UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS

"PROPUESTA DE ASPECTOS TÉCNICOS PARA LA NORMATIVA DE LEY QUE REGULE EL COMERCIO ELECTRÓNICO EN GUATEMALA"

ARNULFO NAPOLEÓN HERNÁNDEZ GONZÁLEZ

ASESORADO POR INGA. ELIZABETH DOMÍNGUEZ ALVARADO

GUATEMALA, OCTUBRE DE 2003

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

"PROPUESTA DE ASPECTOS TÉCNICOS PARA LA NORMATIVA DE LEY QUE REGULE EL COMERCIO ELECTRÓNICO EN GUATEMALA"

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA

POR

ARNULFO NAPOLEÓN HERNÁNDEZ GONZÁLEZ
ASESORADO POR: INGA. ELIZABETH DOMÍNGUEZ ALVARADO

AL CONFERÍRSELE EL TÍTULO DE
INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, OCTUBRE DE 2003

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Sydney Alexander Samuels Milson
VOCAL I	Ing. Murphy Olympo Paiz Recinos
VOCAL II	Lic. Amahán Sánchez Álvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Br. Keneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADOR	Inga. Claudia Liceth Rojas Morales
EXAMINADOR	Ing. Edgar Estuardo Santos Sutuj
EXAMINADOR	Inga. Virginia Victoria Tala Ayerdi
SECRETARIA	Ing. Pedro Antonio Aguilar Polanco

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:

"PROPUESTA DE ASPECTOS TÉCNICOS PARA LA NORMATIVA DE LEY QUE REGULE EL COMERCIO ELECTRÓNICO EN GUATEMALA"

Tema que me fuera asignado por la Coordinación de la Carrera de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería con fecha 30 de Julio de 2003.

Arnulfo Napoleón Hernández González

Guatemala, 30 de Julio de 2003

Ing. Carlos Alfredo Azurdia Morales
Coordinador de Privados y Trabajos de Graduación
Escuela de Ingeniería en Ciencias y Sistemas
Facultad de Ingeniería
Universidad San Carlos de Guatemala

Ing. Azurdia:

Por medio de la presente hago de su conocimiento que he tenido a bien revisar el trabajo de graduación de **ARNULFO NAPOLEÓN HERNANDEZ GONZÁLEZ**, titulado **"PROPUESTA DE ASPECTOS TÉCNICOS PARA LA NORMATIVA DE LEY QUE REGULE EL COMERCIO ELECTRÓNICO EN GUATEMALA"**, por lo cual me permito recomendar dicho trabajo final para la respectiva revisión por parte de la comisión de tesis de la escuela de Ciencias y Sistemas.

Sin otro particular, me suscribo atentamente,

Inga. Elizabeth Domínguez Alvarado
ASESOR

TESIS QUE DEDICO:

A:

Dios:	Por confiar en mí la virtud de la sabiduría y hacerme templo de su Espíritu Santo.
Virgen Santísima:	Por escuchar mis ruegos y acogerme bajo su manto bendito.
Mis padres:	Arnulfo Napoleón Hernández Soto y María Concepción González de Hernández, como un pequeño reconocimiento a sus múltiples esfuerzos para hacer de mi un ciudadano digno.
Mi hermana:	Walkiria Betzhabé Hernández González por su apoyo y motivación para seguir adelante.
Mis abuelos:	María Bersabé Soto Girón Por su apoyo y comprensión. Aniceto Pablo Hernández (+) María Eulogia de León de González (+) Alfredo González Hernández (+) Flores sobre sus tumbas.
Mi familia:	Por todo el apoyo brindado.
Mis amigas y amigos:	Por su apoyo, comprensión y paciencia. Deseándoles éxitos en su futuro.

AGRADECIMIENTOS:

A:

Ingeniera Elizabeth Domínguez Alvarado e ingenieria Claudia Liceth Rojas Morales por el apoyo y asesoría brindada desinteresadamente en la ejecución del presente trabajo.

Mis padres y hermana por el apoyo brindado durante el transcurso de mis estudios universitarios, aconsejándome y guiándome por el camino correcto para concluir con éxitos los mismos.

Mis compañeros y amigos, que en todo momento difícil de esta carrera han estado apoyándome y confiando en mi, han sido un aliciente para alcanzar el éxito que comparto con ellos.

Para muchas personas muy especiales que me han estado ayudando y apoyando en todo sentido para que mi vida se llene de triunfos y así poder llegar a una nueva meta, a la cual digo misión cumplida.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

GLOSARIO

Ataque	Realizar la violación de la seguridad de un sistema de información.
Autentificación	Es el concepto de verificar la identidad de una persona dentro de la red esta se puede realizar por varios métodos.
Autoridades de certificación (CA o *Certification Authorities*):	Son autoridades que vinculan la clave pública a la entidad registrada proporcionando un servicio de identificación. Una CA es a su vez identificada por otra CA creándose una jerarquía o árbol de confianza: dos entes pueden confiar mutuamente entre sí si existe una autoridad común que directa o transitivamente les avala.
B2B	Categoría de comercio electrónico conocida como empresa-empresa (*Business to Business*)
B2C	Categoría de comercio electrónico conocida como empresa-consumidor (*Business to Costumer)*
Business plans	Planes de negocios en lo que se refiere al comercio electrónico

Certificados digitales	Son registros electrónicos que atestiguan que una clave pública pertenece a determinado individuo o entidad. Permiten verificar que una clave pública pertenece a una determinada persona, evitando que alguien utilice una clave falsa para suplantar la personalidad de otro.
Comercio electrónico	Se refiere al proceso que permite al cliente comprar sin necesidad de ver el producto incluyendo la transacción económica asociada al proceso y a los servicios de asesoramiento, postventa y transporte.
Correo electrónico	Fue uno de los primeros usos de la Internet y todavía es el más popular. Permite a los utilizadores enviaren correspondencia entre ellos, sea en modo texto u otro formato digital.
Criptografía	Procedimiento que permite asegurar la transmisión de informaciones privadas por las redes públicas desordenándolas matemáticamente, de manera que sea ilegible para cualquier tercero, excepto para persona que posea la llave capaz de reordenar la información que va en el mensaje.
EDI	Intercambio electrónico de datos (*Electronic Data Interchange*)
E-commerce	Comercio electrónico, su traducción al español.

E-entrepreneurs Son conocidos con este nombre los que poseen un espíritu emprendedor en el ámbito del comercio electrónico.

E-mail Abreviatura de correo electrónico.

Firma digital Es un bloque de caracteres que acompaña a un documento (o fichero) acreditando quién es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad).

Firmware Rutinas de *software* almacenadas en memoria de sólo lectura (ROM). A diferencia de la memoria de acceso aleatorio (RAM), la memoria de sólo lectura permanece intacta incluso cuando no existe un suministro de energía eléctrica.

Frecuencia Ritmo de recurrencia o rapidez de repetición de un fenómeno periódico. Representa el número de ciclos completos por unidad de tiempo para una magnitud periódica tal como corriente alterna, las ondas acústicas u ondas de radio.

Hacker **(Pirata)** Es la persona que goza de un conocimiento profundo sobre el funcionamiento de sistemas de computadoras y con ello alcanza un conocimiento del funcionamiento interno de un sistema, de una computadora o de una red de computadoras, a la cual el accede sin autorización alguna, es decir es un intruso.

Hardware Se refiere a los componentes materiales de un sistema informático. La función de estos componentes suele dividirse en tres categorías principales: entrada, salida y almacenamiento.

Internet Internet es el nombre de la red mundial de computadoras, que se encuentran en constante conexión. Consiste en un conjunto de redes informáticas interconectadas, en las cuales los usuarios pueden intercambiar información y recursos. Inicialmente fue desarrollada en los años 60 en Estados Unidos, con el objetivo de ser utilizada en investigación científica y fines militares y de seguridad, permitiendo que en caso de ataque nuclear las computadoras pudiesen seguir comunicando. En los años 90 se dio su apertura al público en general, y esta masificación correspondió a una revolución de las comunicaciones humanas, siendo actualmente el mayor medio de contacto entre personas.

IP La transmisión de datos en Internet es hecha a través de *Information Packets* o paquetes de información. Cuando un mensaje es enviado se divide en paquetes de información que son transmitidos separadamente para el destinatario. Al llegar, los paquetes son de nuevo reunidos y la información es presentada.

Market places Lugares donde se pueden realizar transacciones comerciales para el comercio electrónico.

PIN	Número de identificación personal (*Personal Indentify Number).*
Protocolo	Descripción formal de formatos de mensajes y de reglas que dos computadoras deben seguir para intercambiar dichos mensajes.
Red	Colección interconectada de computadoras o dispositivos, no importando el medio por el cual estén conectadas.
Red de Telecomunicaciones	Consiste en una infraestructura física a través de la cual se transporta la información desde la fuente hasta el destino, y con base en esa infraestructura se ofrecen a los usuarios los diversos servicios de telecomunicaciones.
Router **Enrutador**	Dispositivo que distribuye el tráfico entre redes. La decisión sobre a dónde enviar se realiza a partir de información de nivel de red y tablas de direccionamiento.
RSA	Algoritmo de criptografía asimétrica (Rivest-Shamir-Aldemar).
SIT	Súper Intendencia de Telecomunicaciones, en Guatemala la dirección del sitio es: http://www.sit.gob.gt

Sociedad de la Información	Es el conjunto de dispositivos, medios, etc. donde se encuentra la información, ya sea que se maneja en Internet, como en las diferentes computadoras. Se refiere a todo lo que interviene en el manejo, envío y manipulación de la misma, desde los medios físicos hasta los medios lógicos.
Software	Programas de computadoras. Son las instrucciones responsables de que el *hardware* (la máquina) realice su tarea.
TCP/IP	Sus siglas significan *Transmisión control protocol / internet protocol* o protocolo de control de transmisión / protocolo de Internet. Es un protocolo de transmisión que asigna a cada máquina que se conecta un número especifico, llamado “número IP”. El protocolo TCP/IP sirve para establecer una comunicación entre dos puntos remotos mediante el envío de información en paquetes.
TAN	Numero de autentificación de transacción (*Transaction Authentic Number)*

Transmisión Análoga	La forma más simple de la transmisión de la voz. Las primeras redes de teléfonos móviles han sido analógicas. Son menos seguras y sufren interferencias cuando la señal es débil.
Transmisión Digital	Cuando la información está codificada en un formato digital antes de que sea transmitida. Las redes digitales ofrecen mejor calidad de voz, transmisiones seguras, varios servicios suplementarios que le permiten aún el envió de datos.
WEB	Ver www.
WWW (*World Wide Web*)	Es una red basada en el protocolo HTTP y el lenguaje HTML, diseñados con el propósito de crear una red donde se pueda en una forma sencilla, presentar información tanto tipo texto, como incrustación de multimedia.

RESUMEN

La problemática de la seguridad en la red pública en Guatemala es muy similar a la que se vive en la mayoría de países a nivel mundial. Nos vemos expuestos a los diferentes tipos de ataques, así como los delitos y fraudes en la misma. Debido a esto, existen varios servicios y mecanismos de seguridad, tal es el caso de la criptografía y sus técnicas, también las diferentes formas de autentificación, todo esto para resguardar la seguridad de los sistemas de información.

La interconexión de redes de telecomunicaciones es la encargada del transporte de la información. Ofrece una serie de servicios, entre ellos la interconexión con otras redes para ampliar la cobertura territorial, de allí la importancia de la misma en el comercio electrónico, porque rompe las fronteras para este nuevo proceso comercial, formando una revolución en la tecnología y en la economía de los países, existiendo varías categorías de negocios y ofreciendo ventajas comparadas a las del comercio normal.

La falta de confianza de las personas en la utilización del comercio electrónico, por el temor a un fraude, conlleva a la formulación de una propuesta de aspectos técnicos para generar una normativa de ley que regule el mismo; en la cual se le de un valor jurídico a los documentos digitales, así como a los contratos digitales por medio de una normativa de firma digital. De esta manera se protegerá tanto al consumidor como al prestador del servicio.

OBJETIVOS

- **General**

  Presentar una propuesta de los aspectos técnicos que permitan realizar una normativa de ley, por medio de la cual se regule el comercio electrónico mediante una firma digital en Guatemala, para que se le de seguridad al cliente de la transacción que está realizando y con esto se evite que ocurra algún fraude que le afecte al mismo.

- **Específicos**

1. Dar a conocer la problemática de seguridad y los riesgos que se corre al utilizar las redes públicas en Guatemala.

2. Establecer por medio de la criptografía como operan los productos comerciales, cuales son sus ventajas y sus problemas, para que a un nivel más técnico se comprendan algunos algoritmos que permitan utilizar redes virtuales

3. Presentar posibles soluciones a partir de los métodos de seguridad para evitar ataques.

4. Promover el conocimiento de la criptografía, para entender la estructura de los certificados y firmas digitales los cuales en su mayoría, se encuentran asociados a la infraestructura de claves públicas (PKI por sus siglas en inglés).

5. Conocer que son los comercios virtuales así como la clasificación de los mismos, la importancia que tiene para el país el crecimiento de los mismos.

6. Proponer que se elabore una legislación para el desarrollo completo del comercio electrónico, como caso práctico una ley de firma digital para Guatemala.

INTRODUCCIÓN

En los últimos años el comercio electrónico en Guatemala ha tomado un mayor auge, debido a que en la actualidad la mayoría de la población en nuestro país poseen computadoras personales las cuales conectadas a Internet les da la opción de realizar una compra, un pago, etc., por lo cual, se ven en la necesidad de que sus transacciones sean seguras y exista alguna ley que regule el comercio electrónico en el país, ya que éste brinda una excelente oportunidad para avanzar en su integración económica con las naciones del resto del mundo.

El problema de no tener una red pública segura en nuestro país, trae como consecuencia y con justificada razón, la desconfianza de la gente de utilizar esta nueva forma de comercialización de productos, debido a los fraudes a que nos vemos expuestos día con día.

Los servicios y mecanismos de seguridad, así como la criptografía, son los medios por los cuales hacemos de la red pública una red más segura; con esta última, se puede generar una técnica conocida como clave pública, la cual nos lleva a desarrollar la firma digital, la cual nos traerá una ventaja a la hora de realizar transacciones porque la información viajará enmascarada por este método, aunque sea interceptado por terceros no podrán conocer cuál es el mensaje oculto.

El desarrollo del comercio electrónico ha sido vertiginoso debido a las grandes ventajas que representa con respecto al comercio tradicional; sin embargo, presentará obstáculos difíciles de superar, si no se resuelven ciertos aspectos técnicos y de índole legal.

La ausencia de una legislación nacional respecto de la firma digital, y las exigencias legales de utilización de soporte papel con firma manuscrita, impiden y dificultan el desarrollo de nuevas y modernas aplicaciones informáticas que permitan mejorar la productividad y reducir los costos de las organizaciones.

Con esta normativa de ley los beneficiados serán todos los clientes de los comercios electrónicos de Guatemala, pues tendrán algún respaldo legal para poder defenderse en caso de que sufran algún fraude. También se verán beneficiados los prestadores de este servicio, debido a que al verse respaldados legalmente, más clientes harán uso de estas aplicaciones y se tendrá un crecimiento en las mismas, lo cual conlleva a brindarle a nuestro país una mejor oportunidad de crecimiento económico.

1. PROBLEMÁTICA DE SEGURIDAD EN REDES PÚBLICAS EN GUATEMALA

1.1 ¿A qué se debe la problemática de seguridad?

La problemática de seguridad en la red pública en Guatemala se genera a partir de: ¿El por qué de la creación de redes en Guatemala?

Las redes nacieron a partir de las necesidades que tenía la sociedad informática de compartir recursos y así hacer que todo el software, el hardware y la esencia en muchas de las empresas: los datos, estén disponibles en cualquier momento para los usuarios que estén conectados a la red.

Los términos de seguridad y privacidad son definitivamente opuestos a la distribución y al compartir recursos que son algunos de los principales objetivos de las redes; desde allí nos podemos dar cuenta en donde empieza el problema de la seguridad.

La red pública Internet fue diseñada para ser sencilla y cómoda, pero no para ser segura. El hecho de que no existan fronteras en Internet representa ciertos riesgos. El mayor peligro para el usuario es que otro usuario vigile el tráfico de información a través de una computadora personal y pueda apropiarse de información sensible y realizar transacciones comerciales en su provecho.

1.2 Ataques y vulnerabilidades

En el lenguaje informático, se denomina *amenaza* a la violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo) que podría efectuar una persona, máquina, suceso o idea, dada una oportunidad. Un ataque no es más que la realización de una amenaza.

1.2.1 Tipos de ataques

Los métodos de ataque están divididos en categorías generales que pueden estar relacionadas entre sí, ya que el uso de un método en una categoría permite el uso de otros métodos en otras. Por ejemplo: después de averiguar una clave, un intruso realiza un ingreso como usuario legítimo para navegar entre los archivos y explotar vulnerabilidades del sistema.

1.2.1.1 Interrupción

Es un ataque contra un recurso del sistema que es destruido o deshabilitado temporalmente. Por ejemplo, destruir un disco duro, cortar una línea de comunicación o deshabilitar un sistema de consulta.

1.2.1.2 Intercepción

Este es un ataque de una entidad que consigue acceso a un recurso no autorizado. Dicha entidad podría ser una persona, un programa o una computadora.

Ejemplos de este tipo de ataque son interceptar una línea para obtener información y copiar ilegalmente archivos o programas que circulen por la red, o bien la lectura de las cabeceras de mensajes para descubrir la identidad de uno o más de los usuarios involucrados en una comunicación que es interceptada ilegalmente.

1.2.1.3 Modificación

Este es un ataque de una entidad no autorizada que consigue accesar a un recurso y es capaz de modificarlo. Ejemplos de este ataque es el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

1.2.1.4 Fabricación

Este es un ataque de una entidad no autorizada que añade mensajes, archivos u otros objetos extraños en el sistema. Ejemplos de este ataque son insertar mensajes no deseados en una red o añadir registros a un archivo.

1.3 Delitos en la red

Un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena.

Se podría definir el delito informático como toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, que se realiza en el entorno informático y está sancionado con una pena, la cual será determinada según la ley correspondiente.

Otra definición que se le puede dar al delito informático sería: actitud ilícita en que se tienen a las computadoras como instrumento o fin para realizar conductas típicas, antijurídicas y culpables de cualquier comportamiento criminal.

Actualmente en muchos países, incluyendo Guatemala se ha podido contemplar el enorme impacto que han tenido las nuevas tecnologías y los grandes beneficios que éstas, sobretodo a través de Internet, han traído consigo. Pero también ha conocido los enormes riesgos que estas innovaciones conllevan sobretodo en forma de lo que se ha venido calificando como delitos en la red. Ante el reconocimiento de la falta de seguridad en Internet, no se duda en defender que los beneficios que ofrece como nueva tecnología son mayores que sus consecuencias negativas.

1.3.1 Sabotaje informático

El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección. Básicamente, se puede diferenciar dos grupos de casos: por un lado, las conductas dirigidas a causar destrozos físicos y, por el otro, los métodos dirigidos a causar daños lógicos.

1.3.2 Delitos en el comercio electrónico

Otro de los ámbitos que se ha visto ampliamente afectado por los delitos en Internet y la falta de garantías de seguridad es el comercio electrónico. El Comercio Electrónico es la adquisición de un bien o el uso de un servicio que utiliza los medios electrónicos tanto para su adquisición como para su pago. Los consumidores desconfían de este tipo de comercio debido a la inseguridad de sus transacciones con un notable miedo a las posibilidades de fraude.

Los fraudes consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizados con el objeto de obtener ganancias indebidas. Los distintos métodos para realizar estas conductas se deducen fácilmente, de la forma de trabajo de un sistema informático: en primer lugar, es posible alterar datos, omitir ingresar datos verdaderos o introducir datos falsos, en una computadora.

En segundo lugar, es posible interferir en el correcto procesamiento de la información, alterando el programa o secuencia lógica con el que trabaja la computadora. Esta modalidad puede ser cometida tanto al modificar los programas originales, como al adicionar al sistema programas especiales que introduce el autor.

Debido a esto difícilmente se podrán realizar previsiones si no se actúa, en primer lugar, sobre las leyes actuales que gobiernan las transacciones comerciales, caracterizadas por su falta de adecuación al fenómeno de las transacciones electrónicas y que, por tanto, obstaculizan claramente el desarrollo del comercio electrónico e incrementan, más si cabe, el pánico de los usuarios hacia la posibilidad de realizar operaciones a través de Internet.

Para disminuir y erradicar con los delitos y la falta de seguridad que afectan al comercio electrónico son importantes los esfuerzos gubernamentales como las iniciativas privadas. En este plano, debe quedar clara la necesidad de establecer una concienciación que son necesarios los servicios de firmas especializadas en la prevención de fraudes en la red.

Un ejemplo claro según Yahoo Noticias, en 1994 uno de los fraudes y estafas que se han dado en la red, es el siguiente: Un empleado del Citibank, tenía acceso a las terminales de computación de la Institución bancaria. Aprovechando esta circunstancia utilizó, en varias oportunidades, las terminales de los cajeros, cuando ellos se retiraban, para transferir, a través del sistema informático, fondos de distintas cuentas a su cuenta personal. Posteriormente, retiró el dinero en otra de las sucursales del banco.

1.3.3 Delitos informáticos contra la privacidad

Estos son un grupo de conductas que de alguna manera pueden afectar la esfera de privacidad del ciudadano mediante la acumulación, archivo y divulgación indebida de datos contenidos en los mismos.

Esta tipificación se refiere a quién, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de terceros, datos reservados de carácter personal o familiar de otro que se hallen registrados en archivos o soportes informáticos, electrónicos, o cualquier otro tipo de archivo o registro público o privado.

2. ASPÉCTOS TÉCNICOS DE SEGURIDAD EN REDES PÚBLICAS

El objetivo de la seguridad en una computadora es preservar los recursos de esta, contra usos y abusos no autorizados, así como proteger los datos que presentan y codifican la información de daños, revelaciones y modificaciones accidentales o deliberadas.

La seguridad en la red donde se tienen computadoras conectadas y comunicándose entre sí, es proteger los datos que representan y codifican la información durante su transmisión en las redes.

2.1 Servicios de seguridad según la arquitectura de seguridad OSI

La arquitectura de seguridad OSI proporciona una descripción general de los servicios y mecanismos relacionados con la seguridad, y discute sus interrelaciones. Muestra también las correspondencias entre la arquitectura de seguridad y la arquitectura estándar, y discute su situación apropiada dentro del modelo OSI.

La arquitectura de seguridad OSI diferencia cinco clases de servicios de seguridad y cada uno de ellos se subdivide en otras subclases: autentificación, control de acceso, confidencialidad de datos, integridad de datos, y no rechazo.

2.1.1 Servicio de autentificación

Estos servicios son utilizados para proporcionar autentificación en el proceso de comunicación entre dos entidades parejas, o para la autentificación del origen de los datos.

2.1.1.1 Servicio de autentificación de entidades parejas

El servicio de autentificación de entidades parejas sirve para proporcionar la capacidad de verificar que la entidad pareja de una asociación es quien dice ser. En concreto, el servicio de autentificación de entidades parejas permite asegurarse de que una determinada entidad no está intentando realizar una réplica no autorizada de una asociación anterior. Este servicio se realiza típicamente durante la fase de establecimiento de la conexión o, en ocasiones, durante la fase de transferencia de datos.

2.1.1.2 Servicio de autentificación del origen de los datos

El servicio de autentificación del origen de los datos permite reclamar el origen de las fuentes de los datos recibidos. Sin embargo, el servicio de autentificación del origen de los datos no proporciona protección contra la duplicación o la modificación de unidades de datos. En este caso, debe utilizarse conjuntamente un servicio de integridad de datos. Este servicio se realiza generalmente durante la fase de transferencia de datos.

2.1.2 Servicios de control de acceso

Los servicios de control de acceso sirven para proteger los recursos del sistema contra su utilización no autorizada. Estos servicios están estrechamente relacionados con los servicios de autentificación: un usuario o proceso que pretenda ocupar el lugar de otro usuario se deberá autentificar antes de que un servicio de control de acceso pueda obtener acceso efectivo a un recurso del sistema.

2.1.3 Servicios de confidencialidad de datos

Los servicios de confidencialidad de datos protegen los datos de revelaciones no autorizadas.

2.1.3.1 Servicios de confidencialidad orientados a conexión y no orientados a la conexión

Los servicios de confidencialidad orientados a la conexión proporcionan confidencialidad a todos los datos transmitidos durante una conexión.

Los servicios de confidencialidad no orientados a la conexión proporcionan confidencialidad a unas unidades simples de estructuras de datos que no son transmitidos en una conexión.

2.1.3.2 Servicios de confidencialidad de campo selectivo

Los servicios de confidencialidad de campo selectivo proporcionan confidencialidad de campos específicos de los datos en una estructura definida con anterioridad, durante una conexión o para una unidad de datos.

2.1.3.3 Servicios de confidencialidad de flujo de tráfico

Los servicios de confidencialidad de flujo de tráfico proporcionan protección de información que de otra forma podría resultar comprometida u obtenida indirectamente mediante un análisis del tráfico.

2.1.4 Servicios de integridad de datos

Los servicios de integridad de datos protegen los datos de modificaciones de entidades no autorizadas para realizar dichos cambios.

2.1.4.1 Servicios de integridad orientados a conexión

Los servicios de integridad de datos orientados a conexión con recuperación proporcionan integridad a los datos durante una conexión. Si es posible, permite la recuperación de fallos de integridad.

Los servicios de integridad orientados a conexión sin recuperación proporcionan integridad a los datos durante una conexión. No se recuperan los fallos de integridad.

Los servicios de integridad de campo seleccionado orientados a conexión proporcionan integridad de campos específicos de una estructura durante la conexión

2.1.4.2 Servicios de integridad no orientados a conexión

Los servicios de integridad no orientados a conexión proporcionan integridad a una unidad de datos.

Los servicios de integridad de campo seleccionado no orientado a la conexión proporcionan integridad de campos específicos de una estructura dentro de las unidades de datos.

2.1.5 Servicios de no rechazo

Los servicios de no rechazo proporcionan cierta protección contra el remitente de un mensaje o acción que niega serlo, o contra el receptor de un mensaje que niega haberlo recibido. Por esta razón se distinguen dos tipos de esta clase de servicios, los cuales son los servicios de no rechazo con prueba de origen y con prueba de destino.

2.1.5.1 Servicios de no rechazo con prueba de origen y destino

Los servicios de no rechazo con prueba de origen sirven para proporcionar el receptor de un mensaje con prueba de origen.

Los servicios de no rechazo con prueba de destino sirven para proporcionar el remitente de un mensaje con prueba de destino.

Este tipo de servicio de no rechazo se están haciendo cada vez más importante en el contexto de intercambio electrónico de datos (EDI – *Electronic Data Interchange*) y comercio electrónico en Internet.

2.2 Mecanismos de seguridad OSI

2.2.1 Mecanismos de seguridad específicos

2.2.1.1 Cifrado

El cifrado se utiliza para proteger la confidencialidad de las unidades de datos y la información de flujo de tráfico, o para dar soporte o complementar otros mecanismos de seguridad.

2.2.1.2 Mecanismo de firma digital

Los mecanismos de firma digital se utilizan para proporcionar una analogía electrónica a la firma manuscrita en los documentos electrónicos. De forma similar a la manuscrita, las firmas digitales no deben ser falsificables, los receptores deben ser capaces de verificarlas, y el firmante no debe poder rechazarlas posteriormente.

2.2.1.3 Mecanismo de control de acceso

Los mecanismos de control de acceso son las identidades autentificadas de los principales, información sobre dichos principales o capacidades de determinar y reforzar los derechos de acceso. Si un principal intenta utilizar un recurso no autorizado o un recurso autorizado con un mecanismo impropio de acceso, la función de control de acceso rechazará el intento y podrá además, informar del incidente con el propósito de generar una alarma y guardarla como parte de los informes de auditoría sobre seguridad.

2.2.1.4 Mecanismo de integridad de datos

Los mecanismos de integridad de datos protegen la integridad bien de unidades de datos y de campos de la misma, bien de secuencias de unidades de datos y campos dentro de dichas secuencias. Nótese que, en general, los mecanismos de integridad de datos no protegen contra ataques tipo réplica.

La protección de la integridad de una secuencia de unidades de datos y de campos dentro de la misma requiere habitualmente algún tipo de ordenación explícita, como numeración en secuencia, marcado temporal o encadenamiento criptográfico.

2.2.1.5 Mecanismo de intercambio de autentificación

Los mecanismos de intercambio de autentificación se utilizan para verificar la supuesta identidad de los principales. Se dice que un mecanismo de intercambio de autentificación es fuerte si se basa en el uso de técnicas criptográficas para proteger los mensajes que se van a intercambiar.

2.2.1.6 Mecanismo de relleno de tráfico

Los mecanismos de relleno de tráfico se utilizan para la protección contra ataques de análisis de tráfico. El término relleno del tráfico se refiere a la generación de ejercicios de comunicación espurios, unidades de datos espurias, y de datos espurios dentro de dichas unidades.

El objetivo es no revelar si los datos que se están transmitiendo representan y codifican realmente la información. En consecuencia, los mecanismos de relleno de tráfico sólo serán efectivos si son protegidos por un servicio de confidencialidad de datos.

2.2.1.7 Mecanismo de control de encaminamiento

Los mecanismos de control de encaminamiento se pueden utilizar para selección dinámica o preestablecida de rutas específicas para la transmisión de los datos. Los sistemas de comunicaciones que detectan de forma persistente ataques activos o pasivos pueden indicar al proveedor de servicios de red que desean establecer una conexión por una ruta diferente. Similarmente, el transporte de datos de cierto nivel de seguridad puede estar prohibido por la política de seguridad para ciertas redes, servidores de reenvío o enlaces.

2.2.1.8 Mecanismo de certificación

Los mecanismos de certificación se pueden emplear para asegurarse de ciertas propiedades de los datos que se comunican entre dos o más entidades, como su integridad, origen, tiempo o destino. La certificación la realiza una tercera entidad de confianza, que es la que da testimonio de la autenticidad.

2.2.2 Mecanismos de seguridad generalizados

Los mecanismos de seguridad generalizados no específicos de un servicio en particular, y en algunos casos pueden ser contemplados también como aspectos de la gestión de la seguridad. La importancia de estos mecanismos está en general relacionada directamente con el nivel de seguridad requerido.

2.2.2.1 Funcionalidad de confianza

El concepto general de funcionalidad de confianza se puede utilizar para extender de otros mecanismos de seguridad o para establecer su efectividad. Cualquier tipo de funcionalidad que proporcione directamente mecanismos de seguridad o el acceso a los mismos deben ser de confianza.

2.2.2.2 Etiquetas de seguridad

Los recursos del sistema pueden tener asociadas etiquetas de seguridad (por ejemplo, para indicar niveles de sensibilidad). A menudo es necesario que los datos en tránsito lleven la etiqueta de seguridad apropiada. Un nivel de seguridad puede implicar datos adicionales que se asocian a los datos transmitidos o pueden ser implícitos (por ejemplo, por el uso de una clave específica para cifrar los datos o por el contexto de los datos, como su fuente o ruta).

2.2.2.3 Detección de eventos

La detección de eventos relevante para la seguridad se utiliza para detectar violaciones aparentes de la seguridad.

2.2.2.4 Rastreo de auditoria de seguridad

La auditoría de seguridad es la revisión y examen independiente de los registros y las actividades del sistema para probar la operatividad de los controles, asegurar el cumplimiento de las políticas y procedimientos operacionales establecidos y recomendar los cambios adecuados en el control, política y procedimientos. En consecuencia, el rastreo de auditoría de seguridad se refiere a los datos que se adquieren y que potencialmente facilitan las auditorías sobre seguridad.

2.2.2.5 Recuperación de seguridad

Las recuperaciones de seguridad tratan con solicitudes de mecanismos como gestores de eventos y funciones de gestión, y realizan acciones de recuperación resultado de la aplicación de una serie de reglas.

2.3 Criptografía

Del antiguo Egipto a la era digital, los mensajes cifrados han jugado un papel destacado en la Historia. Arma de militares, diplomáticos y espías, son la mejor defensa de las comunicaciones y datos que viajan por Internet.

La criptografía (del griego *kryptos*, *escondido*, y *graphein*, *escribir*), es el arte de enmascarar los mensajes con signos convencionales, que sólo cobran sentido a la luz de una clave secreta, nació con la escritura. Su rastro se encuentra ya en las tablas cuneiformes, y los papiros demuestran que los primeros egipcios, hebreos, babilonios y asirios conocieron y aplicaron sus inescrutables técnicas, que alcanzan hoy su máxima expresión gracias al desarrollo de los sistemas informáticos y de las redes mundiales de comunicación.

2.3.1 Técnicas criptográficas

Existen varios tipos clásicos de criptografía, pero los métodos clásicos distan mucho de ser infalibles. En algunos casos, basta hacer un simple cálculo para desentrañar los mensajes ocultos. Si se confronta la frecuencia habitual de las letras en el lenguaje común con la de los signos del criptograma, puede resultar relativamente sencillo descifrarlo.

2.3.1.1 Funciones de hash unidireccional

Las funciones unidireccionales son de suma importancia en cristología. Hablando en términos informales, una función unidireccional es sencilla de calcular pero difícil de invertir. Hablando en términos formales, una función f: A $\rightarrow$ B es una función unidireccional si f(x) es fácil de calcular para todo, si x $\in$ A pero que, dado y $\in$ f(a) = B es computacionalmente irrealizable encontrar un x $\in$ A tal que f(x) = y.

Obviamente es necesario tener un dominio lo suficientemente grande como para evitar la posibilidad de una búsqueda exhaustiva, pero esa condición no es suficiente para asegurar que una función es unidireccional. Además de la condición anterior, es computacionalmente posible encontrar dos valores distintos x_1, $x_2 \in A$ tales que $f(x_1) = f(x_2)$, se dice que f es una función de hash resistente a las colisiones.

2.3.1.2 Criptografía con clave secreta

En la criptografía con clave secreta, las entidades en comunicación establecen y comparten una clave secreta, que se utiliza posteriormente para cifrar y descifrar los mensajes. Por ello, la criptografía con clave secreta se denomina también criptografía simétrica.

La criptografía con clave secreta se ha utilizado desde hace miles de años en sus diversas formas.

Las versiones modernas toman generalmente la forma de algoritmos, que son ejecutados por el hardware, firmware o incluso el software de los sistemas computarizados. La mayor parte de los sistemas de cifrado, con clave secreta se basan en operaciones que se pueden realizar de forma muy eficiente en las computadoras.

En teoría, es posible descifrar un sistema con clave secreta seguro sin tener conocimientos profundos sobre matemáticas ni criptografía. Combinando una serie de transformaciones más o menos complejas, como transposiciones y permutaciones, se puede crear un sistema que parezca extremadamente difícil de analizar incluso frente a un enemigo poderoso.

2.3.1.3 Criptografía con clave pública

La existencia de funciones unidireccionales con puertas traseras condujo a la invención de la criptografía con clave pública. Desde un punto de vista práctico, un criptosistema con clave pública es un criptosistema en el que cada usuario posee una pareja de claves relacionadas matemáticamente. Una de ellas es una clave pública, que puede ser publicada sin dañar la seguridad del sistema, y la otra es una clave privada, que se suponen que nunca deja de estar en poder de su dueño. Tanto la clave privada como la pública son imposibles de tener conociendo la otra.

La aplicación de la criptografía de clave pública requiere un entorno de autentificación que oculte las claves públicas y las entidades de los usuarios. Un certificado de clave pública es una prueba certificada de testimonio obligatorio que realiza una tercera entidad de confianza, denominada autoridad de certificación. El uso de una autoridad de certificación libera a los usuarios de las responsabilidades de verificar directamente la corrección de las claves públicas de los otros usuarios.

En teoría, la criptografía con clave pública puede ser más conveniente que la criptografía con clave secreta ya que evita que las dos entidades que desean autentificarse tengan que compartir la misma clave secreta. Por tanto, no se requiere un sistema de distribuciones tan complicado. Además la criptografía con clave pública que el sistema de autentificación esté bajo control directo del usuario del sistema. Esto es especialmente útil, para el control de acceso ya que la información secreta de autentificación no se distribuye por el sistema.

Los sistemas de firma digital son la analogía en términos computacionales de la firma manuscrita, y se utiliza de la misma forma que ésta para los documentos electrónicos.

Las firmas digitales no deben ser falsificables, los receptores deben ser capaces de verificarlas y los firmantes no deben poder rechazarlas posteriormente. Sin embargo, una importante diferencia entre la firma manuscrita y la electrónica es el hecho de que la firma digital no debe ser constante, y debe ser función del documento al que acompaña. Si no se hiciera así, la firma, debido a su naturaleza electrónica, podría ser cortada y pegada posteriormente en cualquier otro documento y se podría alterar un documento firmado electrónicamente.

Los mensajes firmados se envían directamente de los firmantes a los receptores. En general, un esquema de firma digital consta de:

- Un algoritmo de generación de claves que selecciona aleatoriamente una pareja de claves públicas.
- Un algoritmo de firma que toma un mensaje de entrada y una clave privada y genera como salida la firma digital del mensaje.
- Un algoritmo de verificación de firma que toma como entrada una firma digital y una clave pública, y que genera como salida un bit de información que indica si la firma es consistente con algún mensaje válido para la clave privada correspondiente a la clave pública.

2.3.2 Autentificación

En general, se entiende por autentificación la verificación de la supuesta identidad de un principal. La autentificación tiene como resultado la autenticidad, lo que quiere decir que el principal que verifica (verificador) puede estar seguro de que el principal verificado (solicitante) es quien es o quien dice ser.

Es práctica común dividir las técnicas utilizadas para la autentificación en tres categorías, dependiendo en que se basan.

- Algo que el solicitante sabe (prueba por conocimiento).
- Algo que el solicitante posee (prueba de posesión).
- Algunas características biométricas del solicitante (prueba por prioridad).

Como ejemplos de la primera categoría se encuentran los números de identificación personal (PIN), y los números de autentificación de transacción (TAN); en la segunda categoría se mencionan las claves, las tarjetas de identificación y otros dispositivos físicos o elementos personales. Históricamente, las primeras características biométricas utilizadas para la autentificación fueron las huellas dactilares. Hoy en día es posible utilizar otras características, por ejemplo: imágenes faciales, de la retina y los patrones de voz.

2.3.2.1 Autentificación basada en contraseña

En la mayoría de las redes de computadoras, la protección de los recursos se consigue protegiendo con contraseñas el acceso a los sistemas. Los usuarios seleccionan sus contraseñas y las transmiten de forma clara y no protegida. Este sistema presenta varios problemas, a continuación algunos de ellos:

- Los usuarios tienden a seleccionar contraseñas que no se distribuyen aleatoriamente. Se trata de un problema bien conocido y no necesariamente relacionado con las redes de computadoras.
- No es conveniente que un usuario que posee varias cuentas en sistemas diferentes tenga que recordar una contraseña diferente para cada una de ellas e introducirla cada vez que cambia de sistema.
- La transmisión de la propia contraseña está expuesta a escuchas pasivas y a posteriores ataques de réplica.

Debido principalmente al último problema, la autentificación basada en contraseñas no es adecuada para ser utilizada en redes de computadoras. Las contraseñas que se envían por redes son fáciles de interceptar por lo tanto se pueden suplantar a sus propietarios.

2.3.2.2 Autentificación basada en direcciones

La autentificación basada en direcciones no se basa en el envío de contraseñas por la red, sino que supone que la identidad de la fuente se puede conocer a partir de la dirección de red del que envía los paquetes.

La idea básica es que cada sistema almacene la información que especifique las cuentas de los otros sistemas que pueden tener acceso a sus recursos.

Por ejemplo en UNIX, cada sistema tiene un archivo denominado */etc/hosts.equiv* que contiene una lista con los nombres de los sistemas permitidos. Los usuarios con el mismo nombre en el sistema local y en el sistema remoto pueden utilizar las herramientas de Berkeley desde uno de los sistemas permitidos, sin necesidad de suministrar una contraseña.

Dependiendo del entorno, la autentificación basada en direcciones puede ser más o menos segura que el envío de contraseñas. En todo caso, es más conveniente, y por tanto es el mecanismo de autentificación utilizado en la mayoría de las redes hoy en día.

2.3.2.3 Autentificación criptografía

La idea básica de la autentificación criptográfica es que el solicitante A pruebe su identidad al verificador B realizando una operación criptográfica sobre una cantidad que ambos conocen o que B suministra. La operación criptográfica realizada por A se basa en una clave criptográfica, que puede ser una clave secreta o una clave privada de un criptosistema con clave pública.

En general, la autentificación criptográfica puede hacerse más segura que la autentificación basada en contraseña o en direcciones. Además, existen nuevas técnicas basadas en prueba de conocimiento cero que pueden proporcionar mecanismos de autentificación todavía más poderosos.

Esas técnicas requieren un cálculo matemático intensivo, pero presentan características atractivas para la autentificación. En primer lugar, las pruebas de conocimiento cero, permiten que el solicitante pruebe que conoce el secreto de identificación correcto sin transferir realmente al verificador ningún conocimiento sobre ese secreto. En segundo lugar, algunos esquemas de conocimiento cero propuestos hasta el momento requieren que la verificación de los mensajes de autentificación de cualquier solicitante necesite la misma información pública que evita en conjunto, problemas de distribución de claves.

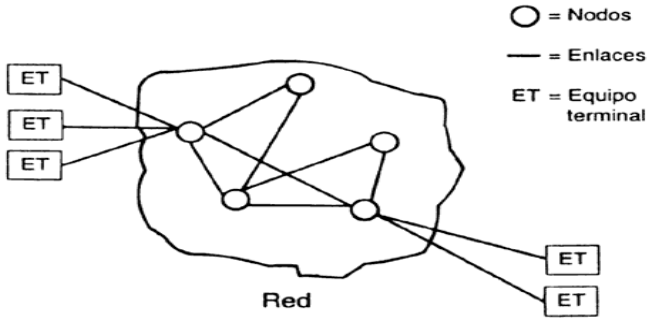
A pesar de la aparente simplicidad de los principios básicos de diseño de los protocolos de autentificación, el diseño de protocolos realistas es notoriamente difícil, y varios de los protocolos diseñados han mostrado, el problema de seguridad sustancial o sutil. Últimamente, los esfuerzos de investigación se han dirigido hacia la provisión de las herramientas necesarias para el desarrollo de protocolos de autentificación y de distribución de claves con garantía formal de seguridad.

3. INTERCONEXIÓN DE REDES DE TELECOMUNICACIONES

Consiste en una infraestructura física a través de la cual se transporta la información desde la fuente hasta el destino, y con base en esa infraestructura se ofrecen a los usuarios los diversos servicios de telecomunicaciones. En lo sucesivo, se denominará red de telecomunicaciones a la infraestructura encargada del transporte de la información. Para recibir un servicio de telecomunicaciones, un usuario utiliza un equipo terminal a través del cual obtiene entrada a la red por medio de un canal de acceso.

Cada servicio de telecomunicaciones tiene distintas características, puede utilizar diferentes redes de transporte y por tanto, el usuario requiere de distintos equipos terminales. Por ejemplo, para tener acceso a la red telefónica, el equipo terminal requerido consiste en un aparato telefónico; para recibir el servicio de telefonía celular, el equipo terminal consiste en teléfonos portátiles con receptor y transmisor de radio, etcétera.

Figura 1. Red y equipo terminal



3.1 Conceptos de interconexión de redes de telecomunicaciones

3.1.1 Definiciones técnicas y jurídicas

A continuación se presentan algunas definiciones tanto técnicas como jurídicas relativas a un marco regulador común de las redes y los servicios de comunicaciones electrónicas.

Acceso: la puesta a disposición de otra empresa, en condiciones definidas y sobre una base exclusiva o no exclusiva, de recursos o servicios con fines de prestación de servicios de comunicaciones electrónicas. Este término abarca, entre otros aspectos, los siguientes: el acceso a elementos de redes y recursos asociados y a servicios que pueden requerir la conexión de equipos, por medios alámbricos o inalámbricos; el acceso a infraestructuras físicas, como edificios, conductos y mástiles; el acceso a sistemas informáticos, incluidos los sistemas de apoyo operativos; el acceso a la traducción de números o a sistemas con una funcionalidad equivalente; el acceso a redes móviles, el acceso a sistemas de acceso condicional para servicios de televisión digital. La interconexión constituye un tipo particular de acceso entre operadores de redes públicas.

Interconexión: la conexión física y lógica de las redes públicas de comunicaciones electrónicas utilizadas por una misma empresa o por otra distinta, de manera que los usuarios de una empresa puedan comunicarse con los usuarios de la misma empresa o de otra distinta, o acceder a los servicios prestados por otra empresa. Los servicios podrán ser prestados por las partes involucradas o por terceros que tengan acceso a la red.

Operador: la empresa que proporciona, explota o controla una red de comunicaciones electrónicas disponible al público o un recurso asociado, como puede ser un sistema de acceso condicional, que le permite limitar o impedir el acceso de los prestadores de servicios a los usuarios finales o la libre elección de servicios por parte de dichos usuarios.

Servicio de televisión digital de formato ancho: el servicio de televisión constituido total o parcialmente de programas producidos y editados para su presentación en formato ancho completo mediante expansión agigantada. La relación de dimensiones 16:9 constituye el formato de referencia para los servicios de televisión de este tipo.

Usuario final: el usuario que no proporciona redes o servicios de comunicaciones electrónicas disponibles al público.

3.1.2 ¿Por qué es importante la competencia en la interconexión de redes?

El sector de las comunicaciones electrónicas se caracteriza por las estrechas relaciones de interdependencia que se establecen entre los agentes del mercado. Por un lado, las redes deben estar directamente o indirectamente interconectadas para que los usuarios puedan comunicarse y efectuar transacciones. Por otro, los prestadores de servicios de comunicaciones o de radiodifusión necesitan tener acceso a las infraestructuras de las redes para poder llegar hasta sus clientes. A su vez, el propietario u operador de las infraestructuras de comunicaciones se encuentra en una posición de fundamental importancia, como prestador de servicios a los usuarios.

Lo anterior, se aplica a todo tipo de redes de comunicaciones que presten servicios de comunicaciones electrónicas disponibles al público, independientemente de que se utilicen para la transmisión de voz, fax, datos o imágenes, como son las redes de telecomunicaciones fijas y móviles, las redes de televisión por cable, las redes utilizadas para radiodifusión terrenal, las redes satelitales y las redes que usan el protocolo Internet (IP). Motivo por el cual se debe de proporcionar un marco favorable a la competencia, que fomente las infraestructuras de redes competidoras y la interoperatividad de los servicios prestados a través de dichas infraestructuras, y garantizar que las situaciones de monopolio que puedan producirse en el mercado sean bloqueadas, para que no impidan la aparición y desarrollo de servicios innovadores y beneficiosos para los consumidores y usuarios.

Debido a la importancia que esto conlleva se ha creado normativa de acceso e interconexión a las redes, incluidas las redes de banda ancha, esta tiene una gran incidencia en los métodos de funcionamiento de todas las empresas del sector y, por consiguiente, en la futura dinámica competitiva del mercado.

Los servicios de comunicaciones —fijos y móviles— de la próxima generación se basarán cada vez más en plataformas de distribución y redes de transporte que utilizarán el protocolo Internet (IP) para el suministro de servicios. Este nuevo entorno de banda ancha será radicalmente distinto del mercado actual, centrado en la voz y caracterizado por las tecnologías de banda estrecha.

Tomando en cuenta el ritmo actual de transformación de los mercados y las tecnologías, no sería conveniente tratar sobre las previsiones de la evolución del mercado sino en el fomento de la competencia.

3.2 Aspectos relevantes de la interconexión

La interconexión de redes comerciales de telecomunicaciones es libremente negociada entre las partes, salvo lo estipulado en la Ley General de Telecomunicaciones con relación a los recursos esenciales.

3.2.1 Aspectos básicos y recursos esenciales en la interconexión

Algunos de los aspectos básicos que cubre el objetivo de la interconexión de redes, son considerados como recursos esenciales para prestar un servicio de este tipo:

- Logrando el objetivo del servicio universal, de manera que el servicio de telecomunicaciones llegue a todos los lugares geográficos y a todas las personas.
- Terminación en la red de una de las partes, de telecomunicaciones originadas en cualquier otra red comercial.
- Transferencia de Telecomunicaciones originadas en la red de una de las partes a cualquier otra red comercial de telecomunicaciones seleccionada por el usuario final implícita o explícitamente.

Todo operador de redes comerciales de telecomunicaciones deberá proporcionar acceso a recursos esenciales a cualquier operador que lo solicite mediante el pago correspondiente.

Todo lo relativo a interconexión y acceso a recursos esenciales está normado en la Ley General de Telecomunicaciones.

3.2.2 Servicios de interconexión

Los servicios que se generan por medio de la interconexión de redes se pueden catalogar en dos tipos: servicios generales y servicios al público. Los primeros son servicios que por lo general se le ofrecen a los proveedores que prestan un servicio al público, por lo general los servicios generales son los parámetros por medio de los cuales se pueden generar servicios específicos de una aplicación la cual estará al servicio del público.

3.2.2.1 Servicios generales

Algunos servicios generales son los que se presentan a continuación, hay que recordar que estos son los parámetros para los servicios al público:

Tipo de red: Se hablará únicamente de servicios ofrecidos al público en general, que utilizan como infraestructura redes públicas de telecomunicaciones, basadas fundamentalmente en transmisiones de radio o en señales guiadas por medio de conductores eléctricos u ópticos.

Cobertura: La extensión del área geográfica que cubre una red es de particular interés en la comparación, ya que los servicios no pueden ser ofrecidos fuera de dicha área geográfica. La cobertura puede ser caracterizada como local, regional o nacional.

Interconexión: A pesar de que la cobertura de una red puede ser local o regional, si está interconectada con otras redes de mayor cobertura se amplía de manera automática el área geográfica cubierta por la red.

También es importante y consecuencia de este atributo el hecho de poder tener acceso a servicios prestados por otras redes interconectadas a la red a la que el usuario tiene acceso.

Direccionalidad: En una comunicación un usuario puede tener un papel pasivo o uno activo. Se ha incluido este rubro en el análisis, caracterizándolo por medio de U = unidireccional (receptor pasivo) o B = bidireccional (el receptor tiene un papel activo y también puede transmitir).

Punto-multipunto: El criterio acerca de los destinos posibles para un servicio se relaciona con varios de los aspectos anteriores, pero es de gran importancia por sí mismo. Se han considerado dos opciones: P-P (punto a punto), en la cual existe un solo transmisor y un solo receptor, y P-MP (punto a multipunto), donde hay un solo transmisor pero una cantidad distinta de uno (posiblemente ilimitada) de receptores.

Tipo de información: Se ha mencionado frecuentemente que la información que se transmite puede ser digital (D) o analógica (A), lo cual define algunos aspectos del alcance de un servicio; éste es otro criterio que se considera digno de mención. Cabe recordar que si se trata de información tipo digital se estaría en posibilidad de tener los beneficios de las comunicaciones digitales, tales como la criptografía digital, la corrección de errores, la compresión del ancho de banda y el procesamiento por medio de microprocesadores de alta velocidad.

Privacía: Normalmente cuando se hace uso de un servicio de telecomunicaciones se desea tener la certeza de que sólo aquellos usuarios a quienes está destinada la información la reciben, y de que ningún intruso puede tener acceso al servicio sin tener autorización para ello.

3.2.2.2 Servicios al público

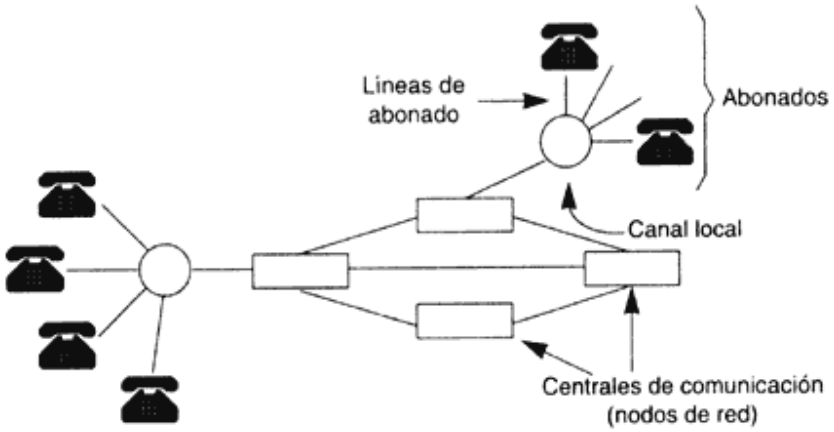
Antes de describir algunos de estos servicios, cabe mencionar que día a día aparecen nuevos servicios al público que los usuarios pueden utilizar para resolver problemas nuevos, o bien para resolver problemas viejos de maneras novedosas. A continuación se presentan un par de estos servicios

La red telefónica: Es sin duda alguna, la más compleja, la de mayor cobertura geográfica, la que mayor número de usuarios tiene, y ocasionalmente se ha afirmado que es el sistema más complejo de que dispone la humanidad. Permite establecer una llamada entre dos usuarios en cualquier parte del planeta de manera distribuida, automática, prácticamente instantánea.

Una llamada iniciada por el usuario origen llega a la red por medio de un canal de muy baja capacidad, el canal de acceso, dedicado precisamente a ese usuario denominado línea de abonado. En un extremo de la línea de abonado se encuentra el aparato terminal del usuario (teléfono o fax) y el otro está conectado al primer nodo de la red, que en este caso se llama central local.

La función de una central consiste en identificar en el número seleccionado la central a la cual está conectado el usuario destino y enrutar la llamada hacia dicha central con el objeto de que ésta le indique al usuario destino que tiene una llamada por medio de una señal de timbre. Al identificar la ubicación del destino, reserva una trayectoria entre ambos usuarios para poder iniciar la conversación. La trayectoria o ruta no siempre es la misma en llamadas consecutivas, ya que ésta depende de la disponibilidad instantánea de canales entre las distintas centrales.

Figura 2. Arquitectura de una red telefónica



Radiodifusión de señales: Dentro de estos servicios existen dos clases: los bidireccionales y los unidireccionales. En el conjunto de los primeros se describirá la operación de la telefonía celular. Como servicio representativo de la segunda clase se analizará la radiolocalización de personas.

La radiotelefonía celular surgió como un avance importante de la radiotelefonía tradicional. En esta última, los conceptos de la red son muy similares a los de la red telefónica pública, con la excepción de que el acceso a la red por parte del usuario es por medio de un canal de radio, con sus equipos terminales correspondientes. En el servicio tradicional de radiotelefonía se cuenta con una sola estación base, es decir, una estación que realiza funciones de transmisión y de repetición. En las transmisiones se utilizan potencias extremadamente grandes, logrando así una gran zona de cobertura. Sin embargo, si durante una conversación un usuario se sale de la zona de cobertura, la conversación se interrumpe ya que este sistema no tiene capacidad de conmutación. Cada usuario tiene asignado un canal de radio con una frecuencia fija para acceder la red, lo cual hace ineficiente el uso del espectro radioeléctrico, ya que, si uno de los usuarios con canales asignados en algún momento no lo utiliza, ese o esos canales estarían desocupados.

Los servicios bidireccionales que han sido descritos tienen la característica común de que, a pesar de tratarse de comunicación por radio (es decir, usando transmisiones basadas en difusión de señales), los equipos terminales de los usuarios son direccionables. Es decir, únicamente responden cuando en la información que reciben identifican su propia dirección electrónica.

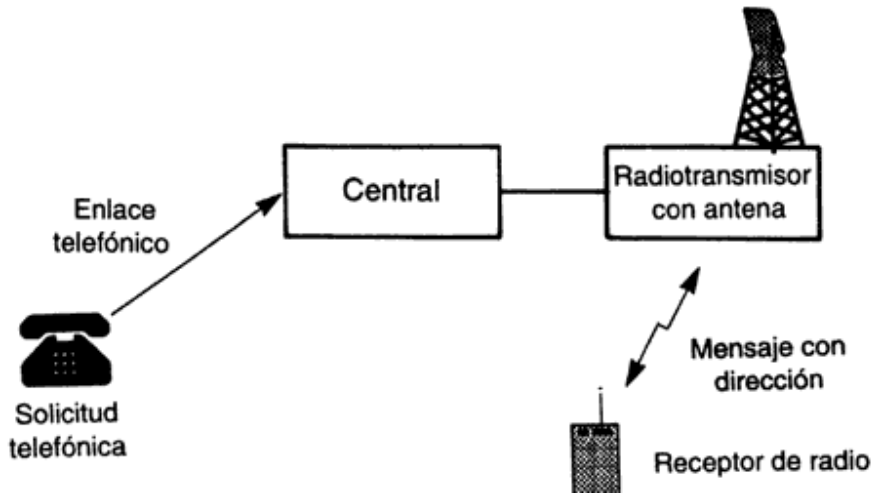
La direccionabilidad, concepto fundamental tanto para servicios unidireccionales como para los bidireccionales, consiste en lo siguiente. Cada equipo receptor tiene grabado en su memoria un número de identificación único (es decir, no hay otro equipo que tenga el mismo número). Cuando se transmite una señal digital que contiene un mensaje, éste va precedido por el número de identificación del usuario a quien va destinado el mensaje.

Todos los equipos dentro del área de cobertura reciben esta señal, extraen del mensaje el número de identificación y lo comparan con el número que tienen grabado en su memoria.

Si ambos números coinciden, entonces el equipo receptor activa sus circuitos para poder recibir el mensaje completo; en caso contrario, hace caso omiso de lo que recibió y vuelve a su estado de espera, verificando las direcciones cada vez que detecta un mensaje.

Es este mismo principio el que utilizan los servicios de radiolocalización de personas (en realidad el nombre del servicio, aun que muy difundido, es erróneo, ya que no se localiza a una persona sino que únicamente se envía un mensaje que llega a dicha persona por medio de su equipo personal). La red en la que se basa este servicio es de radio, con coberturas locales (por ejemplo, ciudades), nacionales o incluso internacionales (en este caso puede aumentarse la cobertura por medio de transmisiones vía satélite).

Figura 3. Esquema de radiodifusión de señales



3.3 Reglamentación de la interconexión de redes

La reglamentación que regula las interconexiones de redes para nuestro país esta a cargo de la superintendencia de telecomunicaciones de Guatemala (SIT), como un ente eminentemente técnico para dicha regulación y reglamentación.

3.3.1 Regímenes locales de interconexión

Como se mencionó en el apartado anterior, la superintendencia de telecomunicaciones de Guatemala es la que tiene a su cargo el régimen local de interconexión.

La superintendencia de telecomunicaciones es un órgano eminentemente técnico. El superintendente es nombrado por el ministro de comunicaciones, transporte y obras públicas de nuestro país.

El registro de telecomunicaciones está establecido bajo la supervisión de la superintendencia. Todos los operadores de redes comerciales de telecomunicaciones, poseedores de derechos de usufructo del espectro radioeléctrico y radioaficionados deberán registrarse proporcionando información básica tal y como se define en la ley.

Actualmente en Guatemala se ha iniciado una reforma revolucionaria del sector de telecomunicaciones, la cual consiste básicamente en la desmonopolización y apertura del mercado de las telecomunicaciones en todos los niveles y todos los servicios, lo cual será posible mediante la Ley General de Telecomunicaciones (Decreto 94-96) aprobada el 18 de noviembre de 1996.

Para mayor información acerca de las leyes y reglamentación de las telecomunicaciones en nuestro país, se puede visitar directamente la superintendencia de telecomunicaciones de Guatemala.

4. COMERCIO ELECTRÓNICO

En los últimos años el mundo empresarial ha experimentado algunos cambios importantes en cuanto a procesos comerciales y organización de las empresas.

Las oportunidades de empresas y consumidores han ido en aumento gracias a las posibilidades de comerciar que ofrece Internet, concepto que actualmente se denomina comercio electrónico o *e-commerce*.

El comercio electrónico permite a las empresas ser más flexibles con sus operaciones internas y dar un mejor servicio a sus clientes. Este fenómeno ha sido toda una revolución tecnológica. Algunas empresas han empezado partiendo de cero a apostar por esta nueva manera de hacer negocios. Sin embargo, la gran mayoría son empresas de carácter tradicional, que consideran el comercio electrónico como un aspecto complementario a su negocio, del que día a día hay que ir aprendiendo.

4.1 ¿Qué es el comercio electrónico?

Existen muchas definiciones de comercio electrónico o e-commerce, una de las posibles definiciones de comercio electrónico es: cualquier forma de transacción comercial en la que las partes interactúan electrónicamente en lugar de por intercambio o contacto físico directo. Sin embargo esta definición difícilmente capta el espíritu del comercio electrónico.

En la práctica, el espíritu del comercio electrónico puede verse más bien como uno de esos casos en los que las necesidades de cambio y las nuevas tecnologías se aúnan para revolucionar la forma en que se llevan a cabo los negocios.

El comercio moderno está caracterizado por un incremento de la capacidad de los suministradores, de la competitividad global y de las expectativas de los consumidores. En respuesta, el comercio mundial está cambiando tanto en su organización como en su forma de actuar. Se están sobrepasando las estructuras jerárquicas antiguas y erradicando las barreras entre divisiones de empresas, así como las existentes entre las empresas y sus suministradores y clientes.

Los procesos comerciales se están rediseñando de manera que atraviesen estos límites. Existen ya muchos ejemplos de procesos que afectan a una empresa entera e incluso algunos que llevan a cabo de manera conjunta las empresas y sus consumidores o suministradores.

El comercio electrónico es un medio de hacer posible y soportar tales cambios a escala global. Permite a las empresas ser más eficientes y más flexibles en sus operaciones internas, trabajar más estrechamente con sus suministradores y dar mejor respuesta a las necesidades y expectativas de sus clientes. Les permite seleccionar los mejores proveedores, sin tener en cuenta su localización geográfica, y vender en un mercado global.

Un tipo especial de comercio electrónico es la venta electrónica, en la que un suministrador provee bienes o servicios a un cliente a cambio de un pago. Como caso especial de venta electrónica estaría aquel en el que el cliente es un consumidor ordinario en lugar de otra empresa.

Sin embargo, aunque estos casos especiales tienen una considerable importancia económica, son sólo casos particulares del caso más general de cualquier forma de operación o transacción comercial llevada a cabo a través de medios electrónicos. Otros ejemplos igualmente válidos son las transacciones internas dentro de una misma empresa o el suministro de información a una organización externa con o sin cargo.

El comercio electrónico es tecnología para el cambio. Las empresas que lo miren como un añadido a su forma habitual de hacer negocio obtendrán sólo beneficios limitados, siendo el mayor beneficio para aquellas que sean capaces de cambiar su organización y sus procesos comerciales para explotar completamente las oportunidades ofrecidas por el comercio electrónico.

4.2 Categorías del comercio electrónico

El comercio electrónico, según los agentes implicados, puede subdividirse en cuatro categorías diferentes:

- empresa-empresa
- empresa-consumidor
- empresa-administración
- consumidor-administración

Un ejemplo de la categoría empresa-empresa sería una compañía que usa una red para ordenar pedidos a proveedores, recibiendo los cargos y haciendo los pagos. Está establecida desde hace bastantes años, usando en particular Intercambio Electrónico de Datos (EDI, *Electronic Data Interchange*) sobre redes privadas o de valor añadido.

La categoría empresa-consumidor se suele igualar a la venta electrónica. Se ha expandido con la llegada de la *Word Wide Web*. Hay ahora galerías comerciales sobre Internet ofreciendo todo tipo de bienes consumibles, desde dulces y vinos a ordenadores y vehículos a motor

La categoría empresa-administración cubre todas las transacciones entre las empresas y las organizaciones gubernamentales. Por ejemplo, en Estados Unidos las disposiciones gubernamentales se publicitan en Internet y las compañías pueden responder electrónicamente. Generalmente esta categoría está empezando, pero puede crecer rápidamente si los gobiernos la usan para sus operaciones para promover la calidad y el crecimiento del comercio electrónico. Además, las administraciones pueden ofrecer también la opción del intercambio electrónico para transacciones como determinados impuestos y el pago de tasas corporativas.

La categoría consumidor-administración, no acaba de emerger. Sin embargo, a la vez que crecen tanto las categorías empresa-consumidor y empresa-administración, los gobiernos podrán extender las interacciones electrónicas a áreas tales como los pagos de pensiones o el autoasesoramiento en devoluciones de tasas.

4.3 Proceso del comercio electrónico

El comercio electrónico implica la conjunción del mundo físico con el virtual, se puede hablar de varios tipos de comercio electrónico. Uno de ellos hace referencia a que todo el proceso (selección del producto, pago y entrega) se realiza en línea; esto únicamente es posible con mercancías que por su naturaleza pueden ser transmitidas por Internet (como información, un curso o datos estadísticos).

Otro tipo se establece con productos que necesariamente deben hacerse llegar físicamente al consumidor (como la ropa, un aparato eléctrico o alimentos).

A continuación se presenta un ejemplo del como a través de el comercio electrónico los compradores potenciales podrán vender sus productos o servicios.

Los catálogos son una forma por medio de la cual los vendedores pueden ofrecer diversas presentaciones de sus productos y estar estructurados de diferentes formas, algunos son prácticamente réplicas de los existentes en el mundo físico, en tanto otros aprovechan las ventajas de la red permitiendo realizar búsquedas según una descripción o palabra clave y enlaces a las diferentes categorías de productos.

De una u otra manera finalmente se llega a la página de descripción completa en la que se ofrece la información (tanto básica como complementaria) y en ocasiones una representación gráfica o multimedia (video, imagen o sonido) del producto o servicio.

Al igual que en el mundo físico, para ofrecer la alternativa de pago con tarjeta de crédito es necesario contar con una afiliación a una institución bancaria para garantizar la operación de cargo a la cuenta del cliente y abono a la tuya.

Si el producto que se quiere mercadear debe ser entregado físicamente, será necesario integrar al sitio herramientas que faciliten la logística de entrega. Estas pueden ser tan sencillas como contratar una compañía que se encargue exclusivamente de recibir los productos y hacerlos llegar al cliente; que almacene y controle el inventario de los productos e incluso, que permita al cliente contar con la visibilidad necesaria desde el momento del pedido de sus productos, hasta la entrega final.

Para garantizar que la tienda será visitada es recomendable realizar un plan de mercadotecnia completo. Toda acción en materia de mercadotecnia estará determinada por tu plan de negocio, el perfil del mercado y las características propias de los productos o servicios que venderás. Las estrategias a emplear pueden ser en el mundo físico, en Internet o, lo más recomendable, una conjunción de ambos.

4.4 Ventajas del comercio electrónico

Cualquier forma de comercio electrónico pone a disposición del usuario (sea comprador o vendedor) lo más vanguardista de la tecnología para garantizarle ventajas competitivas.

El comercio electrónico, al permitir una comunicación directa entre el consumidor y vendedor genera las siguientes ventajas por el lado del cliente:

- No hay intermediarios, por lo que los productos llegarán directamente del productor al comprador.
- Puede elegir los productos (sean bienes o servicios) independientemente del lugar que estos provengan; de esta manera contará con mayores alternativas para tomar una sabia decisión.
- Al tener comunicación directa con el proveedor garantiza que los productos son lo que usted espera de ellos, abriendo la posibilidad de adecuación de productos y asegurando que las dudas que le surjan puedan ser resueltas de manera clara y pronta.
- Los catálogos y especificaciones de productos serán los más actuales, garantizando información precisa y existencias de productos.
- Pagará el precio justo por los productos, no la publicidad de los mismos ni las ganancias de múltiples intermediarios.
- Posibilidad de reunir todos los elementos para tomar una buena decisión (información del producto, y posibilidad de clasificarlo); viabilidad de realizar una compra directa.

Del lado del vendedor el comercio electrónico también ofrece diversas ventajas las cuales se presentan a continuación:

- No hay intermediarios, los productos llegan directamente al cliente.
- Puede colocar sus productos en cualquier región geográfica, con la garantía que siempre estarán a disposición de los clientes los modelos más recientes.

- Al tener trato directo con el mercado (intercambio de información en tiempo real) podrá determinar fácilmente la aceptación que su producto tiene, permitiéndole realizar ajustes que garanticen su venta.
- Podrá ofrecer información actualizada y ampliada, mantener catálogo de existencias al día y controlar la información que se difunde de sus productos.
- Al reducir sus costos de operación (necesidad de catálogos impresos, distribución de ellos y demás gastos inherentes a la publicidad y colocación de productos) sus gastos disminuirán drásticamente, lo cual le permitirá ofrecer mejores precios y aumentar sus ganancias.
- Al contar con una solución de comercio electrónico articulada el control de inventarios, facturación y demás tareas administrativas se realizarán de forma automática.

Como se puede notar por lo presentado anteriormente, hay ventajas realmente fuertes con respecto al comercio que se práctica regularmente, estas ventajas se presentan tanto del lado del cliente como del lado del vendedor.

4.5 Seguridad en el comercio electrónico

La seguridad es un punto medular para el comercio electrónico. Por un lado ambas partes (consumidor y proveedor) deben estar seguros de que el otro es quien dice ser, pues de lo contrario, en el momento de un desacuerdo no sabrán con quién deban solucionarlo.

El cliente requiere que se le garantice que su información personal no será difundida ni empleada por terceros, esto queda más claro si pensamos en el caso de pago con tarjeta de crédito: ni el NIP, nombre, dirección, límite de crédito o número de tarjeta deberá ser compartido o interceptado.

Además, necesita garantía de que el producto que se le ofrece es igual al que se le entrega, y que de lo contrario contará con los instrumentos e instancias jurídicas para hacer valer sus derechos.

El vendedor necesita tener la certeza de que independientemente de la forma de pago se le entregará la cantidad acordada por la mercancía, y que si no sucediera, también tendrá los instrumentos y mecanismos para hacer valer sus derechos.

Debido a que el comercio electrónico no tiene fronteras, las condiciones que debe reunir una comunicación segura a través de Internet (o de otras redes) son en general las siguientes:

- Confidencialidad: evita que un tercero pueda acceder a la información enviada.
- Integridad: evita que un tercero pueda modificar la información enviada sin que lo advierta el destinatario. Autenticación: permite a cada lado de la comunicación asegurarse de que el otro lado es realmente quien dice ser.
- No repudio o irrefutabilidad: Permite a cada lado de la comunicación probar fehacientemente que el otro lado ha participado en la comunicación. En el caso de no repudio de origen, el remitente del mensaje no puede negar haberlo enviado. En el caso de no repudio de destino, el destinatario del mensaje no puede negar haberlo recibido.

Para conocer el origen del ataque, es decir de donde proviene el ataque que se esta recibiendo, existen software que vigila constantemente el tráfico en la red, estos al detectar tráfico que exceda las peticiones normales de su sistema, extraerá la dirección IP (número único que identifica una máquina cuando está conectada a Internet) que no esté incluida en la lista de peticiones de su PC y se la reportará, y de acuerdo a la naturaleza de los datagramas el software reportará el tipo de ataque – Irrupción que se está intentando.

La mayoría de estos programas los puertos que puede ser usado para introducir troyanos o para ataques remotos. Determina si son remotos descartando la dirección IP de su máquina y el conjunto de direcciones con las que esté interactuando. Si determina una dirección remota sospechosa, automáticamente envían la dirección IP. Con esta dirección es posible conocer de donde puede provenir el ataque por los rangos de direcciones que están asignadas a cada país, existen páginas donde se puede introducir la dirección IP y nos rastrea de que país puede provenir el ataque, por ejemplo: http://www.samspade.org/ **.** Y así poder empezar a realizar investigaciones en ese país para encontrar al culpable del mismo.

Realmente es bastante difícil detectar de donde provienen los ataques debido a que los *hackers*, por medio de otro software que ellos poseen logran camuflagear sus direcciones IP para no dejar rastro alguno. Aunque las instituciones internacionales realizan investigaciones extensas para poder dar con los responsables.

5. NORMATIVA DE LEY QUE REGULE EL COMERCIO ELECTRÓNICO

5.1 ¿Por qué la necesidad de una normativa de ley para el comercio electrónico?

Son realmente pocos los consumidores que han utilizado en alguna ocasión Internet para sus compras o contrataciones. A pesar de que hoy casi todo es posible en la red, desde comprar un billete de avión hasta realizar las transacciones comerciales más habituales, la mayor parte de los consumidores todavía se mantiene al margen de las nuevas posibilidades que ofrece el comercio electrónico.

Para explicar esta situación y conocer los temores y las demandas de los usuarios, se realizó un sondeo del comercio electrónico, este se realizó con la siguiente metodología:

El universo (los sujetos) de estudio se compuso de: personas que conozcan el funcionamiento del comercio electrónico, de nacionalidad guatemalteca, ambos sexos, mayores de edad y con capacidad económica para hacer uso del mismo.

El instrumento fue una encuesta publicada en Internet, en la siguiente dirección: http://www33.brinkstern.com/encuestaanhg/encuesta.asp**.** La cual iva dirigida a las personas que conozcan el funcionamiento del comercio electrónico, con preguntas cerradas y de opción de respuesta múltiple, de 7 preguntas. Se utilizaron para obtener la información de manera directa y por su familiaridad entre las personas.

Las preguntas de la encuesta se establecieron desde el punto de vista de la opinión de los consumidores, tomando como base los indicadores siguientes: uso, intención de uso, confianza, protección, seguridad, facilidad, por la definición de los indicadores se plantearon las preguntas necesarias para poder establecer la medición de los mismos, las preguntas a su vez fueron lo más entendibles y comprensibles para el encuestado, reflejando el objetivo del cuestionario, el cual es conocer la situación actual que vive el comercio electrónico en Guatemala.

Con los resultados que reflejó este, se podrá justificar la creación de una nueva norma que regulará el comercio electrónico, resultando imprescindible conocer la demanda del mismo, así como las carencias que los ciudadanos perciben respecto a esta nueva forma de comercio.

El tamaño de la muestra poblacional que contesto la encuesta fue de 437 personas, la cual es justificada y válida por las siguientes razones. Por la dificultad que representa el estimar el total del universo de estudio, debido a la restricción de acceso a datos reales de los usuarios de comercio electrónico, así como al hecho de no poder establecer el total de usuarios de la red para llevar a cabo el comercio electrónico.

Tomando en cuenta lo anterior se hizo uso de la fórmula para establecer la muestra en caso de tener una población infinita, basada en lo expuesto por Kelsey IL, Thompson WD, Evans A., que es la siguiente:

$$n = Z_{\alpha}^{2} \frac{p \cdot q}{i^{2}}$$

Definiéndose cada uno de sus componentes de la siguiente manera:

n = Tamaño muestral

Z = Valor correspondiente a la distribución de Gauss.

p = Prevalencia esperada del parámetro a evaluar.

q = 1-p.

i = Error que se prevé cometer.

Los valores para el cálculo del tamaño de la muestra fueron los siguientes:

Z = 1.96 para α =0.05.

p = 0.5.

q = 0.5.

i = 0.05.

$$n = (1.96)^2 \frac{0.5*0.5}{(0.05)^2}$$

$$n = 384.16 \approx 384$$

Por lo que se estableció que eran 384 personas una muestra aceptable para contestar la encuesta.

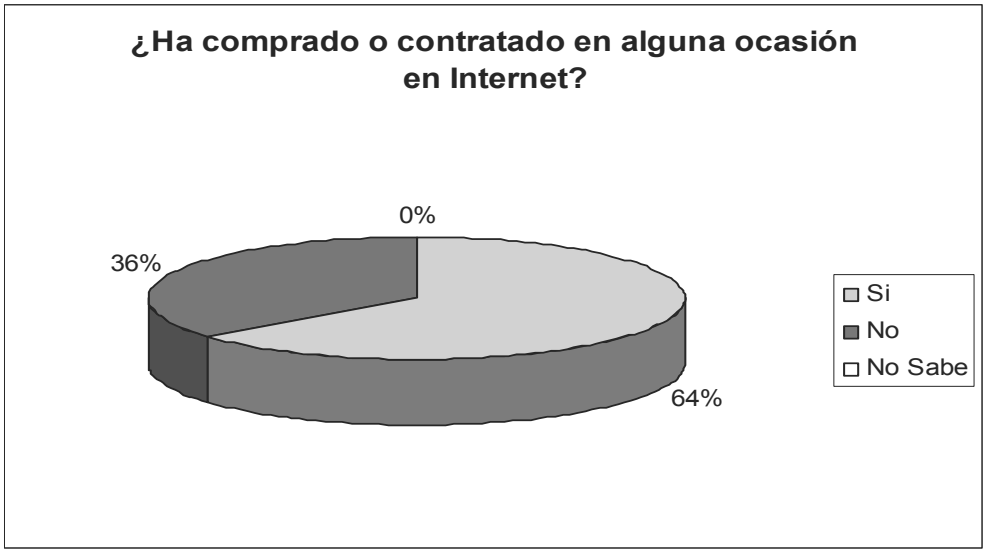
Resultados del sondeo

Empezaremos analizando el comercio electrónico: viendo desde los hábitos de los consumidores, compras en Internet. Según revela el estudio de momento, el comercio electrónico es cuestión de minorías: menos de la mitad de los consumidores han comprado o adquirido algún servicio en alguna ocasión por Internet.

¿Ha comprado o contratado en alguna ocasión en Internet?

Sí..... 36 %
No.....64%
No Sabe.....0%

Figura 4. Gráfica de resultados de la pregunta ¿Ha comprado en alguna ocasión en Internet?



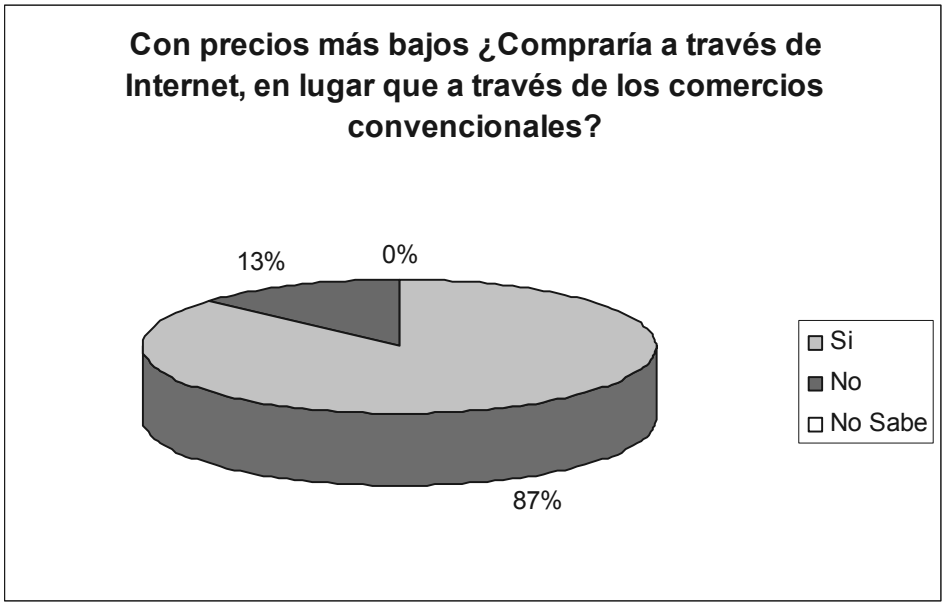
Sin duda, estos datos pueden sorprender si tenemos en cuenta la presencia de la publicidad que hay en la red, la que por una u otra razón se refiere al comercio electrónico. Costosas campañas publicitarias, inversiones, concentraciones y otras estrategias empresariales. ¿Cómo es posible que el resultado efectivo de estos impactos sea, hoy por hoy, tan limitado?

Parece obvio que los consumidores aún encuentran serias dificultades para optar por esta nueva forma de comercio y estos datos ponen en evidencia que, tal vez, se está empezando la casa por el tejado: mientras que el consumidor no perciba que las leyes le protegen de una manera efectiva, al tiempo que se facilita el acceso a Internet a las amplias capas de la población que aún se mantienen al margen de estas nuevas tecnologías, el desarrollo del comercio electrónico estará frenado.

Si, en igualdad de condiciones, en Internet se ofrecen precios más baratos para alguno de los productos o servicios que uno usa normalmente (viajes, billetes de avión, créditos hipotecarios, libros...), ¿compraría a través de Internet, en lugar que a través de los comercios convencionales?

Sí..... 87%
No..... 13%
No Sabe..... 0%

Figura 5. Gráfica de resultados de la pregunta con un precio más bajo ¿Compraría en Internet?



Sin embargo, estos datos hay que analizarlos con cuidado: no debemos concluir que por los precios crezca el interés de los consumidores. De hecho, una de las principales ventajas de Internet es permitir una oferta personalizada frente al comercio de masas. Por sus inabarcables dimensiones, casi todo lo podemos conseguir en la Red y esa peculiaridad tiene su especial sentido en productos o servicios minoritarios.

Los precios y la posibilidad de acceder a una oferta más amplia y en la que el consumidor "decide" (es decir, dispone de más libertad para elegir), parecen explicar dicha ventaja.

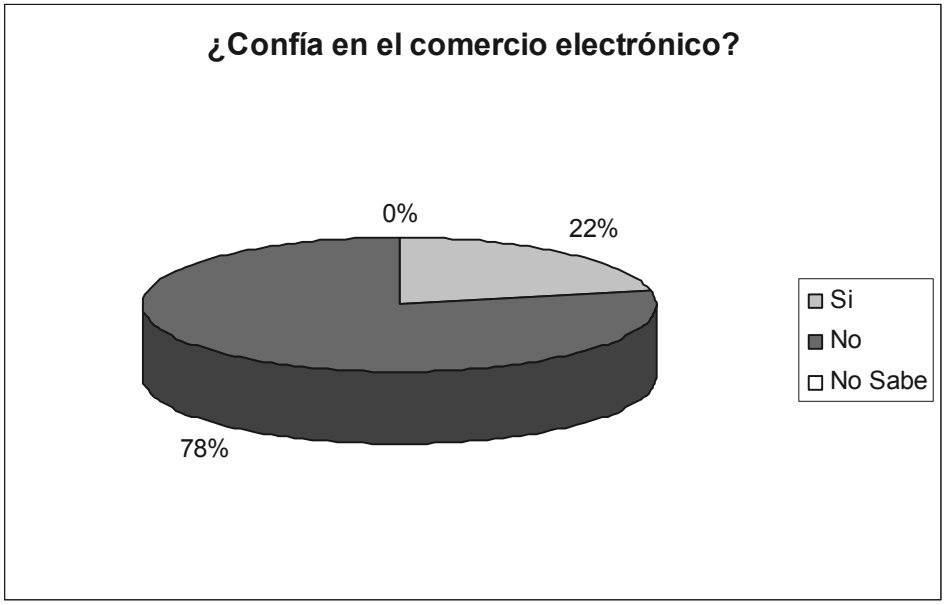
Continuaremos en el estudio examinando la confianza que los consumidores tienen en el comercio electrónico.

Todavía la mayoría de los consumidores no confían en Internet como medio para hacer sus compras y contrataciones. Casi 8 de cada 10 usuarios así lo afirman:

¿Confía en el comercio electrónico?

Sí..... 22%
No..... 78%
No Sabe..... 0 %

Figura 6. Gráfica de resultados de la pregunta ¿Confía en el comercio electrónico?

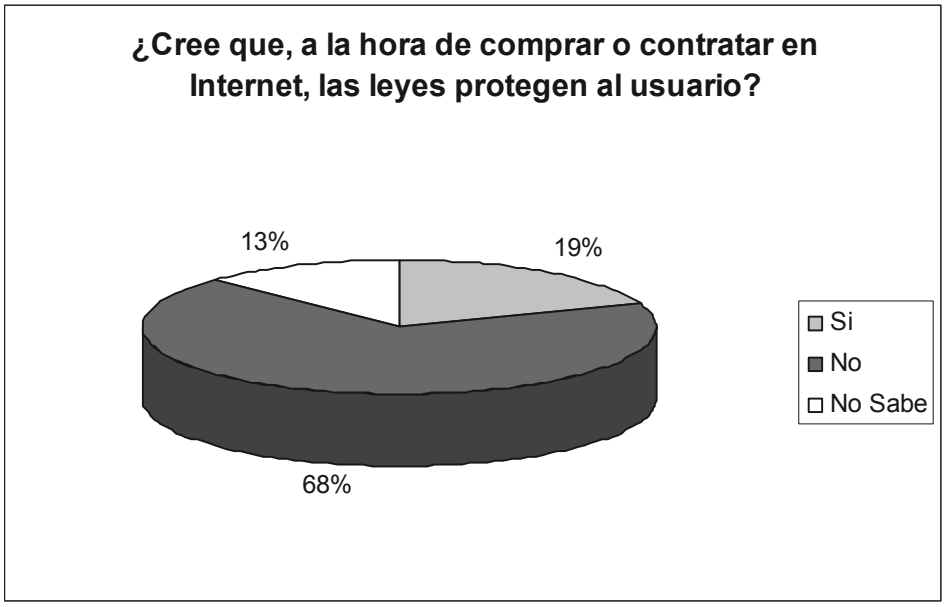


Ya hemos visto como la mayor parte de los consumidores (más de la mitad) aún no ha utilizado el comercio electrónico. A parte de otros inconvenientes que más adelante se enuncian, resulta evidente el peso que tiene el escaso desarrollo de la llamada Sociedad de la Información. Pero, junto a esas otras razones, que también deberán solucionarse, hay que resaltar que la implantación de este sistema de compra no se ampliará en tanto no cambie la percepción de los consumidores sobre su seguridad.

¿Cree que, a la hora de comprar o contratar en Internet, las leyes protegen al usuario?

Sí..... 19%
No..... 68%
No Sabe.....13%

Figura 7. Gráfica de resultados de la pregunta ¿Protegen las leyes a los consumidores?

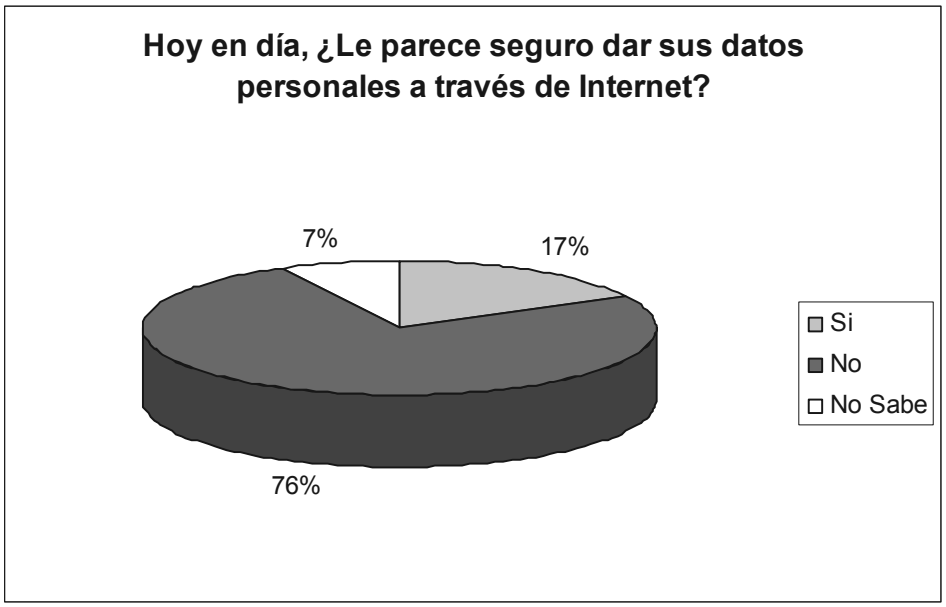


La falta de confianza manifestada por los encuestados se debe a que no existen normas que protejan los intereses del consumidor al momento de presentar algún reclamo por el no cumplimiento a lo solicitado.

Hoy en día, ¿Le parece seguro dar sus datos personales a través de Internet?

Sí.....17 %
No.....76%
Ns/Nc.....7 %

Figura 8. Gráfica de resultados de la pregunta ¿Le parece seguro dar sus datos a través de Internet?



De un modo particular, preocupa a los usuarios, en un porcentaje alto, la posibilidad de que sus datos personales sean transparentes en Internet.

El continuo flujo de información que circula por la Red y la posibilidad de que estos datos queden almacenados, o incluso accesibles, si no se utilizan sistemas de cifrado adecuados, parecen justificar esta desconfianza de los ciudadanos.

Una opinión que lamentablemente justifica la desconfianza se confirma cuando, se descubre la vulnerabilidad de algunas de las redes electrónicas más emblemáticas de las empresas de comercio electrónico.

Seguiremos analizando el problema del comercio electrónico desde el punto de vista de las principales dificultades a la hora de comprar y contratar en Internet.

¿Cree que todavía se dan muchas dificultades para que Ud. vea práctico utilizar el comercio electrónico?

Sí..... 64 %
No……..... 25 %
No sabe.....11%

Figura 9. Gráfica de resultados de la pregunta ¿Cree que todavía se dan muchas dificultades para que Ud. Vea práctico utilizar el comercio electrónico?

El estudio deja pocas dudas sobre la reducida confianza de la mayoría de los consumidores en el comercio electrónico. Además, casi 6 de cada 10 personas ven muy difícil que sea práctica la utilización del comercio electrónico, a pesar de las grandes ventajas aparentes que el mismo nos da.

El comercio electrónico, por sus peculiares condiciones (compra a distancia, ámbito territorial indefinido, ausencia de soporte documental escrito...) dificulta la defensa de los derechos de los usuarios, parece especialmente idóneo para generar una normativa de ley que proteja a los usuarios del mismo y que además, permita un buen funcionamiento de este sistema de comercio.

Si se tuviera una normativa que regule el comercio en Internet ¿Le inspiraría más confianza?

Si……..... 90 %

No….....10%

No Sabe..... 0 %

Figura 10. Gráfica de resultados de la pregunta, si se tuviera una normativa de ley que regule el comercio en Internet ¿Le inspiraría más confianza?

La ausencia de legislación nacional respecto de la regulación del comercio electrónico por medio de la firma digital, y las exigencias legales de utilización de soporte papel con firma manuscrita, impiden y dificultan el desarrollo de nuevas y modernas aplicaciones informáticas que permitan mejorar la productividad y reducir los costos de nuestras organizaciones.

Por los motivos expuestos anteriormente, es importante el generar una normativa de ley en nuestro país que regule el comercio electrónico para que tenga como objetivo: proteger los intereses de los usuarios que, en muchas ocasiones pueden ser víctimas de fraudes comerciales.

5.2 Firma digital

Las redes abiertas como Internet revisten cada vez mayor importancia para la comunicación mundial. Estas redes permiten una comunicación interactiva entre interlocutores que no necesariamente han entablado previamente relación alguna. Además, ofrecen nuevas posibilidades empresariales, creando herramientas que mejoran la productividad y reducen los costos, así como nuevas formas de llegar al cliente. Las redes están siendo utilizadas por empresas que desean aprovechar los nuevos tipos de actividad y nuevas formas de trabajo, los entornos virtuales compartidos.

También las administraciones públicas las utilizan en su gestión interna y en su interacción con empresas y ciudadanos. El comercio electrónico brinda a los países una excelente oportunidad para avanzar en su integración económica con las naciones del resto del mundo.

Para aprovechar todas estas posibilidades es necesario disponer de un entorno seguro en relación con la autenticación digital.

En la práctica existen diversos métodos para firmar documentos digitalmente, que van desde algunos muy sencillos, por ejemplo, insertar la imagen escaneada de una firma manuscrita en un documento creado con un procesador de texto, que no permiten otorgarle validez jurídica a la firma, a otros muy avanzados por ejemplo, la firma digital que utiliza la criptografía de clave pública, que sí lo permiten.

Para tener validez jurídica, las firmas digitales deben permitir verificar tanto la identidad del autor de los datos (autenticación de autoría), como comprobar que dichos datos no han sufrido alteración desde que fueron firmados (integridad).

5.2.1 La importancia de la firma digital con el comercio electrónico

Al facilitar la autenticación a distancia entre partes que no necesariamente se conocen previamente, las firmas digitales constituyen el mecanismo esencial para proveer seguridad y desarrollar la confianza en las redes abiertas. Por ello constituyen un elemento clave para el desarrollo del comercio electrónico en Internet.

En el ámbito nacional el comercio electrónico ya se está manifestando, existiendo supermercados, aerolíneas, agentes bursátiles y bancos que ofrecen sus productos y servicios directamente por Internet, permitiendo así la compra de alimentos y artículos del hogar, de pasajes aéreos, de títulos valores bursátiles, de transferencias de fondos entre cuentas bancarias y el pago de facturas de servicios, algunos otros servicios que se estarán abriendo a partir de que se tenga más confianza en las transacciones a través de la red.

Por señalar un ejemplo, puede mencionarse el efecto del comercio electrónico en Internet respecto del ámbito bursátil, para el cual el valor monetario de las transacciones de compra-venta de títulos valores iniciadas desde Internet en los Estados Unidos de Norteamérica en 1997 ascendió a 120 mil millones de dólares, estimándose que tal cifra se triplicó para 1998.

5.2.2 Otros beneficios de la firma digital

El comercio electrónico no es el único beneficiario de la firma digital. Actualmente las empresas y los organismos públicos de los países avanzados, están atorados de grandes cantidades de documentos en soporte papel que ocupan un significativo y costoso espacio de archivo en sus oficinas y que dificultan su informatización resultando en un acceso a la información mas lento y costoso. Los requerimientos legales que exigen la utilización del papel con firma manuscrita impiden la implementación de modernos sistemas informáticos mediante los cuales se podría acceder a documentos a distancia y a la información en forma inmediata, dando lugar por ejemplo a nuevas modalidades de desempeño laboral, como puede ser el tele-trabajo. Es aquí donde se produce el mayor beneficio de la utilización de la firma digital: tanto estas nuevas modalidades de trabajo como el incremento en la velocidad de circulación de la información que permite hacer factible el documento digital, permitirán que las organizaciones de nuestro país ofrezcan un mejor nivel de servicios a sus clientes y simultáneamente reduzcan sus costos, aumentando su productividad y su competitividad en lo que hoy son mercados cada vez mas globalizados y competitivos

5.3 Normativa de ley de la firma digital

La firma digital es justificable desde el momento en que los contratos, las transacciones económicas, compras, etc. se realizan en línea, es decir sin la presencia física de las partes. Surge de las tecnologías utilizadas para conseguir la confidencialidad en las comunicaciones, ante la proliferación de software que consiguen entrar en ellas obteniendo la información deseada.

Tal es el caso de un programa denominado Satán el cual se desarrolla bajo el contexto que al infectar realizan modificaciones a su código, para evitar ser detectados o eliminados, fue desarrollado y divulgado en Europa luego se expandió a América y al mundo entero, el cual puede recoger todo correo electrónico que lleve determinados contenidos (por ejemplo el número de una tarjeta de crédito) o determinado nombre. Esto quiere decir que nuestras transacciones por Internet están en peligro, por tanto es necesario una buena seguridad evitando que una persona ajena nos haga un fraude.

Esta nueva sociedad de la información necesita de muchas regulaciones puesto que todo lo que esta saliendo es tan innovador que no existe siquiera una referencia legislativa. Difícil será entrar en dicha sociedad si todavía no hemos podido encontrar la forma de proteger la información. Debido a esto y muchas razones es necesario crear una normativa de ley que vele por el buen funcionamiento de la firma digital.

Esta norma tendrá como objetivo establecer el marco legal requerido para el reconocimiento de las transacciones electrónicas. Al garantizar la autoría e integridad de un documento electrónico, la firma digital otorga un marco de confiabilidad al desarrollo de las actividades por Internet.

Algunos aspectos relevantes a considerar en la ley desde el punto de vista técnico y no desde el punto jurídico, que no es el objeto de nuestro estudio son:

Es tecnológicamente neutra, de acuerdo a la última tendencia internacional.

- Establece una Infraestructura de Firma Digital a nivel nacional, a fin de brindar condiciones de uso confiable de los documentos digitales, de acuerdo con estándares tecnológicos internacionalmente aceptados.
- Establece requisitos para la emisión y administración de los certificados digitales.
- Regula la actividad de las entidades prestadoras de servicios de certificación, determinando los alcances de la responsabilidad y las exigencias para obtener la respectiva licencia.
- Prevé mecanismos de reconocimiento de certificados digitales extranjeros.

5.3.1 Antecedentes Internacionales

En el plano internacional han tenido lugar múltiples actividades y debates en torno a los aspectos legales de la firma 4 digital:

La Comisión Europea redactó su borrador final de Directiva de Firma Digital en mayo de 1998, publicado en el Diario Oficial de las Comunidades Europeas del 23 de octubre de 1998, que establece las pautas para la utilización de la firma digital por los Estados miembros.

La Comisión de las Naciones Unidas para el Derecho Comercial Internacional ha aprobado una Ley-Modelo sobre comercio electrónico y ha comenzado a trabajar en la preparación de normas uniformes en materia de firma digital.

La Organización de Cooperación y Desarrollo Económico continúa sus trabajos en este ámbito, a modo de continuación de sus pautas de política criptográfica. Otras organizaciones internacionales, como la Organización Mundial del Comercio, han empezado también a interesarse en el tema.

El Comité de Seguridad de la Información de la Sección de Ciencia y Tecnología de la *American Bar Association* (*ABA* – Asociación de Abogados de los Estados Unidos de Norteamérica) redactó su Normativa de Firma Digital en 1996, en la que participaron casi ochenta profesionales de las disciplinas del derecho, la informática y la criptografía de los sectores público y privado, en la que especifica un mecanismo de firma digital a base a criptografía asimétrica, los certificados de clave pública y los certificadores de clave pública.

Varios países desarrollan ya actividades normativas pormenorizadas en relación con la firma digital:

- **Alemania:**

    - Ley y decreto promulgados en materia de firma digital, estableciendo las condiciones para considerar segura una firma digital; acreditación voluntaria de proveedores de servicios de certificación;
    - Elaboración de un catálogo de medidas de seguridad adecuadas;
    - Consulta pública en curso sobre los aspectos jurídicos de la firma digital y de los documentos firmados digitalmente.

- **Australia:**

    - Estrategia para la creación de una infraestructura de firma digital que asegure la integridad y autenticidad de las transacciones efectuadas en el ámbito gubernamental y en su relación con el sector privado.
    - Prevé la creación de una autoridad pública que administre dicha infraestructura y acredite a los certificadores de clave pública (Proyecto *Gatekeeper*).

- **Bélgica:**

    - Ley de telecomunicaciones: Régimen voluntario de declaración previa para los certificadores de clave pública;
    - Proyecto de ley de certificadores de clave pública relacionados con la firma digital;
    - Proyecto de ley de modificación del Código Civil en materia de prueba digital;
    - Proyecto de ley sobre la utilización de la firma digital en los ámbitos de la seguridad social y la salud pública.

- **Brasil:**

    - Proyecto de ley sobre creación, archivo y utilización de documentos electrónicos.

- **Chile:**

    - Proyecto de ley sobre documento electrónico que regula la utilización de la firma digital y el funcionamiento de los certificadores de clave pública.

- **Colombia:**

    - Proyecto de ley que define y reglamenta el acceso y uso del comercio electrónico, firmas digitales y autoriza los certificadores de clave pública.

- **Dinamarca:**

    - Proyecto de ley de utilización segura y eficaz de la comunicación digital.

- **Finlandia:**

    - Proyecto de ley de intercambio electrónico de datos en la administración y los procedimientos judiciales administrativos;
    - Proyecto de ley por la que la Oficina del Censo actuará como certificador de clave pública.

- **Francia:**

    - Ley de telecomunicaciones (decretos de autorizaciones y exenciones):

        - suministro de productos de firma digital sujeto a procedimiento de información;
        - libertad de uso, importación y exportación de productos y servicios de firma digital;
    - Normativa sobre utilización de la firma digital en los ámbitos de la seguridad social y la sanidad pública.

- **Italia:**

    - Ley general de reforma de los servicios públicos y simplificación administrativa promulgada: Principio del reconocimiento legal de los documentos digitales;
    - Decreto de creación, archivo y transmisión de documentos y contratos digitales;
    - Decreto regulador de productos y servicios, en preparación;
    - Decreto sobre las obligaciones fiscales derivadas de los documentos digitales, en preparación.

- **España:**

    - Circulares de la dirección de Aduanas sobre utilización de la firma digital;
    - Resolución en el ámbito de la seguridad social que regula la utilización de medios digitales;
    - Leyes y circulares en materia de hipotecas, fiscalidad, servicios financieros y registro de empresas que autorizan el uso de procedimientos digitales;
    - Ley de presupuestos de 1998, por la que la Casa de la Moneda actuará como certificador de clave pública.

- **Estados Unidos:**

Iniciativas del Gobierno Federal:

- Iniciativa sobre la creación de una infraestructura de clave pública para el comercio electrónico.
- Ley que autoriza la utilización de documentación electrónica en la comunicación entre las agencias gubernamentales y los ciudadanos, otorgando a la firma digital igual validez que la firma manuscrita. (Ley Gubernamental de Reducción de la Utilización de Papel - *Government Paperwork Elimination Act*).
- Ley que promueve la utilización de documentación electrónica para la remisión de declaraciones del impuesto a las ganancias.
- Proyecto piloto del IRS (Dirección de Rentas - *Internal Revenue Service*) para promover la utilización de la firma digital en las declaraciones impositivas.
- Proyecto de ley de Firma Digital y Autenticación Electrónica para facilitar el uso de tecnologías de autenticación electrónica por instituciones financieras.
- Proyecto de ley que promueve el reconocimiento de técnicas de autenticación electrónica como alternativa válida en toda comunicación electrónica en el ámbito público o privado.
- Resolución de la Reserva Federal regulando las transferencias electrónicas de fondos.
- Resolución de la FDA (Administración de Alimentos y Medicamentos - *Food and Drug Administration*) reconociendo la validez de la utilización de la firma electrónica como equivalente a la firma manuscrita.

- Iniciativa del Departamento de Salud proponiendo la utilización de la firma digital en la transmisión electrónica de datos en su jurisdicción.
- Iniciativa del Departamento del Tesoro aceptando la recepción de solicitudes de compra de bonos del gobierno firmadas digitalmente.

Iniciativas de los Gobiernos Estatales

- Casi todos los estados tienen legislación, aprobada o en proyecto, referida a la firma digital. En algunos casos, las regulaciones se extienden a cualquier comunicación electrónica pública o privada.
- Se destaca la Ley de Firma Digital del Estado de *Utah*, que fue el primer estado en legislar el uso comercial de la firma digital. Regula la utilización de criptografía asimétrica y fue diseñada para ser compatible con varios estándares internacionales. Prevé la creación de certificadores de clave pública licenciados por el Departamento de Comercio del estado.

- **Malasia:**

  - Ley de firma digital, aprobada y pendiente de promulgación, que otorga efecto legal a su utilización y regula el licenciamiento de los certificadores de clave pública.
  - Proyecto piloto de desarrollo de infraestructura de firma digital.

- **Países Bajos:**

    - Régimen voluntario de acreditación para los certificadores de clave pública , en preparación;
    - Normativa fiscal que prevé la presentación digital de la declaración de ingresos;
    - Proyecto de ley de modificación del Código Civil, en preparación.

- **Reino Unido:**

    - Proyectos legislativos en materia de concesión de licencias voluntarias a los certificadores de clave pública y reconocimiento legal de la firma digital.

5.3.2 Necesidad de una normativa compatible

Es imprescindible que el marco legal y técnico que adopte el país para el desarrollo de la firma digital sea compatible con el que ya existe en otros países.

La aplicación de criterios legales diferentes a los aplicables en otros países en cuanto a los efectos legales de la firma digital, y cualquier diferencia en los aspectos técnicos en virtud de los cuales las firmas digitales son consideradas seguras, resultará perjudicial para el desarrollo futuro del comercio electrónico nacional y, por consiguiente, para el crecimiento económico del país y su incorporación a los mercados internacionales, cada vez más globalizados.

Es deseable un alto grado de homogeneidad normativa para fomentar la comunicación y la actividad empresarial por redes abiertas con las naciones del mundo, al facilitar el libre uso y prestación de servicios relacionados con la firma digital y el desarrollo de nuevas actividades económicas vinculadas con el comercio electrónico.

La finalidad de la normativa de ley de la firma digital, es eliminar obstáculos al reconocimiento jurídico de las firmas digitales y facilitar la libre circulación de servicios y productos de certificación con otros países.

Es decir facilitar el uso de las firmas digitales en un espacio sin fronteras en lo que concierne a las obligaciones esenciales de las partes que intervienen, y de los certificadores de clave pública.

5.3.3 Aspectos técnicos de la firma digital

5.3.3.1 Aspectos técnicos de la firma digital

A continuación una breve explicación a fin de esclarecer ciertas cuestiones relativas a la terminología de la tecnología de firma digital.

En primer lugar corresponde hablar de firma digital y no de firma electrónica, vocablo éste último que se utiliza erróneamente en cierta legislación internacional para referirse a la firma mecanizada para los fines de su procesamiento informático y que consiste más precisamente de dígitos binarios y no de electrones.

Aunque es cierto que los dígitos de una firma digital consisten de magnitudes eléctricas cuando la firma digital se encuentra momentáneamente almacenada en la memoria volátil de una PC (RAM), también es cierto que cuando se encuentra almacenada en el disco duro (magnético) de la PC consiste en campos magnéticos, cuando se encuentra perdurablemente almacenada en un CD-ROM consiste en agujeros perforados en la capa de aluminio del CD y cuando es transmitida por una fibra óptica de telecomunicaciones consiste en fotones.

Lo que también es cierto, es que en todas estas modalidades diferentes de almacenamiento y transmisión, la firma mecanizada no pierde su cualidad de numérica, es decir digital, por lo que le corresponde su denominación como tal firma digital.

Se expone el presente argumento sin perjuicio de que el vocablo firma digital se corresponde mejor con la marcada tendencia internacional de la digitalización de la economía, que el vocablo firma electrónica.

También corresponde explicar que la firma digital, nada tiene que ver con la firma escaneada, es decir con el documento de procesador de palabras al cual se le ha anexado al pie la imagen escaneada de una firma manuscrita. La firma escaneada carecerá siempre de valor jurídico, pues por una parte quién recibe en disquete un documento que contiene la imagen escaneada de una firma manuscrita queda en total libertad de modificar el contenido de ese documento.

Por la otra, cualquier persona puede escanear la firma manuscrita de otra y aplicarla al pié de un documento que cree con el contenido a su gusto.

Aunque parezca ahondar más, conviene también explicar que la firma digital nada tiene que ver con la utilización de la impresión dactilar (de, por ejemplo, el pulgar) utilizando una almohadilla de tinta, al pie de un documento en soporte papel.

Establecido ya que la información a la cual se le desea otorgar valor jurídico es digital, o sea numérica (binaria), conviene explicar la naturaleza de los posibles mecanismos disponibles para otorgarle validez jurídica a esa información numérica.

En este sentido cabe aseverar en forma axiomática y tautológica que el mecanismo de firma digital debe ser criptográfico, pues si lo que se desea es proteger la información, o sea los dígitos, se incursiona necesariamente en el campo de la criptografía, la que se define como el arte de proteger la información, tanto como para proteger su privacidad, como para proteger su integridad. El término criptografía proviene del griego (cripto: oculto) y es definido como el arte de escribir con clave secreta o de un modo enigmático.

No se dice que el mecanismo de firma digital deba ser únicamente criptográfico, sino meramente que la criptografía forma parte esencial de ese mecanismo de firma digital, pudiendo intervenir en el proceso de firma otros mecanismos tales como los mecanismos biométricos, pero sólo en forma adicional a la criptografía.

Establecido que el mecanismo de firma digital es necesariamente criptográfico, conviene analizar qué mecanismos criptográficos son considerados aceptables.

Como se expuso en el análisis previo de la firma manuscrita, una de las cualidades esenciales para que la misma tenga validez jurídica es que no sea fácilmente falsificable por un tercero, es decir que existan garantías de que esa firma pueda ser creada sólo por una persona y no por otra.

En el ámbito informático y digital es posible reproducir cualquier información binaria, tal que la copia no se pueda diferenciar de su original. Como ya se mencionó, esta es una de las razones por la que la firma manuscrita escaneada (digitalizada) no puede obtener validez jurídica.

Resta hallar entonces en el ámbito digital aquello que le confiera unicidad a las firmas digitales creadas por una persona, o sea una condición que permita identificar al creador de una firma digital, teniendo en cuenta que cualquier cualidad manifiesta a simple vista puede ser fácilmente copiada y transferida de un documento a otro.

La condición buscada está disponible y consiste en el secreto no compartido. El concepto en su esencia es muy simple: el creador de una firma digital posee un elemento que sólo él conoce y posee y que le permite crear firmas digitales tal que quién las verifica pueda establecer inequívocamente que al firmar el creador de la firma digital necesariamente tuvo posesión de ese elemento, pero sin requerir que el creador de la firma digital tenga que divulgar ese secreto, con lo que el secreto dejaría de serlo.

Este mecanismo existe y en el ámbito de la criptografía se denomina criptografía asimétrica o criptografía de clave pública. La criptografía asimétrica utiliza dos claves diferentes pero íntimamente relacionadas, tal que lo que encripta una clave sólo puede ser desencriptado por la correspondiente otra clave, y no por una clave ajena a ese par.

El mecanismo matemático utilizado asegura además que conociendo la clave pública no se tiene información alguna sobre la correspondiente clave privada. Este mecanismo contrasta con la más tradicional criptografía simétrica que utiliza la misma clave para encriptar que para desencriptar un texto, por lo que el destinatario del texto para poder leerlo necesariamente debe conocer la clave secreta utilizada para encriptar ese texto con lo que esa clave secreta deja de ser secreta. Por ello la criptografía simétrica solo sirve para otorgarle privacidad a la información pero no como tecnología de firma digital.

En la criptografía asimétrica, la clave de encriptado se denomina privada y es mantenida secreta por el firmante, mientras que la otra clave relacionada (de desencriptado) se denomina clave pública y se da a conocer. Las firmas digitales creadas por el firmante utilizando su clave privada y son verificadas por el destinatario del documento con la correspondiente clave pública. El hecho de que una firma digital sea verificable por medio de una cierta clave pública implica necesariamente que esa firma fue creada por la correspondiente clave privada que, por definición, el firmante siempre mantuvo secreta y nunca divulgó.

Es esencial para su validez jurídica que el mecanismo de firma digital contemple la utilización de un secreto no compartido por el creador de una firma digital, pues es este secreto no compartido es lo único que impide que un tercero falsifique su firma, y si un mecanismo de firma permite la falsificación, deja de ser confiable, y si no es confiable no es realmente un mecanismo de firma. Esta seguridad de no falsificación es intrínseca a cualquier mecanismo de firma.

Por lo expuesto, es claro que el requisito de implementar la firma digital únicamente mediante la criptografía asimétrica, más que un requisito es una particularidad que, como se demostró, surge naturalmente de la naturaleza intrínseca del problema a resolver, que es cómo identificar al autor de un documento digital y establecer si dicho documento fue posteriormente modificado.

Como quedó demostrado la criptografía simétrica no se puede utilizar como mecanismo de firma digital, y como la criptografía si no es simétrica entonces es asimétrica. De esta manera queda la criptografía asimétrica como la única alternativa para implementar la firma digital. De hecho el algoritmo de clave asimétrica más popular por un amplio margen es el denominado *RSA* en honor a sus inventores Ronald Rivest, Adi Shamir y Leonard Adleman que lo desarrollaron en el *Massachussetts Institute of Technology* de los Estados Unidos en 1977.

El requisito de implementar la firma digital únicamente mediante la criptografía asimétrica tampoco es restrictivo ni tecnológica ni comercialmente, pues la criptografía asimétrica no es una tecnología ni un algoritmo especial y propietario, sino meramente una definición que abarca a todo y cualquier algoritmo criptográfico que utilice una clave diferente para encriptar que para desencriptar, de los cuales existen por lo menos una treintena de algoritmos diferentes utilizables

5.3.3.2 Documento digital

El documento digital es simplemente una secuencia informática de bits (unos y ceros) que puede representar cualquier tipo de información. Esta representación de la información en base a dígitos implica en el ámbito informático una representación binaria, es decir por medio de unos y ceros.

Todo tipo de información es apta para ser representada digitalmente: mediante el escaneo, la imagen de una fotografía o la imagen de un documento en soporte papel; mediante un procesador de palabras, la información escrita; mediante una plaqueta digitalizadora, la voz, la música y el video; mediante hojas de cálculo, la información numérica y financiera; y mediante bases de datos, la información estadística y diversa información.

Todo tipo de información representada digitalmente constituye un documento digital y es susceptible de ser firmada digitalmente. Es por ello que la firma digital puede utilizarse para otorgar validez jurídica o eficacia probatoria a toda declaración de voluntad o de conocimiento, con independencia de su extensión o de su medio de almacenamiento, sin limitación alguna.

5.3.3.3 Transmisión y almacenamiento de datos

Es importante destacar que la firma digital está ligada íntimamente al documento digital que la origina y que junto a ese documento y el certificado de clave pública correspondiente permiten en conjunto y de manera autosuficiente verificar la integridad del documento y la identidad del creador de la firma.

Como se puede observar, la cuestión de la transmisión de la información en general, y de un documento digital en particular, no forma parte alguna del mecanismo de firma digital y de la validez jurídica del documento digital firmado.

Por ejemplo: una persona puede crear un documento digital y su respectiva firma digital en una PC para que luego ese documento y su firma permanezcan en esa PC, o para ser copiados a un disquete, o para ser enviados por correo electrónico a cualquier lugar del mundo, sin que se vea afectada de manera alguna la capacidad de esa firma digital de verificar la integridad de ese documento y de establecer la identidad de su creador, preservando así la validez jurídica del mismo.

5.3.3.4 Características de la información y diferencias entre ellas

Vale la pena explorar cuidadosamente las diferencias en los conceptos de integridad, inalterabilidad y perdurabilidad de la información y de cómo éstos se relacionan con los conceptos de la firma digital, del archivo de la información y de los distintos medios de almacenamiento.

Integridad significa: que la información no carece de ninguna de sus partes, que no ha sido modificada. La integridad es una cualidad imprescindible para otorgarle validez jurídica a la información. La firma digital detecta la integridad de la información que fuera firmada, en forma independiente al medio de su almacenamiento.

Inalterabilidad significa: que la información no se puede alterar. La inalterabilidad no se refiere a la información en sí, sino a su medio de almacenamiento. La firma digital no impide que la información se altere, sino que detecta si ésta ha sido alterada. La inalterabilidad del medio de almacenamiento no asegura la integridad de la información: El disco digital *CD-ROM*, por ejemplo, es un medio de almacenamiento gravable una sola vez, por lo que impide que se altere la información que en él ha sido grabada, pero no impide que esa información sea copiada a un segundo *CD-ROM* que luego sustituya a su original.

Perdurabilidad significa: que la información perdura en el tiempo y es una cualidad del medio de almacenamiento. La información que debe perdurar en el tiempo debe ser archivada en un medio perdurable. La inalterabilidad del medio de almacenamiento es ortogonal a la perdurabilidad de la información.

Por ejemplo en la antigua informática, la tarjeta perforada de cartón es un medio inalterable porque no es re-perforable, pero no demuestra buenas características de perdurabilidad pues es sensible a la humedad y a los roedores. Por el otro lado, el disco rígido de una computadora no es un medio inalterable de almacenamiento, pero demuestra excelentes características de perdurabilidad cuando opera como parte de un banco de discos, si la información se almacena con suficiente redundancia y si los discos tienen un tiempo promedio entre fallas del orden de 350,000 horas (40 años).

5.3.3.5 Seguridad de la firma digital

La tecnología propuesta de firma digital no es perfecta ni infalible. Los dispositivos en hardware y en software de creación y verificación de firmas digitales deben ser homologados previa auditoria de su funcionamiento, para poder ser utilizados para crear firmas y verificar firmas digitales con plena eficacia jurídica; sin embargo, el requisito de homologación no debe constituirse en una barrera que impida implementar los rápidos avances en el ámbito internacional, por lo que se propone la aprobación tácita de una solicitud de homologación, si la autoridad de aplicación no se expide dentro de los 90 días de presentada dicha solicitud.

Por otro lado, es importante destacar que la firma manuscrita tampoco es perfecta o infalible, puesto que es decididamente posible en ciertos casos alterar de forma indetectable el contenido de un documento en soporte papel o falsificar una firma manuscrita. Adicionalmente, debe considerarse que siempre existe un margen de error en la labor de los peritos caligráficos, con lo cual una firma apócrifa puede darse por auténtica y viceversa.

Es usual, por ejemplo, que importantes contratos de compra-venta entre empresas en soporte papel sean firmados por las partes solo en su última página, contando solamente con iniciales en las restantes, lo que a simple vista resulta riesgoso considerando que generalmente el precio establecido en el contrato tiende a no figurar en la última página, sino en alguna página anterior.

Adicionalmente, en Internet es de público acceso la información que indica que es técnicamente posible sintonizar un láser para que se corresponda con el color de una tinta, tal que al accionar el láser, la tinta literalmente se vaporiza y se levanta del papel sin dejar rastro detectable alguno.

Sin embargo, las aludidas imperfecciones de los mecanismos de firma manuscrita en documentos en soporte papel no impiden los actos jurídicos, ni gubernamentales ni comerciales que se basan en ella, ni que la firma manuscrita figure como requisito en las leyes y reglamentos, por lo que es de inferir que la alternativa propuesta de firma digital de documentos digitales tampoco precisa ser perfecta e infalible para ser de gran utilidad.

Lo que es importante notar es la necesidad de gradualismo y proporcionalidad en la especificación de los sistemas y parámetros de firma digital en relación con el tipo de acto en particular, teniendo en consideración las consecuencias jurídicas del acto y/o el valor económico involucrado.

De la misma manera, que además de requerir soporte papel y firma manuscrita la venta de un inmueble requiere la intervención de un escribano público y la utilización de un protocolo notarial, pero la compra de un electrodoméstico con tarjeta de crédito no, análogamente serán diferentes los requisitos para otorgar validez jurídica a los documentos digitales firmados digitalmente, dependiendo de la naturaleza del acto o de la transacción subyacente.

5.4 Normativa de ley del comercio electrónico

En los últimos años del siglo pasado, se ha producido en nuestro país el lanzamiento de una importante cantidad de portales y sitios, destinados a diferentes actividades y rubros de la economía. Si bien muchos de estos emprendimientos comienzan con la provisión de contenidos, información y también realizando un importante accionar destinado a crear comunidades, la mayoría preveía dentro de sus *business plans* esquemas orientados a la realización de Comercio Electrónico o *e-commerce*.

En este nuevo siglo, fue por el contrario más crítico; comenzó con las aspiraciones estratégicas de muchos iniciadores buscando ingresar a una primera y en algunos casos a una segunda ronda de financiamiento. Pero la caída de las acciones de Internet en el mercado comenzó a hacerse más intensa, con una bajada pareja tanto para las empresas de Internet como para las de tecnología en general. Los inversores se hicieron muchos más cautos y las valuaciones de los emprendimientos bajaron substancialmente

Las empresas se orientaron al comercio directo con clientes (B2C) o con empresas (B2B); la mayor parte de las primeras, que son muy importantes en el despegue de la nuevas formas de economía, debieron ser muchos más cautelosos con sus planes de venta y de crecimiento y también prever sus gastos de estructura y de personal. El problema evidente fue la generación de beneficios en sus balances, ninguna logró cerrar con sus números en negro. Los mercados se mostraron todavía en una etapa muy preliminar, pronosticándose recién su despegue para los el años siguientes. El B2B se presentó con mejores oportunidades, basado en la construcción de algunos incipientes *market places*.

Pese a la crisis actual, Internet sigue avanzando, la gente que ingresa al mundo en virtual de la red es cada vez mayor y la *Web World Wide* mientras tanto sigue cambiando de formas, en busca de caminos que tengan un mayor valor para los clientes y también para su propio crecimiento.

Lo increíble y a la vez desafiante de los negocios en Internet es que ya no existirán los usos de horarios, las fronteras antes tan rigurosamente cuidadas dejarán de tener tanta importancia y los clientes serán atendidos a cualquier hora del día, no solo el de un país en particular, sino que ahora los clientes serán, el mundo entero.

Los límites serán demarcados solo por nuestros propios horizontes creativos y el valor de nuestros productos y servicios podrán ahora ser evaluados por personas, que podrán estar informándose y hasta comprando cuando nuestros ámbitos físicos de trabajo estén cerrados.

Para comenzar un proyecto de *e-business* es fundamental tener en cuenta aspectos referidos a: infraestructura tecnológica, modelos de negocios y también un marco legal lo cual es muy importante e impositivo que permita crear la confianza necesaria entre los potenciales clientes del sitio a lanzar.

En Comercio Electrónico se deben trasladar los mismos mecanismos con que trabajamos en el mundo real y es acá donde radica el desafío de los *e-entrepreneurs* (de espíritu empresarial) que diseñan sus proyectos de Internet. Los distintos modelos de comercio electrónico requieren garantizar la calidad y seguridad del sitio, su privacidad para los clientes, los mecanismos de pago, la firma digital, la encriptación, etc.

Es entonces fundamental contar con una Legislación dinámica y confiable, que en toda transacción electrónica ampare tanto a los clientes-consumidores como también a proveedores y sitios que originen los negocios.

En cuestión de unos pocos años, todo el mundo estará presente en Internet. El miedo de que reemplace a la vida real es infundado: así como la televisión no reemplazó a la radio ni a los libros, el mundo cibernético no ocupará el mundo real, si bien no hay duda de que aportará una nueva dimensión a la vida humana.

5.4.1 Comparaciones de las normativas de otros países

Esta parte del trabajo tiene como finalidad sintetizar de una manera clara y sencilla, las diferentes legislaciones que existen dentro de los países líderes en la materia. Para esto, se han seleccionado las Leyes de los Estados Unidos, España, la Unión Europea, Latinoamérica y El Caribe. El aporte de este análisis está en la comparación y en la búsqueda de las mejores experiencias, con las cuales luego se podrá efectuar un proceso de mejora de la Ley final que se apruebe en nuestro país.

Los principales actores hasta el momento han sido Estados Unidos y la Unión Europea, los cuales han establecido sus marcos legales en forma diversa de acuerdo a sus propios modelos de concepción jurídica: el *common law* de origen anglo-americano y el continental europeo.

Mientras Estados Unidos aborda el tema a través de un concepto de autorregulación y dejando liderar al sector privado la expansión de Internet con la menor intervención del estado, la Unión Europea adopta un concepto de mayor intervención y control por parte del estado.

En efecto, si bien la Directiva Europea sobre Comercio Electrónico establece solamente una serie de líneas de acción y tiene un principio generalista, la misma busca armonizar el tratamiento de las cuestiones a nivel estatal.

La Directiva no establece de por si normativas estrictas, pero trata de asegurarse que sus estados miembro tengan normativas particulares que legislen sobre determinados aspectos con un concepto de control y certificación oficial.

Entre estas dos tendencias conceptuales, los países latinoamericanos tratan de definir sus propias leyes considerando las características particulares de la región (nivel de desarrollo, accesibilidad a computadoras, difusión de las tarjetas de crédito, etc.), pero siguiendo en general el modelo continental europeo.

Respecto de nuestro país, dada su situación económico-cultural, es hoy quizás uno de los que tienen más posibilidades para el desarrollo del comercio electrónico. Sin embargo a diferencia de otros países vecinos, la falta de un marco legal orgánico sobre comercio electrónico, quizás sea su punto más débil.

Más allá de algunas disposiciones vigentes, que pueden considerarse inadecuadas, insuficientes y fragmentarias, nuestro país carece de una normativa jurídica orgánica con relación al comercio electrónico y el formato digital para la celebración de actos jurídicos.

5.4.2 Propuesta de aspectos técnicos

Los principios rectores que han inspirado el proyecto y sus principales directrices son:

- Promover la compatibilidad con el marco jurídico internacional.
- Asegurar la neutralidad tecnológica.
- Garantizar la igualdad en el tratamiento jurídico del uso de las nuevas tecnologías de procesamiento de la información.
- Facilitar el comercio electrónico interno e internacional,
- Fomentar y estimular la aplicación de nuevas tecnologías de la información en la celebración de relaciones jurídicas y
- Respetar la observancia de la buena fe en las relaciones jurídicas instrumentadas según esta ley.

5.4.2.1 Disposiciones generales y marco interpretativo

En esta sección de la normativa se establecen las definiciones y el ámbito de aplicación de la Ley como también los principios generales conforme a los cuales deberán interpretarse las materias que no se encuentran expresamente previstas.

Las disposiciones generales de esta Ley tienen por objeto y se ven orientadas hacia la regulación de determinados aspectos jurídicos de los servicios de la sociedad de la información y, en particular, del comercio electrónico.

Concretamente, se regula el régimen del establecimiento de los prestadores de servicios, el de las comunicaciones comerciales, el de la contratación por vía electrónica, el de la responsabilidad de los prestadores de servicios, incluidos los intermediarios, así como a la prestación de los servicios de la sociedad de la información que se realizará en régimen de libre competencia, sin que quepa establecer ningún tipo de restricciones para los comercios que se encuentren amparados por esta ley.

También, la prestación de servicios de la sociedad de la información por las Administraciones Públicas o los organismos o sociedades de ellas dependientes, se realizará con arreglo a los principios de objetividad transparencia y no discriminación.

5.4.2.2 Validez jurídica y fuerza probatoria de los documentos digitales

En esta sección se establece que todos los actos jurídicos lícitos pueden celebrarse validamente por medio de documentos digitales como también su plena fuerza probatoria. Se establecen además los requisitos para el caso de escrituras públicas.

Este criterio general resulta precisado en su alcance, en función de establecer un distinto reconocimiento a las tecnologías más seguras (“firma digital”) con respecto a las menos seguras y, de mantener aquellas formalidades consagradas en nuestro derecho para la celebración de determinados actos.

De modo tal que la habilitación amplia del uso del formato digital para la celebración de actos jurídicos se complementa con una serie de disposiciones que brindan la necesaria seguridad jurídica, como para inspirar confianza y certidumbre en el uso de estos medios.

5.4.2.3 Comunicaciones digitales

Se establecen las presunciones que se tendrán en cuenta con referencia a la identificación del iniciador, la efectividad del envío y la recepción del mismo, la localización del iniciador y del destinatario. Asimismo se regulan las normas a seguir en caso de notificaciones de intimaciones.

Se debe de definir entre las obligaciones en materia de información, que se establezcan en la normativa, que las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales y, en todo caso, en ellas se deberá indicar la persona física o jurídica en nombre de la cual se realizan.

También se deben de tomar en cuenta los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales cuya prestación esté permitida o autorizada por la normativa; se deberá asegurar además el cumplimiento de los requisitos que se establecerán a la hora de generar la normativa, así como que las condiciones de acceso, o caso de participación, se expresen de forma clara e inequívoca.

Además de los requisitos que se establecen en la normativa, el prestador de servicios de la sociedad de la información que realice comunicaciones comerciales no solicitadas por correo electrónico, cuyo envío estará permitido por la normativa, estará obligado a identificarlas de forma clara e inequívoca como tales en el momento de su envío.

5.4.2.4 Contratos digitales

Se establece en esta parte de la normativa, que todos los contratos civiles o comerciales podrán celebrarse validamente por medios digitales y que los mismos deberán realizarse en un ambiente seguro y debidamente certificados. Asimismo se regula la mínima información exigida en el proceso de oferta de bienes y servicios, así como el tratamiento de la documentación comercial no solicitada.

Aquí se velará porque los contratos celebrados por vía electrónica tengan plena validez legal y producirán todos los efectos previstos por el ordenamiento jurídico, conforme a las normas generales relativas a la celebración, la formalización, la validez y la eficacia de los contratos.

Se entenderá por contrato formalizado por vía electrónica el celebrado sin la presencia simultánea de las partes, prestando éstas su consentimiento en origen y en destino por medio de equipos electrónicos de tratamiento y almacenaje de datos, conectados por medio de cable, radio o medios ópticos o electromagnéticos.

Además del cumplimiento de los requisitos en materia de información que se establecerá en la normativa; el prestador de servicios de la sociedad de la información tendrá la obligación, excepto cuando las partes del contrato no sean consumidores o usuarios y acuerden lo contrario, de informar, de manera clara, comprensible e inequívoca y antes de que el destinatario del servicio efectúe la oportuna petición de informar al consumidor o usuario cual es la información requerida de las partes para generar el contrato.

También se definirá el lugar del contrato electrónico, el cual se presume será el lugar celebrado desde, el que el destinatario del servicio efectúe su petición, salvo que ninguna de las partes contratantes sea consumidor o usuario y ambas pacten lo contrario. El lugar de celebración del contrato así determinado, servirá para interpretarlo conforme a los usos y costumbres y para determinar, en su caso, la exigencia de requisitos especiales para su formalización y la jurisdicción competente para conocer de su impugnación o exigir su cumplimiento.

5.4.2.5 Responsabilidad de los prestadores de servicios intermediarios

Se establece la responsabilidad de los prestadores de servicios intermediarios con relación al contenido de las comunicaciones que transmite, el almacenamiento de datos suministrados por sus clientes, el alojamiento de los datos y la supervisión y búsqueda de los datos.

En esta sección, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos administrativos competentes, acceder de forma permanente, fácil y directa a la información general, por ejemplo: su nombre o denominación social, la dirección de su establecimiento, la dirección de su correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva, así como a los datos de su inscripción en el Registro Mercantil y, en su caso, en cualquier otro Registro Público.

También en este apartado, los prestadores de servicios de la sociedad de la información responderán de los daños y perjuicios que causen en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone esta Ley o no actúen con la debida diligencia. La responsabilidad será exigible conforme a las normas generales sobre culpa contractual o extra contractual, según proceda.

5.4.2.6 Protección al consumidor o usuario

Las previsiones contenidas en este apartado de la normativa son vitales para fortalecer la confianza del público en el uso del formato digital para la celebración de actos jurídicos.

En esta sección también tienen mucho que ver los operadores de redes y proveedores de acceso que presten un servicio de la sociedad de la información, que consista en transmitir por una red de comunicación datos facilitados por el destinatario del servicio o en facilitar acceso, no serán responsables por el contenido de la transmisión. Sin embargo, esa responsabilidad si será exigible cuando hayan originado o modificado ellos mismos los datos o seleccionado éstos o a sus destinatarios. No se entenderá por modificación, la operación estrictamente técnica que no altere la integridad de los datos. Las actividades de transmisión y provisión de acceso incluyen el almacenamiento automático, provisional y transitorio de los datos, siempre que sirva exclusivamente para permitir su remisión a través de la red de comunicaciones y que su duración no supere el tiempo razonablemente necesario.

También, los prestadores de un servicio de la sociedad de la información que consista en transmitir por una red de comunicaciones datos facilitados por el destinatario del servicio y que implique su almacenamiento automático, provisional y temporal, realizado con la única finalidad de hacer más eficaz su transmisión ulterior a otros destinatarios del servicio, a petición de éstos, no les será exigible responsabilidad por el contenido de la transmisión, siempre que:

- No modifiquen la información.
- Cumplan las condiciones que permitan el acceso a ella.
- Respeten las normas relativas a la actualización de la información.
- No interfieran en la utilización lícita de tecnología, con el fin de obtener datos sobre la utilización de la información.
- Retiren la información que hayan almacenado, o hagan imposible el acceso a ella.

De esta manera, con los apartados colocados anteriormente, se estará protegiendo la información del usuario y con esto se esta protegiendo al mismo.

5.4.2.7 Régimen de certificaciones

Se establecen las disposiciones generales y de los certificados digitales, regulando las obligaciones del titular del certificado digital como así también los requisitos, contenido, período de validez, equivalencia y homologación de los certificados digitales, regulando la revocación de los certificados digitales.

Regulan los requisitos, funciones, obligaciones y cese de actividad del certificador autorizado. Establecen la autoridad de aplicación en materia de certificación digital. Asimismo, establecen sus funciones, atribuciones, obligaciones y financiamiento. Establecen las sanciones por violación al régimen de certificación y regula el apercibimiento, las multas, suspensiones, cancelaciones como así también la jurisdicción.

5.4.2.8 Otros aspectos

Para la resolución de conflictos se establece el procedimiento de arbitraje para dirimir las controversias que surjan sobre la interpretación o aplicación de la ley. Asimismo se regula el procedimiento de arbitraje.

Tanto para la resolución de conflictos como la vigilancia, el control y la cooperación, así como las sanciones que resulten de la normativa, estos aspectos ya no son técnicos, por lo general son jurídicos y estos ya son los licenciados en leyes los que debe de ver que se regule conforme a derecho, motivo por el cual no se hace referencia de ello en la propuesta.

5.5 Beneficiados en Guatemala

En Guatemala, al poner la ley que proteja el comercio electrónico, se verán beneficiadas las empresas que realicen transacciones por Internet, como los bancos, puesto que la mayoría de estos prestan el servicio de banca electrónica a sus clientes, en las cuales se pueden realizar transacciones monetarias para diferentes servicios; también las empresas de ventas de insumos que ofrecen sus productos por la red, entre ellas se pueden mencionar Paiz S.A., Cemaco S.A. y muchas otras empresas que prestan este tipo de servicio.

Pero los más beneficiados serán los clientes de estas empresas, debido a que desde cualquier lugar podrán realizar sus transacciones sin necesidad de estar físicamente en una sucursal, además tendrán la certeza de que sus bienes estarán seguros y serán entregados como ha sido acordado.

5.6 Modificación y creación de leyes en Guatemala

En el congreso de Guatemala no existe ninguna iniciativa de ley que regule el comercio electrónico. En el Código Penal, en artículo 274 literal e, dicta: "Adicionado por el artículo 16 del decreto 33-96, el cual queda así: Manipulación de información. Se impondrá prisión de 1 a 5 años y multa de 500 a 3000 quetzales al que utilizare registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para la actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar o alterar los estados contables o la situación patrimonial de una persona fiscal o jurídica".[1]

Debido a que ya se tiene un indicio, pero también este es muy limitado en su redacción y contenido de fondo para regular el comercio electrónico, es necesario redactar una iniciativa de ley, la cual debe de tomar en cuenta, todos los aspectos técnicos y jurídicos, en la cual el proveedor se vea comprometido a responder por los daños y perjuicios que ocasione al usuario con el mal manejo de la información que el ha requerido para dicho comercio. Como este comercio se realiza por medio de una red pública, el prestador del servicio debe de ser responsable de crear una aplicación segura, donde tanto el como el usuario tengan la confianza de que una tercera persona no pueda acceder a la información que viaja a través de la misma.

Deberá de crearse un método regulado y autorizado por el Congreso de Guatemala, en el cual el proveedor y el usuario validen por medios digitales las transacciones, estas deberán realizarse en un ambiente seguro y certificado.

---

[1] Código Penal, "Capitulo 7, Artículo 274, literal E".

Ya cuando se establezca esta ley, deberá de perseguirse este delito y tener su debido proceso para que la persona que se encuentre culpable pague por el hecho en el que el haya incurrido.

Como una observación, debería de crearse una ley universal y general que regule las transacciones comerciales electrónicas, puesto que hay que recordar que la ley juzga en el lugar donde se ha cometido el hecho ilícito y no donde se genero el mismo, es decir que un momento dado, se deberá de pedir la extradición de alguna persona. Si esta fuera universal se podría pagar el hecho en el mismo lugar de origen, evitando así muchas costas procesales que con lleva esto.

CONCLUSIONES

1. La problemática de la seguridad en redes públicas en Guatemala, se localiza en que nos encontramos expuestos a los diferentes tipos de ataques que conllevan a delitos y fraudes, debido las vulnerabilidades que se encuentran en la mayoría de los sistemas de información en nuestro país.

2. La seguridad de los sistemas de información se debe de alcanzar utilizando los diferentes servicios a nivel de la arquitectura de de seguridad OSI, así como los mecanismos de seguridad que esta presta, utilizando una fusión entre un grupo de servicios y mecanismos para alcanzar un nivel más alto de seguridad del que pueda prestar en su momento un solo servicio o mecanismo determinado.

3. Las técnicas de criptografía ofrecen seguridad basándose en el cifrado de los mensajes, teniendo la ventaja que aunque la información sea interceptada por terceros, estos no pueden entender el mensaje que se encuentra oculto ya que solo los interesados podrán entenderlo.

4. La firma digital se basa en la técnica de criptografía de claves públicas, debido a que es un método asimétrico, porque se necesitan de dos claves diferentes pero relacionadas, dado que lo que encripta una clave sólo puede ser desencriptada por la correspondiente y no por una clave ajena a ese par.

5. El comercio electrónico es una transacción comercial que se realiza en la red sin la presencia física de los que se ven afectados por la transacción. Ofreciendo la ventaja de no tener fronteras entre los involucrados, pudiendo así realizar compras y ventas a nivel mundial, teniendo un crecimiento en la economía del país.

6. La falta de seguridad en la red y la falta de una legislación en el comercio electrónico que beneficie tanto al consumidor, como al prestador del servicio es la razón por la cual la gente no hace uso del mismo.

7. La normativa de ley del comercio electrónico debe de ir pegada a la normativa de la firma digital, puesto que esta dará la pauta de la seguridad en los documentos y contratos digitales que se utilizarán en las transacciones del comercio electrónico.

RECOMENDACIONES

1. Que se defina a partir de estos aspectos técnicos, una normativa de ley que regule el comercio electrónico en Guatemala, que permita la firma digital en nuestro país para que se puedan generar documentos y contratos digitales, utilizando la última tecnología de seguridad en redes, y con ello conseguir un mejor desarrollo tanto en el nivel económico como tecnológico en el país.

2. Crear conciencia a la población guatemalteca de la importancia de la utilización del comercio electrónico con una ley que vele por los intereses de los involucrados en el mismo, tanto los clientes que van ha tener la seguridad que sus datos van hacer utilizados con el fin con que fueron previstos desde un principio, como para el que presta el servicio, dándole la certeza que no se verá involucrado en ningún problema, si se apega a la las normas que rijan esta ley.

BIBLIOGRAFÍA

1. **Amenazas típicas y tipos de ataques básicos en Internet**
   http://nuyoo.utm.mx/~redii/99/yuri/seguridad.html**.** 10/08/2002.

2. **Anteproyecto de ley de comercio electrónico.**
   http://www.geocities.com/SiliconValley/Network/5054/marcos/directiva/anteproyecto.htm**.** 06/09/2002.

3. **DOCI - 52000PC0384 - bas-ces.**
   http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&numdoc=500PC0384&lg=ES**.** 25/09/2002

4. **Introducción al Comercio Electrónico - ¿Qué es el comercio electrónico?** http//www.sopde.es/cajon/biblioteca/comercio/quees.html. 25/09/2002

5. **Modalidades Comercio Electrónico**
   http://foroconsumo.cepymev.es/ce/modalidades.htm**.** 13/10/2002

6. **Seguridad Comercio Electrónico**
   http://foroconsumo.cepymev.es/ce/seguridad.htm. 13/10/02

7. **Servicios modernos de telecomunicaciones.**
   http://lectura.ilce.edu.mx:3000/sites/ciencia/volumen3/ciencia3/149/htm/sec_9.htm 28/09/2002

8. **Superintendencia de Telecomunicaciones.** http://www.sit.gob.gt/leyes_tele.htm 7/10/2002

9. Asociación de internautas. **Seguridad en la red - asociación de internautas.** http://seguridad.internautas.org/firmae.php 04/08/2002

10. Asociación Provincial de Profesionales en Informática. **Seguridad informática.** http://www.arcride.edu.ar/appei/revistas/r25a1.htm. 28/07/2002

11. Coral Ortiz, Carlos Marlon. **Estudio del impacto de seguridad en el desempeño de Internet.** http://www.canaldigital-web.com/vcanales.php?idarticulo=272&categoria_sel=9**.** 15/08/2002

12. Fernández, M. **Guía legal sobre comercio electrónico.** http://www.expansiondirecto.com/2000/02/10/tecnologia/5tec.html 10/12/2002

13. Fin Mall. **Que es el comercio electrónico.** http://www.finmall.com.mx/comelec.htm 15/11/2002

14. García, Juan L. **Infraestructuras de PKI - Información técnica.** http://www.unicomsecurity.com/informacion/documentacion/informacionTecnica/PKI/infraestructuraPKI.htm 22/08/2002

15. Gonzalo Álvarez, Marañón**. PKI o los cimientos de una criptografía de clave pública** http://www.iec.csic.es/criptonomicon/susurros/susurros11.html 22/08/2002

16. Herrera Joancomartí, Jordi. **Criptografía de clave pública.** http://www.iec.csic.es/criptonomicon/articulos/expertos44.html 25/08/2002

17. Ramos Suarez**,** Fernando **La firma digital: aspectos técnicos y legales.** http://www.marketingycomercio.com/numero14/00abr_firmadigital.htm 18/12/2002

18. Sáenz, María y Nora Galeano. **Estado de las Telecomunicaciones en Centroamérica.** http://www.acceso.or.cr/tecoci/telecom-ca.shtml 15/11/2002