla sin acceso a la clave, la cual es requerida para obtener este sentido normalmente. El criptoanálisis excluye todos aquellos ataques que no tengan como parte principal explotar los puntos débiles de la criptografía, por ejemplo los ataques denominados de fuerza bruta. [8].

La principal premisa del criptoanálisis es el conocido, Principio de *Kerckhoffs*, que establece que la seguridad del cifrado reside exclusivamente en mantener en secreto la clave, y no en el mecanismo de cifrado.

Para criptoanalizar un criptograma se empieza estableciendo las posibles debilidades del algoritmo, asumiendo las “condiciones del peor caso” que son: el criptoanalista tiene acceso completo al algoritmo de encriptación, el criptoanalista tiene una buena cantidad de texto cifrado, y el criptoanalista sabe cuál fue la entrada que dio lugar al criptograma.

Si el criptoanalista conoce el algoritmo de cifrado, pero sólo tiene acceso al criptograma y no a la entrada, se denomina “ataque sólo al criptograma”; el otro caso es cuando el criptoanalista conoce tanto el criptograma como la entrada, es decir que cumple todas las condiciones del peor caso, entonces el criptoanálisis se denomina “de texto plano conocido”. Cuando el criptoanalista cifra cualquier cantidad de texto plano escogido por él, al ataque se le denomina “de texto plano escogido”.

2.3 Historia de la criptografía

Históricamente, los sistemas criptográficos se dividen en: sistemas criptográficos de sustitución y sistemas criptográficos de transposición.

Los sistemas criptográficos de sustitución mantienen el orden de los símbolos, pero “disfrazan” cada símbolo, utilizando otro símbolo. El sistema criptográfico de sustitución más antiguo que se conoce es el sistema criptográfico César, se llama así porque es atribuido a Julio César. En este método, A se representa por D, B por E, C por F, y así sucesivamente, cada letra se reemplaza por la que se encuentra tres lugares delante de ella, considerando que luego de la Z vuelve a comenzar por la A. Una variante del sistema criptográfico César es permitir que el alfabeto cifrado se pueda desplazar k letras, convirtiéndose entonces k en la clave.

Los métodos de cifrado por transposición no mantienen el orden de los símbolos, sino que los reordenan para cifrarlos. Esto incluye reordenar los datos geoméricamente para hacerlos visualmente ininteligibles. Los griegos utilizaban la escítala espartana, (método de transposición) la cual consistía en enrollar una tira de papiro en un cilindro y escribir el texto sobre el papiro pero a lo largo del cilindro y entonces al desenrollar la tira de papiro y quitar el cilindro se obtenía el mensaje cifrado y para descifrarlo se debía tener un cilindro del mismo diámetro y volver a enrollar el papiro de la misma manera, en este caso el valor del diámetro sería la clave.

Figura 3: Escítala



Fuente: Blog de *Bletchley Park*

Las tropas del rey Felipe II de España utilizaban un método de cifrado con un alfabeto de más de quinientos símbolos, el cual era considerado inviolable; y cuando el matemático francés *Francois Viète* consiguió criptoanalizar este sistema para el rey de Francia Enrique IV, la corte española presentó una queja ante el papa Pío V acusándolo de utilizar magia negra. [9]

La reina María Estuardo, reina de Escocia, fue ejecutada por su prima Isabel I de Inglaterra al descubrirse un complot de aquella tras un criptoanálisis exitoso por parte de los matemáticos de Isabel. [9]

Durante la Primera Guerra Mundial, los alemanes usaron el cifrado ADFGVX que consistía en una matriz de 6 x 6 utilizada para sustituir cualquier letra del alfabeto y los números del 0 al 9 con un par de letras que consiste de A, D, F, G, V, o X. **[9]**

A partir del siglo XX, la criptografía dispone de una nueva herramienta que le permitió conseguir mejores y más seguros cifrados: las máquinas de cálculo. La más conocida probablemente sea la máquina alemana Enigma. Esta máquina disponía de un mecanismo de cifrado rotatorio que permitía usarla tanto para cifrar como para descifrar mensajes. Varios de sus modelos fueron muy utilizados en Europa desde inicios de los años 1920. Su fama se debe a, haber sido utilizada por las fuerzas militares de Alemania desde 1930. Su sistema de cifrado fue finalmente descubierto y la lectura de la información que contenían los mensajes supuestamente protegidos es considerada por algunos, la causa de haber podido concluir la Segunda Guerra Mundial por lo menos dos años antes de lo que hubiera acaecido sin su descifrado. **[10]**

Después de la Segunda Guerra Mundial, la criptografía tuvo un desarrollo teórico importante con Claude Shannon y sus investigaciones sobre teoría de la información que fue importantísima para el desarrollo de la criptografía. Además, los avances en computación suponen tanto una amenaza para los sistemas existentes como una oportunidad para el desarrollo de nuevos sistemas. A mediados de los años 70 la ISO publicó el primer diseño lógico de un sistema criptográfico que fue el principal sistema criptográfico de finales de siglo: el Estándar de Cifrado de Datos o DES por sus siglas en inglés. **[10]**

2.4 Algoritmos de cifrado

Recientemente han existido varios algoritmos de cifrado, la mayoría cuando iniciaron se consideraron muy seguros pero con el pasar del tiempo se les van descubriendo vulnerabilidades y entonces son reemplazados por una nueva versión del mismo o por otro algoritmo completamente nuevo. A continuación describen los algoritmos de cifrado más importantes o que han tenido mayor uso en los últimos años.

2.4.1 *Data Encryption Standard (DES)*

Es un algoritmo de cifrado, escogido como *FIPS*¹ en los Estados Unidos en 1976, y cuyo uso se ha propagado ampliamente por todo el mundo. El algoritmo fue controvertido al principio, con algunos elementos de diseño clasificados, una longitud de clave relativamente corta, y las continuas sospechas sobre la existencia de alguna puerta trasera para la *National Security Agency (NSA)*. Posteriormente DES fue sometido a un intenso análisis académico y motivó el concepto moderno del cifrado por bloques y su criptoanálisis. [11]

¹ FIPS son las siglas en inglés de Estándares Federales de Procesamiento de la Información, son estándares anunciados públicamente, desarrollados por el gobierno de los Estados Unidos para la utilización por parte de todas las agencias del gobierno no militares y por los contratistas del gobierno. Muchos estándares FIPS son versiones modificadas de los estándares usados en comunidades más amplias (ANSI, IEEE, ISO, etc.). [27]

Hoy en día, DES se considera inseguro para muchas aplicaciones. Esto se debe principalmente a que el tamaño de clave de 56 bits es corto y las claves de *DES* se han roto en menos de 24 horas. Existen también resultados analíticos que demuestran debilidades teóricas en su cifrado, aunque son inviables en la práctica. Se cree que el algoritmo es seguro en la práctica en su variante de Triple *DES*, aunque existan ataques teóricos. [11]

Desde hace varios años, este el algoritmo se ha ido sustituyendo por el más reciente, *AES (Advanced Encryption Standard)*.

2.4.2 Triple DES (TDES)

Algoritmo que consiste en hacer tres veces el cifrado del DES. También es conocido como TDES o 3DES, fue desarrollado por IBM en 1978. [12]

Figura 4: Fórmula Triple DES

$$C = E_{DES}^{k_3} \left(D_{DES}^{k_2} \left(E_{DES}^{k_1} (M) \right) \right)$$

Fuente: Wikipedia

2.4.3 Advanced Encryption System (AES)

Es también conocido como *Rijndael*, es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. Se espera que sea usado en el mundo entero y analizado exhaustivamente, como fue el caso de su predecesor, el *Data Encryption Standard (DES)*.

El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología (*NIST*) como *FIPS PUB 197* de los Estados Unidos el 26 de noviembre de 2001 después de un proceso de estandarización que duró 5 años. Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares de criptografía simétrica. **[13]**

2.4.4 *International Data Encryption Algorithm (IDEA)*

Es un sistema criptográfico por bloques diseñado por *Xuejia Lai* y *James L. Massey* de la Escuela Politécnica Federal de Zúrich y descrito por primera vez en 1991. Fue un algoritmo propuesto como reemplazo del *DES*. *IDEA* fue una revisión menor de *PES* (*Proposed Encryption Standard*, del inglés Estándar de Cifrado Propuesto), un algoritmo de cifrado anterior. Originalmente *IDEA* había sido llamado *IPES* (*Improved PES*, del inglés PES Mejorado). **[14]**

IDEA fue diseñado en contrato con la Fundación *Hasler*, la cual se hizo parte de *Ascom-Tech AG*. *IDEA* es libre para uso no comercial, aunque fue patentado y sus patentes se vencerán en 2010 y 2011. El nombre "*IDEA*" es una marca registrada y está licenciado mundialmente por *MediaCrypt*. **[14]**

IDEA fue utilizado como el sistema criptográfico simétrico en las primeras versiones de *PGP* (*PGP v2.0*) y se incorporó luego de que el sistema criptográfico original usado en la v1.0 ("*Bass-O-Matic*") demostró ser inseguro. Es un algoritmo óptimo en *OpenPGP*. **[14]**

2.4.5 *Digital Signature Algorithm*

Es un estándar del Gobierno Federal de los Estados Unidos de América o *FIPS* para firmas digitales. Fue un Algoritmo propuesto por el Instituto Nacional de Normas y Tecnología de los Estados Unidos para su uso en su Estándar de Firma Digital (*DSS*), especificado en el *FIPS* 186. *DSA* se hizo público el 30 de agosto de 1991, este algoritmo como su nombre lo indica, sirve para firmar y no para cifrar información. Una desventaja de este algoritmo es que requiere mucho más tiempo de cómputo que *RSA*. [15]

2.4.6 *RSA*

El sistema criptográfico con clave pública *RSA* es un algoritmo asimétrico de cifrado de bloques, que utiliza una clave pública, la cual se distribuye (en forma autenticada preferentemente), y otra privada, la cual es guardada en secreto por su propietario. [16]

Los mensajes enviados usando el algoritmo *RSA* se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes (mayores que 10100) elegidos al azar para conformar la clave de descifrado. Emplea expresiones exponenciales en aritmética modular. [16]

La seguridad de este algoritmo radica en que no hay maneras rápidas conocidas de factorizar un número grande en sus factores primos utilizando computadoras tradicionales, aunque la computación cuántica podría proveer una solución a este problema de factorización. [16]

2.5 Función de *hash*

Se trata de una función que sirve para representar y resumir de manera unívoca un mensaje o información. Al resultado de una función de hash se le llama resumen o en inglés, *message digest*. Entonces un resumen es único para una sola entrada y que el cambio más mínimo en la entrada, el resumen salida totalmente diferente. En una firma electrónica, este resumen se calcula cuando el remitente envía el mensaje y es adjuntado al mensaje para que el destinatario vuelva a calcularlo y si es igual al que va adjuntado que fue calculado por el emisor, se tiene la seguridad de que no ha cambiado el mensaje en el medio debido a las características de las funciones de *hash* (correspondencia unívoca).

2.5.1 Algoritmos para calcular la función de *hash*

A continuación se describe brevemente los principales algoritmos que se utilizan para calcular la función de *Hash*.

2.5.1.1 MD5

MD5 es la abreviatura de *Message-Digest Algorithm 5* en español, Algoritmo de Resumen del Mensaje 5 y es un algoritmo de reducción criptográfico de 128 bits.

Es uno de los algoritmos de reducción criptográficos diseñados por el profesor *Ronald Rivest* del *MIT* desarrollado en 1991 como reemplazo del algoritmo *MD4* después de que *Hans Dobbertin* descubriese su debilidad. [17]

Los ciento veintiocho bits del MD5 son representados por lo general como un número hexadecimal de treinta y dos dígitos.

A pesar de haber sido considerado criptográficamente seguro en un principio, ciertas investigaciones han revelado vulnerabilidades que hacen cuestionable el uso futuro del *MD5*; en agosto de 2004, *Xiaoyun Wang, Dengguo Feng, Xuejia Lai* y *Hongbo Yu* anunciaron el descubrimiento de colisiones de hash para *MD5*; Su ataque se consumó en una hora de cálculo con un clúster *IBM P690*. [17]

2.5.1.2 SHA

La familia *SHA* (*Secure Hash Algorithm*, Algoritmo de Hash Seguro) es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el *National Institute of Standards and Technology* (*NIST*). El primer miembro de la familia fue publicado en 1993 es oficialmente llamado *SHA.*, sin embargo hoy día, no oficialmente se le llama *SHA-0* para evitar confusiones con sus sucesores; dos años más tarde el primer sucesor de *SHA* fue publicado con el nombre de *SHA-1*. [18]

Existen cuatro variantes más que se han publicado desde entonces cuyas diferencias se basan en un diseño algo modificado y rangos de salida incrementados: *SHA-224, SHA-256, SHA-384, y SHA-512* (llamándose *SHA-2* a todos ellos). [18]

SHA-1 ha sido examinado muy de cerca por la comunidad criptográfica pública, y no se ha encontrado ningún ataque efectivo; no obstante, en el año 2004, un número de ataques significativos fueron divulgados sobre funciones criptográficas de hash con una estructura similar a *SHA-1*; lo que ha planteado dudas sobre la seguridad a largo plazo de *SHA-1*. [18]

SHA-0 y *SHA-1* producen una salida resumen de 160 bits (20 bytes) de un mensaje que puede tener un tamaño máximo de 264 bits, y se basa en principios similares a los usados por el profesor *Ronald L. Rivest* del *MIT* en el diseño de los algoritmos de resumen de mensaje *MD4* y *MD5*. [18]

2.6 Tipos de sistemas criptográficos

Anteriormente se mencionó que los sistemas criptográficos se pueden clasificar por distintos criterios. Es importante la clasificación de los sistemas criptográficos por la clave que utilizan para descifrar. Existen los sistemas criptográficos de clave simétrica que para descifrar utilizan la misma clave que para cifrar y los sistemas criptográficos de clave pública, que utilizan un par de claves, una para cifrar y la otra para descifrar.

2.6.1 Sistemas criptográficos de clave simétrica

La característica primordial de estos sistemas, es que utilizan la misma clave para cifrar que para descifrar. Para mantener la seguridad, esta clave debe ser secreta y únicamente la deben conocer el emisor (Para cifrar) y el receptor. (Para descifrar).

Dado que toda la seguridad está en la clave por el principio de *Kerckhoffs*, es importante que sea muy difícil adivinar la clave; esto quiere decir que el abanico de claves posibles, o sea, el espacio de posibles de claves, debe muy ser amplio. **[19]**

Richard Feynman fue famoso en Los Álamos por su habilidad para abrir cajas de seguridad; para alimentar la leyenda que había en torno a él, llevaba encima un juego de herramientas que incluían un estetoscopio; en realidad, utilizaba una gran variedad de trucos para reducir a un pequeño número la cantidad de combinaciones que debía probar, y a partir de ahí simplemente probaba hasta que adivinaba la combinación correcta. En otras palabras, reducía el tamaño de posibilidades de claves. **[19]**

Actualmente, los ordenadores pueden descifrar claves con extrema rapidez, y ésta es la razón por la cual el tamaño de la clave es importante en los sistemas criptográficos modernos. **[19]**

2.6.2 Sistemas criptográficos de clave pública

Estos sistemas al contrario de los anteriores utilizan una clave para cifrar y otra para descifrar. Las dos claves pertenecen a la misma persona. Una de estas claves es pública y se puede distribuir, mientras que la otra es privada y solamente el propietario debería conocerla. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente una de las dos claves iguales. [20]

Si el emisor usa la clave pública del receptor para cifrar el mensaje, una vez cifrado, sólo la clave privada del receptor podrá descifrar este mensaje. Por tanto se logra la confidencialidad del envío del mensaje, nadie excepto el receptor puede descifrarlo porque solo él conoce su clave privada.

Si el propietario del par de claves usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública; en este caso se consigue por lo tanto la identificación y autenticación del remitente, ya que se sabe que sólo pudo haber sido él quien empleó su clave privada (solo él la conoce) para cifrar el mensaje. Esta idea es el fundamento de la firma electrónica. [20]

2.6.2.1 Funcionamiento

Estos sistemas se basan en funciones trampa (sistema criptográfico de una vía) que aprovechan propiedades particulares de los números primos. Una función de un solo sentido es aquella cuya computación es fácil, mientras que su inversión resulta extremadamente difícil.

Por ejemplo, es fácil multiplicar dos números primos juntos para obtener uno compuesto, pero es difícil factorizar uno compuesto en sus componentes primos. Una función trampa de una vía es algo parecido, pero tiene una "trampa". Esto quiere decir que si se conociera alguna pieza de la información, sería fácil computar el inverso. Por ejemplo, si se tiene un número compuesto por dos factores primos y se conoce uno de los factores, es fácil computar el segundo. **[20]**

Dado un cifrado de clave pública basado en factorización de números primos, la clave pública contiene un número compuesto de dos factores primos grandes, y el algoritmo de cifrado usa ese compuesto para cifrar el mensaje. Entonces el algoritmo para descifrar el mensaje requiere el conocimiento de los factores primos para que el descifrado sea fácil si se posee la clave privada que contiene uno de los factores, pero extremadamente difícil en caso contrario. **[20]**

3. FIRMA ELECTRÓNICA Y PKI

La firma electrónica es una herramienta muy utilizada hoy en día para asegurar las comunicaciones electrónicas. El medio por el que viajan las comunicaciones electrónicas por lo general es Internet y éste es muy inseguro por lo que se puede enviar información importante sin cifrarla. Aparte de la seguridad de que la información no sea robada o accedida sin autorización en Internet se necesita algo que asegure que la identidad de la persona con la que se está estableciendo comunicación es verdadera, toda esta seguridad la brinda la firma electrónica.

Figura 5: En Internet nadie sabe que eres un perro



Fuente: Wikipedia

3.1 Firma electrónica

La firma electrónica es una herramienta tecnología que sirve para asegurar las comunicaciones electrónicas. Las definiciones más relevantes de firma electrónica son las siguientes:

La firma electrónica hace referencia, a la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje. **[21]**

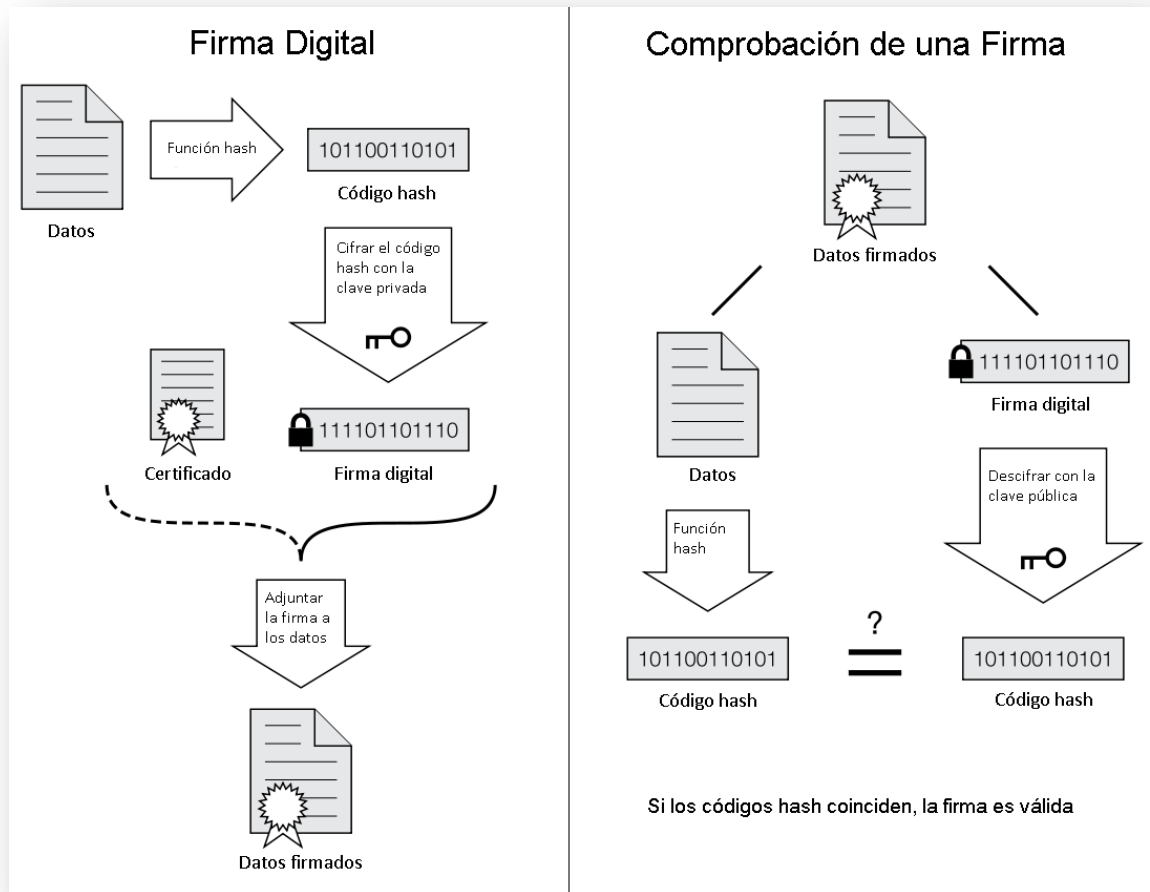
Datos en forma electrónica consignados en una comunicación electrónica, o adjuntado o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante con relación a la comunicación electrónica e indicar que el firmante aprueba la información recogida en la comunicación electrónica. **[2]**

La firma electrónica de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido y, seguidamente, aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica o digital. **[21]**

Resumiendo: la firma electrónica es el análogo en el mundo digital para la firma manuscrita y sirve para asegurar la identidad del firmante, que la información no ha sido modificada después de ser firmada, y que el firmante no puede negar que firmó.

El procedimiento de firma se puede apreciar en el siguiente diagrama.

Figura 6: Generación y verificación de una firma electrónica



Fuente: Wikipedia

Los pasos para firmar electrónicamente son los siguientes:

1. El emisor aplica la función de hash a los datos y el resultado es el resumen.
2. El emisor cifra el resumen utilizando su clave privada. A esto es a lo que se le llama "firma".
3. El emisor adjunta la "firma" y su certificado de identidad al documento. En este punto ya están firmados los datos, ahora el emisor se los envía al receptor.
4. El receptor aplica la función de hash a los datos y con esto obtiene un resumen calculado por el mismo.
5. El receptor descifra el resumen con la clave pública del emisor, que va en el certificado de identidad de éste, con esto el receptor obtiene el resumen que calculó el emisor antes de enviarle los datos.
6. Si el resumen calculado por el receptor coincide con el resumen generado por el emisor, los datos están íntegros y no han sufrido ninguna modificación.
7. A esto únicamente resta ver la información del certificado para estar seguros de la identidad del emisor.

3.3 ¿Qué asegura la firma electrónica?

3.3.1 Autenticación

La autenticación se refiere a la seguridad de que el remitente del mensaje es realmente quien dice ser. Una firma electrónica asegura la autenticación porque existe una autoridad certificadora que se encarga de asegurar que la pareja de claves, pública y privada pertenecen exclusivamente a una persona y dicha autoridad ha verificado su identidad. La firma electrónica garantiza la identidad digital del remitente de una comunicación.

3.3.2 Integridad

La integridad es la propiedad de la información que garantiza que no ha sido modificada intencionalmente, ni debido a errores, de transmisión o de almacenamiento en un período de tiempo determinado.

Esta propiedad la asegura la firma electrónica, a través de la función de hash, porque si al verificar la firma y comparar el resultado de la función de hash calculada, con el que está adjunto a la firma se garantiza que la información no ha sido alterada desde que se firmó electrónicamente hasta el momento en que se vuelve a calcular el resumen, con la función de hash.

3.3.3 No repudio

El no repudio es también conocido como irrenunciabilidad. Hace referencia a la incapacidad de rechazar algo o no aceptarlo, en este caso se refiere a negar que fuera firmada electrónicamente la información que contiene firma.

La firma electrónica garantiza que el emisor de un mensaje no podrá negar que firmó el mensaje, debido que, para firmar algo electrónicamente se necesita tanto de la clave privada como su certificado de identidad. El propietario de un certificado digital está obligado por la ley, a custodiar su certificado de identidad y su clave privada.

El no repudio puede darse de las siguientes maneras.

No Repudio de origen: El emisor no puede negar que envió el mensaje, porque el destinatario tiene pruebas del envío. [22]

No Repudio de destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. [22]

La firma electrónica puede garantizar el no repudio de origen porque se supone que los datos de creación de firma están únicamente bajo el poder del emisor, pero para garantizar el no repudio de destino, se debe acordar entre los participantes de comunicación, enviar un acuse de recibo firmado electrónicamente, al emisor, dentro de cierto tiempo después de enviada la comunicación de manera que el emisor tenga prueba irrefutable de la recepción del mensaje.

3.3.4 Confidencialidad

La confidencialidad de la información es la propiedad que garantiza que únicamente el o los destinatarios podrán tener acceso a ella. Según la norma ISO 17799, la confidencialidad es “garantizar que la información es accesible sólo para aquellos autorizados a tener acceso”.

La firma electrónica en sí no garantiza la confidencialidad; la confidencialidad es asegurada únicamente si tanto el remitente como el destinatario poseen un certificado digital, porque entonces el emisor puede cifrar el mensaje con la clave pública del destinatario de manera que pueda ser descifrado únicamente con la clave privada del destinatario (que solo él conoce) debido a se trata de un sistema criptográfico asimétrico. Entonces si un tercero interceptara el mensaje, no sería capaz de leerlo dado que no posee la clave privada del destinatario.

3.4 Certificado digital

Un certificado digital, o certificado digital de clave pública, o certificado digital de identidad, es un documento digital mediante el cual, un tercero de confianza (Autoridad de Certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública. **[23]**

Si bien existen variados formatos para certificados digitales, los más comúnmente empleados se rigen por el estándar UIT-T X.509. El certificado contiene usualmente información sobre el individuo o entidad certificada y la firma electrónica de la autoridad emisora del certificado de forma que el receptor pueda verificar que esta última ha establecido realmente la asociación. **[23]**

3.4.1 Información que contiene un certificado digital

Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

- Nombre, dirección y domicilio del suscriptor.
- Identificación del suscriptor nombrado en el certificado.
- El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
- La clave pública del usuario.
- La metodología para verificar la firma electrónica del suscriptor impuesta en el mensaje de datos.
- El número de serie del certificado.
- Fecha de emisión y expiración del certificado.

[23]

3.5 Autoridad certificadora

La Autoridad certificadora (CA por sus siglas en inglés *Certification Authority*) es una entidad de confianza, responsable de emitir y revocar los certificados digitales. Jurídicamente es un caso particular de Prestador de Servicios de Certificación o uno de los servicios que presta. [24]

La Autoridad de Certificación, por sí misma o mediante la intervención de otra entidad, verifica la identidad del solicitante de un certificado antes de expedírsele. En este procedimiento de verificación de la identidad del solicitante radica la confianza que se puede tener a las firmas electrónicas.

El principal objetivo de la Autoridad Certificadora es legitimar ante los quienes confían en sus certificados, la relación entre la identidad de un usuario y su clave pública. La confianza de los usuarios en la Autoridad Certificadora es importante para el funcionamiento del servicio y justifica la filosofía de su empleo. [24]

En Guatemala se creó el Registro de Prestadores de Servicios de Certificación, cuya función es inspeccionar, controlar y vigilar las actividades de los Prestadores de Servicios de Certificación; con el objetivo de brindar una mayor confianza a los usuarios de firma electrónica en el país.

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 como Autoridad Certificadora 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 auditorias para dar mayor confianza a los usuarios, por ejemplo en Guatemala el RPSC. Además es recomendable leer el *Certification Practice Statement (CPS)* donde se especifica los procedimientos para comprobar la identidad.

Una analogía que ayuda a entender la función y objetivo de la Autoridad Certificadora y los Certificados es la del Registro Nacional de 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.**

3.5.1 Servicios que provee una autoridad certificadora

Las autoridades certificadoras o en general, los prestadores de servicios de certificación proveen varios servicios además de la firma electrónica, estos servicios por lo general son los siguientes.

3.5.1.1 firma electrónica simple

La firma electrónica simple, únicamente incluye el resultado de la operación de hash y el certificado utilizado con la clave privada para firmar.

3.5.1.2 firma electrónica avanzada

La firma electrónica avanzada, además de tener el resultado de la operación de hash y el certificado utilizado con la clave privada para firmar, incluye también un estampado cronológico calculado a partir del resultado de la función de hash y firmado por una autoridad de estampado cronológico TSA que por lo general es la misma autoridad certificadora CA o entidad prestadora de servicios de certificación.

3.5.1.3 estampado cronológico

También conocido como *Timestamping*, es un mecanismo en línea que permite demostrar que una información ha existido y no ha sido alterada desde un instante específico en el tiempo. Este protocolo se describe en el *RFC 3161* y está en el registro de estándares de Internet. Una Autoridad de estampado cronológico actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos. [25]

Los pasos para hacer un estampado cronológico son los siguientes:

- Se aplica la función de hash para generar el resumen.
- Este resumen es la solicitud que se envía a la autoridad de estampado cronológico.
- La autoridad de estampado cronológico genera el estampado en el resumen, la fecha y hora son obtenidas de una fuente fiable y luego la autoridad firma electrónicamente el resumen con el estampado.
- La autoridad de estampado envía de vuelta el resumen con el estampado.

- La autoridad de estampado mantiene un registro de los estampados emitidos para su futura verificación.

3.5.1.4 custodia de documentos

Es un servicio electrónico basado en la custodia de archivos y documentos electrónicos. Este servicio puede consumirse vía Web o integrarse con distintas aplicaciones de empresas a través de *Web Services*. Está orientado a la custodia de facturas electrónicas, sin embargo se ha utilizado en la aseguración de archivos que necesitan ser almacenados, ya sea especificación de normativas o simplemente para permitir a otros usuarios (clientes por ejemplo) puedan visualizar o descargar los archivos.

Los documentos almacenados pueden llevar un *TimeStamping* de manera de asegurar el minuto en que se agregó el archivo a la plataforma y tener un registro de que este no ha sido modificado.

3.5.2 Diferencias entre la firma electrónica simple y la firma electrónica avanzada

Existen dos tipos de firma electrónica reguladas en la legislación guatemalteca, la simple y la avanzada. La diferencia fundamental es la seguridad que proveen y jurídicamente, la avanzada tiene validez plena, mientras que la simple, queda a criterio del juez.

Técnicamente, la firma electrónica simple, solo incluye el resultado de la operación de hash, mientras que la firma electrónica avanzada, además de tener el resultado de la operación de hash y el certificado utilizado con la clave privada para firmar, incluye también un estampado cronológico calculado a partir del hash y firmado por una autoridad de estampado cronológico (TSA).

Se puede probar el funcionamiento una firma electrónica simple, mediante el siguiente servicio gratuito. <http://ca.albalia.es:8080/democa/>

3.6 Infraestructura de clave pública (PKI)

Es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma electrónica o el no repudio de transacciones electrónicas. [26]

El término *PKI* se utiliza para referirse tanto a la autoridad de certificación y al resto de componentes, como para referirse, de manera más amplia y a veces confusa, al uso de algoritmos de clave pública en comunicaciones electrónicas. Este último significado es incorrecto, ya que no se requieren métodos específicos de *PKI* para usar algoritmos de clave pública. [26]

La tecnología *PKI* permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad para cifrar y descifrar mensajes, firmar electrónicamente información, garantizar el no repudio de un envío, y otros usos. [26]

En una operación criptográfica que use infraestructura *PKI*, intervienen conceptualmente como mínimo las siguientes partes:

1. Un usuario iniciador de la operación
2. Sistemas o servidores que dan fe de la ocurrencia de la operación y garantizan la validez de los certificados implicados en la operación (autoridad de certificación, Autoridad de registro y sistema de Sellado de tiempo)
3. Un destinatario de los datos cifrados/firmados/enviados garantizados por parte del usuario iniciador de la operación.

Las operaciones criptográficas de clave pública son procesos en los que se utilizan unos algoritmos de cifrado que son conocidos y están accesibles para todos. Por este motivo la seguridad que puede aportar la tecnología *PKI*, está fuertemente ligada a la privacidad de la clave privada y los procedimientos operativos o políticas de seguridad aplicadas. **[26]**

Es importante destacar la importancia de las políticas de seguridad en esta tecnología, puesto que ni los dispositivos más seguros ni los algoritmos de cifrado más fuertes sirven de nada, si por ejemplo una copia de la clave privada protegida por una tarjeta criptográfica (*smart card*) se guarda en un disco duro convencional de una computadora conectada a Internet porque la clave privada queda totalmente expuesta. **[26]**

La seguridad en la infraestructura *PKI* depende de cómo se guarden en secreto las claves privadas por ello existen dispositivos especiales denominados *tokens* de seguridad diseñados para facilitar seguridad de la clave privada, así como evitar que ésta pueda ser exportada. Estos dispositivos pueden incorporar biométricos, como la verificación de huella dactilar, que permiten aumentar la confiabilidad. **[26]**

3.6.1 Componentes de una *PKI*

Los componentes más habituales de una infraestructura de clave pública son:

- La Autoridad de Certificación. Es la pieza central y la que proporciona la base de confianza en la *PKI*. Constituido por elementos hardware, software y, evidentemente, humanos.
- Publicación de Certificados. El repositorio de certificados permite a los usuarios operar entre ellos (para la validación de una firma electrónica), y es un requisito legal que cuente con una total disponibilidad de acceso.
- Soporte de la Clave Privada. La elección de un buen soporte para que los usuarios custodien su clave privada es un punto esencial y complejo en sí mismo. Por ejemplo si la clave está en una *SmartCard*, es necesario diseñar el Sistema de Gestión de *SmartCards* que permita la emisión y distribución de las tarjetas a los usuarios.
- Aplicaciones "*PKI-Enabled*". Se denomina así a las aplicaciones software, capaces de operar con certificados digitales. Estas aplicaciones son las que dan el valor real de la *PKI* de cara al usuario.
- Políticas de Certificación. Deben diseñarse una serie de políticas, o procedimientos operativos, que rigen el funcionamiento de la *PKI* y establecen los compromisos entre la Autoridad Certificadora y los Usuarios Finales. Estos documentos tienen un carácter tanto técnico como legal.

[26]

4. ANÁLISIS JURÍDICO DE LA FIRMA ELECTRÓNICA EN GUATEMALA

En Guatemala no existía legislación que diera respaldo jurídico a las comunicaciones por medios electrónicos de ningún tipo hasta el año 2008. Esta es una época en la que se utiliza a diario muchos medios electrónicos en todos los ámbitos, prácticamente es parte de la vida cotidiana, por lo que se hizo necesario y urgente regular las comunicaciones electrónicas y darles el respaldo jurídico pertinente a las que cumplan con ciertos requisitos de seguridad. A raíz de esto nace la iniciativa de ley 3515 que contiene la “Ley para el reconocimiento de comunicaciones y firmas electrónicas” cuyo objetivo principal es: conceder equivalencia jurídica entre las comunicaciones electrónicas y los documentos en papel. Con esta ley, las comunicaciones electrónicas tienen plena validez como medio de manifestar la voluntad siempre que cumplan con garantizar su integridad disponibilidad y autenticación.

La “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” tiene como base la Ley modelo sobre Firma Electrónica debido que la legislación en materia comercial electrónica debe ser homogénea y uniforme con las normas internacionales porque si no existiría un alto riesgo de incompatibilidad.

ANÁLISIS JURÍDICO DE LA FIRMA ELECTRÓNICA EN GUATEMALA

Esta ley está compuesta por 56 artículos contenidos en 3 títulos y 7 capítulos de la siguiente manera:

TITULO I Comercio electrónico en general

CAPITULO I Disposiciones generales

CAPITULO II Aplicación de los requisitos jurídicos a las comunicaciones electrónicas

CAPITULO III Comunicaciones electrónicas y formación de contratos a través de medios electrónicos

TITULO II Comercio electrónico en materias específicas

CAPITULO I Transporte de mercancías

TITULO III Disposiciones complementarias al comercio electrónico

CAPITULO I Firma electrónica avanzada y prestadores de servicios de certificación

CAPITULO II Registro de prestadores de servicios de certificación

CAPITULO III Disposiciones varias

4.1 Antecedentes de la Ley

El 22 de mayo de 2009 en el Centro de Tecnologías de Información y Comunicación del INTECAP, se reunieron varios sectores vinculados con el tema de la firma electrónica en Guatemala, fueron invitados a emitir su opinión entorno a éste tema. La Ingeniera María Mercedes Zaghi comentó cómo nació la iniciativa de ley de la firma electrónica en Guatemala, indicó que se inició en el año 2001. Esta iniciativa de ley fue mal interpretada según manifestó el Diputado Rayo, por lo que se reiteró la iniciativa en el 2002 explicando que el objetivo no era “regular el Internet” como algunos medios de comunicaciones lo interpretaron, sino dar seguridad técnica y jurídica a las comunicaciones electrónicas. Hasta el 19 de septiembre de 2008 dicha iniciativa fue aprobada por la comisión de Economía y Comercio Exterior del Congreso de la República, presidida por el Diputado Mariano Rayo. Según la ingeniera Zaghi la ley contempla tres aspectos: 1) regular el comercio electrónico. 2) Reconocer la validez de los documentos y la contratación electrónica. 3) Certeza jurídica a medios electrónicos.

Anterior a esta ley no existía ninguna ley relacionada con las TICs excepto la Ley de propiedad intelectual. Del lado del gobierno existían ciertos proyectos aislados que si tenían respaldo jurídico a través de decretos gubernativos como por ejemplo el proyecto de las aduanas en la SAT, en el cual ya se utilizaba la firma electrónica con respaldo jurídico a través de del acuerdo del directorio de la SAT número 014—2007, entre estos proyectos también se puede mencionar BancaSAT y la facturación electrónica.

En el capítulo catorce del tratado de libre comercio CAFTA-DR, que está dedicado exclusivamente al comercio electrónico, las partes se comprometieron a facilitar la participación electrónica de las empresas. En el numeral 4.3 del capítulo 14 dice literalmente: “Ninguna de las partes impondrá restricción alguna al libre intercambio tecnológico y comercio electrónico”. Ese compromiso adquirido y el hecho de que la SAT había estado a la vanguardia en ese tema en el país, contribuyó a la aprobación de la iniciativa.

4.2 Puntos clave de la ley

La “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” tiene como objetivo principal, equiparar los medios físicos con su alternativo medio electrónico y por eso hay dos ideas importantísimas que están presentes en esta ley y son: que tiene la misma validez y fuerza probatoria ante la ley que la firma manuscrita; y que es aplicable a cualquier tipo de contrato exceptuando el derecho de familia. A continuación se analizan y describen los puntos principales de la “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” Decreto 47-2008 del Congreso de la República de Guatemala.

4.2.1 Elemento probatorio ante la ley

La Ley no solamente otorga fuerza probatoria a la información electrónica que cuente con firma electrónica y firma electrónica avanzada, sino también a todas aquellas comunicaciones electrónicas que cumplan con los criterios establecidos en la misma ley, los cuales se resumen en fiabilidad de la comunicación y su conservación para poder ser presentada como prueba.

A continuación, se presentan los dos artículos donde se contiene lo anteriormente mencionado:

Artículo 11. Admisibilidad y fuerza probatoria de las comunicaciones electrónicas. *Las comunicaciones electrónicas serán admisibles como medios de prueba. No se negará eficacia, validez o fuerza obligatoria y probatoria en toda actuación administrativa, judicial o privada a todo tipo de información en forma de comunicación electrónica, por el solo hecho que se trate de una comunicación electrónica, ni en razón de no haber sido presentado en su forma original.*

Artículo 12. Criterio para valorar probatoriamente una comunicación electrónica. *Toda información presentada en forma de comunicación electrónica gozará de la debida fuerza probatoria de conformidad con los criterios reconocidos por la legislación para la apreciación de la prueba. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje; la fiabilidad de la forma en la que se haya conservado la integridad de la información; la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.*

4.2.2 Aplicable a todo tipo de contratación, compra o trámite

Según esta ley, cualquier cosa que se pueda hacer en papel, también se podría hacerla por medios electrónicos y tendrá la misma fuerza jurídica. En el primer artículo de la ley se especifica esto y aclara las únicas excepciones, es decir los únicos casos en los que no sería válido utilizar medios electrónicos.

Artículo 1. Ámbito de aplicación. *La presente ley será aplicable a todo tipo de comunicación electrónica, transacción o acto jurídico, público o privado, nacional o internacional, salvo en los casos siguientes:*

- a) En las obligaciones contraídas por el Estado en virtud de Convenios o Tratados internacionales.*
- b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización uso o consumo.*

Como se puede ver en el artículo 1, se excluye a las obligaciones contraídas por el Estado en virtud de Convenios o Tratados internacionales, como el TLC por ejemplo, esto se debe probablemente a la solemnidad que estas obligaciones requieren además de la presencia física de algunos funcionarios.

La otra excepción son las advertencias escritas que deben ir impresas en productos cuyo uso, consumo o comercialización representa riesgo, precisamente para resguardar la seguridad de quienes lo utilizan o manipulan, es sumamente importante que dicha advertencia se encuentre impresa en la etiqueta ya que no sería de la misma utilidad si solamente se encuentra en algún medio electrónico como una página Web por ejemplo porque existe la posibilidad de que no sea visto cuando es necesario.

4.2.3 Misma validez ante la ley que el papel

Al haber analizado las características de la firma electrónica, y sabiendo que garantiza la integridad y la autenticación, esto justifica el que tenga la misma validez y efectos jurídicos que la firma manuscrita. De hecho es mucho más segura la firma electrónica que la firma manuscrita, porque garantiza más aspectos de la información como la confidencialidad y la disponibilidad a través de otros servicios complementarios de los prestadores de servicios de certificación.

En el artículo 33 de la “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” se otorga plena validez jurídica a la firma electrónica, diciendo que ésta 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.

Hay que tener en cuenta que para presentarla como prueba en un juicio, debe ser presentada en alguna forma electrónica confiable y no puede ser trasladada a papel imprimiéndola, debería entonces haber en los tribunales peritos expertos en el tema que puedan valorarla como prueba.

A continuación, se copia literalmente el artículo 33:

Artículo 33. Efectos jurídicos de una firma electrónica o firma electrónica avanzada. *La firma electrónica o la firma electrónica avanzada, la cual podrá estar certificada por una entidad prestadora de servicios de certificación, que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose esta, según los criterios de apreciación establecidos en las normas procesales.*

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

Cuando una firma electrónica haya sido fijada en una comunicación electrónica se presume que el suscriptor de aquella tenía la intención de acreditar esa comunicación electrónica y de ser vinculado con el contenido del mismo. Para considerarse fiable el uso de una firma electrónica avanzada ésta tendrá que incorporar como mínimo los atributos siguientes:

- a) *Que los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante.*
- b) *Que los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante.*
- c) *Que sea posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma y,*
- d) *Cuando uno de los objetivos del requisito legal de la firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, que sea posible detectar cualquier alteración de esa información hecha después del momento de la firma.*

Lo dispuesto en este artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre, de cualquier otra manera, la fiabilidad de una firma electrónica; o, que aduzca pruebas de que una firma electrónica no es fiable.

Este artículo contempla la posibilidad de demostrar la fiabilidad de una firma, así como la no fiabilidad, para ser considerado en un juicio y podría ser la razón de presentar recursos luego de un fallo, aunque demostrar técnicamente que una firma no es fiable, implicaría muchos recursos y que la infraestructura del prestador de servicios de certificación tenga muchas vulnerabilidades, probablemente la forma más común de que una firma electrónica no sea válida, sea porque los datos de creación de la firma han quedado expuestos.

4.2.4 No válida para celebraciones de compromiso de familia

Como se puede ver en el artículo 33, el derecho de familia y las disposiciones por causa de muerte no pueden firmarse electrónicamente debido que son contratos muy solemnes en los que se requiere la presencia física de quien los suscribe.

Este es un punto clave de la ley, el derecho de familia es importantísimo en Guatemala. El hecho de que no se pueda firmar electrónicamente nada de lo concerniente a la familia, por ejemplo el matrimonio, declarar a alguien muerto, le da un mayor énfasis a esa importancia y protege de cierta manera a las familias guatemaltecas.

4.2.5 Información contenida en los certificados digitales

Por último, se quiere resaltar la información que contienen los certificados con los que se firma electrónicamente, tal vez no sea un punto clave de la ley, pero es importante que además de los estándares técnicos que existen como el *DSS* que se revisó en el capítulo anterior, la ley también enumere la información mínima que deben contener los certificados digitales de clave pública.

Artículo 46. Contenido de los certificados. *Un certificado emitido por un prestador de servicios de certificación autorizado, además de estar firmado electrónicamente por éste, debe contener por lo menos lo siguiente:*

- a) Nombre, dirección y domicilio del firmante.*
- b) Identificación del firmante nombrado en el certificado.*
- c) El nombre, la dirección y el lugar donde realiza actividades la prestadora de servicios de certificación.*
- d) La clave pública del usuario den 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.*

4.3 Equiparación de medios electrónicos con medios físicos

Hay tres aspectos importantes en los que se equiparan los medios físicos y los medios electrónicos en la “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” estos aspectos son: el escrito, la firma y el original. Las comunicaciones y firmas electrónicas tienen la capacidad de cumplir estos tres aspectos totalmente porque se basan en tres requisitos importantes de la información que son la disponibilidad, la integridad y la autenticación. La disponibilidad se refiere a la seguridad de poder ver la información cuando se quiera o se necesite. La integridad se refiere a que la información permanezca exactamente igual en un período de tiempo, es decir que no se pueda modificar intencionalmente, ni por alguna falla de los sistemas. La autenticación significa que se tiene la confianza de que el firmante es verdaderamente quien dice ser.

4.3.1 Escrito

A continuación se cita literalmente el artículo 7 de la “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” en el cual se da validez a una comunicación electrónica para que cumpla el requisito de que una información conste por escrito, siempre y cuando sea accesible para su ulterior consulta, es decir que cumpla con el requisito de **disponibilidad** de la información. Esto podría ser por medio del servicio de custodia de documentos que proveen los prestadores de servicios de certificación y mediante el cual garantiza conservar la información íntegra.

***Artículo 7. Escrito.** Cuando cualquier norma jurídica requiera que una información, comunicación o un contrato consten por escrito, en papel o en cualquier otro medio físico, o prevea consecuencias en el caso de que eso no se cumpla, una comunicación electrónica cumplirá ese requisito si la información consignada en su texto es accesible para su ulterior consulta.*

4.3.2 Firma

La firma manuscrita tiene como fin identificar y asegurar la identidad de un autor o remitente, o, como una prueba del consentimiento o aprobación de la información que está firmando, esto se hace a través de un pequeño trazo o dibujo personal que supuestamente solo el dueño puede hacerlo. Igualmente la firma electrónica tiene el objetivo de identificar al autor, pero se vale de procedimientos mucho más confiables, y no solo de la suposición que la firma manuscrita solamente puede hacerla su dueño.

Para firmar electrónicamente, son necesarios datos de creación de firma, que solamente posee la persona vinculada con esa firma, además, para asegurar la identidad del firmante, el prestador de servicios de certificación está obligado por la ley a comprobar su identidad antes de emitirle el certificado y precisamente en eso radica la autenticación en la firma electrónica.

A continuación, se pone el artículo 8 el cual equipara la firma manuscrita con la firma electrónica como medio de **autenticación**.

Artículo 8. Firma. *Cuando cualquier norma jurídica requiera que una comunicación o un contrato sea firmado por una parte, o prevea consecuencias en el caso de que no se firme, ese requisito se dará por cumplido respecto de una comunicación electrónica:*

- a) Si se utiliza un método para determinar la identidad de esa parte y para indicar la voluntad que tiene tal parte respecto de la información consignada en la comunicación electrónica; y,*
- b) Si el método empleado:*
 - 1. Es fiable y resulta apropiado para los fines para los que se generó o transmitió la comunicación electrónica, atendidas todas las circunstancias del caso, inclusive todo acuerdo aplicable; o si,*
 - 2. Se ha demostrado en la práctica que, por si solo o con el respaldo de otras pruebas, dicho método cumple las funciones enunciadas en la literal a) del presente artículo.*

El método fiable y apropiado a que hace referencia este artículo se refiera al procedimiento para asegurar la identidad que utilizan los prestadores de servicios de certificación.

4.3.3 Original

Si se requiere que un documento conste en original, es porque se necesita asegurar dos requerimientos en la información que contiene, el primero es la **integridad**, es decir que permanezca sin modificaciones a lo largo del tiempo y el segundo es la **disponibilidad**, es decir que se pueda consultarlo cuando se necesite o se quiera. Estos dos requerimientos de la información pueden quedar satisfechos con una firma electrónica, porque como ya se vio anteriormente ésta tiene la capacidad de cumplir con ambos requerimientos.

A continuación, el artículo que da validez a las comunicaciones electrónicas como si fueran documentos originales.

Artículo 9. Original. *Cuando cualquier norma jurídica requiera que una comunicación o un contrato se proporcione o conserve en su formato original, o prevea consecuencias en el caso de que eso no se cumpla, ese requisito se tendrá por cumplido respecto de una comunicación electrónica:*

a) Si existe alguna garantía fiable de la integridad de la información que contiene, a partir del momento en que se generó por primera vez en su forma definitiva, tanto en comunicación electrónica como de otra índole; y,

b) Si, en los casos en que exija proporcionar la información que contiene, ésta puede exhibirse a la persona a la que se ha de proporcionar.

Con el procedimiento de comprobar el resumen calculado con la función de hash y compararlo con el contenido en la firma electrónica, se asegura que la información no ha sufrido ninguna alteración desde el momento de la firma, es decir garantiza que desde que se firmó se generó en su forma definitiva y aún la conserva. Además los medios electrónicos dan la libertad de tener más de un original.

4.4 Obligaciones de los usuarios de firma electrónica

Como toda ley, ésta también proporciona derechos y obligaciones, a continuación se describen las obligaciones de los principales actores en el escenario de la firma electrónica, el firmante y el receptor.

4.4.1 Firmante

La “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” tiene el siguiente artículo donde especifica cuál es el proceder del firmante. Se basa en tres obligaciones importantes que son, 1) custodiar adecuadamente su clave privada, 2) dar aviso a la autoridad certificadora si su clave privada ha quedado expuesta y 3) cerciorarse que la información que contiene el certificado digital sea verdadera.

Artículo 35. Proceder de Firmante. *Cuando puedan utilizarse datos de creación de firmas para crear una firma con efectos jurídicos, cada firmante deberá:*

a) Actuar con la diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma.

b) Sin dilación indebida, utilizar los medios que le proporcione el prestador de servicios de certificación conforme la presenta ley, o en cualquier otro caso esforzarse razonablemente, para dar aviso a cualquier persona que, según pueda razonablemente prever el firmante, pueda considerar fiable la firma o prestar servicios que la apoyen si:

- 1) *El firmante sabe que los datos de creación de la firma han quedado en entredicho; o,*
- 2) *Las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho.*
- c) *Cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado o que hayan de consignarse en él son exactas y cabales.*

4.4.2 Receptor

Las obligaciones que establece la ley para quien recibe una firma electrónica son mínimas pero de suma importancia y se resuenen en verificar que la firma electrónica sea válida, esto incluye verificar la integridad, comprobar que el certificado no ha sido revocado, comprobar que el certificado todavía es válido. Todo esto lo hacen los programas informáticos que manejan firmas electrónicas con un solo clic.

Artículo 38. Proceder de la parte que confía en el certificado. Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que produzca el hecho de que no haya tomado medidas razonables para:

- a) *Verificar la fiabilidad de la firma electrónica; o,*
- b) *Cuando la firma electrónica esté refrendada por un certificado:*
 - i. *Verificar la validez, suspensión o revocación del certificado; y,*
 - ii. *Tener en cuenta cualquier limitación en relación con el certificado.*

La mayor parte de programas informáticos realizan estos procedimientos automáticamente al abrir un documento firmado electrónicamente, pero algunos dejan la opción de verificar si el certificado no ha sido revocado manual, por lo que se debe realizar para no caer en riesgos.

4.5 Creación del Registro de Prestadores de Servicios de Certificación (RPSC)

En su artículo 53, la “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” dice que el Ministerio de Economía deberá crear, en un plazo no mayor a sesenta días después de entrada en vigencia de la ley, el Registro de Prestadores de Servicios de Certificación.

Para dar cumplimiento a este artículo, el Ministerio de Economía a pesar de que no le fue asignado un presupuesto para el efecto, el 18 de diciembre de 2008 mediante el acuerdo gubernativo 385-2008 reformó el reglamento interno del Ministerio de Economía donde están creadas todas dependencias de dicho ministerio y se crea el Registro de Prestadores de Servicios de Certificación y se describe sus funciones básicas.

El Artículo 54 dice que el Registro de Prestadores de Servicios de Certificación (RPSC) debe organizar 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. El RPSC 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 de Prestadores de Servicios de Certificación, estas guías son: Solicitud, Guía de Evaluación inicial, Guía de inspecciones periódicas, y Manual de operaciones. Todos estos documentos se encuentran disponibles en la página: <http://www.rpsc.gob.gt>.

También, el Ministerio de Economía, para dar cumplimiento al artículo 55 de la “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” emitió el reglamento de la Ley por medio del acuerdo gubernativo número 135-2009 el 8 de mayo, a pesar de que la ley le daba plazo máximo hasta el 23 de marzo del 2009.

El ministerio de economía piensa que es mucho más factible que este proyecto siga avanzando con la ayuda de cooperaciones internaciones ya que con los fondos ordinarios del estado sería bastante difícil, según el Lic. Erasmo Velázquez Viceministro de inversión y competencia. El MINECO cuenta actualmente con una donación de la unión europea para adquirir el equipo necesario que permita convertir a Garantías Mobiliarios totalmente electrónico y que funcione adecuadamente el RPSC.

El Lic. Velázquez enfatiza que la única forma de dar garantía a los usuarios de firma electrónica, es que el RPSC audite adecuadamente a los Prestadores de Servicios de Certificación e imponga las amonestaciones necesarias si se presenta alguna falta.

El “Reglamento de la ley para el reconocimiento de las comunicaciones y firmas electrónicas” así como las cuatro guías operativas que publicó el Ministerio de Economía, fueron hechas sobre la base de la “Ley para el reconocimiento de las firmas electrónicas” así como sobre la base de la experiencia de otros países de Latinoamérica, principalmente Argentina, Chile, México y Colombia, a donde viajaron el asesor técnico y el administrador del RPSC para recopilar información.

El requisito más importante que impone el “reglamento de la ley para el reconocimiento de las comunicaciones y firmas electrónicas” a las entidades prestadoras de servicios de certificación, es estar certificada con la norma ISO 27001, pero el Lic. Velázquez explica que, si por ejemplo una empresa internacional desea poner una subsidiaria en el país para prestar el servicio de certificación, la norma ISO 27001 únicamente debe cumplirse en la casa matriz o donde se encuentre el *datacenter* y la subsidiaria de Guatemala únicamente debería cumplir la norma ISO 9001.

5. GUÍAS DE USO DE LA FIRMA ELECTRÓNICA

La firma electrónica es un procedimiento poco conocido en el país, por lo que sus potenciales usuarios pueden sentirse un poco desorientados y con falta de información para utilizarla. La información teórica, tanto jurídica como técnica, ya se explicó en los anteriores capítulos de esta tesis, ahora corresponde entrar un poco en el terreno de lo práctico, lo cual es un poco difícil en este tema, porque se está hablando de cosas intangibles como el software.

Se presentan manuales de uso de las principales aplicaciones de firma electrónica de la forma más resumida posible, para que no se haga tedioso seguirlos y aprender. Los manuales que se desarrollaron son: **Instalación del certificado** en la computadora, este abarca todos los procedimientos a seguir desde que se solicita una firma electrónica en la Cámara de Comercio de Guatemala, hasta que queda instalado el certificado en la computadora para poder empezar a utilizarlo; se continua con el manual, **Firmando un correo electrónico**, en el cual se explicará cómo firmar electrónicamente un correo con una firma electrónica simple; y por último el manual sobre, **Verificación de una firma electrónica** en un mensaje de correo electrónico.

Es importante mencionar que en el primer manual se describe el proceso específico de la solicitud de una firma electrónica en la Cámara de Comercio de Guatemala, porque es la única autoridad certificadora del país hasta la fecha, y que además no posee un sistema autónomo, sino que trabaja junco con la Cámara de Comercio de Santiago, por lo que en el manual se hace referencia directa a la empresa *e-certchile*, que es la autoridad certificadora de la Cámara de Comercio de Santiago, Chile.

En el manual de cómo firmar un mensaje de correo electrónico, así como en el de la verificación, se describe el proceso únicamente con una firma electrónica simple debido que es la que se dispone, y no de una firma electrónica avanzada; pero el procedimiento básico no varía. El software que se utiliza para firmar un mensaje de correo el *Mozilla Thunderbird*, el cual es software libre, multiplataforma, y se puede descargar de Internet e instalarlo gratuitamente sin importar que sistema operativo se tenga.

5.1 Trámite ante la CCG e instalación del certificado

Trámite ante la Cámara de Comercio de Guatemala

Los formularios y la lista de requisitos mencionados a continuación fueron proporcionados por la Cámara de Comercio de Guatemala en septiembre del año 2009.

Para adquirir una firma electrónica simple o una firma electrónica avanzada en la Cámara de Comercio de Guatemala, se debe llenar la “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 también se deben presentar los siguientes requisitos:

Para personas jurídicas

- Copia de cédula de vecindad completa del representante legal.
- Copia de patente de comercio de empresa y patente de comercio de sociedad en el caso de la sociedad anónima.
- Constancia de inscripción en el registro tributario unificado.
- Copia de escritura de constitución.
- Copia de nombramiento de representante legal debidamente inscrito.

Para propietarios de empresas mercantiles

- Patente de comercio de empresa.
- Copia de cédula de vecindad completa.
- Constancia de inscripción en el registro tributario unificado.

Para personas individuales

- Copia de cédula de vecindad completa.
- Constancia de inscripción en el registro tributario unificado.

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 comunicará al correo que se haya proporcionado, para informar los pasos a seguir para descargar el certificado de sus servidores y poder instalarlo en la computadora. Los pasos son los siguientes:

Habiendo recibido su solicitud de certificación y dado cumplimiento a todos los requisitos exigidos, tenemos el agrado de comunicarle que ha sido aprobada la emisión de su certificado: Firma Electrónica Simple.

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

1. Ingresar desde su computador al sitio web de la Entidad Certificadora www.e-certchile.cl a la sección Productos, dentro de esta elegir el producto Firma Electrónica Simple que usted adquirió.

2. Escoger la opción o imagen llamada Descargar.

3. Luego deberá ingresar los campos de Identificación, Password y Verificador en el mismo orden que indica la página web

Identificación: xxxxxxxxxxxxxx

Password : xxxxxxxx

Verificador : xxxx

4. Debe otorgar al certificado un nivel de seguridad ALTO (nivel medio está por defecto), en donde se le solicitará que defina una password (esta password es de seguridad y cada vez que utilice el certificado deberá ingresarla).

5. Una vez definida la password, deberá hacer un clic en Aceptar.

6. Luego aparecerá una imagen que dirá Instalar Certificado, debe hacer clic sobre ella, para que sea instalado el certificado en su navegador

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

8. Por último, debe volver al home del sitio y descargar el certificado Raíz a su computador, luego debe presionar botón derecho de su mouse sobre el archivo y seleccionar instalar certificado y continuar con la instalación por defecto.

También puede descargar desde el siguiente link (http://www.e-certchile.cl/html/productos/download/CCS_CadenaCert.p7b)

Hay que tener en cuenta que la aplicación web que se utiliza para esto, solamente funciona en Windows XP (o anterior) e Internet Explorer versión 7 (o anterior) porque está en formato ASP en este momento.

Ahora se va a seguir los pasos que se indican, primero ingresar a la página <http://e-certchile.com/>, que es la siguiente:

Figura 7: Sitio de e-certchile



Se da clic en la imagen de descargar y dependiendo del navegador, puede que se muestre una advertencia de seguridad diciendo que el certificado de la página que se está visitando no está dentro de la lista de certificados confiables, pero como si se puede confiar en la empresa *e-certchile*, se debe elegir la opción de continuar y entonces se mostrará la siguiente pantalla:

Figura 8: Generación de certificado en e-certchile

DESCARGAR CERTIFICADO

Generación de certificado

[CPS](#)

Identificación

Password

Verificador

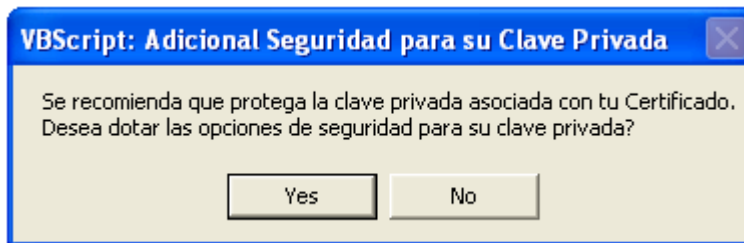
CSP(Cryptographic Service Provider)

Entonces se debe ingresar los datos que fueron enviados en el correo electrónico y pulsar el botón Enviar.

Como se puede apreciar en la imagen, también se muestra un link para ver la *CPS* (*Certificación Practice Statement*) que es la declaración de políticas de certificación donde se puede ver los derechos y obligaciones del usuario, así como los derechos y obligaciones de *e-certchile*.

Ahora se preguntará si se quiere poner las opciones de seguridad para la clave privada, y se debe presionar el botón *Yes*.

Figura 9: Confirmación opciones clave privada



Después de esto, el navegador advertirá que el sitio quiere instalar un nuevo certificado, entonces se debe presionar que *Yes* otra vez.

Figura 10: Advertencia instalación certificado



Entonces ya empieza el proceso de instalación del certificado a través de un asistente, en la primera pantalla del asistente se muestra la opción de nivel de seguridad que por defecto es media, pero se debe colocar en alta, por lo que se debe dar clic en el botón *Set Security Level*.

La diferencia entre el nivel de seguridad medio con el nivel alto es que para el nivel alto se utiliza una contraseña para proteger la clave privada, en cambio en el nivel medio no; esto quiere decir que con nivel alto se preguntará por esa contraseña cada vez que se quiera firmar algo.

Figura 11: Establecer nivel de seguridad



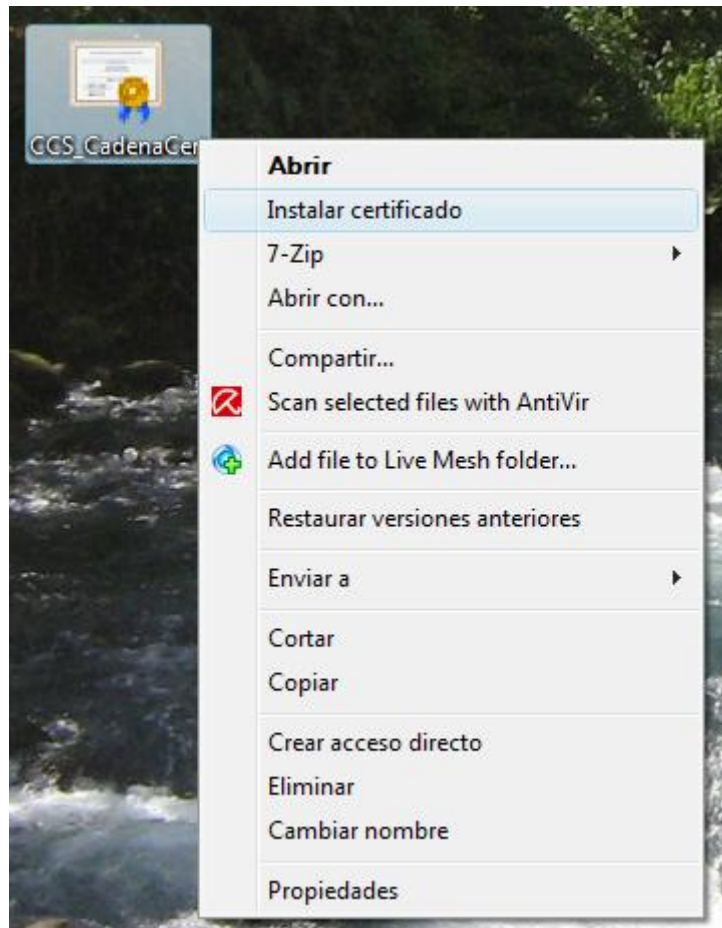
Después se mostrará la opción de ponerlo en nivel alto, y se debe dar clic en *OK*. Ahora se pedirá establecer una contraseña para la clave privada; se ingresa y el asistente finaliza. Ahora ya se tiene instalado en la computadora el certificado.

El último paso es instalar el certificado raíz, el cual contiene la clave pública de e-certchile, que es quien firma el certificado del usuario.

http://www.e-certchile.cl/html/productos/download/CCS_CadenaCert.p7b

Lo que se debe hacer es guardarlo en cualquier ubicación de la computadora, luego darle clic derecho y después en el menú que se desplegó clic en Instalar Certificado, como se muestra en la siguiente figura.

Figura 12: Instalación de certificado raíz



Se debe dejar todas las opciones por defecto, y finalizar el asiste. Si todo ha salido bien, al finalizar se mostrará un cuadro de diálogo indicándolo.

Con esto, todo está listo para empezar a firmar electrónicamente, se recomienda consultar el manual Firmando un correo electrónico, para tener una orientación de cómo hacerlo.

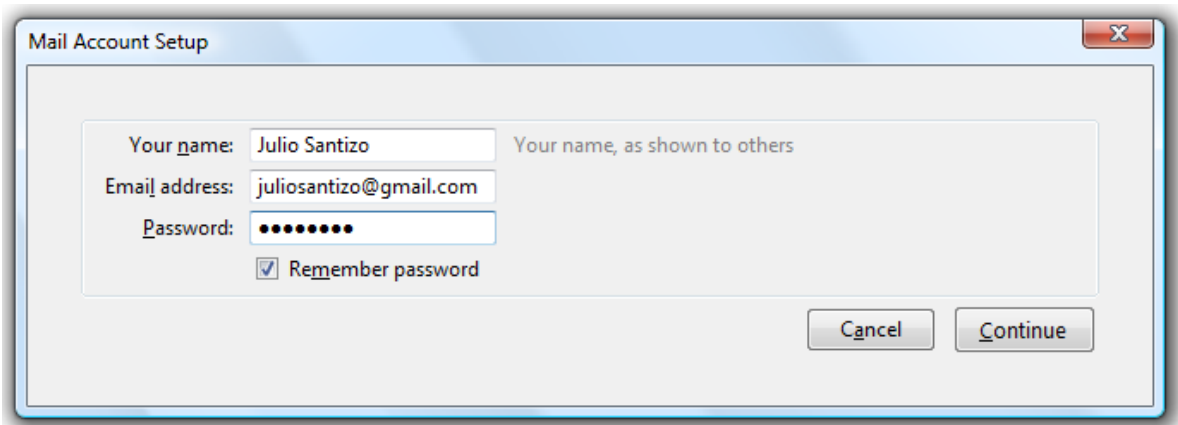
5.2 Firmando un correo electrónico

Existe una gran cantidad de programas que soportan firma electrónica y por lo tanto, se puede firmar electrónicamente con ellos, así como validar firmas. Por ejemplo: *Microsoft Word*, *Adobe Acrobat*, *Microsoft Outlook*, *Mozilla Thunderbird*, entre otros. El proceso de firma electrónica es bastante similar en todos estos programas, por lo que en el manual sólo se explica cómo firmar electrónicamente un correo electrónico utilizando *Mozilla Thunderbird 3.0*.

Si no se tiene instalado *Mozilla Thunderbird 3.0*, se puede descargar gratuitamente de: <http://www.mozillamessaging.com/> si ya se está utilizando este software para leer correo electrónico, puede omitirse los siguientes pasos, si no, habrá que configurar la cuenta de correo electrónico de que se disponga para que funcione con Thunderbird siempre y cuando tenga POP3 o IMAP.

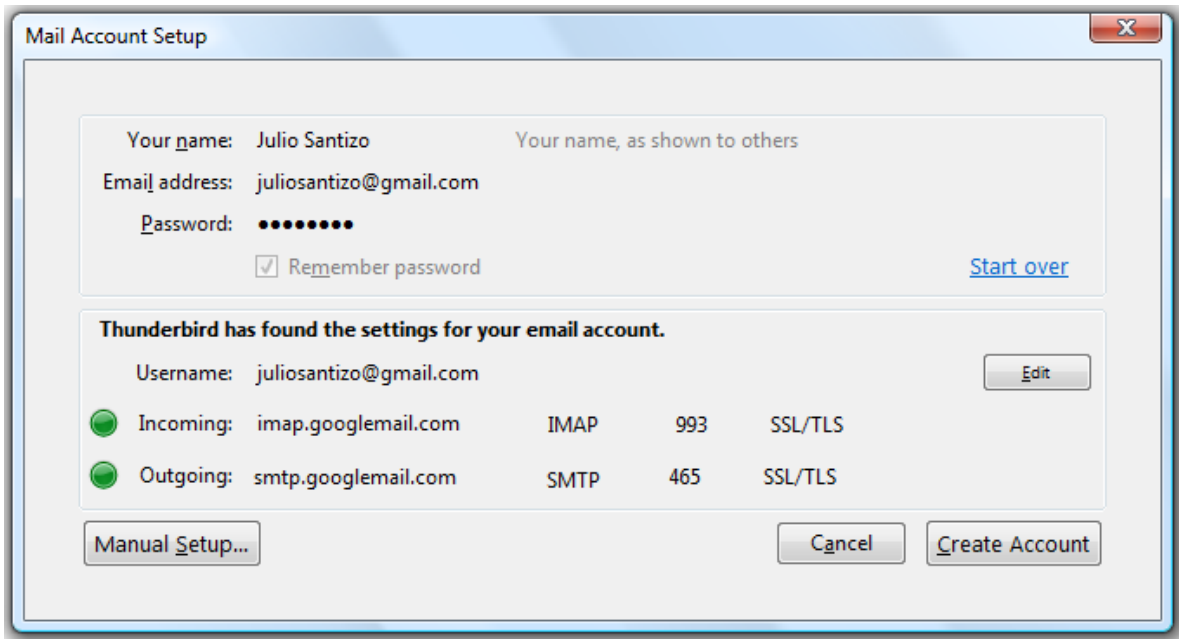
La configuración es sumamente sencilla, después de ejecutar el instalador, aparecerá el siguiente cuadro de diálogo.

Figura 13: Configuración de cuenta de correo en Mozilla Thunderbird



Se tiene que llenar los cuadros de texto con los datos que se piden, y dar clic en continuar. Entonces aparecerá el siguiente cuadro de confirmación de configuración, se da clic en crear cuenta, y ya estaría configurado *Mozilla Thunderbird* como cliente de correo.

Figura 14: Verificación de configuración de cuenta de correo

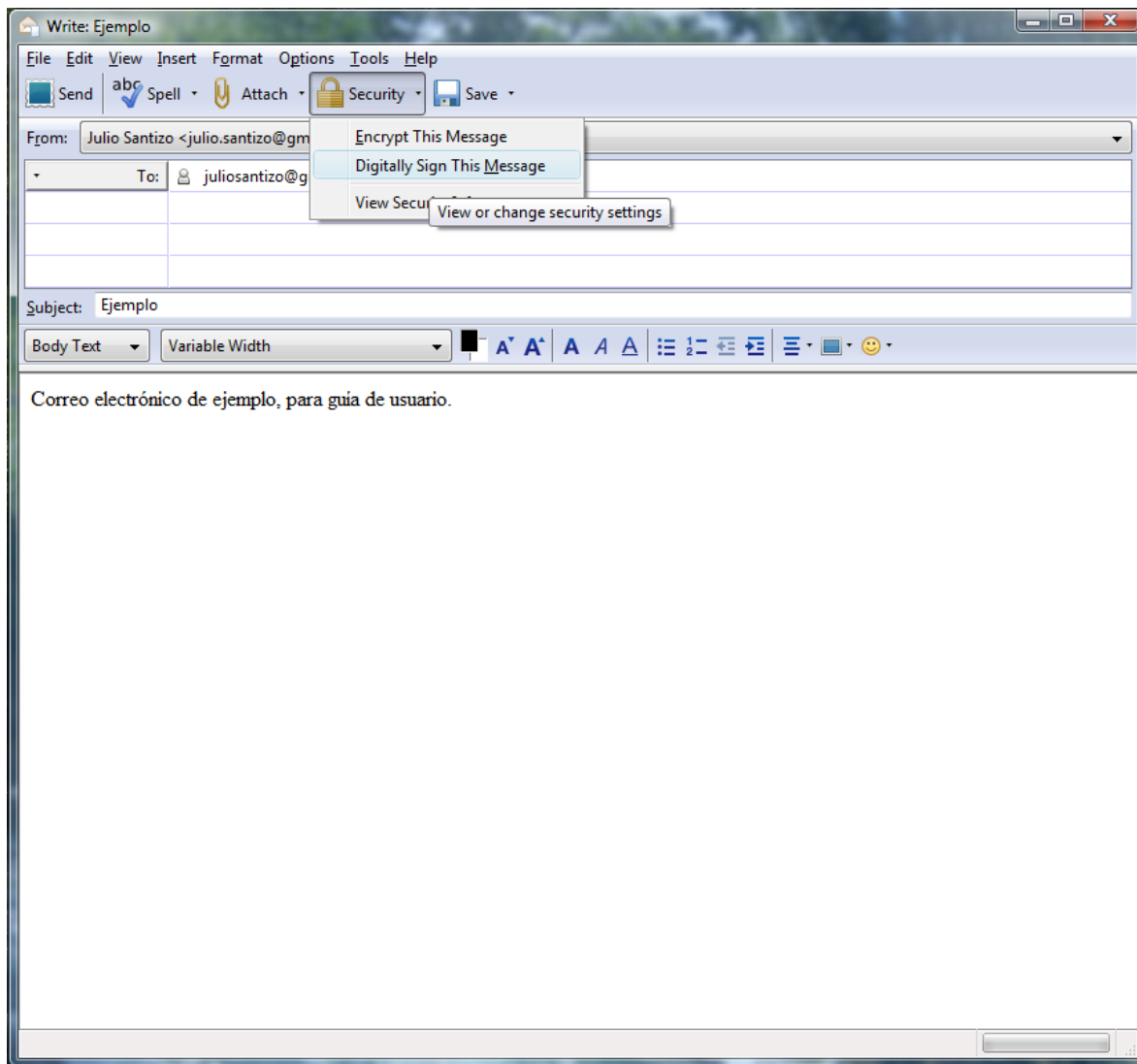


Ahora se escribe un nuevo mensaje de correo electrónico pulsando el botón escribir y se coloca la o las direcciones de destinatario, el asunto del mensaje y el cuerpo.

GUÍAS DE USO DE LA FIRMA ELECTRÓNICA

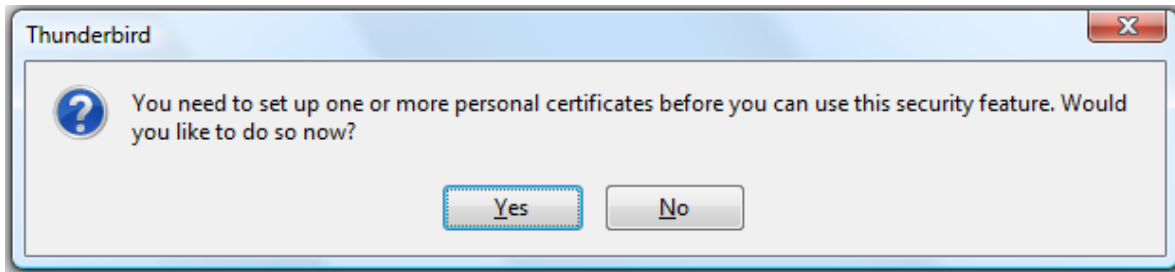
Para firmar el mensaje electrónicamente, se da clic en la flechita del botón seguridad, para que se muestren las opciones de seguridad y luego se hace clic en *digitally sign this message*, como se muestra a continuación.

Figura 15: Firmar correo electrónico en Mozilla Thunderbird



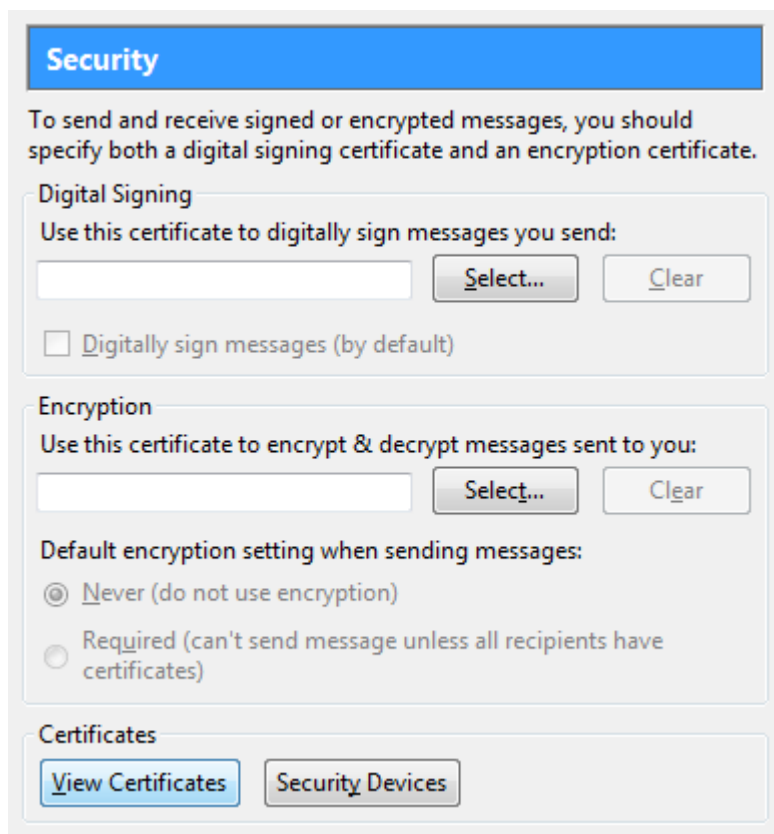
Como es la primera vez que va a firmar un correo electrónico, *Mozilla Thunderbird* preguntará si se quiere instalar un certificado y se debe poner que sí.

Figura 16: Instalación de certificado en Mozilla Thunderbird



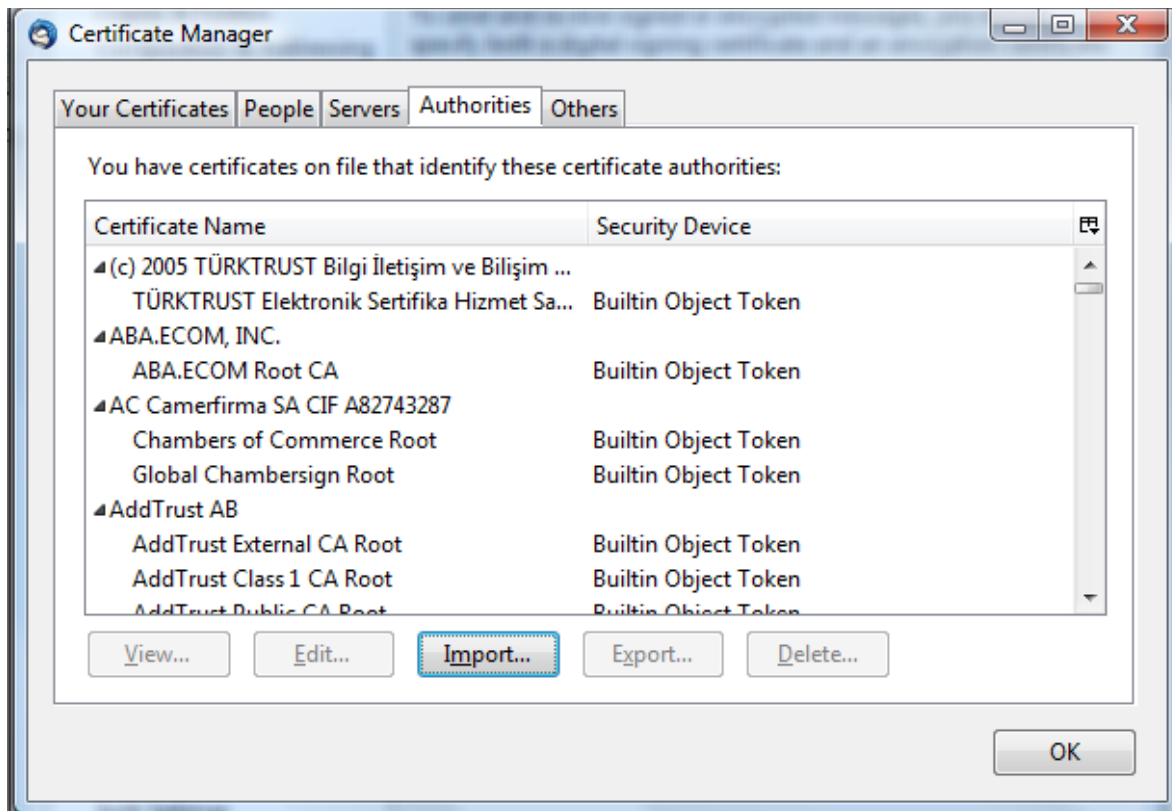
Ahora se mostrarán las opciones de seguridad de la cuenta de correo, y se debe dar clic en el botón *View Certificates*.

Figura 17: Opciones de seguridad en Mozilla Thunderbird



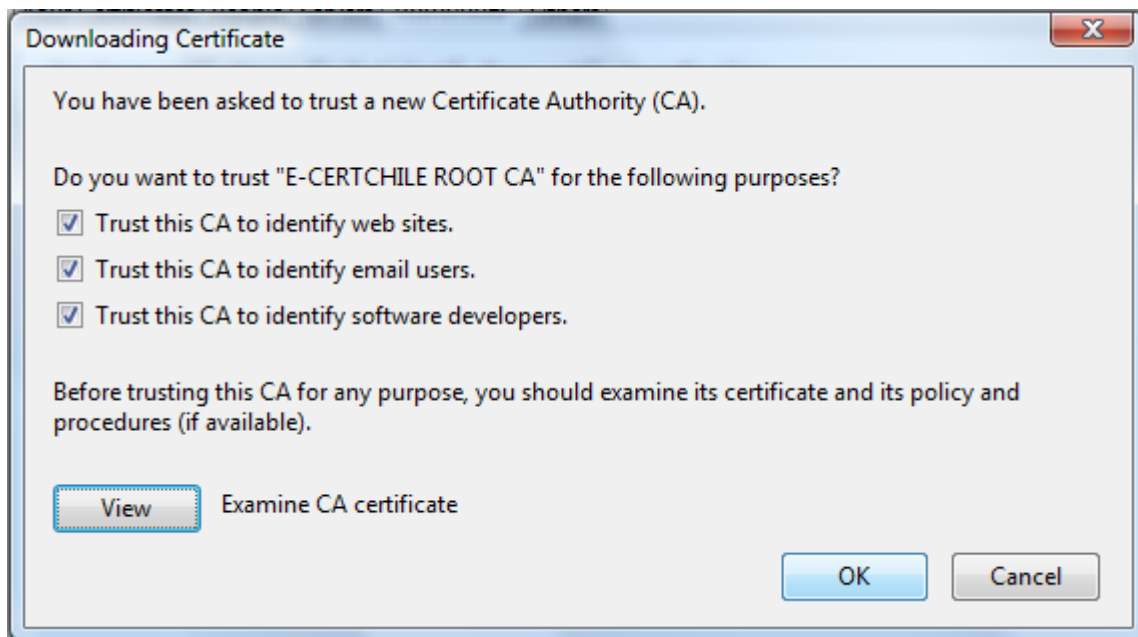
Se abrirá entonces el administrador de certificados de *Mozilla Thunderbird*, y primero se debe agregar el certificado de *e-certchile*; en la pestaña de autoridades, se da clic en el botón *Import*.

Figura 18: Instalación de certificado raíz en Mozilla Thunderbird



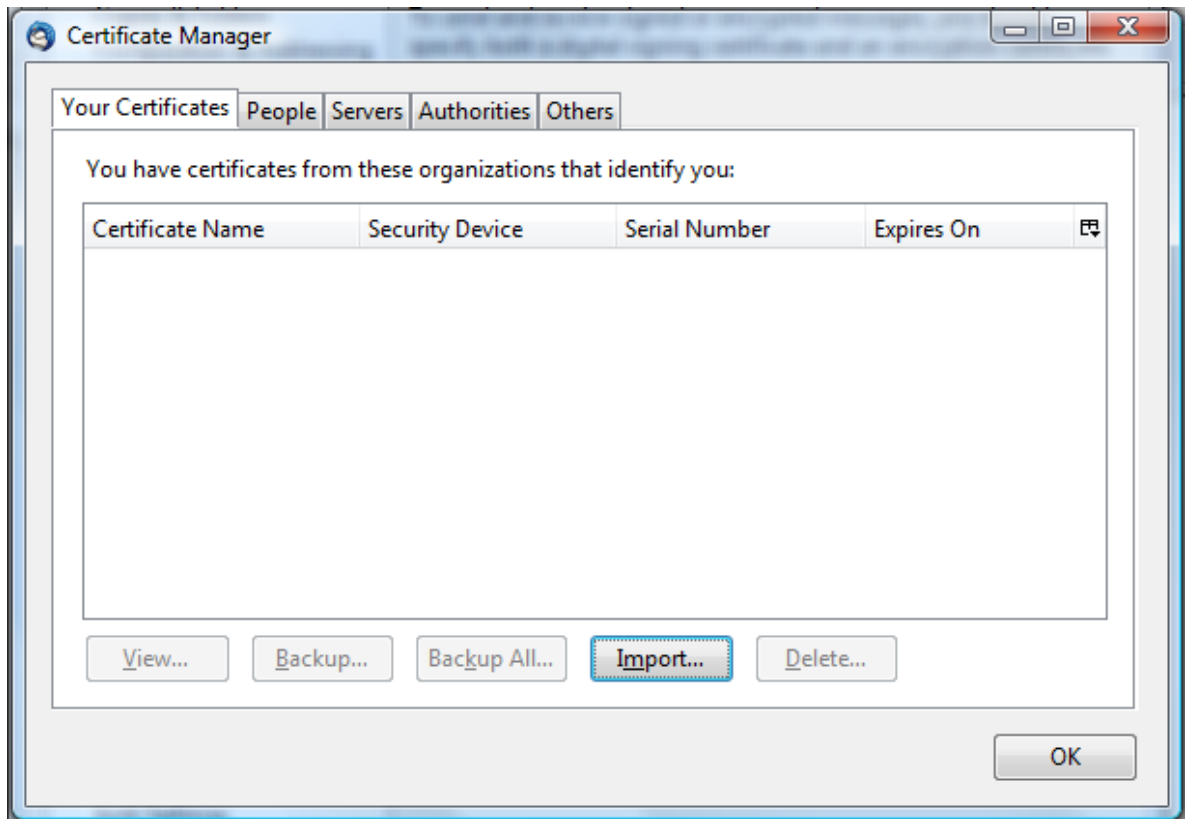
Ahora se debe buscar donde esté guardado el archivo *CCS_CadenaCert.p7b* y se selecciona. Ahora se pregunta: ¿para qué propósitos se desea confiar en este certificado? Lo recomendable es seleccionar todas las casillas dado que se confía en la empresa *e-certchile* porque se sabe sobre sus procedimientos de certificación y se consideran adecuados.

Figura 19: Agregar autoridad confiable en Mozilla Thunderbird



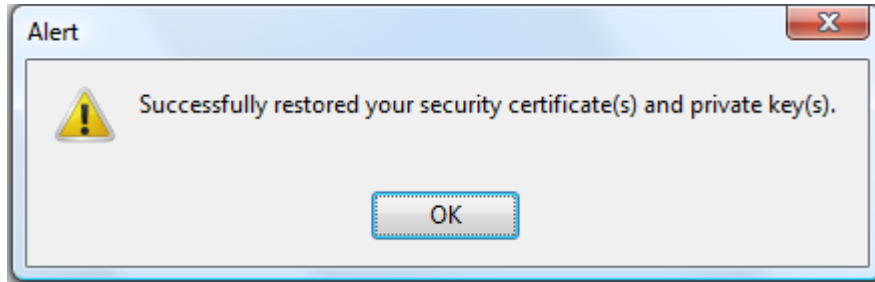
Ahora se da clic en *Ok* y se selecciona la pestaña *Your Certificates*, y ahí también se da clic en el botón *Import*.

Figura 20: Agregar certificado digital en Mozilla Thunderbird



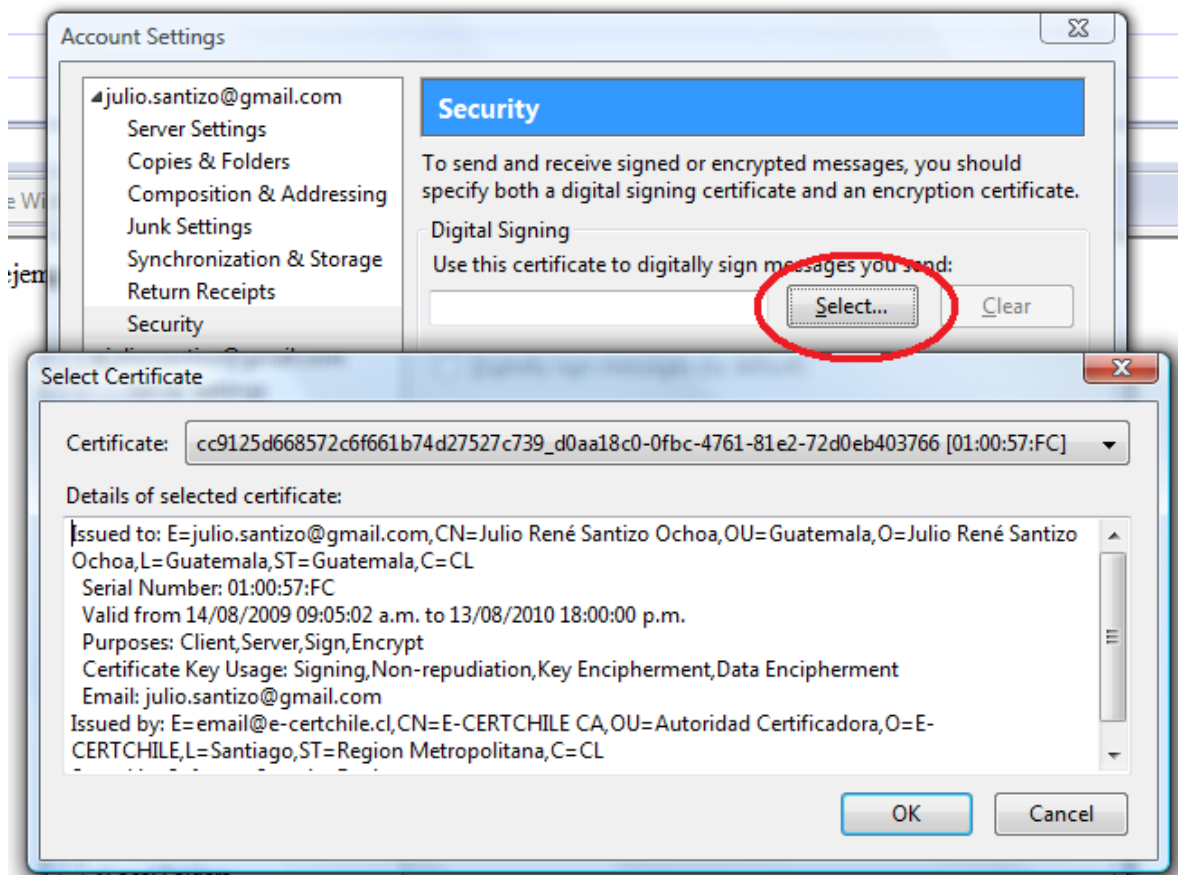
Se busca entonces el certificado y se selecciona, después se preguntará por la contraseña que fue utilizada para cifrar el certificado, cabe mencionar que esto NO es la clave privada, sino que una clave extra que protege la privacidad del archivo del certificado. Si se le colocó una al descargarlo se ingresa, si no, se deja el cuadro en blanco y se da clic en aceptar. Si todo salió bien debería mostrarse el siguiente mensaje de confirmación.

Figura 21: Confirmación de instalación del certificado digital



Se da clic en *Ok* hasta regresar al cuadro de opciones de cuenta, donde se debe dar clic al botón *Select*.

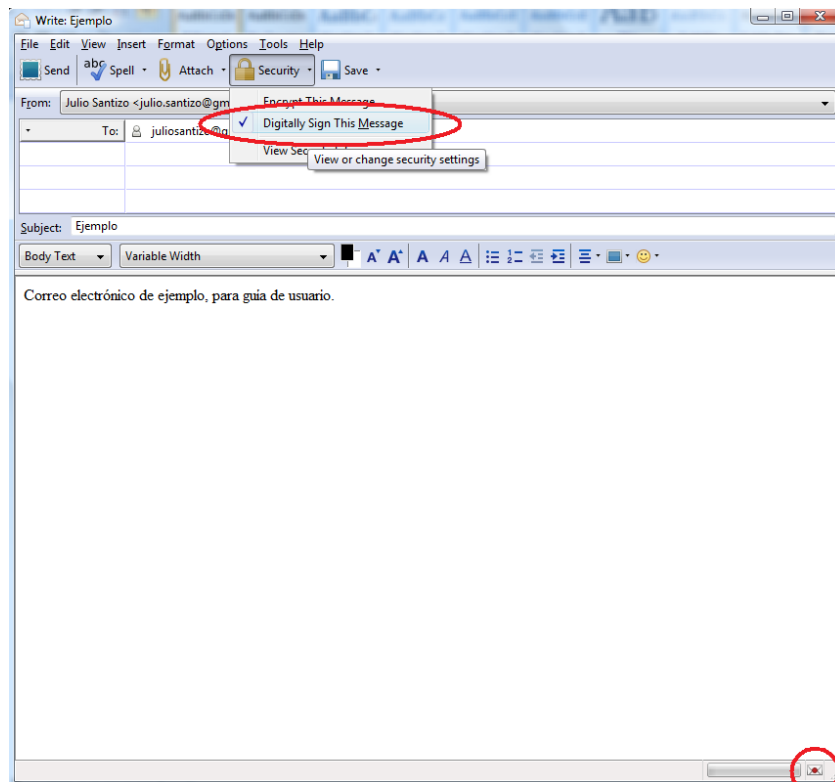
Figura 22: Información del certificado digital



Entonces se selecciona el certificado y se da clic en *Ok* para cerrar esa ventana, y nuevamente en *Ok* para cerrar el cuadro de opciones de cuenta. Ahora ya está configurado todo lo necesario para firmar. El proceso de la firma empieza ahorita, y esto es lo que se debe realizar todas las veces que se quiera firmar, el procedimiento anterior solamente se aplica la primera vez.

Se da clic en la flechita que está a la derecha del botón *Security* y se selecciona la opción *Digitally Sign This Message*, al seleccionarlo aparecerá un sobre con un sello rojo en la esquina inferior derecha de la ventana, esto significa que el correo se enviará firmado electrónicamente cuando se pulse el botón *Enviar*.

Figura 23: Enviando correo electrónico firmado



Como se puede apreciar, para firmar electrónicamente un mensaje de correo electrónico, basta hacer dos clics para seleccionar esa opción.

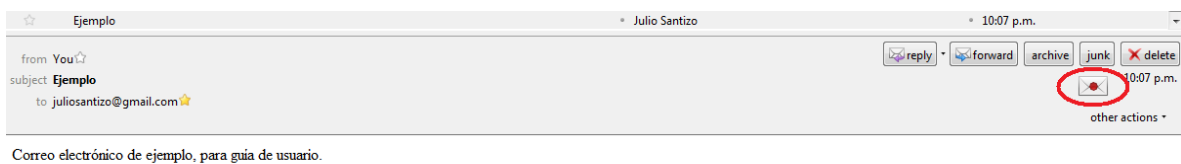
5.3 Verificación de una firma electrónica

Como ya se explicó en la revisión de la “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” como usuarios de la firma electrónica se debe tener cuidado de guardar bien la clave privada, pero como receptores de una comunicación firmada electrónicamente, se debe tener cuidado de verificar que la firma electrónica sea válida.

Todos los programas que soportan firma electrónica, cuando se abre un contenido que esté firmado, automáticamente hacen la comprobación, volviendo a calcular la función de hash y comparándola con el resultado que viene en la firma, para mostrar el resultado que realmente interesa: firma válida, ó, firma no válida.

Mozilla Thunderbird no es la excepción y cuando se abre un correo firmado electrónicamente notificará sobre el resultado de la comprobación, como se muestra en la siguiente imagen.

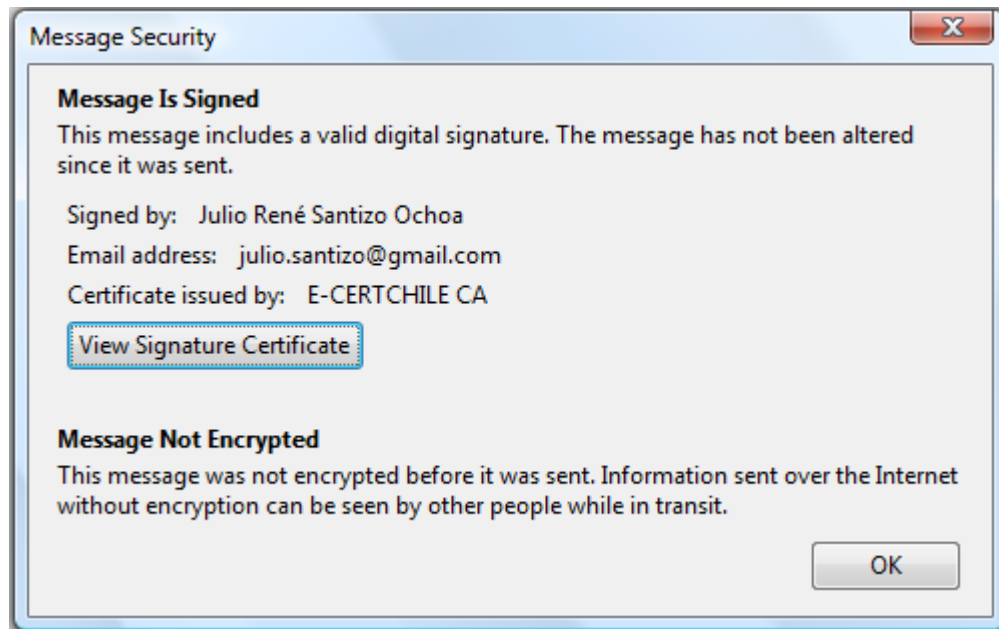
Figura 24: Verificación de correo electrónico firmado



Debido que la firma electrónica es válida, se muestra el sobre con el sello rojo. Además si se le da clic, se puede ver más información acerca de la firma; esto es importante que se revise.

Al dar clic en el sobre, se muestra la siguiente ventana.

Figura 25: Información de firma electrónica de un correo



Como se puede ver, esta ventana confirma que la firma electrónica es válida, entonces se puede confiar totalmente en el contenido del mensaje de correo electrónico.

6. RECOMENDACIONES A LOS USUARIOS DE FIRMA ELECTRÓNICA

La firma electrónica es una herramienta que da mucha seguridad a las comunicaciones por medio de Internet, pero aunque sea muy segura que sea dicha herramienta, si no se utiliza adecuadamente, se puede poner en peligro la información de los usuarios.

Por eso a continuación se describen algunas recomendaciones y buenas prácticas a utilizar la firma electrónica, para que se tenga mayor seguridad.

6.1 Base en la confianza

Para cumplir con el concepto de autenticidad, se tiene un “tercero de confianza” que da fe de las identidades de las personas a las cuales les ha extendido un certificado digital para firmar electrónicamente. Es decir, existe una entidad confiable que certifica que la identidad de la persona que posee un certificado extendido por ésta, es verdadera; este tercero de confianza es la Autoridad Certificadora.

Para esto, las Autoridades Certificadoras tienen procedimientos mediante los cuales comprueban la identidad de cada persona que solicita un certificado de firma electrónica y posterior a comprobar su identidad, se le extiende el certificado. Es algo parecido a la emisión del Documento Personal de Identificación (DPI) el cual acredita la identidad de una persona. Debido a esto, es importante que la autoridad certificadora sea confiable para todos, ya que mientras más confiable sea la autoridad certificadora, mayor seguridad se tiene acerca de la identidad de las personas con firma electrónica de esa autoridad certificadora.

6.2 Descargar el certificado

Como se explicó en las guías de usuario, cuando la solicitud es aprobada, el prestador de servicios de certificación envía por correo electrónico una identificación, un password y un verificador, para que se pueda descargar el certificado, este es un paso importantísimo y nunca debe hacerse en una computadora compartida, porque el certificado se quedará instalado en la computadora, y se supone que solo el propietario puede utilizar ese certificado junto con la clave privada.

También es recomendable hacerlo en una conexión a Internet segura, es decir no utilizar redes inalámbricas públicas. En esas redes puede haber usuarios que estén capturando los paquetes que viajan en el aire y robar el certificado.

6.3 Tramitar una firma electrónica

No está de más mencionar que es necesario que los datos personales que se proporcionen para la emisión del certificado tienen que ser totalmente verídicos, para que no sea negada la solicitud por parte de la autoridad certificadora.

Hay que recordar que la confiabilidad de la firma electrónica está en función de la confiabilidad de la autoridad certificadora que extendió el certificado. Por lo tanto es recomendable adquirir una firma electrónica en una autoridad certificadora confiable y sólida para que las personas que vean y valoren la firma, tengan una mayor confianza. También es importante adquirirla en un prestador de servicios de certificación que esté debidamente registrado con la autoridad competente. En el caso de Guatemala, la autoridad de registro es el Registro de Prestadores de Servicios de Certificación del Ministerio de Economía.

6.4 Validación de firmas electrónicas

Todos los programas que soportan firma electrónica, tienen la opción de verificar la firma, cuando se abre algo que contenga firma electrónica, algunos lo hacen automáticamente y en otros hay que presionar algún botón para que hagan la comprobación.

En ambos casos, el software se encarga de volver a calcular la función de hash y de comparar el resultado con el que viene en la firma para comprobar la integridad de la información, comprobar si el certificado no está en la lista de certificados revocados, y si se trata de un cliente de correo electrónico, también comprueba que la dirección de donde viene el correo sea la misma dirección que se indica en el certificado; el resultado de estas comprobaciones se muestra y eso es lo que se debe interpretar y valorar.

No se debe olvidar que como la firma electrónica se basa en la confianza que se tiene en la entidad prestadora de servicios de certificación, algunos programas pueden mostrar alguna alerta de seguridad, por no tener a la autoridad certificadora dentro la lista de autoridades certificadoras confiables; por eso es importante agregar a las autoridades de certificación en que se confía para que el programa no muestre falsas alertas.

6.5 Firmar comunicaciones electrónicas

Como se explicó en el capítulo de criptografía, la confiabilidad de la firma electrónica está en función de la confiabilidad de la autoridad certificadora que extendió el certificado, por lo tanto es recomendable adquirir una firma electrónica en una autoridad certificadora confiable y solida. Así las personas que vean y valoren la firma tendrán mayor confianza.

Se recomienda no revelar por ningún motivo la clave privada a nadie. La clave privada es personal y si alguien más la conoce, ya no tiene sentido el uso de la firma electrónica porque ya no se tiene seguridad sobre la identidad del remitente.

Por último, también es recomendable no utilizar la opción de “recordar clave privada” a no ser que se tenga la seguridad de nadie más podrá tener acceso a la computadora, porque si otra persona utiliza esa misma computadora y se tiene activada esta opción, podrá firmar por error o malintencionadamente algo con el certificado y clave privada que tiene la computadora.

6.6 Recomendaciones a las empresas e instituciones

En las empresas e instituciones, se debe aplicar cada una de las recomendaciones anteriores por parte de cada trabajador que utilice firma electrónica, pero además a continuación se presenta una serie de recomendaciones generalizadas que las empresas pueden tomar en cuenta si desean utilizar firma electrónica o *PKI*.

6.6.1 Utilizar certificados en sus servidores para seguridad de los clientes.

Es muy común oír hablar de suplantaciones y de *phishing* por lo que es recomendable instalar certificados en los servidores *Web*, de manera que los clientes puedan comprobar que han ingresado al sitio original de la empresa y no a una falsificación por medio de la cual pueden robarle sus datos. Esto es de vital importancia en los sitios Web de Bancos, ya que son los principales objetivos de quienes practican el phishing y está en juego los datos financieros de los clientes.

6.6.2 Obligatoriedad de la firma electrónica para todas las comunicaciones.

En toda comunicación interna de la empresa, se intercambia información importante y privada, es sumamente importante resguardar la integridad de la información y detectar si hubiera suplantaciones dentro de la empresa. Para evitar todos estos problemas, basta con tener la política de que todas las comunicaciones electrónicas internas de la empresa, deban ir firmadas, y de recibir una comunicación que no esté firmada, tratarla como falsa y hacerlo saber a las autoridades competentes.

6.6.3 Obligatoriedad de cifrado mediante certificado para las comunicaciones confidenciales.

Es común que en las empresas medianas o grandes, la mayoría de las comunicaciones se haga electrónicamente por medio de Internet, pero como se sabe ese es un medio muy peligroso como para que viaje información privada o confidencial de la empresa.

La mejor alternativa para reducir el riesgo de que la información confidencial sea descubierta, es cifrando dicha información. Como se vio, en el capítulo sobre el funcionamiento de la firma electrónica y *PKI*, se debe cifrar con clave pública del destinatario, de manera que solo pueda ser descifrada con la clave privada del destinatario, que se supone que solo él conoce, y por lo tanto solo el podrá descifrar la información.

Para realizar esto con la firma electrónica en un correo electrónico por ejemplo, en las opciones de seguridad del correo electrónico, se selecciona la opción de cifrar el mensaje y se mostrará el certificado digital del destinatario con el que será cifrado el mensaje, luego se envía y ya no se corre el riesgo de que la información sea vista incluso si el mensaje es interceptado.

6.6.4 Infraestructura de clave pública propia

Una alternativa bastante factible para las empresas, es instalar su propia infraestructura de clave pública (*PKI*), así es como si la empresa fuera una pequeña autoridad certificadora, que extiende certificados únicamente a sus trabajadores, teniendo sus propias políticas de revocación, de comprobación de identidad, de renovación, etc., y mediante esto es mucho más fácil la aplicación de políticas de obligatoriedad del uso de firma electrónica dentro de la empresa.

7. OBSTÁCULOS PARA LA ACEPTACIÓN Y UTILIZACIÓN DE LA FIRMA ELECTRÓNICA POR LOS GUATEMALTECOS

Según el *Technology Acceptance Model (TAM)* que es un modelo aplicado a los sistemas de información que describe como los usuarios aceptan y utilizan una tecnología nueva, hay dos factores importantísimos que definen la aceptación de una tecnología, y son; la utilidad percibida (*PU*) y la facilidad de uso (*PEOU*). La utilidad percibida se refiere a los beneficios recibidos por el usuario al utilizar determinada tecnología, por ejemplo, mayor productividad. La facilidad de uso se refiere al esfuerzo que tiene que realizar el usuario para utilizar determinada tecnología.

Para el caso de la firma electrónica, los beneficios son muchos, el problema es que no son conocidos por los usuarios potenciales y la facilidad de uso, es bastante alta aunque puede resultar un poco complicado descargar el certificado, e instalarlo en la computadora.

Este trabajo de graduación ha tratado de contribuir a aumentar estos dos factores, la utilidad percibida a través de explicar los beneficios de la firma electrónica y la facilidad de uso, a través de las guías de uso y las recomendaciones de los capítulos anteriores.

7.1 Principales obstáculos

A continuación se presentan los principales obstáculos o barreras que tienen los potenciales usuarios de la firma electrónica en Guatemala. Todos estos obstáculos se pueden disminuir, si se percibe un mayor beneficio del uso de la firma electrónica o si se hace obligatorio el uso para determinadas transacciones.

Dentro de estos obstáculos no se menciona la accesibilidad a este recurso, ni la disponibilidad de una conexión a Internet, porque a pesar de que debido a la situación socioeconómica de Guatemala ese sería el problema más grande (que haya conectividad a Internet y acceso a medios electrónicos por parte de la población) el fenómeno que se está observando es la poca aceptación de esta nueva tecnología por parte de las personas que sí tienen los recursos para utilizarla, pero por una u otra razón prefieren seguir utilizando los medios tradicionales.

7.1.1 Falta de confianza en métodos electrónicos

La característica intangible del software y de los sistemas de información provoca en la mayor parte de los usuarios una falta de confianza en las transacciones electrónicas y por lo tanto resistencia a su uso.

Esta falta de confianza probablemente es por la costumbre de que cuando se hace una transacción presencialmente, se recibe un comprobante de la transacción impreso en papel, en cambio luego de una transacción electrónica, solamente sale en pantalla una confirmación, pero no es algo físico que el usuario pueda tener en sus manos y que le proporcione “seguridad”.

OBSTÁCULOS PARA LA ACEPTACIÓN Y UTILIZACIÓN DE LA FIRMA ELECTRÓNICA POR LOS GUATEMALTECOS

De forma generalizada los usuarios no confían en los medios electrónicos como alternativa para realizar diversas tareas como hacer pagos de servicios, hacer transacciones bancarias, hacer declaraciones ante la SAT, etc. La mayoría de los bancos del país ofrecen la facilidad de realizar muchas operaciones vía Internet (consulta de saldo, transferencias entre cuentas, pagos de servicios de terceros, pago de tarjeta de crédito, pago de préstamos, declaración de cheques, etc.), y son muy pocos usuarios quienes las utilizan a pesar de que son muy convenientes para no perder tiempo ni recursos yendo a una agencia o haciendo innecesarias colas dentro de las agencias de los bancos para ser atendido.

7.1.2 Desconocimiento de la tecnología y su uso

La mayor parte de personas han escuchado sobre la firma electrónica, pero no saben cómo utilizarla y no tienen ninguna motivación para aprender y empezar a utilizarla debido que ignoran el éxito del uso de la firma electrónica y no perciben que sea beneficioso utilizarla.

Para superar este obstáculo es necesario hacer de conocimiento a los usuarios, los beneficios y las ventajas que tiene, así como los principales casos de éxito que han sucedido. Acompañado a esto, también debe ir una atención y apoyo al usuario, para que no perciba difícil su uso.

Deben hacerse campañas de información y capacitación a los usuarios potenciales de la firma electrónica, empezando tal vez en los círculos de pequeños y medianos empresarios.

7.1.3 Falta de percepción de beneficios de su uso

Las personas que conocen sobre el tema no lo ven aplicable o no ven claramente que beneficios trae utilizar la firma electrónica como alternativa a la firma manuscrita. Esto sucede la mayoría de las veces cuando se introduce una nueva tecnología, pero debido a los altos beneficios que tiene la utilización de la firma electrónica, no debería pasar mucho tiempo antes de haya un *boom* y la mayor parte de usuarios de medios electrónicos, quieran empezar a utilizar la firma electrónica.

Para facilitar que las personas tomen conciencia de los beneficios de la firma electrónica se debe dar a conocer, a través de campañas informativas, estudios de casos de éxito, etc.

7.2 Principales beneficios de la firma electrónica

La firma electrónica es una tecnología que le da seguridad a los documentos y comunicaciones electrónicas, lo cual habilita a utilizar los medios electrónicos para transmitir y almacenar información importante, por la seguridad que proporciona. Así mismo la “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” lo que hace es dar validez jurídica a las comunicaciones electrónicas; en otras palabras, lo que se tiene es un universo de nuevas posibilidades y dependiendo de cómo se aprovechen serán los beneficios que se obtengan, pero tomando en cuenta las aplicaciones más generales y conocidas se pueden mencionar los siguientes beneficios:

OBSTÁCULOS PARA LA ACEPTACIÓN Y UTILIZACIÓN DE LA FIRMA ELECTRÓNICA POR LOS GUATEMALTECOS

- Brinda una gran confianza en la utilización de medios electrónicos para manejar información importante y debido a la confiabilidad tiene certeza jurídica en Guatemala, así como en otros países del mundo.
- La contratación se vuelve más eficiente mediante el ahorro de costos y tiempo. No es necesario viajar y tener una reunión presencial para firmar un documento entre varias personas que se encuentran lejos contextualmente.
- Se economiza papel lo cual contribuye a la conservación del medio ambiente.
- Se procesa la información más eficientemente con medios electrónicos, que con papel.
- Se tiene mayor seguridad en la confidencialidad e integridad de la comunicación que por cualquier otro medio.
- Se tiene la confianza otorgada por el prestador de servicios de certificación sobre la identidad y autenticación de los individuos, esto evita el fraude y la suplantación de identidad en las comunicaciones electrónicas.
- Se tiene la misma certeza jurídica que con la información consignada en papel.
- Apoya al desarrollo porque la tecnología fortalece a la economía y la economía es base para el desarrollo.
- Impulsa y da respaldo al comercio electrónico.
- Impulsa y facilita el comercio internacional.
- Ayuda a que haya más inversión internacional.
- Incrementa la productividad.

OBSTÁCULOS PARA LA ACEPTACIÓN Y UTILIZACIÓN DE LA FIRMA ELECTRÓNICA POR LOS GUATEMALTECOS

Para finalizar es importante comentar sobre lo que ocurrió en Estados Unidos debido al pánico que se generó cuando se descubrió de la amenaza del Ántrax, y es que en Estados Unidos, la mayoría de pagos de servicios se hacían por medio correo tradicional, pero las personas tenían miedo de recibir sobres, entonces los servicios de pagos electrónicos empezaron a tener mucha demanda.

8. LA FIRMA ELECTRÓNICA COMO INSTRUMENTO DE E-GOBIERNO

La “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” así como la firma electrónica en sí, abre muchas posibilidades y puede aplicarse en cualquier ámbito. Un ámbito importante y en que ha tenido mucho auge en otros países del mundo es el ámbito del gobierno debido que por sus características y beneficios, la firma electrónica permite tener una administración más eficiente. Es claro que la ley no obliga a utilizar firma, solo reconoce su utilización.

8.1 Casos de éxito

El ingeniero Mauricio Romero indicó que la SAT tiene una gran oportunidad de aplicar la ley y están trabajando en eso, desarrollando nuevos proyectos y expandiendo proyectos existentes.

LA FIRMA ELECTRÓNICA COMO INSTRUMENTO DE E-GOBIERNO

La SAT tiene actualmente tres proyectos que son los más representativos, el primero es BancaSAT, este sistema se diseñó en el año 1999 y se puso en funcionamiento hasta en el año 2001 cuando se publicó el acuerdo del directorio de SAT que lo regulaba y permitía su operación. El pago y la declaración de los impuestos en este caso se realizaban teniendo como intermediario a un banco, debido que no existía una ley de reconocimiento de comunicaciones electrónicas.

Además indicó el ingeniero Romero que en poco tiempo se verá nuevas aplicaciones de BancaSAT orientadas a que el cliente trabaje directamente con la SAT, gracias a las posibilidades que permite la ley.

Otro proyecto de la SAT donde tiene mucha aplicación de la “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” además de ser un caso de éxito específico y precursor de dicha ley, es el proyecto PKI/DUA-GT. Este sistema utiliza certificados digitales para el envío de la Declaración de Mercancías DUA-GT, por lo que los Agentes Aduaneros debieron realizar los trámites necesarios para adquirir su certificado y utilizarlo. Estos certificados eran emitidos por la empresa *eBclosion* y los pasos que debían seguir para adquirir un certificado eran: 1) Presentar escrito de solicitud de trámite ante la SAT. 2) Adquirir el certificado digital ante la Autoridad de Registro autorizada (*eBclosion*). 3) Activar el certificado digital para el sistema PKI/DUA-GT.

LA FIRMA ELECTRÓNICA COMO INSTRUMENTO DE E-GOBIERNO

Este proyecto fue puesto en operación en diciembre de 2007 y para esa fecha aún no existía la “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” pero al igual que el proyecto BancaSAT, éste proyecto fue respaldado y regulado jurídicamente a través de un acuerdo del directorio de la SAT. El acuerdo del directorio de la SAT que da regulación a este proyecto es el 014-2007. En este caso, si se tenía un carácter obligatorio del uso de la firma electrónica, por parte de los agentes aduaneros para presentar la declaración de mercancías. Es importante mencionar que en este proyecto se utiliza la firma electrónica avanzada generada por medio de un dispositivo seguro.

El último proyecto que según la SAT fue fortalecido con la “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” es el de la facturación electrónica, conocido como FACE; para este proyecto, se hizo un *benchmarking* de los modelos técnicos que se podían aplicar. Este proyecto es regulado jurídicamente por medio de otro acuerdo del directorio de la SAT, en este caso es el 024-2007.

Dentro del modelo de implementación del sistema, se contempla que empresas nacionales o extranjeras, especializadas en evaluación y certificación de seguridad informática, emitan una certificación en materia de seguridad informática a las empresas que deseen ser autorizadas como GFACE. Es importante resaltar que se utilizan estándares y proveedores totalmente diferentes a los utilizados para la firma electrónica de las aduanas, a pesar de que en ambos el componente principal es el mismo porque la factura contiene la firma electrónica de la empresa prestadora del servicio de facturación electrónica y la del contribuyente que emite la factura.

LA FIRMA ELECTRÓNICA COMO INSTRUMENTO DE E-GOBIERNO

Aparte de estos proyectos, la SAT tiene otros proyectos a futuro, como por ejemplo, la obligatoriedad de que todos los correos electrónicos internos fueran firmados electrónicamente, anterior mente a la “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” este proyecto tenía el obstáculo de que no existía ley que diera respaldo a las firmas electrónicas, pero ahora que ya existe este respaldo jurídico, este proyecto debería avanzar sin mayores problemas.

Una forma muy recomendable para iniciar a utilizar la firma electrónica como instrumento de e-gobierno, es creando infraestructuras de clave pública dentro de los organismos del gobierno y empezar a utilizar la firma electrónica internamente, justo como lo quiere iniciar a hacer la SAT.

8.2 Uso de la firma electrónica en los organismos del Estado

En el “Reglamento de la ley para el reconocimiento de las comunicaciones y firmas electrónicas” se dedica el segundo capítulo a regular como podría ser utilizada la firma electrónica, por parte del Estado.

Por medio de esos artículos del reglamento, se otorga al Estado la posibilidad de utilizar la firma electrónica en la mayor parte de sus actuaciones. A continuación, se transcribe literalmente dicho capítulo y se analiza su contenido.

Artículo 5. Actos y contratos por parte del Estado. *Los órganos del Estado podrán ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica. En consecuencia, serán válidos de la misma manera y producirán los mismos efectos que los expedidos por escrito y en soporte de papel.*

Se exceptúan aquellas actuaciones para las cuales la legislación vigente exija una solemnidad que no sea susceptible de cumplirse mediante documento electrónico, o requiera la concurrencia personal de la autoridad o funcionario que deba intervenir en ellas.

LA FIRMA ELECTRÓNICA COMO INSTRUMENTO DE E-GOBIERNO

Para los efectos del párrafo primero, los actos administrativos, formalizados por medio de documentos electrónicos y que consten en decretos o resoluciones, en acuerdos de órganos colegiados, así como la celebración de contratos, la emisión de cualquier otro documento que exprese la voluntad de un órgano o servicio público de la administración del Estado en ejercicio de sus potestades legales y, en general, todo documento que revista la naturaleza de instrumento público o aquellos que deban producir los efectos jurídicos de estos, deberán suscribirse mediante firma electrónica avanzada.

En este artículo se le otorga al Estado de Guatemala la posibilidad y la libertad de utilizar la firma electrónica, es decir deja la puerta abierta a que cualquier organismo del Estado utilice la firma electrónica como alternativa plenamente válida. Esto únicamente depende de la buena voluntad que tenga cada organismo para modernizarse, tener procesos optimizados, mejor utilización de tiempo y recursos, que al final se traduce en mejor servicio a la población.

La única condición que tiene este artículo, es que cuando se requiera la presencia de algún funcionario del gobierno, no se podrá utilizar la firma electrónica; y también que es necesario que se utilice firma avanzada y no la simple.

Artículo 6. Relación con los organismos del Estado. *Las personas podrán relacionarse con los organismos del Estado, a través de técnicas y medios electrónicos con firma electrónica, siempre que se ajusten al procedimiento descrito por la ley o el presente reglamento y que tales técnicas y medios sean compatibles con los que utilicen dichos organismos. En aquellos casos en que se haga necesaria la comprobación de su identidad, será necesario el empleo de firma electrónica avanzada. Los organismos del Estado podrán relacionarse por medios electrónicos con los particulares, cuando estos hayan consentido expresamente en esta forma de comunicación.*

Los organismos del Estado deberán evitar al hacer uso de firmas electrónicas, que se restrinja injustificadamente el acceso a las prestaciones o servicios que brinden y a la publicidad y transparencia que rijan sus actuaciones y, en general, que se cause discriminaciones arbitrarias.

La única condición encontrada en este artículo es que se debe utilizar la firma electrónica avanzada preferentemente.

Se puede decir entonces que cualquier ciudadano puede interactuar con cualquier organismo del Estado por medios electrónicos siempre y cuando se utilice una firma electrónica avanzada, para poder tener respaldo jurídico pleno.

Existen muchos servicios ciudadanos en los que se debería empezar a utilizar la firma electrónica para brindar un mejor servicio a la población. Los beneficios serán evitar largas colas, atención a cualquier hora del día, entre otros.

Artículo 7. Contratación del Estado. *Los organismos del Estado podrán contratar los servicios de certificación de firmas electrónicas con prestadores de servicios de certificación autorizados por el Registro de Prestadores de Servicios de Certificación, si ello resultare más conveniente, técnica o económicamente. Para el efecto, la estimación de dicha conveniencia estará basada en criterios de calidad de servicio y precio de este.*

Según este artículo, los organismos del Estado, pueden tener su infraestructura de clave pública propia, o si resultara más conveniente pueden contratar a un prestador de servicios de certificación. La única restricción para contratar a un prestador de servicios de certificación, es que esté registrado en el RPSC del Ministerio de Economía.

Artículo 8. Documentos electrónicos utilizados por el Estado. *Los organismos del Estado que utilicen documentos electrónicos deberán contar con un repositorio o archivo electrónico a los efectos de su archivo una vez que haya finalizado su tramitación. El repositorio será responsabilidad del respectivo funcionario a cargo del archivo, sin perjuicio de la celebración de convenios de cooperación entre diferentes organismos o de la contratación de una empresa privada para que preste el servicio. El repositorio deberá garantizar que se respeten las normas sobre publicidad de los documentos contenidos en las leyes respectivas.*

Así mismo, deberá garantizar la seguridad, integridad y disponibilidad de la información en él contenida. Para ello la información deberá ser respaldada en copias de seguridad, bajo las siguientes características:

LA FIRMA ELECTRÓNICA COMO INSTRUMENTO DE E-GOBIERNO

- a) *La información deberá ser respaldada con cada proceso de actualización de documentos;*
- b) *Mantener una copia de seguridad en el lugar de operación de los sistemas de información y otra en un centro de almacenamiento de datos electrónicos especializado. Este centro de almacenamiento de datos electrónicos, que puede ser propio o previsto por terceros, deberá cumplir con condiciones tales como un estricto control de acceso, un completo y detallado registro de entrada y salida de respaldos, resguardando de la humedad, temperatura adecuada, control del riesgo de incendio y otros; y*
- c) *El esquema de respaldo deberá ser simple, basado en generación de copias acumulativas, con el objeto de mantener la historia de la información en el mínimo de versiones posibles.*

La seguridad, integridad y disponibilidad del repositorio deberán estar caracterizadas por:

- a) *Medidas de seguridad y barreras de protección, frente al acceso no autorizado de usuarios;*
- b) *Contar con monitoreo y alarmas que se activen cuando ocurra un evento no autorizado o fuera de programación, para el caso de eventuales fallas de las medidas de seguridad al acceso;*
- c) *La sustitución de la información, por la versión más reciente que se disponga, en el menor tiempo posible, en casos de alteración no programada de aquella; y,*
- d) *La existencia de un programa alternativo de acción que permita la restauración del servicio en el menor tiempo posible, en caso que el repositorio deje de operar por razones no programadas.*

En este artículo, se faculta al Estado para almacenar información electrónicamente, con mayor eficiencia que almacenarla en papel, ya que no se desperdicia papel, no se necesita espacios especiales para archivar papel, ubicar alguna información puntual es sencillo, mientras que dentro de bodegas llenas de papeles se convierte en una hazaña casi imposible y que requiere de mucho tiempo para su realización.

La alternativa más factible y eficiente para esto es contratar el servicio de custodia de documentos en alguna autoridad certificadora, de manera de tener todo el archivo de forma electrónica y ya no más en papel ocupando grandes espacios, aparte de esos beneficios, también se tiene la garantía de que se protegerá la integridad de la información electrónica, mientras que el papel puede deteriorarse y causar pérdida de información.

Artículo 9. Regulación. *Cada organismo del Estado podrá regular la forma como se garantizará la publicidad, seguridad, integridad y eficacia en el uso de las firmas electrónicas, y las demás necesarias para la aplicación de las normas establecidas en la ley o el presente reglamento.*

Por último, el reglamento deja libertad a cada organismo del Estado a hacer su propia regulación para el uso de la firma electrónica siempre y cuando se cumplan con las normas establecidas en la ley o en el reglamento. Esta libertad de regulación es importante porque cada organismo del Estado, presenta diferentes necesidades respecto a la información que maneja. Por ejemplo, en algunos casos será necesario establecer la obligatoriedad del cifrado de las comunicaciones, mientras que para otros casos no, y esto debe ser regulado independientemente por cada organismo.

CONCLUSIONES

1) A través de la historia, el hombre ha tenido la necesidad de enviar información secreta o confidencial, con garantía de que no sea del conocimiento de nadie más que el destinatario. Esto ha llevado al hombre a inventar métodos para ocultar esa información mientras viaja en el medio, proveyendo al receptor la clave, para que la pueda descifrar. En los últimos años se han desarrollado métodos y algoritmos que hacen que se pueda transmitir información por medios electrónicos de manera segura. La firma electrónica asegura la integridad, autenticación, confidencialidad y no repudio de la información. Es más segura que la firma manuscrita y se utiliza actualmente en el mundo, como una alternativa totalmente válida y con respaldo jurídico, que puede sustituir los medios tradicionales basados en papel y la firma manuscrita.

2) El objetivo principal de la “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” es equiparar los medios físicos con su alternativo medio electrónico, por eso hay dos ideas importantísimas que están presentes en dicha ley: 1) la firma electrónica tiene la misma validez jurídica y fuerza probatoria ante la ley que la firma manuscrita; y 2) es aplicable a todo tipo de contrato exceptuando el derecho de familia. Con la seguridad técnica que tiene la firma electrónica y con el respaldo jurídico con el que cuenta desde hace algún tiempo en Guatemala; se puede decir que es la alternativa más segura y más eficiente para intercambiar información que tienen los guatemaltecos.

3) Un ámbito importante y en el que la firma electrónica ha tenido mucho auge en otros países del mundo, es en el ámbito del gobierno electrónico, porque permite tener una administración más eficiente y ordenada, optimizando recursos. La ley de firma electrónica y su reglamento avalan la utilización de firmas electrónicas por los organismos del Estado ya sea con una infraestructura de clave pública (*PKI*) propia o comprando las firmas en una entidad prestadora de servicios de certificación registrada en el RPSC del Ministerio de Economía. Es claro que la ley no obliga a utilizar la firma electrónica, sólo reconoce su utilización.

4) Existen dos tipos de firma electrónica reguladas en la legislación guatemalteca: la simple y la avanzada. La diferencia fundamental entre ambas es la seguridad que proveen. Jurídicamente, la avanzada tiene validez plena, mientras que la simple, queda a criterio del juez. Técnicamente, la firma electrónica simple sólo incluye el resultado de la operación de hash y el certificado de identidad utilizado para firmar, mientras que la firma electrónica avanzada además de tener el resultado de la operación de hash y el certificado utilizado, incluye también un estampado cronológico calculado a partir del hash y firmado por una autoridad de estampado cronológico (TSA). El estampado cronológico es uno de los servicios que ofrecen las entidades prestadoras de servicios de certificación, el cual avala el tiempo de creación de la firma. Además, algunas también ofrecen la custodia de documentos. Dependiendo de las operaciones con respaldo jurídico que se necesite realizar, se debe elegir correctamente entre una firma electrónica y una firma avanzada y complementarla con otros servicios de certificación.

5) La confianza que se tiene sobre la identidad del remitente de una comunicación firmada electrónicamente, radica en la confianza que se tenga en la Autoridad Certificadora que emitió el certificado de identidad del remitente. Por eso es importante la tarea de la Autoridad Certificadora de verificar la identidad de todas las personas a quienes les extiende un certificado. Esto puede verificarse en el *Certification Practice Statement (CPS)* dónde se describen las operaciones que realiza una autoridad certificadora.

6) Los principales obstáculos que se observaron para que los guatemaltecos empiecen a utilizar la firma electrónica son: la falta de conocimiento de sus beneficios, la falta de confianza en los medios electrónicos y la aparente dificultad de aprender su utilización. En la presente tesis se describen los beneficios de utilizarla, se explica su fundamento informático y jurídico y se presentan unas guías para facilitar el aprendizaje de su uso. Con el objetivo de que todos estos resultados estén al alcance de la mayoría de los guatemaltecos, se creó el sitio web <http://firmaelectronicagt.com> que contiene toda esta información.

RECOMENDACIONES

1) La “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” abre muchas posibilidades al permitir utilizar los medios electrónicos como medios jurídicamente válidos de expresar la voluntad, al mismo tiempo da ciertos derechos y obligaciones a quienes los usan. Se recomienda a los usuarios de firma electrónica: custodiar adecuadamente su clave privada, dar aviso a la autoridad certificadora si su clave privada ha quedado expuesta y cerciorarse que la información que contiene el certificado digital sea verdadera; al recibir una comunicación firmada electrónicamente: verificar que la firma sea válida, esto incluye verificar la integridad, comprobar que el certificado no haya sido revocado y que no haya vencido. En general, al manejar información electrónica importante se recomienda utilizar una conexión a Internet segura, sobre todo, no utilizar redes inalámbricas públicas.

2) Según el *Technology Acceptance Model (TAM)* que es un modelo aplicado a los sistemas de información y que describe cómo los usuarios aceptan y utilizan una tecnología nueva; hay dos factores importantísimos que definen la adopción de una tecnología, estos son: la utilidad percibida y la facilidad de uso. La utilidad percibida se refiere a los beneficios que obtiene el usuario al utilizarla, por ejemplo, mayor productividad. La facilidad de uso se refiere al esfuerzo que tiene que realizar el usuario para aprenderla. Se recomienda entonces tomar en cuenta los dos factores que menciona el *Technology Acceptance Model* en todo el proceso de implementación de la firma electrónica en Guatemala para que sea exitoso y la mayoría de guatemaltecos empiecen a utilizar sin mayor dificultad, la firma electrónica.

3) Se recomienda a las empresas medianas y grandes e instituciones del estado, principalmente a las entidades financieras, establecer políticas por medio de las cuales se promueva el uso de firma electrónica en las comunicaciones internas para evitar la suplantación de identidad y el cifrado con certificado digital en las comunicaciones que contengan información de carácter confidencial, para evitar robo de información; que utilicen certificados públicos en sus servidores y comunicarles a sus clientes que verifiquen dicho certificado de identidad antes de hacer cualquier operación, para garantizarles que están accediendo al servicio original, protegiéndolos de *phishing*; y utilizar un protocolo seguro (*https*) al transmitir los datos privados de sus clientes para evitar el *sniffing*.

5) Que las empresas grandes que se dedican al manejo de información electrónica entre otras cosas, evalúen los beneficios y posibilidades de utilizar la firma electrónica como instrumento de gobierno electrónico, por medio del cual los organismos y las instituciones del estado puedan incrementar la eficiencia en sus operaciones y den un mejor servicio a la ciudadanía; y así invertir en la infraestructura necesaria para extender los certificados e inscribirse en el Registro de Prestadores de Servicios de Certificación (RPSC) del Ministerio de Economía para prestar servicios de certificación a los organismos y las instituciones del estado y a la población en general.

6) Que las instituciones relacionadas con la implementación y adopción de la firma electrónica en el país, promuevan el uso de la firma electrónica a través de campañas informativas dentro de la población más propensa a utilizar firma electrónica para empezar a crear la necesidad y la demanda de firma electrónica, resaltando los grandes beneficios de su uso, otorgando premios o beneficios a los ciudadanos que prefieran hacer transacciones por medios electrónicos, publicar casos de éxito para incentivar y dar a conocer su uso, y publicar manuales de uso para reducir todo lo posible la percepción de dificultad de uso.

REFERENCIAS

1. Real Academia Española. *Diccionario de la lengua española*. 22 ed; 2001.
2. Congreso de la República de Guatemala **Ley para el reconocimiento de las comunicaciones y firmas electrónicas**.
3. Wikipedia. **Confidencialidad**. *Wikipedia*. Disponible en: <http://es.wikipedia.org/wiki/Confidencialidad>. Visitado el 20 de noviembre de 2009.
4. Wikipedia. **Correspondencia unívoca**. *Wikipedia*. Disponible en: http://es.wikipedia.org/wiki/Correspondencia_un%C3%ADvoca. Visitado el 25 de noviembre de 2009.
5. Wikipedia. **Integridad del mensaje**. *Wikipedia*. Disponible en: http://es.wikipedia.org/wiki/Integridad_del_mensaje. Visitado el 15 de noviembre de 2009.
6. RFC Editor. **Overview of RFC Document Series**. *RFC Editor*. Disponible en: <http://www.rfc-editor.org/RFCoverview.html>. Visitado el 20 de noviembre de 2009.
7. UNAM. **Criptografía**. *Revista Digital Universitaria*. Disponible en: <http://www.revista.unam.mx/vol.7/num7/art55/art55.htm>. Visitado el 21 de septiembre de 2009.

8. Wikipedia. **Criptoanálisis.** *Wikipedia.* Disponible en: <http://es.wikipedia.org/wiki/Criptoan%C3%A1lisis>. Visitado el 23 de septiembre de 2009.
9. Wikipedia. **Criptografía.** *Wikipedia.* Disponible en: <http://es.wikipedia.org/wiki/Criptograf%C3%ADa>. Visitado el 3 de noviembre de 2009.
10. Wikipedia. **Enigma (máquina).** *Wikipedia.* Disponible en: [http://es.wikipedia.org/wiki/Enigma_\(m%C3%A1quina\)](http://es.wikipedia.org/wiki/Enigma_(m%C3%A1quina)). Visitado el 23 de septiembre de 2009.
11. Wikipedia. **Data Encryption Standard.** *Wikipedia.* Disponible en: http://es.wikipedia.org/wiki/Data_Encryption_Standard. Visitado el 23 de septiembre de 2009.
12. Wikipedia. **Triple DES.** *Wikipedia.* Disponible en: http://es.wikipedia.org/wiki/Triple_DES. Visitado el 23 de septiembre de 2009.
13. Wikipedia. **Advanced Encryption Standard.** *Wikipedia.* Disponible en: http://es.wikipedia.org/wiki/Advanced_Encryption_Standard. Visitado el 23 de septiembre de 2009.
14. Wikipedia. **International Data Encryption Algorithm.** *Wikipedia.* Disponible en: http://es.wikipedia.org/wiki/International_Data_Encryption_Algorithm. Visitado el 23 de septiembre de 2009.

15. Wikipedia. **Digital Signature Algorithm.** *Wikipedia.* Disponible en: http://es.wikipedia.org/wiki/Digital_Signature_Algorithm. Visitado el 10 de noviembre de 2009.
16. Wikipedia. **RSA.** *Wikipedia.* Disponible en: <http://es.wikipedia.org/wiki/RSA>. Visitado el 11 de noviembre de 2009.
17. Wikipedia. **MD5.** *Wikipedia.* Disponible en: <http://es.wikipedia.org/wiki/MD5>. Visitado el 06 de octubre de 2009.
18. Wikipedia. **Secure Hash Algorithm.** *Wikipedia.* Disponible en: http://es.wikipedia.org/wiki/Secure_Hash_Algorithm. Visitado el 06 de octubre de 2009.
19. Wikipedia. **Criptografía simétrica.** *Wikipedia.* Disponible en: http://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica. Visitado el 23 de septiembre de 2009.
20. Wikipedia. **Criptografía asimétrica.** *Wikipedia.* Disponible en: http://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica. Visitado el 24 de septiembre de 2009.
21. Wikipedia. **Firma digital.** *Wikipedia.* Disponible en: http://es.wikipedia.org/wiki/Firma_digital. Visitado el 21 de septiembre de 2009.
22. Instituto Nacional de Tecnologías de la Información de España. **Conceptos de seguridad.** *Instituto Nacional de Tecnologías de la Información de España.* Disponible en: http://cert.inteco.es/Formacion/Conceptos_de_seguridad/. Visitado el 19 de diciembre de 2009.

23. Wikipedia. **Certificado digital.** *Wikipedia.* Disponible en: http://es.wikipedia.org/wiki/Certificado_digital. Visitado el 07 de octubre de 2009.
24. Wikipedia. **Autoridad de certificación.** *Wikipedia.* Disponible en: http://es.wikipedia.org/wiki/Autoridad_de_certificaci%C3%B3n. Visitado el 20 de diciembre de 2009.
25. Wikipedia. **Sellado de tiempo.** *Wikipedia.* Disponible en: http://es.wikipedia.org/wiki/Sellado_de_tiempo. Visitado el 15 de diciembre de 2009.
26. Wikipedia. **Infraestructura de clave pública.** *Wikipedia.* Disponible en: http://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica. Visitado el 07 de octubre de 2009.
27. Wikipedia. **Federal Information Processing Standard.** *Wikipedia.* Disponible en: http://es.wikipedia.org/wiki/Federal_Information_Processing_Standard. Visitado el 23 de septiembre de 2009.

BIBLIOGRAFÍA

1. Congreso de la República de Guatemala **Ley para el reconocimiento de las comunicaciones y firmas electrónicas**. Decreto 47-2008, septiembre 2008
2. Laudon, Kenneth C. y Carol Guercio Traver. **E-commerce: bussines, technology. society**. 3ª edición. Estados Unidos: Pearson Prentice Hall, 2007. 879pp
3. Ministerio de Economía Gobierno de Guatemala. **Reglamento de la ley para el reconocimiento de las comunicaciones y firmas electrónicas**. Acuerdo Gubernativo 135-2009, mayo 2009
4. National Institute of Standards and Technology. **Digital Signature Standard**. Federal Information Processing Standards. Publicación 186-3, junio 2009

APÉNDICES

Apéndice A – Construcción del sitio informativo

Parte de este trabajo de tesis fue el desarrollo de un sitio web con información importante sobre la utilización de la firma electrónica, a manera de aporte a la sociedad guatemalteca. El propósito del sitio es informar a la los guatemaltecos sobre los beneficios y las posibilidades que abre la firma electrónica. También guiar el proceso de aprendizaje y su uso.

Para alojar el sitio, se arrendó durante un año el dominio <http://firmaelectronicagt.com/> y un *hosting* con espacio suficiente y servidor de base de datos como para poder instalar un *CMS*.

Se analizó entre varias opciones de *CMS* y al final se decidió que el que más se adaptaba a las necesidades era *WordPress*. Se instaló entonces *WordPress* en el hosting y se configuró y personalizó para que cumpliera con las características que se necesitaban. Los requerimientos eran los siguientes:

- Botones para compartir en redes sociales.
- Formulario de contacto.
- Recopilación de estadísticas de visitas
- Plantilla agradable a la vista.
- Generación automática de mapa de sitio para indexación en buscadores.

Todos estos requerimientos se cumplieron a través de diferentes *plugins* de *WordPress* que proveían esas funcionalidades y la plantilla que se utilizó fue una plantilla gratuita, liberada con licencia *GPL*.

Al finalizar la investigación, se procedió a la publicación del contenido más importante. El contenido que se publicó fue:

- Breve base teórica de criptografía.
- Base teórica de la firma electrónica.
- Análisis Jurídico completo (Capítulo 4).
- Guías de uso en *PDF*.
- Recomendaciones a los usuarios
- Casos de éxito.

A continuación, se presentan algunas pantallas de cómo quedó el sitio Web.

Figura 26: Sitio <http://firmaelectronica.gt.com/>

FIRMA ELECTRÓNICA EN GUATEMALA

Más segura que la firma manuscrita y con el mismo reconocimiento jurídico

Inicio Base teórica Análisis Jurídico Guías Blog Preguntas frecuentes Acerca de Contáctenos Mapa del sitio

Buscar IR

Criptografía

La palabra criptografía proviene del griego kryptos, que significa "ocultar", y graphos, que significa "escritura", la traducción literal entonces sería "escritura oculta".

En su clasificación dentro de las ciencias, la criptografía proviene de una rama de las matemáticas, que fue iniciada por el matemático Claude Elwood Shannon en 1948, denominada: "Teoría de la Información". Esta rama de las ciencias se divide en: "Teoría de Códigos" y en "Criptología". Y a su vez la Criptología se divide en Criptoanálisis y Criptografía.

```
graph TD;
  A[Matemáticas] --> B[Teoría de la Información];
  B --> C[Teoría de códigos];
  B --> D[Criptología];
  D --> E[Criptografía];
  D --> F[Criptoanálisis];
```

Clasificación de la criptografía

Criptografía es la técnica para convertir un mensaje o información en cifrado utilizando algoritmos, de manera que solo el destinatario pueda leerlo porque es el único que sabe como descifrarlo (conoce la clave) y así se asegura que aunque el mensaje viaje por un medio inseguro y sea interceptado no podrá ser entendido.

Un algoritmo de cifrado es una función matemática para desordenar una información de manera que ésta se transforme en incomprensible, usando una o más claves. A la entrada de esta función, es decir el mensaje que se quiere proteger, se llama información plana, y a la salida después de aplicar el algoritmo con la clave para cifrar, se le llama información cifrada o criptograma.

ENLACES DE INTERÉS

- [Cámara de Comercio de Guatemala](#)
- [CONCYT](#)
- [Ley para el reconocimiento de las comunicaciones y firmas electrónicas](#)
- [Registro de Prestadores de Servicio de Certificación](#)
- [Reglamento de la ley para el reconocimiento de las comunicaciones y firmas electrónicas](#)

SUSCRIBASE AL BLOG

ÚLTIMOS POSTS DEL BLOG

- [Apertura del Registro de Prestadores de Servicios de Certificación](#)
- [Lanzamiento de la firma electrónica en](#)

Figura 27: Sitio <http://firmaelectronica.gt.com/>

FIRMA ELECTRÓNICA EN GUATEMALA

Más segura que la firma manuscrita y con el mismo reconocimiento jurídico

Inicio Base teórica Análisis Jurídico Guías Blog Preguntas frecuentes Acerca de Contáctenos Mapa del sitio

Buscar IR

Equiparación De Medios Electrónico Con Medios Físicos

Hay tres aspectos importantes en los que se equiparan los medios físicos y los medios electrónicos en la "Ley para el reconocimiento de las comunicaciones y firmas electrónicas" estos aspectos son: el escrito, la firma y el original. Las comunicaciones y firmas electrónicas tienen la capacidad de cumplir estos tres aspectos totalmente porque se basan en tres requisitos importantes que son la disponibilidad, la integridad y la autenticación. La disponibilidad se refiere a la seguridad de poder ver la información cuando necesitemos o queramos, la integridad se refiere a que la información permanezca exactamente igual a lo largo del tiempo, es decir que no se pueda modificar intencionalmente ni por alguna falla de los sistemas y por último la autenticación significa que tengamos la confianza de que el firmante es verdaderamente quien dice ser.

Escrito

A continuación se cita literalmente el artículo 7 de la "Ley para el reconocimiento de las comunicaciones y firmas electrónicas" en el cual se da validez a una comunicación electrónica para que cumpla el requisito de que una información conste por escrito siempre y cuando sea accesible para su ulterior consulta, es decir que cumpla con el requisito de **disponibilidad** de la información. Esto podría ser por medio de la custodia de documentos que proveen los prestadores de servicios de certificación y mediante el cual nos garantizan conservar la información íntegra y confidencialmente.

Artículo 7. Escrito. Cuando cualquier norma jurídica requiera que una información, comunicación o un contrato consten por escrito, en papel o en cualquier otro medio físicos, o prevea consecuencias en el caso de que eso no se cumple, una comunicación electrónica cumplirá ese requisito si la información consignada en su texto es accesible para su ulterior consulta.

Firma

La firma manuscrita tiene como fin identificar y asegurar la identidad de un autor o remitente, o como una prueba del consentimiento o aprobación de la información que está firmando, esto se hace a través de un pequeño trazo o dibujo personal que supuestamente solo el dueño puede hacerlo. Igualmente la firma electrónica tiene el objetivo de identificar al autor, pero se vale de procedimientos mucho más confiables, y no solo de la suposición de que la firma solamente puede hacerla el dueño.

Para firmar electrónicamente, son necesarios datos de creación de firma, que solamente posee la persona vinculada con esa firma, además, para asegurar la identidad del firmante, el prestador de servicios de certificación está obligado por la ley a comprobar su identidad antes de emitirle el certificado y precisamente en eso radica la autenticación en la firma electrónica.

A continuación se pone el artículo 8 el cual equipara la firma manuscrita con la firma electrónica.

Artículo 8. Firma. Cuando cualquier norma jurídica requiera que una comunicación o un contrato sea firmado por una parte, o prevea consecuencias en el caso de que no se firma, ese requisito se dará por cumplido respecto de una comunicación electrónica:

a) Si se utiliza un método para determinar la identidad de esa parte y para indicar la voluntad que tiene tal parte respecto de la información consignada en la comunicación electrónica; y,

ENLACES DE INTERÉS

- [Cámara de Comercio de Guatemala](#)
- [CONCYT](#)
- [Ley para el reconocimiento de las comunicaciones y firmas electrónicas](#)
- [Registro de Prestadores de Servicio de Certificación](#)
- [Reglamento de la ley para el reconocimiento de las comunicaciones y firmas electrónicas](#)

SUSCRIBASE AL BLOG



ÚLTIMOS POSTS DEL BLOG

- [Apertura del Registro de Prestadores de Servicios de Certificación](#)
- [Lanzamiento de la firma electrónica en](#)

ANEXOS

Anexo 1 - Ley para el reconocimiento de las comunicaciones y firmas electrónicas

Diario de Centro América

DECANO DE LA PRENSA CENTROAMERICANA | ÓRGANO OFICIAL DE LA REPÚBLICA DE GUATEMALA, C. A.

MARTES 23 de septiembre de 2008 No. 23 Tomo CCLXXXV

Directora General: Ana María Rodas

www.dca.gob.gt

Sumario

ORGANISMO LEGISLATIVO

CONGRESO DE LA REPÚBLICA DE GUATEMALA

DECRETO NÚMERO 47-2008

DECRETO NÚMERO 48-2008

ORGANISMO EJECUTIVO

MINISTERIO DE RELACIONES EXTERIORES

SEGUNDO PROTOCOLO AL TRATADO MARCO DEL MERCADO ELÉCTRICO DE AMÉRICA CENTRAL.

MINISTERIO DE FINANZAS PÚBLICAS

Acuérdase derogar el Acuerdo Gubernativo sin número, de fecha 16 de enero de 1978, publicado en el Diario de Centro América el 25 de enero de 1978.

PUBLICACIONES VARIAS

MUNICIPALIDAD DE EL TUMBADOR, DEPARTAMENTO DE SAN MARCOS

ACTA NÚMERO 47-2008 PUNTO TERCERO

MUNICIPALIDAD DE JALAPA

ACTA NÚMERO 40-25-08-2008

ANUNCIOS VARIOS

Matrimonios • Líneas de Transporte • Constituciones de Sociedad • Modificaciones de Sociedad • Disolución de Sociedad • Patentes de Invención • Registro de Marcas • Títulos Supletorios • Edictos • Remates •

ATENCIÓN ANUNCIANTES:

IMPRESIÓN SE HACE CONFORME ORIGINAL

Toda impresión en la parte legal del Diario de Centro América, se hace respetando el original. Por lo anterior, esta administración ruega al público tomar nota.

ORGANISMO LEGISLATIVO



CONGRESO DE LA REPÚBLICA DE GUATEMALA

DECRETO NÚMERO 47-2008

EL CONGRESO DE LA REPÚBLICA DE GUATEMALA

CONSIDERANDO:

Que el Estado como responsable del bien común debe mantener, reforzar y aplicar políticas y acciones que permitan una mayor participación en la dinámica y beneficios del desarrollo económico y social libre, la modernización, los procesos económicos sin trabas ni obstáculos artificiales, así como la inserción del país en las corrientes del progreso mundial de manera sostenible y equitativa.

CONSIDERANDO:

Que la inmersión masiva de la tecnología en nuestra sociedad es una realidad que no podemos ignorar y por ende se debe revisar los conceptos y visiones tradicionales del mundo físico para adaptarlos al actual contexto del mundo digital.

CONSIDERANDO:

Que la promoción del comercio electrónico en todos sus aspectos requiere de una legislación cuyo fundamento sea, entre otros, la facilitación del comercio electrónico en el interior y mas allá de las fronteras nacionales, la validación, fomento y estímulo de las operaciones efectuadas por medio de las nuevas tecnologías de la información sobre la base de la autonomía de la voluntad y el apoyo a las nuevas prácticas comerciales, tomando en cuenta en todo momento la neutralidad tecnológica.

CONSIDERANDO:

Que la integración al comercio electrónico global requiere que sean adoptados instrumentos técnicos y legales basados en los modelos de legislación internacional que buscan la uniformización de esta rama del derecho tan especializada, y que debe dársele seguridad jurídica y técnica a las contrataciones, comunicaciones y firmas electrónicas mediante el señalamiento de la equivalencia funcional a estas últimas con respecto a los documentos en papel y las firmas manuscritas.

POR TANTO:

En ejercicio de las atribuciones que le confiere la literal a) del artículo 171 de la Constitución Política de la República,

DECRETA:

La siguiente:

LEY PARA EL RECONOCIMIENTO DE LAS COMUNICACIONES Y FIRMAS ELECTRÓNICAS

**TÍTULO I
COMERCIO ELECTRÓNICO EN GENERAL**

**CAPÍTULO I
DISPOSICIONES GENERALES**

Artículo 1. Ámbito de aplicación. La presente ley será aplicable a todo tipo de comunicación electrónica, transacción o acto jurídico, público o privado, nacional o internacional, salvo en los casos siguientes:

- a) En las obligaciones contraídas por el Estado en virtud de Convenios o Tratados Internacionales.
- b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.

El Estado y sus instituciones quedan expresamente facultados para la utilización de las comunicaciones y firmas electrónicas.

En las transacciones y actos realizados exclusivamente entre sujetos privados y que no afecten derechos de terceros, las partes podrán convenir en la aplicación de los mecanismos previstos en esta ley o bien de cualesquiera otras alternativas que deseen para asegurar la autenticidad e integridad de sus comunicaciones electrónicas.

Las disposiciones contenidas en esta ley se aplicarán sin perjuicio de las normas relativas a la celebración, la formalización, la validez y la eficacia de los contratos y otros actos jurídicos; el régimen jurídico aplicable a las obligaciones; y de las obligaciones que para los comerciantes les establece la legislación vigente.

Las normas sobre la presentación de servicios de certificación de firma electrónica que recoge esta ley, no sustituyen ni modifican las que regulan las funciones que corresponde realizar a las personas facultadas, con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en su elevación a públicos.

Artículo 2. Definiciones. Para los efectos de la presente ley, se entenderá por:

Certificado: Todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma, usualmente emitido por un tercero diferente del originador y el destinatario.

Comercio Electrónico: Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de una o más comunicaciones electrónicas o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, incluyendo el factoraje y el arrendamiento de bienes de equipo con opción a compra; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; de inversión; de financiación; de banca; de seguros; de todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.

Comunicación: Toda exposición, declaración, reclamación, aviso o solicitud, incluye una oferta y la aceptación de una oferta, que las partes hayan de hacer o decidan hacer en relación con la formación o el cumplimiento de un contrato.

Comunicación Electrónica: Toda comunicación que las partes hagan por medio de mensajes de datos.

Datos de creación de firma: los datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

Destinatario: La parte designada por el iniciador para recibir la comunicación electrónica, pero que no esté actuando a título de intermediario con respecto a esa comunicación electrónica.

Estampado Cronológico: Comunicación electrónica firmada por una entidad de certificación que sirve para verificar que otra comunicación electrónica no ha cambiado en un período que comienza en la fecha y hora en que se presta el servicio y termina en la fecha y hora en que la firma de la comunicación electrónica generada por el prestador del servicio de estampado pierde validez.

Firma Electrónica: Los datos en forma electrónica consignados en una comunicación electrónica, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante con relación a la comunicación electrónica e indicar que el firmante aprueba la información recogida en la comunicación electrónica.

Firma Electrónica Avanzada: La firma electrónica que cumple los requisitos siguientes:

- a. Estar vinculada al firmante de manera única;
- b. Permitir la identificación del firmante;
- c. Haber sido creada utilizando los medios que el firmante puede mantener bajo su exclusivo control;
- d. Estar vinculada a los datos a que se refiere, de modo que cualquier cambio ulterior de los mismos sea detectable.

Firmante: La persona que posee los datos de creación de la firma y que actúe en nombre propio o de la persona a la que representa.

Iniciador: Toda parte que haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar una comunicación electrónica antes de ser archivada, si ese es el caso, pero que no haya actuado a título de intermediario con respecto a esa comunicación electrónica.

Intercambio Electrónico de Datos (IED): La transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto.

Intermediario: En relación con una determinada comunicación electrónica, se entenderá toda persona que, actuando por cuenta de otra, envía, recibe o archiva dicha comunicación electrónica o preste algún otro servicio con respecto a ella.

Mensaje de Datos: El documento o información generada, enviada, recibida o archivada por medios electrónicos, magnéticos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (IED), el correo electrónico, el telegrama, el télex o el telefax.

Parte que confía: La persona que pueda actuar sobre la base de un certificado o de una firma electrónica.

Prestador de Servicios de Certificación: Se entenderá la entidad que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas.

Sede o lugar del establecimiento comercial: Se entenderá todo lugar donde una parte mantiene un centro de operaciones no temporal para realizar una actividad económica distinta del suministro transitorio de bienes o servicios desde determinado lugar.

Sistema Automatizado de Mensajes: Todo programa informático o un medio electrónico o algún otro medio automatizado utilizado para iniciar una acción o para responder a operaciones o mensajes de datos, que actúe, total o parcialmente, sin que una persona física haya de intervenir o revisar la actuación cada vez que se inicie una acción o que el sistema genere una respuesta.

Sistema de Información: Todo sistema que sirva para generar, enviar, recibir, archivar o procesar de alguna otra forma comunicaciones electrónicas.

Artículo 3. Interpretación. En la interpretación de la presente ley habrán de tenerse en cuenta su origen internacional, la necesidad de promover la uniformidad de su aplicación y de velar por la observancia de la buena fe, tanto en el comercio nacional como internacional.

Las cuestiones relativas a materias que se rijan por la presente ley y que no estén expresamente resueltas en ella, serán dirimidas de conformidad con los principios generales en que ella se inspira.

Artículo 4. Modificación mediante acuerdo mutuo. Salvo que se disponga otra cosa, la manera como se formalizan las relaciones entre las partes que generan, envían, reciben, archivan o procesan de alguna otra forma comunicaciones electrónicas, podrán ser modificadas mediante acuerdo mutuo entre las partes.

En caso de no haber acuerdo, se entenderán formalizadas conforme a lo que estipula el Capítulo III del Título I de esta Ley.

**CAPÍTULO II
APLICACIÓN DE LOS REQUISITOS JURÍDICOS A LAS COMUNICACIONES
ELECTRÓNICAS**

Artículo 5. Reconocimiento jurídico de las comunicaciones electrónicas. No se negarán efectos jurídicos, validez o fuerza obligatoria a una comunicación o a un contrato por la sola razón de que esa comunicación o ese contrato estén en forma de comunicación electrónica.

Nada de lo dispuesto en esta ley hará que una parte esté obligada a utilizar o a aceptar información en forma de comunicación electrónica, pero su conformidad al respecto podrá inferirse de su conducta. Así mismo, nada de lo dispuesto en la presente ley obligará a que una comunicación o un contrato tengan que hacerse o probarse de alguna forma particular.

Artículo 6. Incorporación por Remisión. Salvo acuerdo en contrario entre las partes, cuando en una comunicación electrónica se haga remisión total o parcial a directrices, normas, estándares, acuerdos, cláusulas, condiciones, cualquier información o términos fácilmente accesibles con la intención de incorporarlos como parte del contenido o hacerlos vinculantes jurídicamente, se presume que esos términos están incorporados por remisión a esa comunicación electrónica. Entre las partes y conforme a la ley, esos términos serán jurídicamente válidos como si hubieran sido incorporados en su totalidad en la comunicación electrónica.

Artículo 7. Escrito. Cuando cualquier norma jurídica requiera que una información, comunicación o un contrato consten por escrito, en papel o en cualquier medio físico, o prevea consecuencias en el caso de que eso no se cumpla, una comunicación electrónica cumplirá ese requisito si la información consignada en su texto es accesible para su ulterior consulta.

Artículo 8. Firma. Cuando cualquier norma jurídica requiera que una comunicación o un contrato sea firmado por una parte, o prevea consecuencias en el caso de que no se firme, ese requisito se dará por cumplido respecto de una comunicación electrónica:

- a) Si se utiliza un método para determinar la identidad de esa parte y para indicar la voluntad que tiene tal parte respecto de la información consignada en la comunicación electrónica; y,
- b) Si el método empleado:
 1. Es fiable y resulta apropiado para los fines para los que se generó o transmitió la comunicación electrónica, atendidas todas las circunstancias del caso, inclusive todo acuerdo aplicable; o si,
 2. Se ha demostrado en la práctica que, por sí solo o con el respaldo de otras pruebas, dicho método cumple las funciones enunciadas en la literal a) del presente artículo.

Artículo 9. Original. Cuando cualquier norma jurídica requiera que una comunicación o un contrato se proporcione o conserve en su formato original, o prevea consecuencias en el caso de que eso no se cumpla, ese requisito se tendrá por cumplido respecto de una comunicación electrónica:

- a) Si existe alguna garantía fiable de la integridad de la información que contiene, a partir del momento en que se generó por primera vez en su forma definitiva, tanto en comunicación electrónica como de otra índole; y,
- b) Si, en los casos en que se exija proporcionar la información que contiene, ésta puede exhibirse a la persona a la que se ha de proporcionar.

Artículo 10. Integridad de una comunicación electrónica. Para efectos del artículo 9 anterior, se considerará que la información consignada en una comunicación electrónica es íntegra, si atiende a los criterios siguientes:

- a) Ésta se ha mantenido completa y sin alteraciones que no sean la adición de algún endoso o algún cambio sobrevenido en el curso normal de su transmisión, archivo o presentación; y,
- b) El grado de fiabilidad requerido se determinará teniendo en cuenta la finalidad para la que se generó la información, así como todas las circunstancias del caso.

Artículo 11. Admisibilidad y fuerza probatoria de las comunicaciones electrónicas. Las comunicaciones electrónicas serán admisibles como medios de prueba. No se negará eficacia, validez o fuerza obligatoria y probatoria en toda actuación administrativa, judicial o privada a todo tipo de información en forma de comunicación electrónica, por el sólo hecho que se trate de una comunicación electrónica, ni en razón de no haber sido presentado en su forma original.

Artículo 12. Criterio para valorar probatoriamente una comunicación electrónica. Toda información presentada en forma de comunicación electrónica gozará de la debida fuerza probatoria de conformidad con los criterios reconocidos por la legislación para la apreciación de la prueba. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje; la fiabilidad de la forma en la que se haya conservado la integridad de la información; la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

Artículo 13. Conservación de las comunicaciones electrónicas. Cuando cualquier norma jurídica requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho mediante la conservación de las comunicaciones electrónicas, siempre que se cumplan las condiciones siguientes:

- a) Que la información que contengan sea accesible para su posterior consulta;
- b) Que la comunicación electrónica sea conservada en el formato en que se haya generado, enviado o recibido o con algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida; y,
- c) Que se conserve, de haber alguna, toda información o dato que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido.

No estarán sujetos a la obligación de conservación, los documentos, registros o informaciones que tenga por única finalidad facilitar el envío o recepción de la comunicación electrónica. Los libros y papeles podrán ser conservados en cualquier medio tecnológico que garantice su reproducción exacta.

Artículo 14. Conservación de mensajes de datos y archivo de documentos a través de terceros. El cumplimiento de la obligación de conservar documentos, registros o informaciones en comunicaciones electrónicas, se podrá realizar directamente o a través de terceros, siempre y cuando se cumplan las condiciones enunciadas en el artículo anterior.

CAPÍTULO III COMUNICACIONES ELECTRÓNICAS Y FORMACIÓN DE CONTRATOS A TRAVÉS DE MEDIOS ELECTRÓNICOS

Artículo 15. Formación y validez de los contratos. En la formación de un contrato por particulares o entidades públicas, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de una comunicación electrónica. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación una o más comunicaciones electrónicas.

Artículo 16. Reconocimiento de las comunicaciones electrónicas por las partes. En las relaciones entre el iniciador y el destinatario de una comunicación electrónica, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de comunicación electrónica.

Artículo 17. Atribución de una comunicación electrónica. Se entenderá que una comunicación electrónica proviene del iniciador, si ha sido enviado por el propio iniciador.

En las relaciones entre el iniciador y el destinatario, se entenderá que una comunicación electrónica proviene del iniciador si ha sido enviado:

- a) Por alguna persona facultada para actuar en nombre del iniciador respecto de esa comunicación; o,
- b) Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

Artículo 18. Presunción del origen de una comunicación electrónica. En las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que una comunicación electrónica proviene del iniciador, y a actuar en consecuencia, cuando:

- a) Para comprobar que la comunicación provenía del iniciador, el destinatario haya aplicado adecuadamente un procedimiento aceptado previamente por el iniciador con ese fin; o,
- b) La comunicación electrónica que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar una comunicación electrónica como propia.

Lo expresado en este artículo, no se aplicará a partir del momento en que el destinatario haya sido informado por el iniciador que la comunicación electrónica no provenía del iniciador y haya dispuesto de un plazo razonable para actuar en consecuencia; o, en los casos previstos en la literal b) de este artículo, desde el momento en que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la comunicación electrónica no provenía del iniciador.

Artículo 19. Concordancia de la comunicación electrónica enviada con la comunicación electrónica recibida. Siempre que una comunicación electrónica provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, éste último tendrá derecho a considerar que la comunicación electrónica recibida corresponde a la que quería enviar el iniciador, y podrá proceder en consecuencia.

El destinatario no gozará de este derecho si sabía, o hubiera sabido, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a un error en la comunicación electrónica recibida.

El destinatario tendrá derecho a considerar que cada comunicación electrónica recibida es una comunicación electrónica separada y al actuar en consecuencia, salvo en la medida en que duplique otra comunicación electrónica, y que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la nueva comunicación electrónica era un duplicado.

Artículo 20. Acuse de recibo. Si al enviar o antes de enviar una comunicación electrónica, el iniciador solicita o acuerda con el destinatario que se acuse recibo de la comunicación electrónica, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

- a) Toda comunicación del destinatario, automatizada o no; o,
- b) Todo acto del destinatario que baste para indicar al iniciador que se ha recibido la comunicación electrónica.

Cuando el iniciador haya indicado que los efectos de la comunicación electrónica estarán condicionados a la recepción de un acuse de recibo, se considerará que la comunicación electrónica no ha sido enviada en tanto que no se haya recibido el acuse de recibo.

Artículo 21. Falta de Acuse de Recibo. De conformidad con el artículo anterior, cuando el iniciador no haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, si no ha recibido acuse en el plazo fijado o convenido o no se ha fijado o convenido ningún plazo, en un plazo de cinco días el iniciador podrá:

- a) Dar aviso al destinatario de que no ha recibido acuse de recibo y fijar un plazo razonable para su recepción; y,
- b) De no recibir acuse dentro del plazo fijado conforme a la literal a) anterior, podrá, dando aviso de ello al destinatario, considerar que la comunicación electrónica no ha sido enviada o ejercer cualquier otro derecho que pueda tener.

Artículo 22. Presunción de recepción de una comunicación electrónica. Cuando el iniciador reciba acuse de recibo del destinatario, se presumirá que éste ha recibido la comunicación electrónica correspondiente.

Esa presunción no implicará que la comunicación electrónica corresponda al mensaje recibido. Cuando en el acuse de recibo se indique que la comunicación electrónica recibida cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que ello es así.

Artículo 23. Efectos jurídicos. Salvo en lo que se refiere al envío o recepción de comunicaciones electrónicas, los artículos 21 y 22, no obedecen al propósito de regir las consecuencias jurídicas que puedan derivarse de esa comunicación electrónica o de su acuse de recibo. Las consecuencias jurídicas de las comunicaciones electrónicas se regirán conforme a las normas aplicables al acto o negocio jurídico contenido en dicho mensaje de datos.

Artículo 24. Tiempo y lugar del envío y la recepción de las comunicaciones electrónicas. De no convenir otra cosa el iniciador y el destinatario, la comunicación electrónica se tendrá por:

- a) **Expedida:** en el momento en que salga de un sistema de información que esté bajo el control del iniciador o de la parte que la envíe en nombre de éste o, si la comunicación electrónica no ha salido de un sistema de información que esté bajo el control del iniciador o de la parte que la envíe en nombre de éste, en el momento en que esa comunicación se reciba.
- b) **Recibida:** en el momento en que pueda ser recuperada por el destinatario en una dirección electrónica que él haya designado. La comunicación electrónica se tendrá por recibida en otra dirección electrónica del destinatario en el momento en que pueda ser recuperada por el destinatario en esa dirección y en el momento en que el destinatario tenga conocimiento de que esa comunicación ha sido enviada a dicha dirección. Se presumirá que una comunicación electrónica puede ser obtenida por el destinatario en el momento en que llegue a la dirección electrónica de éste.
- c) La comunicación electrónica se tendrá por expedida en el lugar en que el iniciador tenga su establecimiento y por recibida en el lugar en que el destinatario tenga el suyo, conforme se determine en función de lo dispuesto en esta ley.
- d) La literal b) del presente artículo será aplicable aun cuando el sistema de información que sirva de soporte a la dirección electrónica esté ubicado en un lugar distinto de aquel en que se tenga por recibida la comunicación en virtud de la literal c) del presente artículo.

Artículo 25. Invitaciones para presentar ofertas. Toda propuesta de celebrar un contrato presentada por medio de una o más comunicaciones electrónicas, que no vaya dirigida a una o varias partes determinadas, sino que sea generalmente accesible para toda parte que haga uso de sistemas de información, así como toda propuesta que haga uso de aplicaciones interactivas para hacer pedidos a través de dichos sistemas, se considerará una invitación a presentar ofertas, salvo que indique claramente la intención de la parte que presentará la propuesta de quedar obligada por su oferta en caso de que sea aceptada.

Artículo 26. Empleo de sistemas automatizados de mensajes para la formación de un contrato. No se negará validez ni fuerza obligatoria a un contrato que se haya formado por la interacción entre un sistema automatizado de mensajes y una persona física, o por la interacción entre sistemas automatizados de mensajes, por la simple razón de que ninguna persona física haya revisado cada uno de los distintos actos realizados a través de los sistemas o el contrato resultante de tales actos ni haya intervenido en ellos.

Artículo 27. Disponibilidad de las condiciones contractuales. Nada de lo dispuesto en la presente ley afectará a la aplicación de regla de derecho alguna por la que se obligue a una parte que negocie algunas o todas las condiciones de un contrato mediante el intercambio de comunicaciones electrónicas a poner a disposición de la otra parte contratante, de determinada manera, las comunicaciones electrónicas que contengan las condiciones del contrato, ni eximirá a una parte que no lo haga de las consecuencias jurídicas de no haberlo hecho.

Artículo 28. Error en las comunicaciones electrónicas. Cuando una persona física cometa un error al introducir los datos de una comunicación electrónica intercambiada con el sistema automatizado de mensajes de otra parte y dicho sistema no le brinde la oportunidad de corregir el error, esa persona, o la parte en cuyo nombre ésta haya actuado, tendrá derecho a retirar la parte de la comunicación electrónica en que se produjo dicho error, si:

- a) La persona, o la parte en cuyo nombre haya actuado esa persona, notifica a la otra parte el error tan pronto como sea posible después de haberse percatado de éste y le indica que lo ha cometido; y si,
- b) La persona, o la parte en cuyo nombre haya actuado esa persona, no ha utilizado bienes o servicios ni ha obtenido ningún beneficio material o valor de los bienes o servicios, si los hubiere, que haya recibido de la otra parte.

Nada de lo dispuesto en el presente artículo afectará a la aplicación de regla de derecho alguna que regule las consecuencias de un error cometido, a reserva de lo dispuesto en el primer párrafo de este artículo.

Artículo 29. Ubicación de las partes. Para los fines de la presente ley, se presumirá que la sede o el lugar del establecimiento comercial de una parte está en el lugar por ella indicado, salvo que otra parte demuestra que la parte que hizo esa indicación no tiene sede o establecimiento comercial alguno en ese lugar.

Si una parte no ha indicado la sede o el lugar del establecimiento comercial, y tiene más de un establecimiento comercial, se considerará como tal, para los efectos de la presente Ley, el que tenga la relación más estrecha con el contrato pertinente, habida cuenta de las circunstancias conocidas o previstas por las partes en cualquier momento antes de la celebración del contrato o al concluirse éste.

Si una persona física no tiene establecimiento comercial, se tendrá en cuenta su lugar de residencia habitual.

Un lugar no constituye un establecimiento comercial por el solo hecho de que sea el lugar:

- a) Donde estén ubicados el equipo y la tecnología que sirven de soporte para el sistema de información utilizado por una de las partes para la formación de un contrato; o,
- b) Donde otras partes puedan obtener acceso a dicho sistema de información.

El hecho de que una parte haga uso de un nombre de dominio o de una dirección de correo electrónico vinculados a cierto país no crea la presunción de que su establecimiento comercial se encuentra en dicho país.

Artículo 30. Requisitos de información. Nada de lo dispuesto en la presente ley afectará a la aplicación de norma jurídica alguna en virtud de la cual las partes deban revelar su identidad, la ubicación de su establecimiento u otros datos, ni eximirá de consecuencias jurídicas a una parte que haya hecho a este respecto declaraciones inexactas, incompletas o falsas.

TÍTULO II COMERCIO ELECTRÓNICO EN MATERIAS ESPECÍFICAS

CAPÍTULO I TRANSPORTE DE MERCANCÍAS

Artículo 31. Actos relacionados con los contratos de transporte de mercancías. Sin perjuicio de lo dispuesto en el Título I de la presente ley, el presente capítulo será aplicable a cualquiera de los siguientes actos que guarden relación con un contrato de transporte de mercancías, o con su cumplimiento, sin que la lista sea exhaustiva:

- a) Indicación de las marcas, el número, la cantidad o el peso de las mercancías; declaración de la índole o el valor de las mercancías; emisión de un recibo, factura o comprobante por las mercancías; confirmación de haberse completado la carga de las mercancías.
- b) Notificación a alguna persona de las cláusulas y condiciones del contrato; comunicación de instrucciones al portador.
- c) Reclamación de la entrega de las mercancías; autorización para proceder a la entrega de las mercancías; notificación de la pérdida de las mercancías o de los daños que hayan sufrido.
- d) Cualquier otra notificación o declaración relativas al cumplimiento del contrato.
- e) Promesa de hacer entrega de las mercancías a la persona designada o a una persona autorizada para reclamar esa entrega.
- f) Concesión, adquisición, renuncia, restitución, transferencia o negociación de algún derecho sobre mercancías.
- g) Adquisición o transferencia de derechos y obligaciones con arreglo al contrato.

Artículo 32. Documentos de transporte. Con sujeción a lo dispuesto en el tercer párrafo de este artículo, en los casos en que la ley requiera que alguno de los actos enunciados en el artículo 31 anterior se lleve a cabo por escrito o mediante un documento que conste de papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos.

El párrafo anterior será aplicable tanto si el requisito en él previsto está expresado en forma de obligación, como si la ley simplemente prevé consecuencias en el caso de que no se lleve a cabo el acto por escrito o mediante un documento.

Cuando se conceda algún derecho a una persona determinada y a ninguna otra, o ésta adquiere alguna obligación, y la ley requiera que, para que ese acto surta efecto, el derecho o la obligación hayan de transferirse a esa persona mediante el envío o la utilización de un documento, ese requisito quedará satisfecho si el derecho o la obligación se transfieren mediante la utilización de uno o más mensajes de datos, siempre que se emplee un método fiable para garantizar la singularidad de ese mensaje o esos mensajes de datos.

Para los fines del párrafo anterior, el nivel de fiabilidad requerido será determinado conforme a los fines para los que se transfirió el derecho o la obligación y de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

Cuando se utilicen uno o más mensajes de datos para llevar a cabo alguno de los actos enunciados en las literales f) y g) del artículo 31 anterior, no será válido ningún documento utilizado para llevar a cabo cualquiera de esos actos, a menos que se haya puesto fin al uso de

mensajes de datos para sustituirlo por el de documentos. Todo documento que se emita en esas circunstancias deberá contener una declaración a tal efecto. La sustitución de mensajes de datos por documentos no afectará a los derechos ni a las obligaciones de las partes.

Cuando se aplique obligatoriamente una norma jurídica a un contrato de transporte de mercancías que esté consignado, o del que se haya dejado constancia en un documento, esa norma no dejará de aplicarse a un contrato de transporte de mercancías del que se haya dejado constancia en uno o más mensajes de datos por razón de que el contrato conste en ese mensaje o esos mensajes de datos en lugar de constar en un documento.

TÍTULO III DISPOSICIONES COMPLEMENTARIAS AL COMERCIO ELECTRÓNICO

CAPÍTULO I FIRMA ELECTRÓNICA AVANZADA Y PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Artículo 33. Efectos jurídicos de una firma electrónica o firma electrónica avanzada. La firma electrónica o la firma electrónica avanzada, la cual podrá estar certificada por una entidad prestadora de servicios de certificación, que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta, según los criterios de apreciación establecidos en las normas procesales.

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

Cuando una firma electrónica avanzada haya sido fijada en una comunicación electrónica se presume que el suscriptor de aquella tenía la intención de acreditar esa comunicación electrónica y de ser vinculado con el contenido del mismo. Para considerarse fiable el uso de una firma electrónica avanzada, ésta tendrá que incorporar como mínimo los atributos siguientes:

- Que los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;
- Que los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;
- Que sea posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y,
- Cuando uno de los objetivos del requisito legal de la firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, que sea posible detectar cualquier alteración de esa información hecha después del momento de la firma.

Lo dispuesto en este artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre, de cualquier otra manera, la fiabilidad de una firma electrónica; o, que aduzca pruebas de que una firma electrónica no es fiable.

Artículo 34. Órgano competente. El Estado a través del órgano o entidad correspondiente, podrá atribuir competencia a una persona, órgano o entidad pública o privada, para determinar qué firmas electrónicas cumplen con lo dispuesto en el artículo 33 anterior. Para tal efecto, dicha determinación que se haga deberá ser compatible con las normas o criterios internacionales reconocidos.

Artículo 35. Proceder del firmante. Cuando puedan utilizarse datos de creación de firmas para crear una firma con efectos jurídicos, cada firmante deberá:

- Actuar con la diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma.
- Sin dilación indebida, utilizar los medios que le proporcione el prestador de servicios de certificación conforme la presente ley, o en cualquier caso esforzarse razonablemente, para dar aviso a cualquier persona que, según pueda razonablemente prever el firmante, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen en:
 - El firmante sabe que los datos de creación de la firma han quedado en entredicho;
 - 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.
- Cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado o que hayan de consignarse en él son exactas y cabales.

Serán a cargo del firmante las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos anteriores enunciados en este artículo.

Artículo 36. Proceder del prestador de servicios de certificación. Cuando un prestador de servicios de certificación preste servicios para apoyar una firma electrónica que pueda utilizarse como firma con efectos jurídicos, ese prestador de servicios de certificación deberá:

- Actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas.
- Actuar con diligencia razonable para cerciorarse que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él son exactas y precisas.
- Proporcionar a la parte que confía en el certificado, medios razonablemente accesibles que permitan a esta determinar mediante el certificado:
 - La identidad del prestador de servicios de certificación;
 - Que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;

3. Que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella.
- d) Proporcionar a la parte que confía en el certificado, medios razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera:
1. El método utilizado para comprobar la identidad del firmante;
 2. Cualquier limitación de los fines o del valor respecto de los cuales pueden utilizarse los datos de creación de la firma o el certificado;
 3. Si los datos de creación de la firma son válidos y no están en entredicho;
 4. Cualquier limitación del alcance o del grado de responsabilidad que haya establecido el prestador de servicios de certificación;
 5. Si existe un medio para que el firmante de aviso de que los datos de creación de la firma están en entredicho, conforme a lo dispuesto en la literal b) del artículo 35 de la presente ley;
 6. Si se ofrece un servicio de revocar oportunamente el certificado.
- e) Cuando se ofrezcan servicios conforme al numeral 5 de la literal d) del presente artículo, proporcionar un medio para que el firmante de aviso conforme a la literal b) del artículo 35 de esta ley y, cuando se ofrezcan servicios en virtud del numeral 6 del inciso d) del presente artículo, cerciorarse que existe un servicio para revocar oportunamente el certificado.
- f) Utilizar, al prestar servicios, sistemas, procedimientos y recursos humanos fiables.

Serán a cargo del prestador de servicios de certificación las consecuencias jurídicas que produzca el hecho de no haber cumplido los requisitos anteriores enunciados en este artículo.

Artículo 37. Fiabilidad. A los efectos de la literal f) del artículo 36 anterior, para determinar si los sistemas, procedimientos o recursos humanos utilizados por un prestador de servicios de certificación son fiables, y en qué medida lo son, podrán tenerse en cuenta los factores siguientes:

- a) Los recursos humanos y financieros, incluida la existencia de activos;
- b) La calidad de los sistemas de equipo y programas informáticos;
- c) Los procedimientos para la transmisión del certificado y las solicitudes de certificados, y la conservación de registros;
- d) La disponibilidad de la información para los firmantes nombrados en el certificado y para las partes que confían en éste;
- e) La periodicidad y el alcance de la auditoría realizada por un órgano independiente;
- f) La existencia de una declaración del Estado, de un órgano de acreditación o del prestador de servicios de certificación respecto del cumplimiento o la existencia de los factores que anteceden; o,
- g) Cualesquiera otros factores pertinentes.

Artículo 38. Proceder de la parte que confía en el certificado. Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que produzca el hecho de que no haya tomado medidas razonables para:

- a) Verificar la fiabilidad de la firma electrónica; o,
- b) Cuando la firma electrónica esté refrendada por un certificado:
 - i. Verificar la validez, suspensión o revocación del certificado; y,
 - ii. Tener en cuenta cualquier limitación en relación con el certificado.

Artículo 39. Reconocimiento de certificados extranjeros y de firmas electrónicas extranjeras. Al determinar si un certificado o una firma electrónica producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración:

- a) Lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica; ni,
- b) El lugar en que se encuentre el establecimiento del expedidor o del firmante.

Todo certificado expedido en el extranjero producirá los mismos efectos jurídicos que el expedido dentro del territorio de la República, si se presenta un grado de fiabilidad sustancialmente equivalente.

Toda firma electrónica creada o utilizada en el extranjero producirá los mismos efectos jurídicos que la expedida dentro del territorio de la República, si presenta un grado de fiabilidad sustancialmente equivalente.

A efectos de determinar si un certificado o una firma electrónica presentan un grado de fiabilidad sustancialmente equivalente para los fines de los dos párrafos anteriores del presente artículo, se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente.

Cuando, sin perjuicio de lo dispuesto en los tres párrafos anteriores del presente artículo, las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas o certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que el acuerdo no sea válido o eficaz conforme al derecho aplicable.

Artículo 40. Características y requerimientos de los prestadores de servicios de certificación. Podrán ser prestadores de servicios de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero, que previa solicitud sean autorizadas por el Registro de Prestadores de Servicios de Certificación del Ministerio de Economía y que cumplan con los requerimientos establecidos por ésta, con base en las condiciones siguientes:

- a) Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como prestadores de servicios de certificación.

- b) Contar con la capacidad y elementos técnicos necesarios para la generación de firmas electrónicas avanzadas, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley.

- c) Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a pena privativa de libertad, o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética o hayan sido excluidas de aquella. Esta inhabilidad estará vigente por el mismo período que la ley penal o administrativa señale para el efecto.

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

El Ministerio de Economía podrá emitir los requerimientos y regulaciones que considere pertinentes, siempre sobre la base de su adecuación a las normas y principios internacionales reconocidos.

Artículo 41. Actividades de los prestadores de servicios de certificación. Los prestadores de servicios de certificación autorizados por el Ministerio de Economía para prestar sus servicios en el país, podrán realizar, entre otras, las actividades siguientes:

- a) Emitir certificados en relación con las firmas electrónicas avanzadas de personas naturales o jurídicas, ya sean éstas digitales o de cualquier otra índole.
- b) Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción de las comunicaciones electrónicas.
- c) Ofrecer o facilitar los servicios de creación de firmas electrónicas avanzadas certificadas, ya sean estas digitales o de cualquier otra índole.
- d) Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en las literales f) y g) del artículo 31 de la presente ley.
- e) Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de comunicaciones electrónicas.
- f) Ofrecer los servicios de archivo y conservación de comunicaciones electrónicas.
- g) Certificar en los certificados que expidan, las condiciones profesionales del titular de la firma para efectos de constituir prueba frente a cualquier entidad pública o privada.

Artículo 42. Obligaciones de los prestadores de servicios de certificación. Las sociedades de certificación tendrán entre otros, los deberes siguientes:

- a) Emitir certificados conforme a lo solicitado o acordado con el firmante.
- b) Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas electrónicas avanzadas, la conservación y archivo de certificados y documentos en soporte de mensaje de datos.
- c) Garantizar la protección, confidencialidad y debido uso de la información suministrada por el firmante.
- d) Garantizar la prestación permanente del servicio de entidad de certificación.
- e) Atender oportunamente las solicitudes y reclamaciones hechas por los firmantes.
- f) Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas electrónicas y certificados emitidos y en general sobre cualquier comunicación electrónica que se encuentre bajo su custodia y administración.
- g) Permitir y facilitar la realización de las auditorías por parte del Registro de Prestadores de Servicios de Certificación.
- h) Elaborar los reglamentos que definen las relaciones con el firmante y la forma de prestación del servicio.
- i) Llevar un registro de los certificados.

Artículo 43. Remuneración por la prestación de servicios. La remuneración por los servicios de los prestadores de servicios de certificación será establecida libremente por éstos.

Artículo 44. Terminación unilateral. Salvo acuerdo entre las partes, el prestador de servicios de certificación podrá dar por terminado el acuerdo de vinculación con el firmante dando un preaviso no menor al plazo de noventa (90) días. Vencido este término, el prestador de servicio de certificación revocará los certificados que se encuentren pendientes de expiración.

Igualmente, el firmante podrá dar por terminado el acuerdo de vinculación con la sociedad de certificación dando un preaviso no inferior al plazo de treinta (30) días.

Artículo 45. Terminación de actividades por parte de los prestadores de servicios de certificación. Las sociedades de certificación autorizadas pueden cesar en el ejercicio de actividades, siempre y cuando hayan recibido autorización por parte del Registro de Prestadores de Servicios de Certificación.

Artículo 46. Contenido de los certificados. Un certificado emitido por un prestador de servicios de certificación autorizada, además de estar firmado electrónicamente por éste, debe contener por lo menos lo siguiente:

- a) Nombre, dirección y domicilio del firmante.
- b) Identificación del firmante nombrado en el certificado.
- c) El nombre, la dirección y el lugar donde realiza actividades la prestadora de servicios de certificación.
- d) La clave pública del usuario en los casos de la tecnología de criptografía asimétrica.
- e) La metodología para verificar la firma electrónica del firmante impuesta en la comunicación electrónica.

- f) El número de serie del certificado.
g) Fecha de emisión y expiración del certificado.

Artículo 47. Revocación de certificados. Los certificados podrán revocarse por:

- a) El firmante de una firma electrónica avanzada certificada, podrá solicitar a la prestadora de servicios de certificación que expidió un certificado, la revocación del mismo. En todo caso, estará obligado a solicitar la revocación en los eventos siguientes:
- Por pérdida de la clave privada, en el caso de la tecnología de criptografía asimétrica;
 - La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido, en el caso de la tecnología de criptografía simétrica.
- b) Si el firmante no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exenta de culpa que confiaron en el contenido del certificado.
- c) Una prestadora de servicios de certificación revocará un certificado emitido por las razones siguientes:
- A petición del firmante o un tercero en su nombre y representación;
 - Por muerte del firmante;
 - Por liquidación del firmante en el caso de las personas jurídicas;
 - Por la confirmación de que alguna información o hecho contenido en el certificado es falso;
 - La clave privada de la prestadora de servicios de certificación o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado;
 - Por el cese de actividades de la prestadora de servicios de certificación; y,
 - Por orden judicial o de entidad administrativa competente.

Artículo 48. Término de conservación de los registros. La información y registros de certificados expedidos por una prestadora de servicios de certificación deben ser conservados por el término exigido en la ley que regule el acto o negocio jurídico en particular, o por diez años en caso de no existir dicho término.

CAPÍTULO II REGISTRO DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Artículo 49. Funciones del Registro de Prestadores de Servicios de Certificación. El Registro de Prestadores de Servicios de Certificación, adscrito al Ministerio de Economía, ejercerá las facultades que legalmente le han sido asignadas respecto de las entidades prestadoras de servicios de certificación, y adicionalmente tendrá las funciones siguientes:

- Autorizar la actividad de las entidades prestadoras de servicios de certificación.
- Velar por el funcionamiento y la eficiente prestación del servicio por parte de las prestadoras de servicios de certificación.
- Realizar visitas de auditoría a las prestadoras de servicios de certificación.
- Revocar o suspender la autorización para operar como prestador de servicios de certificación.
- Solicitar la información pertinente para el ejercicio de sus funciones.
- Imponer sanciones a las prestadoras de servicios de certificación en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio.
- Ordenar la revocación de certificados cuando la prestadora de servicios de certificación los emita sin el cumplimiento de las formalidades legales.
- Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y prácticas comerciales restrictivas, competencia desleal y protección del consumidor, en los mercados atendidos por las prestadoras de servicios de certificación, debiéndose coordinar, según el caso, con las autoridades específicas.
- Impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las prestadoras de servicios de certificación.
- Emitir las regulaciones que considere basadas en las normas, regulaciones, criterios o principios internacionales reconocidos.

Artículo 50. Sanciones. El Registro de Prestadores de Servicios de Certificación del Ministerio de Economía, de acuerdo con el debido proceso y el derecho de defensa, podrá imponer, por intermedio del despacho ministerial de economía, según la naturaleza y la gravedad de la falta, las sanciones a las sociedades de certificación siguientes:

- Amonestación.
- Multas institucionales hasta por el equivalente a dos mil quinientos (2500) salarios mínimos no agrícolas legales mensuales vigentes, y personales a los administradores y representantes legales de las entidades prestadoras de servicios de certificación, hasta por quinientos (500) salarios mínimos no agrícolas legales mensuales vigentes, cuando se compruebe que han autorizado, ejecutado o tolerado conductas violatorias de la ley.
- Suspender de inmediato todas o algunas de las actividades de la entidad infractora.
- Prohibir a la entidad infractora prestar directa o indirectamente los servicios de certificación hasta por el término de cinco (5) años.
- Revocar definitivamente la autorización para operar como entidad prestadora de servicios de certificación.

CAPÍTULO III DISPOSICIONES VARIAS

Artículo 51. Prevalencia de las leyes de protección al consumidor. La presente Ley se aplicará sin perjuicio de las normas vigentes en materia de protección al consumidor.

Las entidades o empresas involucradas en el comercio electrónico deben respetar los intereses de los consumidores y actuar de acuerdo a prácticas equitativas en el ejercicio de sus actividades empresariales, publicitarias y de mercadotecnia. Así mismo, las entidades o empresas no deben realizar ninguna declaración, incurrir en alguna omisión, o comprometerse en alguna práctica que resulte falsa, engañosa, fraudulenta o desleal.

Siempre que las entidades o empresas publiquen información sobre ellas mismas o sobre los bienes o servicios que ofrecen, deben presentarla de manera clara, visible, precisa y fácilmente accesible. Así mismo, deben cumplir con cualquier declaración que hagan respecto a sus políticas y prácticas relacionadas con sus transacciones con consumidores.

Las empresas no deben aprovecharse de las características especiales del comercio electrónico para ocultar su verdadera identidad o ubicación, o para evadir el cumplimiento de las normas de protección al consumidor o los mecanismos de aplicación de dichas normas.

Las empresas deben desarrollar e implementar procedimientos efectivos y fáciles de usar, que permitan a los consumidores manifestar su decisión de recibir o rechazar mensajes comerciales no solicitados por medio del correo electrónico. Cuando los consumidores manifesten que no desean recibir mensajes comerciales por correo electrónico, tal decisión debe ser respetada.

Artículo 52. Información en Línea. Sin perjuicio de cumplir con la legislación vigente para comerciantes y empresas mercantiles, las empresas que realicen comercio electrónico deberán proveer la siguiente información:

- Información sobre la empresa: Las empresas que realicen transacciones con los consumidores por medio del comercio electrónico deben proporcionar de manera precisa, clara y fácilmente accesible, información suficiente sobre ellas mismas, que permita al menos:
 - La identificación de la empresa – incluyendo la denominación legal y el nombre o marca de comercialización; el principal domicilio geográfico de la empresa; correo electrónico u otros medios electrónicos de contacto, o el número telefónico; y, cuando sea aplicable, una dirección para propósitos de registro, y cualquier número relevante de licencia o registro gubernamental;
 - Una comunicación rápida, fácil y efectiva con la empresa;
 - Apropiados y efectivos mecanismos de solución de disputas;
 - Servicios de atención a procedimientos legales; y,
 - Ubicación del domicilio legal de la empresa y de sus directivos, para uso de las autoridades encargadas de la reglamentación y de la aplicación de la ley.

Cuando una empresa de a conocer su membresía o afiliación en algún esquema relevante de autorregulación, asociación empresarial, organización para resolución de disputas u otro organismo de certificación, debe proporcionar a los consumidores un método sencillo para verificar dicha información, así como detalles apropiados para contactar con dichos organismos, y en su caso, tener acceso a los códigos y prácticas relevantes aplicados por el organismo de certificación.

- Información sobre los bienes o servicios: Las empresas que realicen transacciones con consumidores por medio del comercio electrónico deben proporcionar información precisa y fácilmente accesible que describa los bienes o servicios ofrecidos, de manera que permita a los consumidores tomar una decisión informada antes de participar en la transacción y en términos que les permita mantener un adecuado registro de dicha información.

Artículo 53. Plazo. El Ministerio de Economía creará y organizará el Registro de Prestadores de Servicios de Certificación en un plazo no mayor a sesenta (60) días después de entrada en vigencia la presente ley.

Artículo 54. Transitorio. El Registro de Prestadores de Servicios de Certificación del Ministerio de Economía contará con un término adicional de seis (6) meses, contados a partir de la publicación de la presente ley, para organizar la función de inspección, control y vigilancia de las actividades realizadas por las entidades prestadoras de servicios de certificación, así como para emitir las normas técnicas aplicables a las firmas electrónicas avanzadas y los certificados de cualquier tipo.

Artículo 55. Reglamento. El Organismo Ejecutivo, por conducto del Ministerio de Economía, deberá emitir el reglamento de esta Ley, en un plazo no mayor a seis (6) meses contados a partir de su publicación. Así mismo, podrá emitir las reglamentaciones o disposiciones que considere para el debido desempeño del Registro de Prestadores de Servicios de Certificación.


Artículo 56. Vigencia y Derogatorias. La presente ley entra en vigencia ocho (8) días después de su publicación y deroga las disposiciones que le sean contrarias.

REMÍTASE AL ORGANISMO EJECUTIVO PARA SU SANCIÓN, PROMULGACIÓN Y PUBLICACIÓN.

EMITIDO EN EL PALACIO DEL ORGANISMO LEGISLATIVO, EN LA CIUDAD DE GUATEMALA, EL DIECINUEVE DE AGOSTO DE DOS MIL OCHO.


ARISTIDES BALDOMERO CRESPO VILLEGAS
PRESIDENTE


JOSÉ ROBERTO ALEJOS CAMBARÁ
SECRETARIO


ROSA ELVIRA ZAPETA OSORIO
SECRETARIA



PALACIO NACIONAL: Guatemala, dieciséis de septiembre del año dos mil ocho.

PUBLÍQUESE Y CUMPLASE

Colom Caballeros
COLOM CABALLEROS



Alvaro Caballeros Osorio
MINISTRO DE ECONOMÍA

Carlos Larín Ochoa
Lic. Carlos Larín Ochoa
SECRETARIO GENERAL
DE LA PRESIDENCIA DE LA REPUBLICA

[E-709-2008]-23-septiembre



**CONGRESO DE LA
REPÚBLICA DE GUATEMALA**

DECRETO NÚMERO 48-2008

EL CONGRESO DE LA REPÚBLICA DE GUATEMALA

CONSIDERANDO:

Que durante el enfrentamiento armado interno ocurrido en el país, la población guatemalteca sufrió graves violaciones a sus derechos humanos.

CONSIDERANDO:

Que la Comisión para el Esclarecimiento Histórico, presentó el 25 de febrero del año 1999 su informe final, conteniendo entre sus recomendaciones las siguientes: "Que el Estado asuma el contenido del presente informe y apoye iniciativas para su difusión y promoción.", "En la currícula de educación primaria, secundaria y universitaria se incluyan las enseñanzas del enfrentamiento armado y del contenido de los Acuerdos de Paz".

CONSIDERANDO:

Que con fecha 25 de febrero de 2004, el Congreso de la República aprobó el Decreto Número 06-04, Ley que Conmemora el 25 de febrero de cada año como el Día Nacional de la Dignidad de las Víctimas del Conflicto Armado Interno, sin establecer un procedimiento y contenido que hagan operativa dicha conmemoración y que cumpla con los objetivos para lo cual la Comisión del Esclarecimiento Histórico recomendó tal conmemoración.

POR TANTO:

En ejercicio de las atribuciones que le confiere el artículo 171 literal a) de la Constitución Política de la República,

DECRETA:

Las siguientes:

**REFORMAS AL DECRETO NÚMERO 06-04 DEL CONGRESO DE LA REPÚBLICA,
LEY QUE CONMEMORA EL 25 DE FEBRERO DE CADA AÑO COMO EL DÍA NACIONAL
DE LA DIGNIDAD DE LAS VÍCTIMAS DEL CONFLICTO ARMADO INTERNO**

Artículo 1. Se reforma el artículo 1 del Decreto Número 06-04 del Congreso de la República, para que quede de la siguiente manera:

"Artículo 1. Se establece el 25 de febrero de cada año, como el "Día Nacional de la Dignidad de las Víctimas del Conflicto Armado Interno", debiéndose conmemorar tal fecha en instituciones autónomas y descentralizadas, establecimientos educativos y oficinas públicas y privadas, en la forma que se honre de mejor manera la memoria de las víctimas del conflicto armado interno. Los Ministerios de Cultura y Deportes y de Educación, en coordinación, deberán promover dichas actividades conmemorativas para que cumplan su cometido.

El Ministerio de Educación deberá incluir en la currícula de educación primaria y secundaria las enseñanzas sobre las causas y consecuencias del enfrentamiento armado y del contenido de los Acuerdos de Paz."

Artículo 2. El presente Decreto entrará en vigencia el día de su publicación en el Diario Oficial.

REMÍTASE AL ORGANISMO EJECUTIVO PARA SU SANCIÓN, PROMULGACIÓN Y PUBLICACIÓN.

EMITIDO EN EL PALACIO DEL ORGANISMO LEGISLATIVO, EN LA CIUDAD DE GUATEMALA, EL VEINTE DE AGOSTO DE DOS MIL OCHO.

Aristides Baldomero Crespo Villegas
ARISTIDES BALDOMERO CRESPO VILLEGAS
PRESIDENTE



José Roberto Alejos Cámara
JOSÉ ROBERTO ALEJOS CÁMBARA
SECRETARIO

Rosa Elvira Zapeta Osorio
ROSA ELVIRA ZAPETA OSORIO
SECRETARIA

PALACIO NACIONAL: Guatemala, dieciséis de septiembre del año dos mil ocho.

PUBLÍQUESE Y CUMPLASE

Colom Caballeros
COLOM CABALLEROS



Carlos Larín Ochoa
Lic. Carlos Larín Ochoa
SECRETARIO GENERAL
DE LA PRESIDENCIA DE LA REPUBLICA

Jerónimo Lancaster Chingó
Jerónimo Lancaster Chingó
MINISTRO DE CULTURA Y DEPORTES

Alvaro Caballeros Osorio
Alvaro Caballeros Osorio
MINISTRO DE EDUCACIÓN



[E-708-2008]-23-septiembre

ORGANISMO EJECUTIVO



**MINISTERIO DE
RELACIONES EXTERIORES**

SEGUNDO PROTOCOLO AL TRATADO MARCO DEL MERCADO ELÉCTRICO DE AMÉRICA CENTRAL.

YO, ÁLVARO COLOM CABALLEROS
Presidente de la República de Guatemala

DECLARO:

Que el Gobierno de la República de Guatemala, habiendo suscrito en la ciudad de Campeche, de los Estados Unidos Mexicanos, con fecha 10 de abril de dos mil siete el SEGUNDO PROTOCOLO AL TRATADO MARCO DEL MERCADO ELÉCTRICO DE AMÉRICA CENTRAL, ratifica por el presente dicho Protocolo y se comprometo a cumplir y aplicar fielmente las disposiciones que en él figuran.

EN TESTIMONIO DE LO CUAL, firmo el presente Instrumento.

Hecho en la Ciudad de Guatemala, a los veintidós días del mes de abril de dos mil ocho.

Álvaro Colom Caballeros

Anexo 2 - Reglamento de la ley para el reconocimiento de las comunicaciones y firmas electrónicas



MINISTERIO DE ECONOMÍA

Acuérdase crear la COMISIÓN INTERINSTITUCIONAL DE APOYO A PROCESOS DE ARBITRAJE, como parte del Organismo Ejecutivo, con carácter temporal.

ACUERDO GUBERNATIVO NÚMERO 128-2009

Guatemala, 5 de mayo de 2009

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que es obligación fundamental del Estado, promover el desarrollo ordenado y eficiente del comercio interior y exterior del país, fomentando mercados para los productos nacionales. Asimismo, corresponde al Presidente de la República dirigir la política exterior y las relaciones Internacionales; celebrar, ratificar y denunciar tratados y convenios de conformidad con la Constitución.

CONSIDERANDO:

Que el Ministerio de Economía, por delegación del Presidente de la República, tiene asignada la función de conducir las negociaciones de los convenios y tratados de comercio internacional bilateral y multilateral, y una vez aprobados y ratificados, encargarse de su ejecución.

CONSIDERANDO:

Que dos inversionistas de la Empresa Eléctrica de Guatemala, Sociedad Anónima, Iberdrola Energía, S.A. y Tecu Guatemala Holdings LLC, han iniciado el procedimiento de controversias con fundamento, la primera en el "Acuerdo entre la República de Guatemala y el Reino de España para la Promoción y Protección Recíproca de Inversiones" y la segunda en el "Tratado de Libre Comercio República Dominicana, Centroamérica y Estados Unidos de América", por sus siglas en inglés "DR-CAFTA". Para tal efecto se hace necesario designar una comisión interinstitucional de carácter temporal, que se encargará de coordinar las acciones que deban seguirse para el desarrollo de los arbitrajes Internacionales.

PORTANTO:

En ejercicio de las funciones que establece el artículo 183 literales a), e) y f) de la Constitución Política de la República de Guatemala y el artículo 5 del Decreto número 114-97 del Congreso de la República, Ley del Organismo Ejecutivo.

ACUERDA:

Artículo 1. Creación. Se crea la COMISIÓN INTERINSTITUCIONAL DE APOYO A PROCESOS DE ARBITRAJE, como parte del Organismo Ejecutivo, con carácter temporal.

Artículo 2. Objeto. La Comisión tiene por objeto apoyar y dar seguimiento a los arbitrajes Internacionales de inversionistas de la Empresa Eléctrica de Guatemala, Sociedad Anónima, IBERDROLA ENERGÍA, S.A. y Tecu Guatemala Holdings LLC, que han planteado procedimiento de controversias, con fundamento en el "Acuerdo entre la República de Guatemala y el Reino de España para la Promoción y Protección Recíproca de Inversiones" y en el "Tratado de Libre Comercio República Dominicana, Centroamérica y Estados Unidos de América" por sus siglas en inglés "DR-CAFTA", respectivamente, en contra del Estado de Guatemala en los Centros de Arbitraje correspondientes. La Comisión funcionará hasta la finalización de los procesos arbitrales y emisión de los laudos arbitrales respectivos o se llegue a un acuerdo satisfactorio para las partes.

Artículo 3. Atribuciones de la Comisión. Son atribuciones de la Comisión las siguientes:

- a) Apoyar y dar seguimiento a los arbitrajes Internacionales de inversionistas de la Empresa Eléctrica de Guatemala, sociedad Anónima, IBERDROLA ENERGÍA, S.A. y Tecu Guatemala Holdings LLC, en los procedimientos de controversias con fundamento en el "Acuerdo entre la República de Guatemala y el Reino de España para la Promoción y Protección Recíproca de Inversiones" y en el "Tratado de Libre Comercio República Dominicana, Centroamérica y Estados Unidos de América" por sus siglas en inglés "DR-CAFTA", respectivamente, en contra del Estado de Guatemala en los Centros de Arbitraje correspondientes;
- b) Apoyar las estrategias que se deciden por parte de los abogados responsables de los casos antes referidos; y,
- c) Elaborar los cronogramas de los procesos de arbitraje indicados.

Artículo 4. Integración. La Comisión se integra así:

- a) Un representante del Ministerio de Economía, designado por el Ministro de Economía;
- b) Un representante del Ministerio de Relaciones Exteriores, designado por el Ministro de Relaciones Exteriores;
- c) Un representante del Ministerio de Energía y Minas, designado por el Ministro de Energía y Minas;
- d) Un representante de la Procuraduría General de la Nación, designado por el Procurador General de la Nación; y

e) Un representante de la Secretaría General de la Presidencia, designado por el Secretario General de la Presidencia.

Artículo 5. Coordinación. La Comisión, estará a cargo de un Coordinador que será el designado por el Ministerio de Economía, bajo la dirección del Presidente de la República quien la presidirá.

Artículo 6. Plazo de la Comisión. El plazo de la Comisión será de dos años, a partir de la vigencia de este Acuerdo o en la fecha en la que finalicen los procesos de arbitraje correspondientes.

Artículo 7. Informes. La Comisión, entregará al Presidente de la República informes periódicos, de las actividades realizadas por la misma.

Artículo 8. Confidencialidad. Todas las actuaciones de la Comisión, por su naturaleza gozarán de confidencialidad.

Artículo 9. Cargos Ad-honorem. Los integrantes de la Comisión, desempeñarán sus cargos en forma ad-honorem.

Artículo 10. Presupuesto. El presupuesto de la Comisión, dependerá de la Presidencia de la República, para lo cual se realizarán las gestiones correspondientes ante el Ministerio de Finanzas Públicas.

Artículo 11. Vigencia. El presente Acuerdo Gubernativo empezará a regir al día siguiente de su publicación en el Diario de Centro América.

COMUNIQUESE,

Alvaro Colom

ALVARO COLOM CABALLEROS



RUBÉN MORALES MONROY
MINISTRO DE ECONOMÍA



Haroldo Rodas Mejías
Ministro de Relaciones Exteriores



Enrique Carlos Peláez Viqueo
Ministro de Energía y Minas



Rafael Ángel Salazar
Subsecretario General de la Presidencia de la República Encargado del Despacho

(E-363-2009)-13 mayo



MINISTERIO DE ECONOMÍA

Acuérdase emitir el siguiente: REGLAMENTO DE LA LEY PARA EL RECONOCIMIENTO DE LAS COMUNICACIONES Y FIRMAS ELECTRÓNICAS.

ACUERDO GUBERNATIVO NÚMERO 135-2009

Guatemala, 8 de mayo de 2009

El Presidente de la República

CONSIDERANDO:

Que la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto 47-2008 del Congreso de la República de Guatemala, tiene por objeto la promoción del comercio electrónico, la validación, fomento y estímulo de las operaciones efectuadas por medio de las nuevas tecnologías de la información y, especialmente, el otorgamiento de seguridad jurídica y técnica a las contrataciones, comunicaciones y firmas electrónicas.

CONSIDERANDO:

Que para aplicar los preceptos contenidos en la ley antes referida, es necesario contar con el instrumento legal que desarrolle los procedimientos para la utilización de medios electrónicos y permita al Registro de Prestadores de Servicios de Certificación, como autoridad administrativa responsable en esa materia, cumplir todas las funciones y atribuciones que le asigna la mencionada ley.

PORTANTO:

En el ejercicio de las funciones que le confiere el artículo 183, literal a) de la Constitución Política de la República de Guatemala y con fundamento en el artículo 59 de la Ley Para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto 47-2008 del Congreso de la República de Guatemala.

ACUERDA:

Emitir el siguiente:

REGLAMENTO DE LA LEY PARA EL RECONOCIMIENTO DE LAS COMUNICACIONES Y FIRMAS ELECTRONICAS

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto. El presente reglamento tiene por objeto desarrollar los preceptos normativos contenidos en la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto Número 47-2008 del Congreso de la República de Guatemala, y las funciones del Registro de Prestadores de Servicios de Certificación, como autoridad administrativa responsable del registro y autorización para operar de los prestadores de servicios de certificación.

Artículo 2. Definiciones. Son aplicables al presente reglamento las definiciones contenidas en el artículo 2 de la ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas y las siguientes:

- **Clave Privada:** valor o valores numéricos que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de una comunicación electrónica.
- **Clave Pública:** valor o valores numéricos que son utilizados para verificar que una firma digital fue generada con la clave privada del emisor.
- **Declaración de Prácticas de Certificación -DPC:** manifestación del prestador de servicios de certificación sobre las políticas, procedimientos y mecanismos que se obliga a cumplir en la prestación de sus servicios de certificación y homologación.
- **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.
- **Entidad Autorizadora:** el Registro de Prestadores de Servicios de Certificación adscrito al Ministerio de Economía -RPSC-.
- **Electrónico:** características de la tecnología que tiene capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares.
- **Ley:** cualquier referencia a la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.
- **Políticas de Certificados:** conjunto de reglas declaradas que indica la aplicabilidad de un certificado para una comunidad particular o clase de aplicación con requerimientos de seguridad comunes.
- **Repositorio:** sistema de información utilizado para almacenar y recuperar certificados y otra información relacionada con los mismos, al igual que de cualquier tipo de documento electrónico.

Artículo 3. Actos y contratos. Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, públicas o privadas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten por escrito, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando consten por escrito.

Lo dispuesto en el párrafo anterior no será aplicable a los actos y contratos otorgados o celebrados en los casos siguientes:

- a) Aquellos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico;
- b) Aquellos en que la ley requiera la concurrencia personal de alguna de las partes; y,
- c) Aquellos relativos al derecho de familia.

La firma electrónica, cualquiera sea su naturaleza, se tendrá como firma manuscrita para todos los efectos legales, sin perjuicio de lo establecido en el artículo siguiente.

Artículo 4. Calidad de Instrumento Público. Los documentos electrónicos que pudieran tener la calidad de instrumento público, deberán suscribirse mediante firma electrónica avanzada.

CAPÍTULO II

USO DE LAS FIRMAS ELECTRONICAS POR LOS ORGANISMOS DEL ESTADO

Artículo 5. Actos y contratos por parte del Estado. Los órganos del Estado podrán ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica. En consecuencia, serán válidos de la misma manera y producirán los mismos efectos que los expedidos por escrito y en soporte de papel.

Se exceptúan aquellas actuaciones para las cuales la legislación vigente exija una solemnidad que no sea susceptible de cumplirse mediante documento electrónico, o requiera la concurrencia personal de la autoridad o funcionario que deba intervenir en ellas.

Para los efectos del párrafo primero, los actos administrativos, formalizados por medio de documentos electrónicos y que consten en decretos o resoluciones, en acuerdos de órganos colegiados, así como la celebración de contratos, la emisión de cualquier otro documento que exprese la voluntad de un órgano o servicio público de la administración del Estado en ejercicio de sus potestades legales y, en general, todo documento que revista la naturaleza de instrumento público o aquellos que deban producir los efectos jurídicos de éstos, deberán suscribirse mediante firma electrónica avanzada.

Artículo 6. Relación con los organismos del Estado. Las personas podrán relacionarse con los organismos del Estado, a través de técnicas y medios electrónicos con firma electrónica, siempre que se ajusten al procedimiento descrito por la ley o el presente reglamento y que tales técnicas y medios sean compatibles con los que utilicen dichos organismos. En aquellos casos en que se haga necesaria la comprobación de su identidad, será necesario el empleo de firma electrónica avanzada. Los organismos del Estado podrán relacionarse por medios electrónicos con los particulares, cuando estos hayan consentido expresamente en esta forma de comunicación.

Los organismos del Estado deberán evitar, al hacer uso de firmas electrónicas, que se restrinja injustificadamente el acceso a las prestaciones o servicios que brinden y a la publicidad y transparencia que rijan sus actuaciones y, en general, que se cause discriminaciones arbitrarias.

Artículo 7. Contratación del Estado. Los organismos del Estado podrán contratar los servicios de certificación de firmas electrónicas con prestadores de servicios de certificación autorizados por el Registro de Prestadores de Servicios de Certificación, si ello resultare más conveniente, técnica o económicamente. Para el efecto, la estimación de dicha conveniencia estará basada en criterios de calidad de servicio y precio de éste.

Artículo 8. Documentos electrónicos utilizados por el Estado. Los organismos del Estado que utilicen documentos electrónicos deberán contar con un repositorio o archivo electrónico a los efectos de su archivo una vez que haya finalizado su tramitación. El repositorio será responsable del respectivo funcionario a cargo del archivo, sin perjuicio de la celebración de convenios de cooperación entre diferentes organismos o de la contratación de una empresa privada para que preste el servicio. El repositorio deberá garantizar que se respetan las normas sobre publicidad de los documentos contenidas en las leyes respectivas.

Así mismo, deberá garantizar la seguridad, integridad y disponibilidad de la información en él contenida. Para ello la información deberá ser respaldada en copias de seguridad, bajo las siguientes características:

- a) La información deberá ser respaldada con cada proceso de actualización de documentos;
- b) Mantener una copia de seguridad en el lugar de operación de los sistemas de información y otra en un centro de almacenamiento de datos electrónicos especializado. Este centro de almacenamiento de datos electrónicos, que puede ser propio o provisto por terceros, deberá cumplir con condiciones tales como un estricto control de acceso, un completo y detallado registro de entrada y salida de respaldos, resguardo de la humedad, temperatura adecuada, control del riesgo de incendio y otras; y,
- c) El esquema de respaldo deberá ser simple, basado en generación de copias acumulativas, con el objeto de mantener la historia de la información en el mínimo de versiones posibles.

La seguridad, integridad y disponibilidad del repositorio deberán estar caracterizadas por:

- a) Medidas de seguridad y barreras de protección, frente al acceso no autorizado de usuarios;
- b) Contar con monitoreo y alarmas que se activen cuando ocurra un evento no autorizado o fuera de programación, para el caso de eventuales fallos de las medidas de seguridad al acceso;
- c) La sustitución de la información, por la versión más reciente que se disponga, en el menor tiempo posible, en casos de alteración no programada de aquella; y,
- d) La existencia de un programa alternativo de acción que permita la restauración del servicio en el menor tiempo posible, en caso que el repositorio deje de operar por razones no programadas.

Artículo 9. Regulación. Cada organismo del Estado podrá regular la forma cómo se garantizará la publicidad, seguridad, integridad y eficacia en el uso de las firmas electrónicas, y las demás necesarias para la aplicación de las normas establecidas en la ley o el presente reglamento.

CAPÍTULO III

DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACION

Artículo 10. Prestadores autorizados. Son prestadores autorizados de servicios de certificación las personas jurídicas nacionales o extranjeras, públicas o privadas, domiciliadas en la República de Guatemala, que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que puedan prestar, de conformidad con la ley y el presente reglamento.

El cumplimiento de las normas técnicas fijadas para la aplicación del presente Reglamento es obligatorio para los prestadores autorizados de servicios de certificación.

Artículo 11. Actos Administrativos. Los actos administrativos que impliquen la modificación de normas técnicas para la prestación del servicio establecerán los plazos en los cuales un prestador autorizado de servicios de certificación deberá adecuarse a las mismas.

El incumplimiento en la adecuación a las nuevas normas técnicas será calificado como incumplimiento grave y facultará al Registro de Prestadores de Certificación a dejar sin efecto la autorización, conforme a la ley y el presente reglamento.

Artículo 12. Modificación de normas técnicas. De oficio, y con el objeto de fijar o modificar las normas técnicas establecidas por este reglamento o cualesquiera otros emanados del Ministerio de Economía, la Entidad Autorizadora podrá iniciar el procedimiento para la elaboración y fijación de normas técnicas, con el objeto de permitir el uso de diversas tecnologías y medios electrónicos, conforme a la ley y el presente reglamento.

Artículo 13. Obligaciones de los prestadores. Son obligaciones de los prestadores de servicios de certificación de firma electrónica, adicionales a las establecidas en la ley:

- a) Contar con reglas o declaración sobre Prácticas de Certificación que sean objetivas y no discriminatorias y comunicadas a los usuarios de manera sencilla y en idioma español. Estas deben declarar el cumplimiento de los requisitos señalados en el artículo 23 del presente reglamento, con excepción de la póliza de seguro que se acredita por medio de la presentación de la misma y deberán contener al menos:
- 1) Una introducción, que deberá contener un resumen de las prácticas de certificación de que se trate, mencionando tanto la entidad que suscribe el documento, como el tipo de usuarios a los que son aplicables;
 - 2) Consideraciones generales, debiendo contener información sobre obligaciones, responsabilidades, cumplimiento de auditorías, confidencialidad, y derechos de propiedad intelectual, con relación a todas las partes involucradas;
 - 3) Identificación y autenticación, debiendo describirse tanto los procesos de autenticación aplicados a los solicitantes de certificados, como los procesos para autenticar a los mismos cuando pidan suspensión o revocación de certificado;
 - 4) Requerimientos operacionales, debiendo contener información operacional para los procesos de solicitud de certificado, emisión de certificados, suspensión y revocación de certificados, procesos de auditoría de seguridad, almacenamiento de información relevante, cambio de datos de creación de firma electrónica, superación de situaciones críticas, casos de fuerza mayor y caso fortuito, y procedimiento de término del usuario del servicio de certificación;
 - 5) Controles de procedimiento, personal y físicos, debiendo describir los controles de seguridad no técnicos utilizados por el prestador de servicios de certificación para asegurar las funciones de generación de datos de creación de firma electrónica, autenticación de usuarios, emisión de certificados, suspensión y revocación de certificados, auditoría y almacenamiento de información relevante;
 - 6) Controles de seguridad técnica, debiendo señalar las medidas de seguridad adoptadas por el prestador de servicios de certificación para proteger los datos de creación de su propia firma electrónica;
 - 7) Perfiles de certificados y del registro de acceso público, debiendo especificar el formato del certificado y del registro de acceso público para todos los tipos ofrecidos como servicio; y,
 - 8) Especificaciones de administración de la política de certificación, debiendo señalar la forma en que la misma está contenida en la Práctica, los procedimientos para cambiar, publicar y notificar la política.
- b) Comunicar al Director Ejecutivo del Registro mediante comunicación electrónica suscrita con firma electrónica avanzada del representante legal del prestador de servicios de certificación del inicio de sus operaciones con el objeto de la verificación de la verificación final del certificado. Además de remitir a la Entidad Autorizadora una copia de cada tipo de Certificado generado.
- c) Mantener un registro de acceso público de todos los tipos de certificados emitidos, en el que se garantice la disponibilidad de la información contenida en él de manera regular y continua. A dicho registro se podrá acceder por medios electrónicos y en él deberán constar los certificados emitidos por el certificador, indicando si los mismos se encuentran vigentes, revocados, suspendidos, traspasados de otro prestador de servicios de certificación u homologados. Para mantener este registro, el prestador de servicios de certificación podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para ese efecto, y no podrá utilizarlos para otros fines. Dichos datos deberán ser conservados a lo menos durante diez años desde la emisión inicial de los certificados, cualquiera que sea el estado en que se encuentren los certificados. En caso el prestador de servicios de certificación cese en su actividad, deberá transferir dichos datos a un prestador de servicios de certificación, que deberá estar autorizado al que lo fuera, o a una empresa especializada en la custodia de datos electrónicos, por el tiempo para completar el plazo. Esta situación se deberá ver reflejada en el registro público de la Entidad Autorizadora. En el restante se aplicarán las disposiciones contenidas en la legislación vigente relacionadas con la protección de datos, protección a la vida privada y cualquier tema relacionado;
- d) En el caso de cesar en su actividad, los prestadores de servicios de certificación deberán comunicarlo previamente a cada uno de los titulares de firmas electrónicas certificadas por ellos, con antelación de al menos quince (15) días hábiles y señalando al titular que de no existir objeción a la transferencia de los certificados a otro prestador de servicios de certificación, dentro del plazo de quince (15) días hábiles contados desde la fecha de la comunicación, se entenderá que el usuario ha consentido en la transferencia de los mismos. En este caso, si el prestador es autorizado, deberá traspasar los certificados, necesariamente, a un certificador autorizado en la fecha en que el cese se produzca.
- En caso de existir oposición, dejarán sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia;
- e) Publicar en sus sitios de dominio electrónico las resoluciones de la Entidad Autorizadora que los afecten;
 - f) En el otorgamiento de certificados de firma electrónica avanzada, comprobar fehacientemente la identidad del solicitante, para lo cual el prestador requerirá previamente, ante sí o ante notario, la comparecencia personal y directa del solicitante o de su representante legal si se tratare de persona jurídica;
 - g) Pagar el arancel de la supervisión, el que será fijado anualmente por la Entidad Autorizadora y comprenderá el costo del peritaje y del sistema de autorización e inspección de los prestadores;
 - h) Solicitar la cancelación de su inscripción en el registro de prestadores de servicios de certificación llevado por la Entidad Autorizadora, con una antelación no inferior a veinte (20) días hábiles cuando vayan a cesar su actividad, y comunicarle el destino que vaya a dar a los datos de los certificados especificando, en su caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto. El cese de la actividad del prestador de servicios de certificación autorizado será registrado como nota de cancelación de la inscripción de la autorización por la Entidad Autorizadora en el registro a que se refiere este reglamento;

- i) En caso de cancelación de la inscripción en el registro de prestadores de servicios de certificación autorizados, los certificadores de servicios de certificación comunicarán inmediatamente esta circunstancia a cada uno de los usuarios y deberán, de la misma manera que respecto al cese de actividades, traspasar los datos de sus certificados a otro prestador, si el usuario no se opusiere;
- j) Indicar a la Entidad Autorizadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento de quiebra o que se encuentre en cesación de pagos o cualquier procedimiento similar;
- k) El prestador autorizado o su representante legal no debe revelar los datos de firma electrónica que correspondan a su propio certificado y, en todo caso, será responsable de su mala utilización; y,
- l) Cumplir con las demás obligaciones legales, especialmente las establecidas en la ley, el presente reglamento, la Ley de Protección al Consumidor y las situaciones relacionadas con la protección de datos y la vida privada.

Artículo 14. Cumplimiento por parte de los prestadores. El cumplimiento, por parte de los prestadores no autorizados de servicios de certificación de firma electrónica, de las obligaciones señaladas en las letras a), c), d) y l) del artículo anterior, será considerado por el juez como un antecedente para determinar si existió la debida diligencia, para los efectos previstos en el artículo siguiente.

Artículo 15. Responsabilidad de los prestadores. 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.

Artículo 16. Seguro de Responsabilidad Civil. Para los efectos de este artículo, los prestadores autorizados de servicios de certificación de firma electrónica deberán contratar y mantener un seguro de responsabilidad civil, que cubra los daños y perjuicios que ocasionen con motivo de su actividad, tanto por los certificados propios como por aquellos homologados en virtud de lo dispuesto en el párrafo final del artículo 18, y que deberá contener las siguientes estipulaciones mínimas:

- a) Una suma asegurada de al menos doscientos mil dólares de los Estados Unidos de América (\$200,000.00);
- b) La responsabilidad civil asegurada, que comprenderá la originada en hechos acontecidos durante la vigencia de la póliza, no obstante sea reclamada con posterioridad a ella;
- c) La responsabilidad civil por sus dependientes, representantes, apoderados y por cualquier persona que participe en la prestación de los servicios;
- d) La responsabilidad civil de toda otra persona por la cual el asegurado sea civilmente responsable en el ejercicio de su actividad de prestador de toda clase de servicios de certificación.

Los prestadores autorizados de servicios de certificación 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, hasta que concluya el mismo. Lo anterior deberá quedar consignado expresamente en la póliza del seguro.

Artículo 17. Evaluación de la responsabilidad del prestador. Al evaluarse la responsabilidad del prestador de servicios de certificación, respecto al no cumplimiento de los requisitos para prestar servicios para apoyar una firma electrónica que pueda utilizarse como firma con efectos jurídicos, deberán tomarse en cuenta, entre otras cosas, los siguientes factores:

- a) El costo de obtención del certificado;
- b) La naturaleza de la información que se certifique;
- c) La existencia de limitaciones de los fines para los que pueda utilizarse el certificado y el alcance de esas limitaciones;
- d) La existencia de declaraciones que limiten el alcance o la magnitud de la responsabilidad del prestador de servicios de certificación; y
- e) Toda conducta de la parte que confía en la firma que contribuya a la responsabilidad.

CAPITULO IV

DE LOS CERTIFICADOS DE FIRMA ELECTRÓNICA

Artículo 18. Certificado de firma electrónica. El certificado de firma electrónica es la certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de firma electrónica.

Los certificados de firma electrónica emitidos por un prestador de servicios de certificación autorizado, deberán contener adicionalmente a lo requerido en la ley, las siguientes menciones:

- a) Un código de identificación único del certificado y/o el número de serie del certificado;
- b) 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;
- c) 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
- d) Su plazo de vigencia.

Los atributos adicionales que los prestadores de servicios de certificación introduzcan con la finalidad de incorporar límites al uso del certificado, no deberán dificultar o impedir la lectura de las mencionadas en el presente artículo ni su reconocimiento por terceros.

Los prestadores de servicios de certificación autorizados en el país, podrán homologar certificados de firma electrónica emitidos por entidades no establecidas en Guatemala, bajo su responsabilidad y cumpliendo los requisitos fijados en la ley y el presente reglamento, o en virtud de convenio internacional ratificado por Guatemala y que se encuentre vigente. Para ello el prestador autorizado de servicios de certificación deberá demostrar a la Entidad Autorizadora que los certificados homologados por él han sido emitidos por un prestador de servicios de certificación no establecido en Guatemala que cumple con normas técnicas equivalentes a las establecidas en la ley y el presente reglamento para el desarrollo de la actividad.

Una vez practicada la homologación de un certificado o de un grupo de certificados de firma electrónica avanzada el prestador autorizado de servicios de certificación deberá, dentro del plazo de tres (3) días, comunicar tal situación a la Entidad Autorizadora y se deberá publicar, inmediatamente, en el registro de acceso público del prestador autorizado estipulado en la literal c) del artículo 13 de este reglamento. Las prácticas de homologación deberán estar declaradas en las Prácticas de Certificación.

Artículo 19. Datos de creación de firma. Los datos de creación de firma serán generados y entregados por el prestador de servicios de certificación en presencia física del titular.

Queda prohibido al prestador de servicios de certificación mantener copia de los datos de creación de firma electrónica una vez que éstos hayan sido entregados a su titular momento desde el cual éste comenzará a ser responsable de mantenerlos bajo su exclusivo control.

Artículo 20. Uso del certificado de firma electrónica. El certificado de firma electrónica podrá ser usado por su titular conforme a las operaciones que han sido autorizadas a realizar en las prácticas de certificación y las políticas del certificado del prestador de servicios de certificación con quien se ha 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 21. Suspensión del certificado. Procederá la suspensión de la vigencia del certificado cuando se verifique alguna de las siguientes circunstancias:

- a) Solicitud del titular del certificado; y,
- b) Decisión del prestador de servicios de certificación en virtud de razones técnicas.

El efecto de la suspensión del certificado es el cese temporal de los efectos jurídicos del mismo conforme a los usos que le son propios e impide el uso legítimo del mismo por parte del titular.

La suspensión del certificado terminará por cualquiera de las siguientes causas:

- a) Por la decisión del prestador de servicios de certificación de revocar el certificado, en los casos previstos en la Ley o el presente reglamento;
- b) Por la decisión del prestador de servicios de certificación de levantar la suspensión del certificado, una vez que cesen las causas técnicas que la originaron; y,
- c) Por la decisión del titular del certificado, cuando la suspensión haya sido solicitada por éste.

En todo caso el prestador debe señalar en sus políticas cual debe ser el plazo máximo de suspensión permitida para el certificado. Para el caso del inciso b) del presente artículo, una vez vencido el plazo el prestador deberá proporcionar, en forma gratuita, un reemplazo para no perjudicar al titular.

Artículo 22. Certificados de firma sin efecto por disposición legal. Los certificados de firma electrónica quedarán sin efecto, adicionalmente a lo establecido en la ley, en los siguientes casos:

1. Por extinción del plazo de vigencia del certificado, el cual no podrá exceder de tres (03) años contados desde la fecha de su emisión;
2. Por revocación del prestador, la que tendrá lugar en las siguientes circunstancias:

- a) A solicitud del titular del certificado;
- b) Por fallecimiento del titular o disolución de la persona jurídica que represente, en su caso;
- c) Por resolución judicial ejecutoriada;
- d) Cuando el titular del certificado al momento de solicitarlo no haya proporcionado los datos de la identidad personal u otras circunstancias objeto de certificación, en forma exacta y completa;
- e) Cuando el titular del certificado no haya custodiado adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que le proporcione el certificado;
- f) Cuando el titular del certificado no haya actualizado sus datos al cambiar estos;
- g) Por incumplimiento de las obligaciones del usuario establecidas en el artículo 30 del presente reglamento; y,
- h) Por las demás causas que convaliden al prestador de servicios de certificación con el titular del certificado por medio de la política de certificados.

El efecto de la revocación del certificado es el cese permanente de los efectos jurídicos de este conforme a los usos que le son propios e impide el uso legítimo del mismo.

La revocación de un certificado de firma electrónica podrá producirse de oficio o a petición de su titular por la concurrencia de algunas de las causales previstas en la ley o el presente reglamento.

La solicitud de suspensión o revocación, según corresponda, se podrá dirigir al prestador de servicios de certificación en cualquiera de las formas que prevean sus prácticas de certificación.

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

Tratándose de la suspensión por razones técnicas o revocación del certificado de firma electrónica por las causales de las letras d), e) o f) del presente numeral, dicha decisión deberá ser comunicada al titular con anterioridad a su puesta en práctica, indicando la causa que la provoca y el momento en que se hará efectiva.

3. Por cancelación de la autorización y de la inscripción del prestador en el registro de prestadores de servicios de certificación autorizados que señala el artículo 24, en razón de lo dispuesto en el artículo 25 ó del cese de la actividad del prestador, a menos que se verifique el traspaso de los datos de los certificados a otro prestador, conforme a lo dispuesto en las literales d) e) l) del artículo 13 del presente reglamento; y,

4. Por cese voluntario de la actividad del prestador no autorizado, a menos que se verifique el traspaso de los datos de los certificados a otro prestador, conforme a la literal d) del artículo 13 del presente reglamento.

La revocación de un certificado en las circunstancias previstas en la literal g) del numeral 2) del presente artículo, así como la suspensión cuando ocurriere por causas técnicas, será comunicada previamente por el prestador al titular del certificado, indicando la causa y el momento en que se hará efectiva la revocación o la suspensión. En cualquier caso, ni la revocación ni la suspensión privarán de valor a los certificados antes del momento exacto en que sean verificadas por el prestador.

El término de la vigencia del certificado será oponible a terceros desde el momento de la publicación de esta en el registro de acceso público que señala el artículo 13 de este Reglamento.

El término de vigencia de un certificado por alguna de las causales señaladas en el presente artículo será inoponible a terceros mientras no sea anotado en el registro de acceso público del prestador.

CAPITULO V

DE LA AUTORIZACIÓN E INSPECCIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Artículo 23. Autorización. La autorización es el 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 los recursos humanos necesarios para otorgar los certificados en los términos que se establecen en la ley y en el presente reglamento, permitiendo su inscripción en el registro que se señala en el artículo siguiente.

Para ser autorizado, el prestador de servicios de certificación deberá cumplir, sin perjuicio de lo establecido en la ley, con las siguientes condiciones:

- a) Demostrar la fiabilidad necesaria de sus servicios;
- b) Garantizar la existencia de un servicio seguro de consulta del registro de certificados emitidos;
- c) Emplear personal calificado para la prestación de los servicios ofrecidos y los procedimientos de seguridad y de gestión adecuados;
- d) Utilizar sistemas y productos confiables que garanticen la seguridad de sus procesos de certificación;

- e) Haber contratado un seguro apropiado en los términos que señala el artículo 18;
- f) Contar con la capacidad tecnológica necesaria para el desarrollo de la actividad de certificación; y,
- g) Cumplir con todas las regulaciones emitidas por el Registro.

El cumplimiento de estas condiciones será evaluado por la Entidad Autorizadora de conformidad con las normas técnicas aplicables a la prestación del servicio, durante el procedimiento de autorización.

Artículo 24. Proceso de autorización. El procedimiento de autorización se iniciará mediante solicitud ante la Entidad Autorizadora, a la que se deberá acompañar los antecedentes relativos a los requisitos del artículo 40 de ley, el artículo anterior (con excepción de la póliza de seguro) del presente reglamento, las regulaciones debidamente emitidas y el comprobante de pago de los costos de la autorización. La Entidad Autorizadora por medio de resolución fijará dentro del primer trimestre de cada año el arancel de los costos de la autorización y el arancel de supervisión. Los costos de autorización serán pagados por el prestador de servicios de certificación que solicita autorizarse, los que no serán restituidos en el evento que la autorización no sea concedida por incumplimiento de los requisitos y obligaciones legales y reglamentarias exigidas para el desarrollo de la actividad de certificación como autorizador. El arancel de supervisión comprenderá los costos correspondientes a las inspecciones, ordinarias y extraordinarias, y del sistema de autorización. El arancel deberá ser pagado por los prestadores autorizados de servicios de certificación dentro de los 90 días siguientes a la fecha de la resolución que los fija.

En la solicitud que presente el interesado deberá individualizarse debidamente y para ello señalará su denominación o razón social, su número de identificación tributaria, el nombre completo y número de identificación tributaria del Representante Legal, su sede social y dirección de correo electrónico, aceptando expresamente dicho medio electrónico como forma de comunicación.

Recibida la solicitud, la Entidad Autorizadora procederá a verificar la admisibilidad de la misma mediante la verificación de los antecedentes requeridos, dentro de cinco días hábiles. De ser inadmisibile la solicitud, dentro del plazo indicado se procederá a comunicar al interesado tal situación y que podrá completar los antecedentes dentro del plazo de quince (15) días hábiles, bajo apercibimiento de ser rechazada la solicitud. Admitida a trámite la solicitud, la Entidad Autorizadora procederá a un examen sobre el cumplimiento de los requisitos y obligaciones exigidas por la ley y el presente reglamento para obtener la autorización, certificando dentro del plazo de 90 días contados desde la fecha de la admisibilidad de la solicitud, prorrogables por una vez en igual período y por motivos fundados, que el interesado cumple los requisitos y obligaciones para ser autorizado y que dispone de un plazo de treinta (30) días para presentar la póliza de seguros que exige el artículo 16 de este reglamento, bajo apercibimiento de ser rechazada la solicitud.

En caso que la Entidad Autorizadora determine que el prestador de servicios de certificación no cumple con las normas técnicas fijadas para el desarrollo de la actividad, señalará si los incumplimientos son subsanables, y si no afectan el correcto funcionamiento del sistema ni los fines previstos en la ley. En caso que los incumplimientos no sean subsanables, la Entidad Autorizadora procederá a dictar una resolución en la que rechaza la solicitud de acreditación. Si los incumplimientos son subsanables y no afectan el correcto funcionamiento del sistema ni los fines previstos en la ley, la Entidad Autorizadora podrá autorizar al interesado, previa autorización de un plan de medidas correctivas. Si el interesado incumpliere el plazo de entrega del plan de medidas correctivas, o una vez aprobado este lo incumpliere, la entidad autorizadora quedará facultada para rechazar o cancelar la solicitud, según corresponda.

Una vez completados los requisitos exigidos, la Entidad Autorizadora procederá a autorizar al interesado en el plazo de veinte (20) días hábiles contados desde que, a petición del interesado, se certifique que la solicitud se encuentra en estado de resolverse. Si el interesado denunciare el incumplimiento de ese plazo ante la propia autoridad y ésta no se pronunciare dentro del mes siguiente, la solicitud se entenderá aceptada.

Durante todo el proceso de autorización, la Entidad Autorizadora podrá solicitar documentación adicional y/o realizar visitas a las instalaciones del interesado para verificar el cumplimiento de los requisitos señalados en el artículo 23 del presente reglamento; para el efecto, lo podrá hacer por intermedio de sus funcionarios o por expertos especialmente contratados para dichos fines. Los contratos que se suscriban con éstos últimos deberán incluir normas sobre probidad administrativa.

La acreditación del prestador de servicios de certificación producirá los siguientes efectos:

- a) La incorporación al registro público de prestadores de servicios de certificación autorizados que mantiene la Entidad Autorizadora;
- b) Habilitara al certificador a emitir certificados de firma electrónica avanzada;
- c) Someter al certificador a la inspección de la Entidad Autorizadora; y,
- d) Los demás que establecen la ley y este reglamento.

Durante la vigencia de su inscripción en el registro, el prestador autorizado deberá informar a la Entidad Autorizadora cualquier modificación de las condiciones que permitieron su autorización. El registro público de prestadores autorizados de servicios de certificación, deberá contener el número de la resolución que concede la autorización, la denominación o razón social del certificador, la sede social, el nombre de su representante legal, el número telefónico de la entidad, su sitio de dominio electrónico y correo electrónico así como la compañía de seguros con que ha contratado la póliza de seguros que exige la ley o el presente reglamento. El referido registro público deberá permitir su acceso por medios electrónicos, sin perjuicio de mantener el mismo en soporte de papel en la Entidad Autorizadora. Este Registro deberá ser actualizado permanentemente, manteniendo un acceso regular y continuo.

Artículo 25. Resolución de entidades autorizadas. Mediante resolución fundada de la Entidad Autorizadora se podrá dejar sin efecto la autorización y cancelar la inscripción en el registro público antes mencionado, por alguna de las siguientes causas:

- a) Solicitud del prestador de servicios de certificación autorizado ante la Entidad Autorizadora con una antelación de un mes a la fecha del término previsto por el prestador para que se haga efectiva, indicando el destino que dará a los certificados y a los datos de ellos. Para el efecto, deberá cumplir con lo dispuesto en el presente reglamento, y garantizar el pago del aviso que deberá ser publicado;
- b) Pérdida de las condiciones que sirvieron de fundamento a su autorización, la que será calificada por los funcionarios o peritos que la Entidad Autorizadora ocupe en la inspección a que se refiere el artículo 26 del presente reglamento; y,
- c) Incumplimiento grave o reiterado de las obligaciones que establece la ley y el presente reglamento.

En los casos de las literales b) y c), la resolución será adoptada de conformidad con lo que se estipula en el capítulo VIII del presente reglamento.

Los certificadores cuya inscripción haya sido cancelada, deberán comunicar inmediatamente este hecho a los titulares de firmas electrónicas certificadas por ellos. Sin perjuicio de ello, la Entidad Autorizadora publicará un aviso en un diario de mayor circulación dando cuenta de la cancelación, a costa del certificador, sin perjuicio de la publicación de la resolución en el registro público que señala el presente reglamento. A partir de la fecha de esta publicación, quedarán sin efecto los certificados, a menos que los datos de los titulares sean transferidos a otro certificador autorizado, en conformidad con lo dispuesto en la letra j) del artículo 13 de presente reglamento. Los perjuicios que puede causar la cancelación de la inscripción del certificador para los titulares de los certificados que se encontraban vigentes hasta la cancelación, serán de responsabilidad del prestador de servicios de certificación.

Artículo 26. Comprobación de cumplimiento de obligaciones. Con el fin de comprobar el cumplimiento de las obligaciones de los prestadores autorizados, la Entidad Autorizadora ejercerá la facultad inspectora sobre los mismos y podrá en cualquier momento, a tal efecto, requerir información y ordenar visitas a sus instalaciones mediante funcionarios o peritos especialmente contratados, de conformidad con el presente reglamento y las regulaciones que se emitan para el efecto.

La facultad inspectora comprende tanto inspección ordinaria como la extraordinaria. La inspección ordinaria consiste en la facultad de practicar como mínimo una visita anual a las instalaciones del prestador autorizado de servicios de certificación, como asimismo requerir, en forma semestral o como se indique en las regulaciones correspondientes, información sobre el desarrollo de la actividad. La inspección extraordinaria será practicada de oficio o por denuncia motivada sobre la prestación del servicio, ordenada por el director ejecutivo del Registro mediante resolución fundada.

Las inspecciones podrán ser practicadas por medio de funcionarios o peritos especialmente contratados y habilitados para estos fines, los que en el ejercicio de sus funciones podrán requerir al certificador información adicional a la proporcionada por él.

La información solicitada por la Entidad Autorizadora deberá ser proporcionada dentro del plazo de cinco (5) días, contado desde la fecha de la solicitud, sin perjuicio del otorgamiento de plazos especiales atendida la información requerida, bajo apercibimiento de imponerle las sanciones correspondientes.

Artículo 27. Confidencialidad. La Entidad Autorizadora, así como el personal que actúe bajo su dependencia o por cuenta de ella, deberá guardar la confidencialidad y custodia de los documentos y la información que le entreguen los prestadores de servicios de certificación autorizados o que hayan presentado solicitud para calificación y autorización.

Artículo 28. Recursos. Los recursos que perciba la Entidad Autorizadora por parte de los prestadores autorizados de servicios de certificación constituirán ingresos propios de dicha entidad y se incorporarán a su presupuesto.

CAPÍTULO VI

DERECHOS Y OBLIGACIONES DE LOS USUARIOS DE FIRMAS ELECTRÓNICAS

Artículo 29. Derechos. Los usuarios o titulares de firmas electrónicas tendrán los siguientes derechos:

- 1) A ser informado por el prestador de servicios de certificación, de las características generales de los procedimientos de creación y de verificación, así como de las reglas sobre prácticas de certificación, políticas de los certificados y las demás que éstos se comprometan a seguir en la prestación de los servicios que ofrece, previamente a que se empiece a efectuar;
- 2) A la confidencialidad en la información proporcionada a los prestadores de servicios de certificación. Para ello, éstos deberán emplear los elementos técnicos disponibles para brindar seguridad y privacidad a la información aportada, y los usuarios tendrán derecho a que se les informe, previamente al inicio de la prestación del servicio, de las características generales de dichos elementos;
- 3) A ser informado, antes de la emisión de un certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago, en su caso; de las condiciones preclaus para la utilización del certificado y de sus limitaciones de uso, de los procedimientos de reclamación y de resolución de conflictos previstos en las leyes o que se conviniere;
- 4) A que el prestador de servicios le proporcione la información sobre su sede social en Guatemala y sobre todos los medios a los que el usuario pueda acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;

- 5) A ser informado, de todo tipo de sanción que le sea impuesta al prestador de servicios de certificación por la entidad autorizadora. Para el efecto, el prestador deberá publicar en su registro de acceso público todas las sanciones que le sean impuestas dentro de un plazo de cinco (5) días hábiles de haber sido notificado;
- 6) A ser informado, al menos con dos meses de anticipación, por los prestadores de servicios de certificación, del cese de su actividad, con el fin de hacer valer su oposición al traspaso de los datos de sus certificados a otro certificador, en cuyo caso dichos certificados se extinguirán conforme al presente reglamento, o bien, para que tomen conocimiento de la extinción de los efectos de sus certificados, si no existiere posibilidad de traspaso a otro certificador;
- 7) A ser informado inmediatamente de la cancelación de la inscripción en el registro de prestadores autorizados, con el fin de hacer valer su oposición al traspaso de los datos de sus certificados a otro certificador, en cuyo caso dichos certificados se extinguirán de conformidad con el presente reglamento, o bien, para tomar conocimiento de la extinción de los efectos de sus certificados, si no existiere posibilidad de traspaso a otro certificador;
- 8) A traspasar sus datos a otro prestador de servicios de certificación;
- 9) A que el prestador no proporcione más servicios y de otra calidad que los que haya prestado, salvo autorización expresa del usuario;
- 10) A no recibir publicidad comercial de ningún tipo por intermedio del prestador, salvo autorización expresa del usuario;
- 11) A acceder, por medios electrónicos, al registro de prestadores autorizados que mantendrá la Entidad Autorizadora; y,
- 12) A ser indemnizado y hacer valer los seguros comprometidos, conforme al presente reglamento.

Los usuarios gozarán de estos derechos, sin perjuicio de lo que pueda disponer alguna otra ley vigente, y podrán, con la salvedad de lo señalado en el numeral 12) de este artículo, ejercerlos conforme al procedimiento establecido en la Ley de Protección al Consumidor, Decreto 8-2003. El derecho a ser indemnizado y hacer valer los seguros comprometidos se regirá por el derecho común.

Artículo 30. Obligaciones. Los usuarios de los certificados de firma electrónica 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 éstos vayan cambiando.

CAPÍTULO VII

DEL REGISTRO DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Artículo 31. Autoridad Superior. La autoridad superior del Registro es el Director Ejecutivo, quien tiene las funciones que le asigna este reglamento o la ley, y será nombrado por el Ministro de Economía. El Director Ejecutivo organizará al personal en la forma que resulte conveniente para el buen funcionamiento del Registro. Sin embargo, contemplará dentro de su estructura, como mínimo, las siguientes plazas:

- a) Secretaria Ejecutiva.
- b) Asesor Jurídico.
- c) Asesor Técnico.

Artículo 32. Director Ejecutivo. Le corresponde, entre otras, las siguientes funciones:

- a) Proponer al Ministro de Economía al personal que debe ser contratado o nombrado para dicho Registro, el cual estará a su cargo;
- b) Supervisar las operaciones diarias del Registro;
- c) Verificar todas las autorizaciones que correspondan;
- d) Firmar en forma física o electrónica los documentos que se generen por el Registro, cuando su intervención sea necesaria conforme a la ley, este reglamento o las disposiciones que el mismo Registro genere;
- e) Emitir los instructivos o guías de uso necesarios para complementar o facilitar las gestiones del Registro;
- f) Verificar que todas las inscripciones o autorizaciones se lleven a cabo de conforme a la ley, el presente reglamento y cualquier otra regulación vigente;
- g) Emitir acuerdos y demás disposiciones de orden interno;
- h) Designar al Sub-Director si fuere el caso o persona que deba sustituirlo cuando se ausente temporalmente del cargo; e,
- i) Cualquier otra función inherente al cargo de Director Ejecutivo, dentro de los límites de su competencia.

Artículo 33. Sub-Directores del Registro de Prestadores de Servicios de Certificación. De ser el caso, si o los sub-directores serán nombrados por el Ministro de Economía; asistirán al Director Ejecutivo en el ejercicio de su cargo; y el que sea designado sustituirá al Director Ejecutivo cuando éste se ausente temporalmente.

Artículo 34. Personal del Registro. El Registro de Prestadores de Servicios de Certificación contará con el personal necesario para su funcionamiento, el cual será contratado o nombrado por el Ministro de Economía a propuesta del Director Ejecutivo. Al personal del Registro le serán aplicables lo dispuesto en la literal c) del artículo 40 de la ley.

CAPÍTULO VIII

PROCEDIMIENTO PARA IMPOSICIÓN DE SANCIONES A LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Artículo 35. Responsabilidades de prestación de servicios. Las sanciones previstas en la ley se aplicarán sin perjuicio de las demás responsabilidades en que pueda incurrir el prestador de servicios de certificación, sus representantes legales o su personal contratado bajo cualquier forma.

Artículo 36. Sanciones. Se entenderá por sanciones, aquellas impuestas a los Prestadores de Servicios de Certificación, como consecuencia del incumplimiento de las obligaciones que les impone la ley, el presente reglamento o cualquier otra regulación pertinente, la cual podrá ser de carácter pecuniario y/o administrativo.

El Registro deberá llevar un archivo de las sanciones impuestas a los prestadores de servicios de certificación, habilitándolo para que sea de acceso público por cualquier medio escrito o electrónico.

Artículo 37. Amonestación. Se impondrá amonestación a los prestadores de servicios de certificación cuando a criterio del Registro incumplan alguna obligación de carácter administrativo. Toda amonestación deberá constar por escrito y el prestador de servicios de certificación deberá llevar un registro físico y electrónico a manera que cualquier interesado pueda verificarlo.

El máximo de amonestaciones que podrá imponerse a un prestador de servicios de certificación por los mismos motivos o circunstancias será de dos (2), luego de las cuales el Registro estará facultado para imponer por conducto del Ministerio de Economía cualquiera de las sanciones estipuladas en las literales b, c, d y e del artículo 50 de la ley atendiendo a la naturaleza y gravedad de la falta.

Artículo 38. Suspensión. El Registro sancionará con suspensión temporal de uno (1) hasta tres (3) meses en el ejercicio de sus funciones al prestador de servicios de certificación en los casos siguientes:

- a) Si omite determinar y hacer del conocimiento de los usuarios si los servicios que les ofrecen cumplen o no los requerimientos dispuestos en la ley, el reglamento y sus regulaciones;
- b) Si actúa en contravención de los procedimientos definidos y específicos para la emisión de un Certificado;
- c) No permite que se efectúe la consulta inmediata sobre la validez, suspensión o revocación de los certificados que emita;
- d) No informe, antes de la emisión de un certificado, a la persona que solicita sus servicios, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y, en su caso, de la forma en que garantiza su posible responsabilidad;
- e) Si cambia su sede social, objeto social o estatutos sin dar aviso a la entidad autorizadora según lo establecido en el presente Reglamento;
- f) Si omite remitir a la entidad Autorizadora una copia de cada tipo de certificado por el generado;
- g) Si omite el requisito que los datos de creación de firma sean generados y entregados por el prestador de servicios de certificación en presencia física del titular;
- h) Si omite proporcionar los medios de acceso al certificado que permitan a la Parte que Confía en el Certificado determinar su estado;
- i) No cuente con el seguro de responsabilidad civil vigente, en las condiciones establecidas en este reglamento;
- j) Provoque la nulidad de un acto jurídico por su negligencia, imprudencia o dolo, en la expedición de un Certificado; y,
- k) Omite notificar a la entidad autorizadora de cualquier cambio que pretenda efectuar respecto de las condiciones de operación con las que fue autorizada.

Artículo 39. Prohibición de la Prestación de Servicios. El Registro podrá prohibir al prestador de servicios de certificación la prestación directa o indirecta de los servicios que presta autorizados previamente por el Registro, de uno (01) a cinco (05) años en los casos siguientes:

- a) Que el prestador de servicios de certificación sea sancionado más de dos (02) veces por las conductas u omisiones a que se refiere el artículo anterior.
- b) No compruebe la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de un certificado, en los términos establecidos por la ley, el presente reglamento y las regulaciones pertinentes;
- c) Altere, modifique o destruya los certificados que emita sin que medie resolución de la Entidad Autorizadora o de autoridad judicial competente;
- d) Impida a la Entidad Autorizadora efectuar las auditorías a que se refiere la ley, el presente reglamento y las regulaciones pertinentes;
- e) Revela los datos de creación de firma electrónica que correspondan a su propio certificado; y,
- f) Difunde sin autorización la información que le ha sido confiada o realice cualquier otra conducta que vulnere la confidencialidad de la misma.

Artículo 40. Revocación Definitiva. El Registro revocará definitivamente la autorización para operar como prestador de servicios de certificación en los casos siguientes:

- a) Cuando sea sancionado más de dos (2) veces en los casos previstos en el artículo 40 del presente Reglamento; y,
- b) Proporcione documentación o información falsa para obtener la acreditación como Prestador de Servicios de Certificación.

Artículo 41. Trámite de las Sanciones. Las sanciones a que se refiere el artículo 50 de la ley, se tramitarán de la siguiente forma:

1. Si como resultado de la facultad que le confieren las literales b, c, e, y h del artículo 40 de la ley y el artículo 26 del presente reglamento, la Entidad Autorizadora determine que algún prestador de servicios de certificación ha incumplido en sus obligaciones y como consecuencia amerita la imposición de una sanción, notificará al prestador de servicios de certificación a imponer por cualquier medio que considere oportuno siempre que quede constancia de dicho acto, corriéndole audiencia por el plazo de cinco (05) días para que se pronuncie al respecto y puede aportar elementos que justifiquen el incumplimiento y la improcedencia de la sanción.
2. La Entidad Autorizadora con la contestación o no del prestador de servicios de certificación, deberá emitir resolución en la que determine la sanción a imponer, si considera que es necesaria la imposición de la sanción, enviará el expediente en el que consten las justificaciones para imponerla y la petición al Ministro de Economía para que imponga la sanción determinada según la naturaleza y gravedad de la falta. Si como consecuencia de los elementos aportados por el prestador de servicios de certificación se determina que no procede la imposición de sanción alguna la Entidad Autorizadora ordenará el archivo de la medida.
3. El Ministro de Economía deberá emitir la resolución sancionando al prestador de servicios de certificación según los requerimientos de la Entidad Autorizadora como consecuencia de las inspecciones o auditorías que haya efectuado dentro de los ocho (08) días siguientes de recibir la petición de la Entidad Autorizadora, fijándole plazo para que haga efectivo el monto de la sanción si ésta fuera de carácter pecuniario el cual no podrá exceder de 20 días, bajo apercibimiento que en caso de incumplimiento dicha multa se duplicará automáticamente y de no hacerla efectiva el Registro puede proceder a prohibir a prestar sus servicios hasta en un plazo máximo de cinco (5) años. El Ministerio de Economía notificará la resolución al prestador de servicios de certificación y posteriormente devolverá el expediente de la Sanción a la Entidad Autorizadora.
4. Si el prestador de servicios de certificación no está de acuerdo con la resolución emitida, podrá acogerse a los recursos idóneos que establece la Ley de lo Contencioso Administrativo.

CAPITULO IX

DISPOSICIONES FINALES

Artículo 42. Arancel. El Ministro de Economía emitirá el acuerdo ministerial que contenga el Arancel del Registro de Prestadores de Servicios de Certificación, para que este cuente con ingresos adecuados y suficientes para su funcionamiento y cumplir con las obligaciones que le imponen la ley y el presente reglamento.

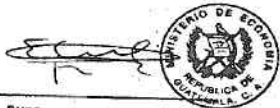
Artículo 43. Situaciones No Previstas. Cualquier situación no prevista en el presente reglamento, será resuelta por el Director Ejecutivo atendiendo al espíritu de las disposiciones de la ley y a la naturaleza del asunto de que se trate.

Artículo 44. Epígrafes. Los epígrafes relativos a la identificación del contenido de las normas contenidas en el presente reglamento y que preceden a cada artículo no tienen valor interpretativo.

Artículo 45. Vigencia. El presente reglamento entrará en vigencia ocho días después de su publicación en el Diario de Centro América.

COMUNIQUESE

ALVARO COLOM CABALLEROS



RUBEN MORALES MONROY
MINISTRO DE ECONOMIA

[Signature]
Lic. Roberto Samayoa Salazar
Subsecretario General
de la Presidencia de la República
Encargado del Despacho

(E-364-2009)-13-mayo



MINISTERIO DE GOBERNACIÓN

Acuérdase reconocer la personalidad jurídica y aprobar las bases constitutivas de la Iglesia Evangélica denominada IGLESIA EVANGÉLICA PENTECOSTÉS DEL DIOS OMNIPOTENTE.

ACUERDO MINISTERIAL NÚMERO 308-2009

Guatemala, 28 de abril de 2009

EL MINISTRO DE GOBERNACIÓN

CONSIDERANDO:

Que el Presidente de la Junta Directiva Provisional y Representante Legal de la Iglesia Evangélica denominada IGLESIA EVANGÉLICA PENTECOSTÉS DEL DIOS OMNIPOTENTE, con sede en el Municipio de Villa Nueva, Departamento de Guatemala, se presentó a este Ministerio solicitando el reconocimiento de la personalidad jurídica y aprobación de bases constitutivas.

CONSIDERANDO:

Que el ejercicio de todas las religiones en el país es libre, sin más límites que el orden público y el respeto debido a la dignidad de la jerarquía y a los feites de otros credos como lo establece la Constitución Política de la República de Guatemala; y, siendo que, el interesado cumplió con los requisitos que la ley exige para el reconocimiento respectivo, es procedente dictar el Acuerdo Ministerial correspondiente.

FOR TANTO:

En ejercicio de las funciones que le confieren los artículos 194 literales a) y f) de la Constitución Política de la República de Guatemala; 27 literal m) y 36 literal b) de la Ley del Organismo Ejecutivo, Decreto número 114-97 del Congreso de la República de Guatemala y con fundamento en el artículo 15 numeral 1º Decreto Ley número 106, Código Civil.

ACUERDA:

ARTÍCULO 1. Reconocer la personalidad jurídica y aprobar las bases constitutivas de la Iglesia Evangélica denominada IGLESIA EVANGÉLICA PENTECOSTÉS DEL DIOS OMNIPOTENTE, las cuales están contenidas en Escritura Pública número uno (1) de fecha dieciséis de enero del año dos mil nueve, autorizada en la ciudad de Guatemala, por el Notario Victor Hugo Santos Barahona.

ARTÍCULO 2. Para el funcionamiento de cualquier proyecto o programa de los no contemplados dentro de sus fines y cualquier otra modificación a sus bases constitutivas, la Iglesia Evangélica denominada IGLESIA EVANGÉLICA PENTECOSTÉS DEL DIOS OMNIPOTENTE, deberá contar con la autorización previa de la entidad Gubernativa correspondiente.

ARTÍCULO 3. El presente Acuerdo empieza a regir a partir del día siguiente de su publicación en el Diario de Centro América.

COMUNIQUESE.

[Signature]
Lic. María Concepción Gaitán
Segunda Viceministra
Ministerio de Gobernación

ISS178-21-13-mayo



MINISTERIO DE GOBERNACIÓN

Acuérdase reconocer la personalidad jurídica y aprobar las bases constitutivas de la Iglesia MISION CRISTIANA KABOD.

ACUERDO MINISTERIAL NÚMERO 312-2009

Guatemala, 28 de abril de 2009

EL MINISTRO DE GOBERNACIÓN

CONSIDERANDO:

Que la Presidente de la Junta Directiva Provisional y Representante Legal de la Iglesia MISION CRISTIANA KABOD, con sede en el departamento de Guatemala; se presentó a este Ministerio, solicitando el reconocimiento de la personalidad jurídica y aprobación de las bases constitutivas.

