F E S UNAM ACATLAN

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES

"ACATLAN"

T E S I N A

"Análisis de Riesgos y medidas de Seguridad que se deben tener presentes al incursionar en el Comercio Electrónico".

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN MATEMATICAS APLICADAS Y COMPUTACION

P R E S E N T A :

I S A B E L N E R Y V E G A

ASESOR: M. EN C. SARA CAMACHO CANCINO

NAUCALPAN, EDO. DE MEXICO NOVIEMBRE, 2007

AGRADECIMIENTOS

A DIOS: Al Ser Infinito; Creador del Universo, por su mano de amor, misericordia y poder siempre manifiesto en mi vida.

A MI ASESORA DE TESIS: M. en C. Sara Camacho Cancino

Con agradecimiento y respeto por sus sabios consejos y asesoramiento en la elaboración de este trabajo.

A MIS PADRES: Edelmira e Isidro

Con amor, respeto y agradecimiento por su amor, apoyo y sacrificio.

A MI ESPOSO: José de Jesús Gutiérrez Mendoza

Por el apoyo, compañía, amor, aliento y confianza brindados.

A MIS HIJOS: Armando, Danaé y Ariana

Por su cariño e inspiración para la realización de esta meta.

A MIS HERMANOS (AS) y CUÑADOS: Silvia, Toño, Jovis, Rafa, Isidro, Noé, Yolanda, Hortensia, Víctor, Joel y Felicitas

Por el amor, apoyo, sacrificio, aliento y confianza incondicional brindados en todo tiempo.

A MIS AMIGOS:

Por su amistad, apoyo y motivación brindada. Y en especial a Claudia Pasarán

A LA F.E.S. Acatlán Y LA U.N.A.M.:

Por la oportunidad para la realización de mi Carrera Profesional.

A MIS PROFESORES:

Por compartir sus conocimientos profesionales.

ANÁLISIS DE RIESGOS Y MEDIDAS DE SEGURIDAD QUE SE DEBEN TENER PRESENTES AL INCURSIONAR EN EL COMERCIO ELECTRÓNICO

INDICE

INTRODUCCIÓN

En la actualidad, las compañías buscan que sus productos y servicios estén en cualquier lado en donde los compradores potenciales puedan verlos y adquirirlos, además de que sean atractivos y fáciles de comprar.

Dada la importancia que ha tomado el uso de Internet como medio de publicidad para productos, noticias, eventos, servicios, etc., éste resulta ser el lugar indicado para realizar negocios y convertirlo en como actualmente lo llaman: “Mercado Electrónico o Virtual”.

Algunas compañías al darse cuenta de las ventajas que ofrecen los “Negocios Electrónicos” han realizado esfuerzos para tener un sitio en Internet para promocionar y vender sus productos desde este lugar. Estas empresas se han encontrado con problemas al tratar de implantar estos sitios. El problema principal es el de la seguridad de los datos que viajan desde la computadora del cliente hasta el servidor en donde se encuentran instaladas las aplicaciones que soportan la “Tienda Electrónica”, y viceversa.

La seguridad y discreción de estos datos es de suma importancia ya que estos van desde el nombre y referencias personales del cliente, hasta el número de cuenta de sus créditos bancarios, con los cuales se pueden realizar hurtos y fraudes en manos de personas no deseadas.

El objetivo del presente trabajo es mostrar, de manera general, los aspectos más relevantes que se tienen que cubrir en materia de Seguridad para el proceso de compra-venta a través de la Internet: "Comercio Electrónico".

Se mencionan los riesgos a los que son susceptibles las entidades que intervienen en el proceso, así como los mecanismos necesarios para disminuirlos.

También se hace un análisis de los aspectos de seguridad señalados y se definen los riesgos que protege cada uno de éstos. Terminando con una pequeña propuesta de esquema de seguridad para la implantación de un sistema de Comercio Electrónico.

La estructura de lo antes dicho se hace dentro de 4 capítulos, distribuida de la siguiente manera:

En el Capítulo 1 se describirán conceptos de importancia para tener una adecuada compresión sobre el tema. Se menciona que el hacer negocios electrónicamente permite a un negociante tomar fuerza dentro de un mercado, así mismo conceptos claros de Internet para dar origen al Comercio Electrónico.

Por otro lado, en el Capítulo 2 se menciona que no existe una seguridad total en Internet, tanto vendedores como compradores, siempre están cerca de un riesgo que puede ocasionar pérdidas de un lado o del otro, estos riesgos generados por la popularización de Internet y de sus transacciones comerciales. Se presentará también una descripción a detalle de diferentes riesgos que pueden afectar al Comercio Electrónico.

Continuando con el Capítulo 3, sabiendo que la seguridad es un aspecto muy importante para la correcta y segura funcionalidad de las transacciones comerciales electrónicas, se analizarán a detalle algunos sistemas de seguridad. Teniendo como conocer cómo funcionan dichos sistemas para proteger la confidencialidad de la información, o para vigilar lo referente a la protección de los datos, así como la identidad de la fuente y el destinatario; referente a lo dicho se explican métodos de encripción, de firma electrónica, de certificados digitales y protocolos de seguridad

(SET, SSL, EDI). En este mismo capítulo se integrará una explicación de los servidores, considerando aspectos como plataformas de operación (UNIX, NT, Macintosh) y seguridad en su funcionamiento para efectuar una transmisión de datos confiable y seguro.

Actualmente las empresas que manejan el Comercio Electrónico deben contar con sistemas de seguridad para disminuir los riesgos en la transmisión constante de su información o también aún estando fija en un determinado sitio; para esto, el Capítulo 4 englobará una presentación de aquellas técnicas, hardware y software útiles para eliminar los problemas citados, mecanismos como Firewalls para aislar una red de otras, software confiable para realizar transacciones de manera correcta, hardware como servidores de alta disponibilidad para tener una información segura y confiable en el momento preciso para asegurar la continuidad del negocio. Se presentará una lista de productos para ejecutar adecuadamente nuestras transacciones y un costo de software, haciendo una evaluación de todos estos y elaborando una pequeña propuesta de un esquema de seguridad que satisfaga con todos los puntos en donde se necesite reducir o desaparecer un riesgo.

Si bien es cierto que cada día hay gente que conoce más y se involucra con el Comercio Electrónico, también es cierto que cada día habrá gente que le interese y necesite saber al respecto. Y con todo lo anterior, el presente trabajo aportará una base teórica necesaria para todas esas personas y así señalar la importancia de la seguridad para que el Comercio Electrónico sea alcanzado.

CAPITULO I

MARCO TEÓRICO

Hablar de Internet, es hablar de la red mundial de computadoras, a través de la cual llegamos a millones de personas y computadoras en el mundo entero, es una herramienta de comunicación que reporta utilidad en los diferentes ámbitos de la actividad profesional. Por lo general, cada usuario utiliza Internet en función de su trabajo, estudios, comunicaciones, etc. Actualmente las empresas la han aprovechado para lo que se ha llamado “comercio electrónico”.

Este capítulo describe los antecedentes y las características del comercio electrónico, además de definir conceptos importantes que nos ayudan a comprender la importancia de la seguridad en el comercio electrónico.

1.1 Internet

1.1.1 Definición

Internet es la denominación de una red de computadoras a nivel mundial que tienen en común el protocolo TCP/IP.

El éxito de Internet es la libertad que ofrece. No existe ninguna compañía u organización que posea o controle Internet. Las redes que componen Internet pueden tener presidentes o directores ejecutivos, pero en Internet, eso es distinto, no existe la figura de autoridad máxima como un todo. No hay censura, no hay jefes, ni directores ni accionistas. No hay costos por largas distancias, ni costo por tiempo de acceso; el costo solamente depende de la integración de servicios que se desea obtener y su nivel de conexión, es decir, si el enlace es a través de una línea telefónica y un MODEM, o si se realiza un enlace de mayor complejidad, el costo dependerá del equipo que se utilice (estaciones de trabajo, equipo de súper cómputo, etc.) y del tipo de enlace necesario (satelital, fibra óptica, RDI, etc.). Cada organización, grupo o compañía que está conectado a Internet es responsable de sus propias máquinas y su sección de la línea.

1.1.2 Historia de Internet

Internet nació hace cerca de 30 años, surgió por el esfuerzo de interconectar la red ARPAnet del Departamento de Defensa estadounidense con varias redes enlazadas por medio de satélite y de radio. ARPAnet era una red experimental que apoyaba la investigación militar, en particular la investigación de cómo construir redes que soportaran fallas parciales (como las producidas por bombardeos) y aún así funcionar. En el modelo ARPAnet, la comunicación siempre ocurre entre una computadora fuente y una computadora destino. La red asume por sí misma que es falible; cualquier parte de la red puede desaparecer en cualquier momento, cualquier catástrofe por ejemplo.

Para enviar un mensaje en la red, una computadora tiene que poner la información en un sobre, llamado paquete de protocolo internet (IP:Internert Protocol) y le asigna el domicilio o destino en forma correcta. Las computadoras que se comunican tienen la responsabilidad de asegurar que la comunicación se lleve a cabo.

Con estas suposiciones, Estados Unidos fue capaz de desarrollar una red que funcionara (antecesora de la actual internet) y los usuarios que tenían acceso a ella rápidamente se volvieron adictos. La demanda por la red muy pronto se esparció. A pesar de que la Organización de Estandarización Internacional (ISO: Internacional Organization for Standarization) dedicaba una gran parte de tiempo al diseño del último estándar para la comunicación entre computadoras, la gente no podía esperar. Los desarrolladores de Internet en Estados Unidos, el Reino Unido y Escandinava, en respuesta a las presiones del mercado, empezaron a poner el software de IP en todo tipo de computadoras, se llegó a convertir en el único método práctico para comunicar computadoras de diferentes fabricantes.

Al mismo tiempo que Internet se consolidaba las redes locales Ethernet eran desarrolladas. La tecnología de redes locales maduró hasta 1983, cuando aparecieron las primeras estaciones de trabajo para escritorio y las redes locales se multiplicaron. La mayor parte de las Estaciones tenían instalado el software de red IP. Esto creó una nueva demanda; las Organizaciones requerían conectar toda su red local a ARPAnet, lo cual permitiría que todas las computadoras que estuviesen en la red usaran los servicios de ARPAnet.

De estas nuevas redes, una de las más importantes fue la NSFNET, auspiciada por la Fundación Nacional de la Ciencia (NSF: Nacional Science Foundation), una Agencia de Gobierno de Estados Unidos. Al final de los ochenta NSF creó cinco centros de súper cómputo en universidades importantes. Al principio, la NSF trató de utilizar la red de ARPAnet para la comunicación de los centros, pero esta estrategia falló debido a problemas burocráticos.

La NSF decidió construir su propia red basada en la tecnología IP de ARPAnet. Esta red conectaba los centros mediante enlaces telefónicos de 56000bits por segundo. “A partir de entonces” se decidió crear redes regionales. En cada región del país las escuelas podían conectarse a su vecino más cercano. El tráfico en la red se incrementó con el tiempo hasta que las computadoras que la controlaban y las líneas de teléfono conectadas a ellas se saturaron. En 1987 se celebró un contrato para administrar y actualizar la red, con la compañía Merit Network Inc. Que operaba la red educacional de

Michigan, en colaboración con IBM y MCI. La vieja red fue mejorada con líneas telefónicas de mayor velocidad y con computadoras más poderosas.

El aspecto más importante del esfuerzo de conectividad de la NSF fue el hecho de permitir a todos el acceso a la red. Hasta entonces el acceso a la red sólo estaba permitido a investigadores en ciencias computacionales, empleados y contratistas de gobierno. La NSF promovió el acceso universal a las instituciones educativas, financiando conexiones en las universidades únicamente si éstas tenían un plan para permitir el acceso en la zona. De esta manera, toda persona que estuviera inscrita podría ser usuaria de Internet.

Todas las máquinas o nodos en esta creciente red-de-redes fueron divididos en variedades básicas. Algunas computadoras de Estados Unidos y otros países escogieron denominarse por su localización geográfica. Las demás se agruparon dentro de los seis dominios de Internet básicos: gob, mil, edu, com, org y net. Gob., mil y edu denotan instituciones del gobierno, militares y educacionales, las cuales, por supuesto, fueron las pioneras debido a que ARPANET había empezado como un ejercicio de investigación de alta tecnología de seguridad nacional (de los Estados Unidos) . com, sin embargo se utiliza para las instituciones comerciales quienes pronto entraron a la red como furiosa estampida seguida por una gran nube de polvo formada por las organizaciones que no persiguen fines de lucro (org). Las computadoras denominadas .com y .net funcionan como enlaces entre los segmentos de la red.

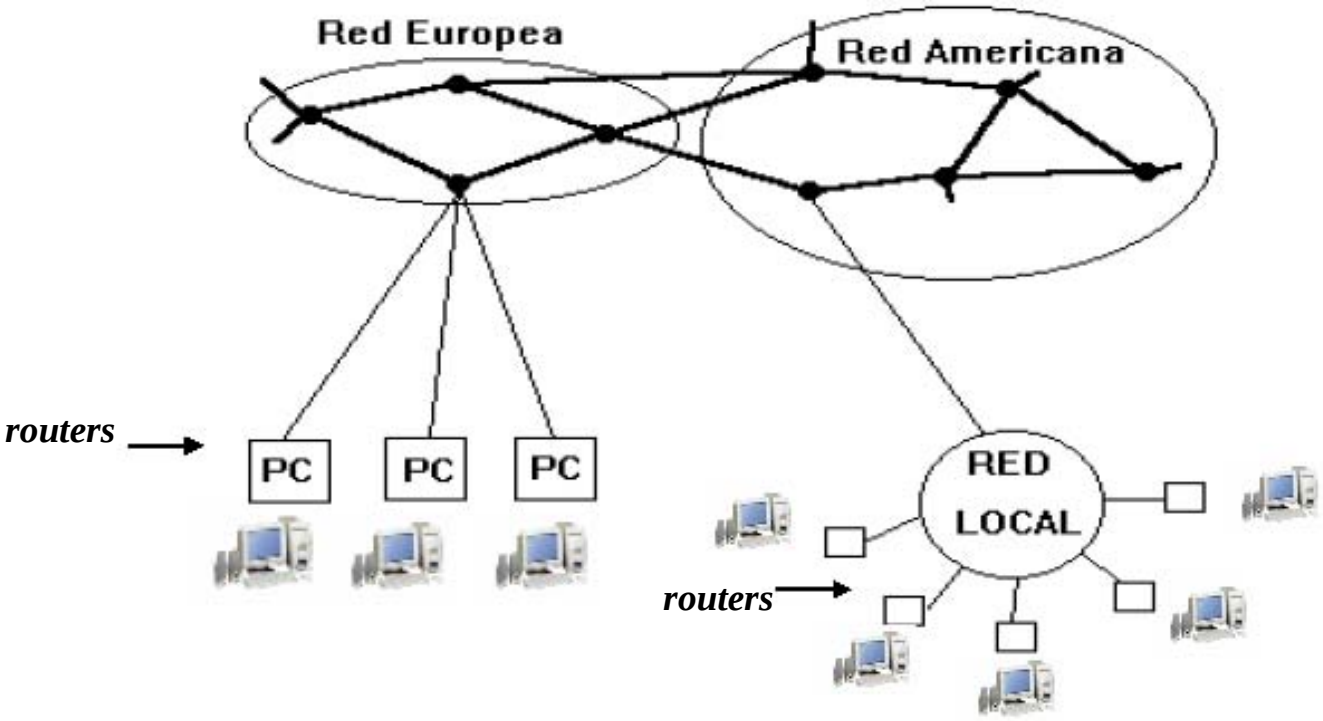
ARPANET por sí misma expiró formalmente en 1989, una víctima feliz de su propio y omnipresente éxito. Sus usuarios apenas y lo notaron, pero las funciones de ARPANET no solo continuaron sino que fueron mejorando a un paso fijo. En el año de 1971, había cuatro nodos en la red ARPANET. El día de hoy existen miles de nodos de Internet alrededor de 42 países y aún más que se ponen en línea cada día. Alrededor de 4 millones (seguramente más) de personas utilizan esta gigantesca madre-de-las-redes actualmente y la demanda sigue creciendo.

1.1.3 Esquema de la Red

Desde el punto de vista puramente físico, Internet puede ser visto como una colección de subredes o Sistemas Autónomos conectados unos a otros. No tiene ninguna estructura real, sino que existen canales principales de comunicación y transmisión (red telefónica u otras). Los canales suelen ser líneas de banda ancha, que permiten la transmisión de gran cantidad de datos, y ser controlados por *router*s.

La conexión tiene una estructura descendente: desde los Canales, a través del *router*, se conecta a una red local y de ahí a los ordenadores individuales.

Cuando nosotros accesamos desde nuestro ordenador a cualquier otro del mundo, lo hacemos a través de nuestro servidor, que es el que nos da acceso a las otras redes locales por medio de los canales. Dentro de cada red local, el *router* se encargará de pasar nuestros mensajes de petición de información a cada dirección (ordenador) especificada. El *router* de cada red local suele ir integrado en el servidor de dicha red, aunque existen *router*s independientes que simplemente dirigen el tráfico, como se muestra en la imagen siguiente.



1.1.4 Funcionamiento de Internet

Todos los nodos de la red son iguales en estatus a los demás nodos, cada nodo con su propia autoridad para generar, pasar y recibir mensajes. Los propios mensajes son divididos en unidades más pequeñas (paquetes), los cuales son direccionados separadamente. Cada paquete puede empezar en algún nodo especificado y finalizar en otro nodo especificado de destino. Cada paquete encontrará su camino a través de la red sobre una base individual.

La ruta particular que el paquete toma no es importante, sólo los resultados finales. Básicamente, el paquete es enviado como una papa caliente de nodo a nodo más o menos en la dirección de su destinatario, hasta que termina llegando al lugar correcto.

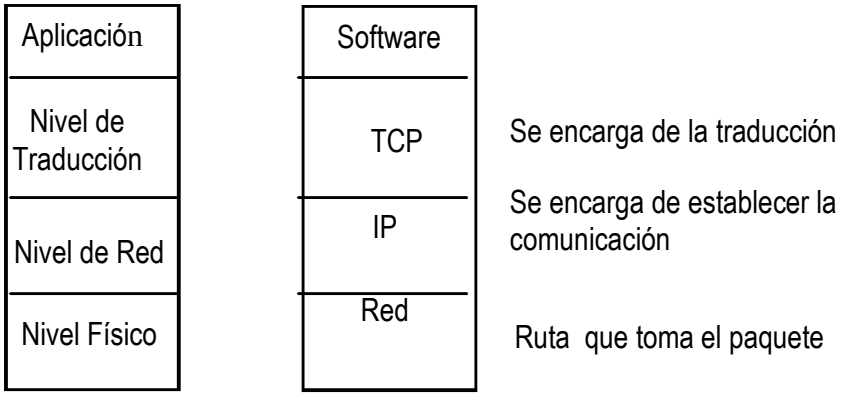
El estándar original de comunicaciones de ARPA (sobre nombre con el que se conocería a ARPANET) se denominaba NCP (Network Control Protocol) pero mientras avanzó el tiempo y con él la tecnología, NCP fue cedido por un estándar más sofisticado de nivel más alto conocido como TCP/IP. La parte TCP (Transmission Control Protocol), convierte los mensajes en flujos de paquetes en el nodo fuente o emisor y los vuelve a ensamblar como mensajes completos en el destinatario. La parte IP (Internet Protocol) maneja el direccionamiento, verificando que los paquetes sean dirigidos por una ruta a través de múltiples nodos y aún a través de múltiples redes con múltiples estándares adicionales, como aquellos diferentes de ARPA desarrollados por otras empresas y organizaciones (algunos ejemplos son Ethernet de IBM y X.25 de la International Standars Organization).

Es un hecho comprobado que una máquina de fax es muy valiosa sólo si todo el resto del mundo también tiene una. Mientras no la tengan, una máquina de fax es sólo una curiosidad. Esta situación se comprobó también con ARPA y su TCP/IP; y la liberación del conjunto de protocolos TCP/IP como un software de dominio público hizo posible que la comunicación por Internet se convirtiera en una necesidad primaria en muchos aspectos.

1.1.5 Protocolos TCP/IP

Se llama protocolo a un conjunto de normas y estándares que sirven para aislar el software particular de cada usuario (nivel de aplicación) de la red (nivel físico), haciendo compatibles distintos ordenadores.

En Internet los protocolos nos sirven de intermediarios entre nuestros programas de correo, navegadores, etc. y red en general, permitiéndonos leer información diversa y con distintos formatos.



1.1.5.1 Protocolo IP

Las siglas IP significan Internet Protocol (Protocolo de Internet), y es el encargado de establecer la comunicación entre los distintos ordenadores. Es el protocolo del llamado nivel de red. Para establecer la comunicación entre dos ordenadores es necesario que ambos tengan asignada una dirección IP. Esta dirección está formada por una serie de 32 bits (unos y ceros), que por comodidad se agrupan en paquetes de 8. Para acortar la notación de ceros y unos, se suele dar cada paquete de 8 bits en notación decimal, y así la dirección:

10000000.00001010.00000010.00011110

Pasa a ser ésta, más sencilla de escribir y recordar: **128.10.2.30**

Los dos primeros grupos describen la red a donde pertenece esta dirección y los dos grupos de la derecha describen la computadora.

Como esta notación no es lo suficientemente cómoda, se suele asignar un nombre significativo a una dirección o red específica.

Así la dirección anterior es, por ejemplo:

www.ucm.es

La traducción entre este formato de texto y los números binarios se realiza a través de las URL (Uniform Resource Locator, localizador uniforme de recursos). La dirección URL, como comúnmente se le llama se compone de:

servicio://tipo_de_servidor.máquina.domino[:puerto] /camino/archivo

Servicio: Indica el tipo de servicio que queremos (http, ftp, gopher, news, telnet, mailto, etc.)

Tipo_de_servidor: indica el tipo de servidor al que accedemos (www para http, ftp para ftp, etc.)

Máquina: indica el servidor que nos da el servicio.

Todas las aplicaciones de Internet permiten el uso de nombres en lugar de una combinación de números para definir los domicilios de las computadoras, solo hay que asegurarse de que nunca dos computadoras de Internet se llamen igual.

Dominio: sirve para localizar más fácilmente el recurso. Nos indica la clase de dirección IP. Puede indicar el país (es: España, us: Estados Unidos, dk: Dinamarca, etc.), o el uso del servidor (com: comercial, org: organización difícil de clasificar, Gob.: instituciones de gobierno, edu: educación y universidades, mil: militar, net: servicios de gestión y mantenimiento de la red).

Camino/archivo: indica el directorio y el archivo pedido.

Dependiendo del tamaño de la red local (y lo que estemos dispuestos a pagar), las direcciones se clasifican en 5 tipos:

- Clase A: Hay 128 redes distintas, con 16 millones de direcciones cada una. En la actualidad se encuentran agotadas.
- Clase B: Hay unas 16.000 redes con 64.000 direcciones cada una. Queda alguna libre pero es difícil obtener una.
- Clase C: Hay unos 2 millones de redes con 256 direcciones. Son las más comunes en empresas, universidades, etc.
- Clase D: Direcciones para multicast
- Clase E: Uso futuro.

Si queremos construir nuestra propia sub-red de Internet, deberemos tener un grupo de direcciones asignadas (generalmente de clase C). Para ello deberemos dirigirnos al NIC (Network Information Center, Centro de Información de la Red).

El intercambio de información en la red se produce mediante paquetes. Un paquete está formado por una cabecera, donde se indican distintas características del paquete, y los datos tal cual del paquete. La longitud máxima del paquete es de 64 k-bytes, y la mínima; debe ser la longitud de la cabecera. Si la información a intercambiar es mayor, se divide ésta en varios paquetes.

La cabecera del protocolo IP tiene el siguiente formato:

VERSIÓN: Versión del Protocolo IP. Actualmente se utilizan la 4 y la 6.
LONCAB: Indica la longitud de la cabecera en múltiplos de 32 bits. Puede ser 5 ó 6, según lleve o no opciones.
TIPO DE SERVICIO: Indica la prioridad, fiabilidad, tipo de transporte, etc.
LONGITUD TOTAL: Indica la longitud del paquete.

IDENTIFICACIÓN: Hace referencia al conjunto total de paquetes que forman la información transferida.

FLAGS: Son 3 bits que funcionan independientemente. El primero, llamado R, esta reservado, valiendo siempre 0. El segundo, llamado D, indica la posibilidad de fragmentación del paquete (1 no se puede, 0 sí). El tercero, llamado M, indica si hay más fragmentos o si es el último. (1 sí los hay, 0 es el último paquete).

NUM. DE PAQUETE: Indica el orden del paquete dentro de la serie.

TIEMPO DE VIDA: Indica el tiempo en saltos (paso de un browser a otro) que el paquete permanecerá en la red sin ser destruido.

PROTOCOLO: Indica el protocolo utilizado a nivel de transporte, en nuestro caso será TCP (TCP=6, UDP=17, etc.)

CONTROL DE CABECERA: Es el resultado de un algoritmo de codificación que nos ayuda a ver si la cabecera ha sido recibida correctamente.

DIRECCIÓN IP DEL REMITENTE: Dirección IP del que manda la información.

DIRECCIÓN IP DE DESTINO: Dirección IP del destinatario.

OPCIONES: Es opcional e indica lo que queramos. El tamaño es variable.

RELLENO: También es opcional y sirve para completar los 32 bits del campo de opciones.

1.1.5.2 Protocolo TCP

El protocolo TCP (Transmission Control Protocol, protocolo de control de la transmisión) es el encargado de establecer la comunicación entre los ordenadores. En concreto se encarga de establecer la conexión, cuidar de la temporización, confirmar al otro *host* que sus datos han llegado bien, colocar los paquetes, verificar el contenido de los datos para evitar errores y, en caso de pérdida, se encargará de retransmitir los paquetes extraviados. Para gestionar todos estos cometidos el protocolo TCP tiene las siguientes propiedades:

Conexión a circuito virtual: Antes de transferir cualquier tipo de datos ha de establecerse la conexión indicando la dirección del *host* al que queremos conectarnos y

que éste nos confirme su *disponibilidad*. Una vez hecho esto puede transferir datos por el circuito virtual (la conexión es como la que se establece vía telefónica, pero la unión es de software, no es por un cable). Para la desconexión han de hacerse otro tipo de confirmaciones similares indicando a cada sistema que el canal de conexión va a quedar libre.

Este tipo de conexión da fiabilidad al sistema. Crea la apariencia de que existe una conexión permanente entre dos aplicaciones, garantizando de esta forma que lo que se transmite de un lado llegue a otro. Transferencia fragmentada: El tamaño de los datos que el paquete TCP puede contener es limitado y por tanto es necesaria la fragmentación.

Conexión en ambos sentidos: Las conexiones del protocolo TCP han de ser en ambos sentidos, permitiendo el intercambio de información en ambos sentidos. Consentimiento mutuo: El *host* remoto es libre de aceptar o no la conexión, luego siempre debe existir un acuerdo mutuo.

El protocolo TCP, como responsable de una correcta comunicación, es el que se va a encargar de fragmentar los datos, y al igual que el protocolo IP, el TCP también añade una cabecera a cada uno de los paquetes de datos. La cabecera está formada por: Protocolo TCP.

PUERTOS FUENTE Y DESTINO: Puertos emisor y receptor.

LCAB: Indica la longitud de la cabecera TCP

RESERV.: Esta serie de bits se reserva para posibles usos futuros.

BITS CÓDIGO (Flags): Conjunto de 6 bits independientes. Cada uno tiene una utilidad. El primero se le llama URG y si esta activado indica que el paquete es urgente. El 2º se llama ACK y si esta activado indica aceptación general (ver más adelante). El 3º se llama PSH e indica que el protocolo TCP receptor ha de juntar todos los trozos antes de entregárselos a la aplicación. El 4º se llama RST e indica que la comunicación se establece de forman anormal. El 5º se llama SYN e indica la petición de

conexión. El 6º se llama FIN e indica el final de la transmisión.

VENTANA: Indica el número identificador del segmento CONTROL DE CABECERA: Es el resultado de un algoritmo de codificación que nos ayuda a ver si la cabecera ha sido recibida correctamente.

PUNTERO URGENTE: Sirve para enviar datos urgentes o fuera de la banda. OPCIONES: Sirve para implementar una serie de opciones del protocolo TCP. Su tamaño es variable.

RELLENO: Sirve para completar el tamaño de 32 bits de la cabecera.

La conexión que establece el protocolo TCP es la llamada conexión a 3 segmentos. Este nombre significa que la conexión se realiza del siguiente modo:

1.1.5.3 Proceso de conexión a 3 segmentos

Detallando la conexión que establece el protocolo TCP, en primer lugar el emisor manda un paquete pidiendo la conexión (flag "syn" activado). Entonces el *host* remoto manda otro aceptando la conexión (flags "syn" y "ack" activados). Cuando el emisor recibe la aceptación de la conexión manda un tercer paquete confirmando la recepción correcta de la aceptación (flag "ack" activado) y empieza a enviar los paquetes de datos.

El envío de los datos se realiza mediante el proceso de las ventanas deslizantes: Se envían los primeros paquetes, por ejemplo del 1 al 8, y según va llegando la confirmación de recepción de éstos se envían los siguientes, es decir, cuando se recibe la confirmación de que ha llegado satisfactoriamente el paquete 1, se manda el 9, cuando llega la confirmación del 2º paquete, se envía el 10°, etc., etc. Si no se recibe la confirmación de algún paquete, el 5 por ejemplo, entonces no se enviarán los siguientes, el 13, 14, etc., sino el 5 de nuevo hasta obtener la confirmación.

La desconexión se realiza de modo similar a la conexión, el emisor manda un paquete de corte de conexión (flag "fin" activado). Cuando el receptor lo recibe manda la confirmación de final, un paquete de aceptación (flag "ack" activado) y otro de fin de su transmisión (flag "fin" activado). Éstos llegan al emisor que manda otra confirmación (flag "ack" activado) y corta la conexión dejando libre ese canal de conexión. Cuando la confirmación llega al receptor, hace lo propio, cortando y liberando la línea.

1.1.6 Servidores y Clientes

En Internet hay dos maneras de ver la red: la de los clientes (nosotros, con nuestra PC) y la de los servidores.

Desde el punto de vista de los usuarios la Web consiste en una vasta colección de documentos distribuidos por todo el mundo, llamados páginas. Cada página contiene links (enlaces) a otras páginas situadas en cualquier parte del mundo a las que el usuario puede acceder dando click con el Mouse, en ese link, y formando así la llamada Web (tela de araña). Para diseñar éstas páginas se utiliza el Hipertexto, que se vera más adelante.

Debido a la particularidad de estas páginas, deben ser vistas con programas especiales llamados browsers (navegadores) como el Netscape o el Explorer. Estos programas se encargan de leer las páginas, interpretar el texto y los comandos, presentándolos al usuario en la pantalla.

La mayoría de las páginas contienen imágenes de gran tamaño que necesitan bastante tiempo para ser leídas. Para visualizarlas se utilizan dos métodos. El primero consiste en visualizarlas según se cargan. El segundo consiste en esperar a cargarlas del todo y entonces se presentan en la pantalla.

No todas las páginas se pueden visualizar de manera convencional. Por ejemplo algunas contienen archivos de audio y/o video.

Para ello los navegadores también se encargan de inicializar los programas necesarios para su reproducción (siempre que se tenga el hardware necesario).

Desde el punto de vista del servidor la red consiste en una gran colección de direcciones, en las que se accede a información pedida por el usuario. Por lo tanto el

servidor debe conectarse con otros servidores utilizando los protocolos necesarios (TCP/IP).

Cada servidor dispone de un puerto TCP (puerto 80) por el que espera las peticiones de los clientes. Cuando un cliente se conecta a un servidor, manda una petición de conexión, y el servidor le responde según vimos en el protocolo TCP. En este caso se utiliza un protocolo llamado HTTP (HiperText Transfer Protocol, protocolo de transferencia de hipertexto) que es el encargado de establecer la comunicación, etc. En definitiva, cumple la función del TCP/IP pero además incluye comandos para interpretar el Hipertexto. No todos los servidores "hablan" HTTP, sino que también los hay FTP (File Transfer Protocol, protocolo de transferencia de archivos), GOPHER, etc.

Los pasos que un servidor debe realizar desde que el usuario pide una página hasta que la visualiza son los siguientes:

1.- El navegador determina la dirección URL.
2.- El browser pide al servidor la traducción a binario de la dirección URL al servicio DNS (encargado de la traducción).
3.- El servidor le manda la dirección binaria.
4.- El navegador realiza una conexión TCP mediante el puerto 80 de la dirección.
5.- Manda la petición de información.
6.- El servidor de la dirección requerida envía el archivo requerido.
7.- La conexión TCP se finaliza.
8.- El navegador interpreta y visualiza el texto, las imágenes, etc.

Los navegadores actuales además de visualizar los archivos nos permiten tener información acerca de la transmisión de los datos, tales como el estado actual de la transmisión y su velocidad.

1.1.7 ¿Qué es http y ftp?

Los protocolos a utilizar en la red son muy diversos; actualmente los dos más utilizados son el http y el ftp, si bien en un principio se empezó utilizando Mosaic y Gopher.

El protocolo estándar de la Web es el HTTP. Contiene dos partes bien distinguidas, una de petición del navegador al servidor, y la segunda la respuesta del servidor al navegador. El mecanismo que sigue este proceso es el indicado en el punto anterior.

Para realizar estas operaciones se basa en una serie de comandos que son realizados por el navegador:

COMANDO	*DESCRIPCIÓN*
GET	Lectura de página.
HEAD	Lectura de encabezado de página.
PUT	Escritura de página. Opuesto a GET.
POST	Anexión de información a un documento.
DELETE	Borrado de una página.
LINK	Conectar dos recursos.
UNLINK	Romper la conexión entre dos recursos.

El otro protocolo utilizado habitualmente es FTP (File Transfer Protocol) es uno más de los componentes del paquete de protocolos TCP/IP. Este protocolo permite la transferencia de archivos de texto en formato ASCII, o binarios; programas ejecutables o archivos de imágenes, voz y/o video, entre dos máquinas pero sin permitir la visualización, obteniendo una mayor rapidez en el proceso. Si nos conectamos a través de un navegador, el uso de ftp es muy sencillo, y basta hacer click con el Mouse para traer automáticamente el archivo a nuestra PC. Pero también es posible la conexión "manual" mediante una serie de comandos similares a los de HTTP.

1.1.8 Paginas WEB

Seguramente cualquier persona que se ha percatado del crecimiento de Internet ha oído hablar del término página web, sitio web o documento web. Aunque parezca que se trate de conceptos diferentes, todos se refieren a un mismo tipo de recurso

disponible en Internet con el cual puede presentarse información a través de una gran variedad de medios que van más allá de simples letras y números.

Es necesario presentar una serie de conceptos adicionales para la mejor comprensión del funcionamiento y características de una página web, que a continuación presentamos:

Navegador o Browser, es un programa de computadora que es una interfaz para la navegación, por Internet. Este software es en realidad el medio más popular para visitar cualquier computadora que esté conectada a la red. Su interfaz con el usuario es de fácil uso y puede incluir gráficos de alta resolución, video y sonido, lo cual lo ha hecho tan famoso (y casi una adicción) entre los usuarios de Internet.

URL o Universal Resource Locator. Cuando escuchamos que alguno de nuestros amigos nos recomienda visitar algún sitio en Intenet, nos dice: ve a la dirección www.unagranpagina.com.mx/aqui/est/loquequieres. ¿Cómo? ¿Que vaya a dónde? La dirección que nos mencionan es un Localizador Universal de Recursos, es decir la dirección en Internet de un recurso almacenado en la computadora que tiene asignada ésa dirección. Un URL es en realidad:

Nombredecomputadora.dominiosysubdominios/directorio

Donde:

nombredecomputadora es el seudónimo con el que se conoce a la computadora en Internet, la convención de usar las letras www, es sólo por costumbre; ya que; la máquina puede tener en realidad otro nombre registrado en su configuración interna.

dominiosysubdominios es el tipo de organización al que pertenece la computadora. La identificación de dominios es también una convención de nombres que sirven únicamente para identificar las organizaciones. Los dominios pueden identificarse con las terminaciones com, edu, gob, mil, net, org y otras más, según los diferentes tipos de organización. Estos dominios y sus denominaciones en Internet están registrados en entidades reguladoras como NIC (Network Information Center), y sus extensiones en otros países; así como la administración de la mencionada ARPA, NSF y otros organismos reguladores regionales en cada país.

Directorio es la ruta o localización específica del recurso dentro de la máquina e incluye el nombre del documento.

www o world wide web o simplemente Web. Es la denominación que mejor define a Internet: una red de cobertura mundial. Accesible a cualquier usuario de una computadora a través de un navegador o browser.

Una vez definidos los conceptos básicos más relacionados con las páginas web, podemos definirlas como: un documento o conjunto de información, que contiene datos de cualquier clase y puede transmitirse y ser visto por Internet con la ayuda de un browser o navegador. Una página web puede localizarse en el Web por medio de un URL, el cual le indica al navegador que documento presentará, así como la computadora y red específica en donde se encuentra.

1.1.8.1 Características

Técnicamente, una página web es únicamente un conjunto de instrucciones que debe ejecutar la computadora para presentar información a través de un navegador de Internet. Pero si en la actualidad existe un gran número de lenguajes de programación, ¿Qué puede tener de especial otro más?

El lenguaje de programación en que se escriben las páginas web se llama HTML (HyperText Markup Languaje) o Lenguaje de Marcación de HiperTexto. El Hipertexto es mejor conocido por aplicaciones como los menús de ayuda de cualquier programa: cuando se despliega una lista de temas, al seleccionar el elegido se despliega en la misma pantalla la información referente a la selección escogida.

Pero lo que hace realmente notable el uso del lenguaje HTML es su facilidad de uso: un programa en HTML puede escribirse en cualquier editor de texto y sin ningún requisito adicional (únicamente una sintaxis correcta), puede ser interpretado por un browser y producir la anhelada página web.

Además, un programa escrito en HTML es capaz de incluir en una página las bondades más impactantes de Internet como gráficos en tercera dimensión o animaciones, video, sonido, trasmisión y recepción de datos, menús gráficos, etc; para crear una interfaz que puede captar inmediatamente la atención del usuario. Esto es lo

que ha hecho que HTML y las páginas web sean el medio por excelencia para la presentación y transmisión de información en la red.

1.1.9 Tiendas Virtuales

Otro concepto que es importante conocer en el tema de comercio electrónico es la llamada tienda o realidad virtual, que a final de cuentas es el medio por el que se lleva acabo el comercio electrónico.

Realidad Virtual: Ambiente creado por un sistema de computación que parece real pero en realidad no existe. ¿Es posible que algo exista y no exista al mismo tiempo? Según Internet y las nuevas tendencias en informática, la respuesta es sí.

Si extendemos el uso de la definición de realidad virtual también podemos crear edificios virtuales, autos virtuales y tiendas virtuales, pero ¿para qué nos sirve una tienda que en realidad no existe? ¿O sí?

Una tienda virtual es en realidad una página web que funciona como tienda: un cliente puede entrar en ella, darle un vistazo a los aparadores y comprar algún artículo que le guste. Este es uno de los enfoques más nuevos y revolucionarios que se ha dado a Internet y a todo el ejército de facilidades de representación de datos que ofrece. En estos días en que las personas están utilizando sus computadoras casi todo el tiempo, es más fácil ofrecerles los productos que necesitan en la comodidad de sus hogares y al alcance de sus ojos: en el monitor de su máquina.

1.1.9.1 Características

Las principales características de una tienda virtual no difieren mucho de las de una tienda o almacén normal y son únicamente el equivalente electrónico de las mismas:

INFRAESTRUCTURA. Incluye el lugar en donde reside la tienda y ofrece los servicios necesarios para albergar a los vendedores y facilitar sus operaciones y las de los clientes. Esta estructura permite al vendedor agregar a la tienda sus propias funciones para personalizar la lógica del negocio a sus necesidades. Todas estas facilidades incluyen generalmente las conexiones para internet, las máquinas donde se almacenan todas las páginas e información referente al negocio.

SOPORTE ADMINISTRATIVO. Incluye la provisión de servicios comunes para los vendedores y clientes como mantenimiento y seguridad. Este soporte es un conjunto de diversos programas que funcionan como herramientas de administración, mantenimiento y control.

PRODUCTOS Y SERVICIOS. Son los bienes tangibles o intangibles objeto de la venta. Así como en una tienda común, en una tienda virtual se pueden establecer precios por diferentes criterios y calcular impuestos y cargos por envío. La mayoría de las tiendas virtuales organizan sus categorías de productos en catálogos que pueden incluir descripciones del producto, imágenes y especificaciones especiales.

COMPRADORES, VENDEDORES Y ADMINISTRADORES. Son los tipos de usuarios de una tienda virtual, cada uno con diferentes funciones según el papel que juegan dentro del proceso de negocio de la empresa. Es importante mencionar que cada uno de los usuarios de la tienda virtual puede acceder a la misma a través del mismo browser de Internet, lo que resulta una estandarización de la herramienta de acceso gracias a su fácil manejo.

1.2 Comercio Electrónico

Es la forma propia de Internet en el que se realiza una transacción económica, compra o venta, de forma ágil, rápida y directa entre comprador y vendedor, favorecida por la comodidad y facilidad de utilización por parte de los usuarios en Internet. La evolución de la informática, y el fin del aislamiento del usuario que ha provocado Internet generan múltiples aplicaciones, que corroboran el futuro de este medio.

1.2.1 Categorías de 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 publican 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 auto-asesoramiento en devoluciones de tasas.

1.2.2 Impacto

El comercio electrónico no es un sueño futurista, sino que está ocurriendo ahora, con algunas actuaciones satisfactorias y bien implantadas. Tiene lugar sobre todo el mundo, y aunque USA, Japón y Europa están lidereando el camino, el comercio electrónico es esencialmente global, tanto en concepto como en realización; va más allá. Con la maduración de EDI (Electronic Data Interchange) y el rápido crecimiento de Internet y la World Wide Web, todo el proceso se está acelerando.

El impacto del comercio electrónico se dejará sentir tanto en las empresas como en la sociedad en general. Para aquellas empresas que exploten completamente su

potencial, el comercio electrónico ofrece la posibilidad de cambios que modifiquen radicalmente las expectativas de los clientes y redefinan el mercado o creen mercados completamente nuevos. Todas las empresas, incluidas aquellas que ignoran las nuevas tecnologías, sentirán el impacto de estos cambios en el mercado y las expectativas de los clientes.

Igualmente, los miembros individuales de la sociedad se enfrentarán con formas completamente nuevas de adquirir bienes y servicios, acceder a la información e interactuar con testamentos gubernamentales. Las posibilidades estarán realmente extendidas y las restricciones geográficas y de tiempo eliminadas. El impacto general en el modo de vida puede ser comparable, se dice, a la implantación, en su momento, de los automóviles o del teléfono.

1.2.3 Ventajas para proveedores y clientes

El comercio electrónico ofrece variadas oportunidades a los proveedores y múltiples ventajas a los clientes/consumidores como las siguientes:

Ventajas para los proveedores	Ventajas para los clientes
* Presencia global	* Cuando no se encuentran cerca del negocio
* Aumento de la competitividad	* Poder comprar en cualquier momento y desde cualquier lugar
* Personalización masiva y amoldamiento	* Con toda comodidad y sin dejar su mesa de trabajo o su salón
* Cadenas de entrega más cortas o inexistentes	* La posibilidad de visitar más de un sitio a la vez.
* Reducción sustancial de costos	* La posibilidad de comparar y/o buscar mas de un artículo a la vez
* Nuevas oportunidades de negocio	
* Medio de publicidad	

Nota: Aunque no siempre el cliente tiene el software/hardware para realizar la compra, a veces se tiene un costo adicional el manejo y envío, y los productos salen mas caros, además del tiempo que tienen que esperar para recibir sus productos.

1.2.4 Ámbito del comercio electrónico

El comercio electrónico no es una tecnología única y uniforme, sino que se caracteriza por su diversidad. Puede implicar un amplio rango de operaciones y transacciones comerciales, incluyendo:

1. Establecimiento del contacto inicial, por ejemplo entre un cliente potencial y un proveedor potencial.
2. Intercambio de información.
3. Soporte pre y posventa (detalles de los productos y servicios disponibles, guía técnica del uso del producto, respuestas a preguntas de adecuación)
4. Ventas.
5. Pago electrónico (usando transferencia electrónica de fondos, tarjetas de crédito, cheques electrónicos, caja electrónica).
6. Distribución, incluyendo tanto gestión de distribución y reparto para productos físicos, como distribución de los productos que puedan ser repartidos electrónicamente).
7. Asociaciones virtuales, grupos de empresas independientes que aúnan sus competencias de manera que puedan ofrecer productos o servicios que van más allá de la capacidad de cada una de ellas individualmente.
8. Procesos empresariales compartidos que son llevados a cabo.
9. Propietarios de una empresa y sus socios.

Igualmente, el comercio electrónico implica un amplio rango de tecnologías de comunicaciones incluyendo correo electrónico, fax, intercambio electrónico de datos (EDI) y transferencia electrónica de fondos (EFT). La elección de unas u otras depende del contexto.

Además es necesario un soporte legal y regulador bien definido que guíe el comercio electrónico, facilitando las transacciones comerciales electrónicas en lugar de imponiendo barreras. De igual forma que la posibilidad de interacción global es uno de los pilares fundamentales del comercio electrónico, este soporte legal y regulador debe ser también de ámbito global.

1.2.5 Niveles del comercio electrónico

Hay distintos niveles para el comercio electrónico, cuyo rango va desde una simple presencia en la red al soporte electrónico de procesos acometidos de forma conjunta por varias empresas.

La mayoría de las veces se distingue entre aquellas operaciones que necesitan transacciones nacionales y las que precisan de transacciones internacionales. Tal distinción no es técnica, ya que como hemos dicho conceptualmente el comercio electrónico es global. El comercio electrónico es más complejo a nivel internacional que a nivel nacional debido a factores como la tasación, las leyes contractuales, las formas de pago y las diferentes prácticas financieras.

Los niveles básicos de comercio electrónico son los que conciernen a la presencia básica en las redes de información, promoción de las empresas, y soporte pre y posventa. Usando las tecnologías disponibles (un simple enlace a través de una línea telefónica y un MODEM o si se realiza un enlace de mayor complejidad) estos niveles pueden ser baratos y fáciles de implantar, como lo pueden atestiguar miles de empresas de todo tamaño que ya los usan.

Por el contrario, las formas más avanzadas de comercio electrónico (como transacciones internacionales u operaciones que requieren transacciones más complejas) suponen problemas complejos de índole más legal o cultural que tecnológica. A estos niveles no hay soluciones estándar, por lo que las empresas se ven forzadas a desarrollar sus propios sistemas a medida, lo que hace que, en la actualidad, las empresas grandes y ricas sean las pioneras en estos niveles. Sin embargo a partir de estas experiencias se irán extrayendo gradualmente soluciones comunes que harán que estos procesos también pasen a formar parte de las tecnologías más usuales, como ha ido ocurriendo con lo que hoy son procesos de los niveles básicos.

1.2.6 Los actores y sus roles

Muchas de las líneas de estudio aún abiertas en el tema del comercio electrónico deben ser resueltas de manera global. Esto hace que entre los actores con responsabilidad para resolverlas y promocionar el comercio electrónico deban incluirse cuerpos multi-nacionales. Igualmente, hay un papel para los gobiernos nacionales que es eliminar las barreras nacionales y asegurar la competencia abierta, y para los sectores representativos promocionando prácticas mejores y de poco costo.

Finalmente, hay un papel obvio para los suministradores de tecnología, las compañías de usuarios y los consumidores individuales en habilitar y explotar el comercio electrónico. En muchos casos cada actor asume responsabilidades en varios roles y a la inversa cada rol es compartido por varios actores.

1.2.7 Seguridad Informática

1.2.7.1 Definición

La seguridad informática es la administración y protección de los recursos de cómputo que tiene la empresa y que accesan los usuarios. (1)

El objetivo es el proteger el patrimonio informático de la Institución, entendiendo por tal, instalaciones, equipos e información, ésta última en todas sus formas (en cualquier dispositivo de almacenamiento magnético como son los disquetes, discos duros, cintas, etc.)

La seguridad Informática debe establecer los controles suficientes para disminuir los riesgos que se generan en el ámbito informático.

1.2.7.2 Importancia

La importancia de seguridad informática se encarga básicamente de llevar a cabo las siguientes tareas:

- Establecer controles para disminuir riesgos.
- Establecer normas, políticas, procedimientos y técnicas para la protección de los bienes informáticos.

1.3 Otras Definiciones Importantes

Riesgo: Proximidad o posibilidad de un daño, peligro, etc. Cada uno de los imprevistos, hechos desafortunados, etc., que puede cubrir un seguro.

Sinónimos: amenaza, contingencia, emergencia, urgencia, apuro. (2)

Encripción: Basada en la criptografía o ciencia de ocultar información. Acto por el cual un mensaje es codificado para transformarse en un mensaje cifrado. (3)

Función resumen o de hash: H es una transformación que, tomando como entrada una cadena x de bits de longitud variable, produce como salida una cadena h de bits de longitud fija (h = H(x)). Una de las aplicaciones criptográficas más importante de las funciones resumen es sin duda la verificación de integridad de archivos.

En un sistema del que tengamos constancia que está `limpio' (esto es, que no ha sido modificado de cualquier forma por un pirata) podemos generar resúmenes de todos los archivos que consideremos clave para el correcto funcionamiento de la máquina y guardar dichos resúmenes - como ya indica su nombre, mucho más cortos que los archivos originales - en un dispositivo de sólo lectura como un CD-ROM. Periódicamente, o cuando sospechemos que la integridad de nuestro entorno ha sido violada, podemos volver a generar los resúmenes y comparar su resultado con el almacenado previamente: si no coinciden, podemos estar seguros (o casi seguros) de que el archivo ha sido modificado.

Para este tipo de aplicaciones se suele utilizar la función resumen MD5 diseñada por Ronald Rivest y que viene implementada `de serie' en muchos clones de Unix, como Solaris o Linux (órdenes `md5' o `md5sum'):

A continuación se muestra como se emplea:

luisa:~$ echo "Esto es una prueba" >/tmp/salida
sluisa:~$ md5sum /tmp/salida
3f8a62a7db3b276342d4c65dba2a5adf /tmp/salida
luisa:~$ echo "Ahora modifico el archivo" >>/tmp/salida
luisa:~$ md5sum /tmp/salida
1f523e767e470d8f23d4378d74817825 /tmp/salida
luisa:~$

Otra aplicación importante de las funciones resumen es la firma digital de mensajes, dado que los algoritmos de firma digital suelen ser lentos, o al menos más lentos que las funciones *hash*, es habitual calcular la firma digital de un resumen del archivo original, en lugar de hacer el cálculo sobre el propio archivo (evidentemente, de tamaño mayor que su resumen). (4)

Firma Digital: Herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, posibilitando que éstos gocen de una característica que únicamente era propia de los documentos en papel. (5) Son una característica de casi todos los sistemas de encripción e involucran dos tipos de claves: 1. Las públicas utilizadas para desencriptar el mensaje y 2. Las privadas para encriptarlo. Para verificar las firmas digitales, las claves deben estar acreditadas y para ello es necesario un depósito donde pueda llevarse a cabo esta comprobación.

Certificado Digital: Es una clave pública y el nombre de su propietario. (6) Este certificado es firmado digitalmente por una autoridad de certificación, cuya clave pública es fácilmente verificable.

Adicionalmente puede contener la fecha de expedición del certificado, la de expiración de la clave, el nombre del notario electrónico que emitió el certificado y un número de serie. De todo ello calcula la huella digital con la función hash adecuada y la cifra con su clave privada

Identificación: La identificación, un subtipo de autentificación, verifica que el emisor de un mensaje sea realmente quien dice ser. (7)

Autentificación: La autentificación va un paso más allá de la identificación al verificar no sólo la identidad del emisor sino también que el mensaje enviado no haya sido alterado. (8)

No Repudio: La no-repudiación es un requerimiento importante en las transacciones comerciales, pues instrumentarla evita que alguien pueda negar haber enviado o recibido ciertos datos o archivos, es similar a enviar una carta certificada con acuse de recibo. (9)

Virus informático: Es un programa elaborado accidental o intencionadamente, que se introduce y se transmite a través de diskettes o de la red telefónica de comunicación entre ordenadores, causando diversos tipos de daños a los sistemas de cómputo. (10)

Sistema de Seguridad: Es el conjunto de software, hardware, políticas y procedimientos, que permitan mantener y garantizar la integridad física de los recursos implicados en la función informática. (11)

Auditoria Informática: Es un proceso formal ejecutado por especialistas del área de auditoria y de informática; (12) se orienta a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología de informática en la organización se lleven a cabo de una manera oportuna y eficiente.

De una manera más sencilla se podría definir como: “La revisión a la suficiencia de controles establecidos en el ámbito de la informática”.

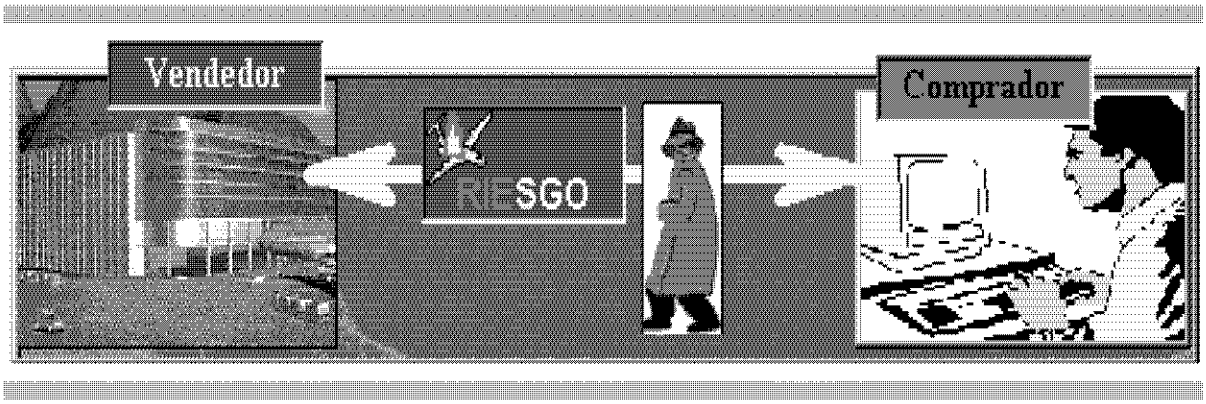
CAPITULO II
RIESGOS DE LA INFORMACIÓN EN EL COMERCIO ELECTRÓNICO

Nadie tiene una seguridad absoluta en Internet, tanto los proveedores como los compradores tienen un riesgo.

Los riesgos a la seguridad relacionados con la tecnología no son nuevos. En 1878 se informó la primera fechoría en cuanto a llamadas telefónicas, apenas dos años después de que se había inventado el teléfono. Sin embargo, la tecnología ofrece medios de transacciones cada vez más seguros. Las técnicas de encripción de datos pueden convertir el comercio electrónico en más seguro que el comercio tradicional basado en tarjetas de crédito.

La dificultad se encuentra en convencer al consumidor digital de que el sitio es realmente seguro así como de que el comercio electrónico también lo es.

Pero también se corre un riesgo cuando se compra en una tienda normal o se come en un restaurante y se paga con la tarjeta de crédito. De hecho existen muchos fraudes al respecto. Cada transacción que se realiza en el comercio tradicional y en el comercio electrónico está expuesta a un riesgo.



Se ha incrementado la variedad y cantidad de usuarios que usan Internet para fines diversos como el aprendizaje, la docencia, la investigación, la búsqueda de socios, búsqueda de mercados (Comercio Electrónico), la práctica política o, simplemente distracción. En medio de esta variedad han ido aumentando las acciones poco respetuosas con la privacidad, autenticación, integridad y con la propiedad de recursos y sistemas. Hackers (persona interesada en las computadoras y que le gusta explorar sistemas), crackers (hackers maliciosos, que infringen la seguridad de un sistema con la finalidad de dañarlo) ... y demás familias han hecho aparición en el vocabulario común de los usuarios y de administradores de redes.

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. Además de las técnicas y herramientas utilizadas, es importante recalcar que una componente muy importante para la protección de los comercios o mercados consiste en la atención y vigilancia continua y detallada por parte de los administradores de la red.

Una vez expuesto en el capítulo anterior algunos conceptos y definiciones que nos permitirán comprender mejor el tema de la seguridad en el comercio electrónico, entramos al tema de los riesgos de la información en el comercio electrónico.

2. 1 Análisis de Riesgos

Al crear una política de seguridad, se debe saber cuáles recursos de la red vale la pena proteger, y entender que algunos son más importantes que otros. El análisis de riesgos implica determinar lo siguiente:

¿Qué necesitas proteger?

¿De quién necesitas protegerlo?

¿Cómo lo proteges?

Este es el proceso de examinar todos los riesgos y de ponderar los diferentes niveles de seguridad que quieres ofrecer. En este proceso hay que tomar decisiones de costo-efectividad de lo que quieres proteger.

Se debe llegar a una situación donde el gasto económico sea mayor para proteger aquello que es menos valioso.

Los posibles riesgos de una red pueden incluir:

- Accesos no autorizados.
- Servicios no disponibles que pueden incluir corrupción de los datos, virus, ...
- Revelación de información confidencial que le pueda dar a alguien alguna ventaja particular como por ejemplo información sobre una tarjeta de crédito.

Esto permitirá la política a seguir en función de los esfuerzos que haya que gastar para proteger los recursos.

En el análisis de riesgos es necesario determinar los siguientes factores:

1. Estimación del riesgo de pérdida del recurso.
2. Estimación de la importancia del recurso.

Otros factores que debe considerar para el análisis de riesgo de un recurso de red son:

su *disponibilidad*,

su integridad y

su carácter confidencial.

Así mismo identificar recursos de red que deben ser considerados al estimar las amenazas a la seguridad general:

- HARDWARE: procesadores, tarjetas, teclados, terminales, líneas de comunicación, enrutadores, etc.
- SOFTWARE: programas fuente, programas objeto, utilerías, programas de comunicación, sistemas operativos, etc.
- DATOS: durante la ejecución, almacenados en línea, bitácora de auditoría, bases de datos, en tránsito sobre medios de comunicación, etc.
- GENTE: usuarios, personas para operar sistemas.
- DOCUMENTACIÓN: sobre programas, hardware, sistemas, procedimientos administrativos locales.
- ACCESORIOS: papel, formas, cintas, información grabada

2.2 Riesgos en la Autenticación de las partes

Las conexiones activas con Internet hacen posible que un intruso capture identidades de usuarios de la red, con lo cual pueden establecerse conexiones a la red interna desde el exterior, aparentemente legales a la vista de los sistemas operativos de red. La identidad de usuarios puede ser utilizada para ejecutar acciones delictivas sobre otras redes.

2.3 Riesgos en la privacidad de la información

La seguridad es un aspecto muy importante debido a que al proveer comunicación con Internet, la empresa se encuentra expuesta a una variedad de ataques a la red interna a nivel de instalaciones, equipos e información concentrada en la misma. Los elementos que conforman este riesgo potencial son:

- Los servicios de mensajería electrónica son vulnerables a ser manipulados, perdiendo la privacidad de los mensajes transmitidos y la legitimidad de los usuarios que intercambian mensajes en el entorno de red.

- La información contenida en bases de datos presentes en la red se encuentra en riesgo de ser capturada por empresas externas.
- Los espacios por donde entrar y salir de la red, son mayores.
- Los recursos accesibles del exterior son considerablemente grandes.
- La importancia que se le da a los datos con posibilidad de ser intrometidos o con posibilidad de robo es mínima.
- Los controles establecidos en la red interna y externa son considerablemente insuficientes.

2.4 Riesgos en la integridad de los mensajes

Los datos contenidos en la red son susceptibles a ser completamente eliminados o modificados.

2.5 Riesgos en la elección de un Software para Comercio Electrónico

1) **Tiempo de entrega:** Uno de los problemas comunes en soluciones de comercio electrónico es que tienden a ser más complicadas de lo que parecen al principio, y a menudo el desarrollador se tarda mucho más en entregarlas. Se debe tomar en cuenta que cada mes de retrazo es un mes sin vender y las utilidades no obtenidas de esas ventas deben ser añadidas al costo final de la solución; también se debe tener la seguridad de contratar con alguien que sabe lo que hace.
2) **El Programa no es robusto:** Es importante asegurar que el programa de comercio electrónico no se 'caiga' o falle cada que sucede algo inusual. En general los paquetes stándard son más robustos que los desarrollos programados desde el principio para su negocio.
3) **El Programa no es seguro:** Si la solución no ofrece transacciones seguras, difícilmente los clientes se arriesgarán a proporcionar sus datos de tarjeta de crédito, la forma más común de pagar en comercio electrónico.
4) **El programa es muy lento:** En general la velocidad de un programa de comercio electrónico depende de su base de datos. Esta debe ser adecuada para el número de productos que usted maneja.

5) **El programa es difícil de mantener y actualizar:** Una buena solución de comercio electrónico debe estar compuesta de dos mitades de igual importancia: una el front-end o lo que ven los consumidores y otra el back-end o lo que solo ve el administrador de la tienda. Esta última parte debe permitirle añadir registros, borrarlos, editarlos, actualizar precios, incorporar nuevas imágenes, variar el diseño e información del sitio, etc. cada que usted lo desee y desde donde usted se encuentre a través de su browser.
6) **El programa se vuelve obsoleto:** El mundo de Internet evoluciona a velocidades vertiginosas. Se debe asegurar que la solución esta siendo continuamente actualizada por la compañía que la desarrolló de tal forma que se pueda realizar un *upgrade* cada determinado tiempo, cada semana por ejemplo.

2.6 Otros Riesgos

Lista de peligros más comunes en sistemas conectados a Internet (que en este trabajo no se explicarán a detalle)

- Un factor que puede limitar el crecimiento electrónico es la falta de recursos e iniciativas. Existe el peligro de que muchas empresas, sobre todo las pequeñas, puedan estar en desventaja simplemente por quedar al margen de este tipo de posibilidades y oportunidades. De aquí que sea una necesidad urgente promover iniciativas, dar publicidad a ejemplos afortunados y promover la formación y el entrenamiento.
  - De todos los problemas, el mayor son los fallos en el sistema de passwords.
  - Los sistemas basados en la autenticación de las direcciones se pueden atacar usando números consecutivos.
  - Es fácil interceptar paquetes UDP (User Datagram Protocol).
  - Los paquetes ICMP (Internet Control Message Protocol) pueden interrumpir todas las comunicaciones entre dos nodos.
  - Los mensajes ICMP Redirect pueden corromper la tabla de rutas.
  - El encaminamiento estático de IP puede comprometer la autenticación basada en las direcciones.
  - Es fácil generar mensajes RIP (Routing Information Protocol) falsos.

- El árbol inverso del DNS (Domain Name System) se puede usar para conocer nombres de máquinas.
- Un atacante puede corromper voluntariamente la caché de su DNS para evitar responder peticiones inversas.
- Las direcciones de vuelta de un correo electrónico no son fiables.
- El programa sendmail es un peligro en sí mismo.
- No se deben ejecutar a ciegas mensajes MIME (Multipurpose Internet Mail Extensions).
- Es fácil interceptar sesiones telnet.
- Se pueden atacar protocolos de autenticación modificando el NTP (Network Time Protocol).
- Finger da habitualmente demasiada información sobre los usuarios.
- No debe confiarse en el nombre de la máquina que aparece en un RPC (Remote Procedure Call).
- Se puede conseguir que el encargado de asignar puertos IP ejecute RPC en beneficio de quien le llama.
- Se puede conseguir, en muchos casos, que NIS (Network Information Service) entregue el archivo de passwords al exterior.
- A veces es fácil conectar máquinas no autorizadas a un servidor NIS.
- Es difícil revocar derechos de acceso en NFS (Network File System).
- Si está mal configurado, el TFTP (Trivial File Transfer Protocol) puede revelar el password.
- No debe permitirse al FTP escribir en su directorio raíz.
- No debe ponerse un archivo de passwords en el área de FTP.
- A veces se abusa de FSP (File Service Protocol), y se acaba dando acceso a archivos a quien no se debe dar.
- El formato de información de www debe interpretarse cuidadosamente.
- Los servidores www deben tener cuidado con los punteros de archivos.
- Se puede usar FTP para crear información de control del gopher.
- Un servidor www puede verse comprometido por un script interrogativo pobremente escrito.

- El MBone (Multicast Backbone)se puede usar para atravesar algunos tipos de firewalls
- Desde cualquier sitio de la Internet se puede intentar la conexión a una estación X11 (X-Server).
- No se debe confiar en los números de puerto facilitados remotamente.
- Es casi imposible hacer un filtro seguro que deje pasar la mayoría del UDP.
- Se puede construir un túnel encima de cualquier transporte.
- Un firewall no previene contra niveles superiores de aquellos en los que actúa.
- Las herramientas de monitoreo de red son muy peligrosas si alguien accede ilegítimamente a la máquina en que residen.
- Es peligroso hacer peticiones de finger (protocolo proporciona información de los usuarios de un máquina) a máquinas no fiables.
- Se debe de tener cuidado con archivos en áreas públicas cuyos nombres contengan caracteres especiales.
- Los caza-passwords actúan silenciosamente.
- Hay muchas maneras de conseguir /copiar el password
- Registrando completamente los intentos fallidos de conexión, se capturan passwords.
- Un administrador puede ser considerado responsable (si se demuestra conocimiento o negligencia) de las actividades de quien se introduce en sus máquinas.

2.7 Fraudes en el Comercio Electrónico

El ciberespacio es un mundo virtual en el que los defectos, miserias y malos hábitos del ser humano se reproducen con la misma fidelidad que las virtudes. El efecto de “global”, generado por la estructura de redes y la proliferación de nodos en todo el planeta ayuda a la difusión inmediata de los mensajes y permite el acceso a cualquier información introducida en la red. A las reconocidas ventajas que ello supone se unen las distorsiones y los malos usos que pueden tener lugar en el sistema y que confirman una vez más que el mal no está en el medio utilizado sino en la persona que lo utiliza.

Existen partidarios de una regulación donde apoyan una tesis de que las redes de telecomunicaciones como Internet han generado un submundo en el que los delitos son difíciles de perseguir debido a la propia naturaleza del entorno y a la falta de tipificación de las modalidades de comisión y de los medios empleados. Entre los delitos, infracciones administrativas y malos usos que se pueden llevar a cabo en la llamada infraestructura de la información, destacan, sin ánimo de clasificarlos, los siguientes:

2.7.1 Delitos tradicionalmente denominados informáticos

A pesar de que el concepto de delito informático engloba tanto los delitos cometidos contra el sistema como los delitos cometidos mediante el uso de sistemas informáticos, cuando hablamos del ciberespacio como un mundo virtual distinto a la "vida real", se habla del delito informático como aquél que está íntimamente ligado a la informática o a los bienes jurídicos que históricamente se han relacionado con las tecnologías de la información: datos, programas, documentos electrónicos, dinero electrónico, información, etc.

Dentro de este tipo de delitos o infracciones se pueden destacar:

Acceso no autorizado: La corriente reguladora sostiene que el uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

Destrucción de datos: Los daños causados en la red mediante la introducción de virus (programas de cómputo diseñados para reproducir copias de sí mismo una y otra vez) , bombas lógicas y demás actos de sabotaje informático no disponen en algunos países de preceptos que permitan su persecución.

Infracción de los derechos de autor: La interpretación de los conceptos de copia, distribución y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial. No existe una opinión uniforme sobre la responsabilidad del propietario de un servicio on-line o de un sysop (operador del sistema) respecto a las copias ilegales introducidas en el sistema. Mientras un tribunal condenó a un sysop porque en su BBS (Bulletin Borrad System) había

imágenes scaneadas de la revista Playboy, en el caso LaMacchia, el administrador del sistema fue hallado no responsable de las copias de programas que albergaba su BBS . El recurso de los propietarios de sistemas on-line y BBS ha sido incluir una advertencia o una cláusula contractual que los exonera de responsabilidad frente a un "upload" de un programa o archivo que infrinja los derechos de autor de terceros.

Infracción del copyright de bases de datos: No existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet. El sistema de protección más habitual es el contratual: el propietario del sistema permite que los usuarios hagan "downloads" de los archivos contenidos en el sistema, pero prohibe el replicado de la base de datos o la copia masiva de información.

Interceptación de e-mail: En este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

Estafas electrónicas: La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra. No obstante seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los casos en los que la operación se hace engañando al ordenador.

Transferencias de fondos: Este es el típico caso en el que no se produce engaño a una persona determinada sino a un sistema informático. A pesar de que en algunas legislaciones y en sentencias aisladas se ha asimilado el uso de passwords y tarjetas electrónicas falsificadas al empleo de llaves falsas, calificando dicha conducta como robo, existe todavía una falta de uniformidad en la materia.

2.7.2 Delitos convencionales

Al hablar de delitos convencionales se refiere a todos aquellos que tradicionalmente se han venido dando en la "vida real" sin el empleo de medios informáticos y que con la irrupción de las autopistas de la información se han reproducido también en el ciberespacio. También en este caso se incluyen actos que no son propiamente delitos

sino infracciones administrativas o ilícitos civiles. No obstante, teniendo en cuenta el carácter global de Internet, alguna de las conductas reseñadas pueden constituir un delito en unos países y en otros no.

Espionaje: Se han dado casos de acceso no autorizado a sistemas informáticos gubernamentales e interceptación de correo electrónico del servicio secreto, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera. Entre los casos más famosos se puede citar el acceso al sistema informático del Pentágono y la divulgación a través de Internet de los mensajes remitidos por el servicio secreto norteamericano durante la crisis nuclear en Corea del Norte en 1994, respecto a campos de pruebas de misiles. Aunque no parece que en este caso haya existido en realidad un acto de espionaje, se ha evidenciado una vez más la vulnerabilidad de los sistemas de seguridad gubernamentales.

Espionaje industrial: También se han dado casos de accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales, fórmulas, sistemas de fabricación y *know how* estratégico que posteriormente ha sido aprovechado en empresas competidoras o ha sido objeto de una divulgación no autorizada.

Terrorismo: La existencia de *hosts* que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo ha podido ser aprovechado por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional. De hecho, se han detectado mensajes con instrucciones para la fabricación de material explosivo.

Narcotráfico: Tanto el FBI como el Fiscal General de los EEUU han alertado sobre la necesidad de medidas que permitan interceptar y descifrar los mensajes encriptados que utilizan los narcotraficantes para ponerse en contacto con los cárteles. También se ha detectado el uso de la red para la transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas. El notable avance de las técnicas de encripción permite el envío de mensajes que, a pesar de ser interceptados, pueden resultar indescifrables para los investigadores policiales. Debe tenerse en cuenta que sólo en 1994 los jueces americanos concedieron 1,154 órdenes de vigilancia electrónica, de las cuales un importante número tuvieron resultado negativo a causa de la utilización de técnicas de

encripción avanzadas. Por ello, tanto el FBI como los fiscales americanos reclaman que todos los programas de encripción generen puertas traseras que permitan a los investigadores acceder al contenido del mensaje.

Otros delitos: Las mismas ventajas que encuentran en Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

2.7.3 Mal uso: cybertorts

Usos comerciales no éticos: Algunas empresas no han podido escapar a la tentación de aprovechar la red para hacer una oferta a gran escala de sus productos, llevando a cabo "mails electrónicos" al colectivo de usuarios de una página web, un nodo o un territorio determinado. Ello, aunque no constituye una infracción, es mal recibido por los usuarios de Internet, poco acostumbrados, hasta fechas recientes, a un uso comercial de la red.

Actos parasitarios*:* Algunos usuarios incapaces de integrarse en grupos de discusión o foros de debate on- line, se dedican a obstaculizar las comunicaciones ajenas, interrumpiendo conversaciones de forma repetida, enviando mensajes con insultos personales, etc. Aunque la mayoría de estas conductas están previstas por los suministradores de servicios on-line, resolviendo el contrato con los reincidentes, existen algunos partidarios de que se establezcan normas para sancionar estos actos.

CAPITULO III

SISTEMAS DE SEGURIDAD PARA LA OPERACIÓN DEL COMERCIO ELECTRÓNICO

Para proteger las comunicaciones de los usuarios a través de una red, es necesario dotar a las mismas con una serie de servicios, que se conocen como **servicios de seguridad** y son:

- **Autenticación de la entidad par**: este servicio verifica la fuente de los datos. La autenticación puede ser sólo de la entidad origen, de la entidad destino o de ambas a la vez.
- **Control de acceso**: este servicio verifica que los recursos son utilizados por quien tiene derecho a hacerlo.
- ***Confidencialidad* de los datos**: este servicio evita que se revelen, deliberada o accidentalmente, los datos de una comunicación.
- **Integridad de los datos**: este servicio verifica que los datos de una comunicación no se alteren, esto es, que los datos recibidos por el receptor coincidan por los enviados por el emisor.

- **No repudio (irrenunciabilidad)**: este servicio proporciona la prueba, ante una tercera parte, de que cada una de las entidades han participado, efectivamente, en la comunicación. Puede ser de dos tipos:
    - **Con prueba de origen o emisor**: el destinatario tiene garantía de quien es el emisor concreto de los datos.
    - **Con prueba de entrega o receptor**: el emisor tiene prueba de que los datos de la comunicación han llegado íntegramente al destinatario correcto en un instante dado.

Para proporcionar los servicios de seguridad citados, es necesario incorporar los siguientes mecanismos de seguridad:

- **Cifrado**: el cifrado puede hacerse mediante el uso de criptosistemas simétricos o asimétricos y puede aplicarse extremo a extremo o a cada enlace del sistema de comunicaciones. El mecanismo de cifrado soporta el servicio de *confidencialidad* de los datos y puede complementar a otros mecanismos para conseguir diversos servicios de seguridad.
- **Firmado digital**: la firma digital se puede definir como un conjunto de datos que se añaden a una unidad de datos de modo que protejan a ésta contra cualquier falsificación, permitiendo al receptor comprobar el origen y la integridad de los datos. Para ello, se cifra la unidad de datos junto con alguna componente secreta del firmante, y se obtiene un valor de control ligado al resultado cifrado. El mecanismo de cifrado digital soporta los servicios de integridad de los datos, autenticación del emisor y no repudio con prueba de origen. Para que se pueda proporcionar el servicio de no-repudio con prueba de entrega, hay que forzar al receptor para que envíe un acuse de recibo firmado digitalmente.
- **Control de acceso**: se usa para autentificar las capacidades de una entidad para acceder a un recurso dado. El control de acceso se puede llevar a cabo en el origen o en un punto intermedio, y se encarga de asegurar que el emisor está

autorizado a comunicarse con el receptor o a usar los recursos de comunicación. El mecanismo de control de acceso soporta el servicio de control de acceso.

- **Integridad de datos**: Hay que distinguir entre la integridad de una unidad de datos individual (un dato) y la integridad de una secuencia de unidades de datos. Para lograr integridad de una unidad de datos, el emisor añade datos suplementarios, estos datos se obtienen en función de la misma unidad y generalmente, se cifran. El receptor genera los mismos datos suplementarios a partir de la unidad original y los compara con los recibidos para verificar la integridad. Por otro lado, para proporcionar integridad a una secuencia de unidades de datos se requiere, adicionalmente, algún mecanismo de ordenación, tal como el uso de números de secuencia o un encadenamiento criptográfico entre las unidades.
- **Intercambio de autenticación**, que tiene dos grados:
    - **Autenticación simple**: el emisor envía su identificador y una contraseña al receptor, el cual los comprueba.
    - **Autenticación fuerte**: utiliza propiedades de los criptosistemas de clave pública. Un usuario se autentifica mediante su identificador y su clave privada. Su interlocutor debe verificar que aquel, efectivamente, posee la clave privada, para lo cual debe obtener, de algún modo, la clave pública del primero. Para ello deberá obtener su certificado. Un certificado es un documento firmado por una Autoridad de Certificación (una tercera parte de confianza) y válido durante el periodo de tiempo determinado, que asocia una clave pública a un usuario.

El mecanismo de intercambio de autenticación soporta el servicio de autenticación de entidad par.

A continuación se describen algunos de los sistemas de seguridad existentes para el comercio electrónico.

3.1 Criptografía como Sistema de Seguridad

La **criptografía** (que, etimológicamente, procede de la raíz griega, *kriptós*, "oculto", y de *grafía*, que significa "escritura oculta") se puede definir como la disciplina que estudia los principios, métodos y medios de ocultar la información contenida en un mensaje.

Es decir, se trata de permitir que dos entidades, ya sean usuarios o aplicaciones, puedan enviarse mensajes por un canal que aunque puede ser intervenido por una tercera entidad, sólo los destinatarios autorizados puedan leer los mensajes.

Pero la criptografía no es en sí seguridad; simplemente es la herramienta utilizada por mecanismos más complejos para proporcionar no sólo *confidencialidad*, sino también otros servicios de seguridad, ya que, en el contexto de Internet, la *confidencialidad* es, a menudo, un factor secundario. Generalmente se está más interesado en el mantenimiento de la integridad de los mensajes y en los mecanismos de autenticación que, implícitamente, proporciona la criptografía. En efecto, un mensaje cifrado sólo puede ser descifrado si la clave que vamos a utilizar para ello pertenece a quien ha cifrado previamente el mensaje.

La criptografía es solo un instrumento. De hecho, durante los últimos diez años se describen vulnerabilidades en algunos sistemas, que podrían haber sido evitadas si el uso de la criptografía hubiese sido generalizado.

La ciencia o arte que se ocupa del estudio sistemático de los métodos de descifrar informaciones cifradas se le denomina **criptoanálisis**, y es practicada por los criptoanalistas (ambas disciplinas, el criptoanálisis y la criptografía se engloban en una rama de las matemáticas conocida como **criptología**, cuyos especialistas son los criptólogos).

La forma en que se emplea la criptografía, es la siguiente:

El texto en claro se representa como M (por *message*) o también por P (de *plain text*). M es simplemente un dato binario. El texto cifrado se designa por C (de *ciphertext*). No existe relación directa entre los tamaños de ambos mensajes. Unas veces su tamaño coincide. Otras, el del texto cifrado es mayor que el del texto en claro. Puede ocurrir, incluso, que el texto cifrado sea de menor tamaño. Esto sucede cuando, además de las técnicas de cifrado, se emplean técnicas de compresión.

La función de cifrado, E, opera sobre M para producir C. En notación matemática:

$$E(M) = C$$

Inversamente, la función de descifrado, D, se aplica a C para producir M:

$$D(C) = M$$

En todo caso, debe cumplirse la siguiente igualdad:

$$D(E(M)) = M$$

Un algoritmo criptográfico es una función matemática utilizada para el cifrado y descifrado de mensajes. Generalmente, hay dos funciones relacionadas: una para el cifrado y otra para el descifrado.

3.1.1 Breve Historia

Los usos más primitivos de la criptografía se encuentran documentados desde la época de Julio César (el cifrado de César, aunque hay constancia también de su uso por persas y espartanos). Estos mecanismos de cifrado se basaban en técnicas de transposición de caracteres y fundamentan su eficacia en el secreto del algoritmo empleado para el cifrado. Algoritmos de este tipo son sólo de interés histórico.

Los algoritmos modernos usan una clave para controlar el cifrado y descifrado de los mensajes. Generalmente, el algoritmo de cifrado es públicamente conocido y sometido a escrutinio por parte de expertos y usuarios. Se acepta, por tanto, la denominada

hipótesis de Kerckhoffs, que establece que la seguridad del cifrado debe residir, exclusivamente, en el secreto de la clave y no en el del mecanismo de cifrado. (13)

3.1.2 Ataques a la criptografía

Una comunicación, protegida o no mediante sistemas criptográficos, está sujeta a una gran variedad de ataques de los cuales es imposible dar una taxonomía completa. Los citados habitualmente son los siguientes:

- **Ataque sólo al criptograma**: es el más desfavorable para el intruso o criptoanalista. En este caso, sólo tiene acceso al texto cifrado. El trabajo del intruso consiste en recuperar el texto en claro de tantos mensajes como sea posible. En tales condiciones, y aunque conociera el algoritmo de cifrado, sólo puede intentar vulnerar dicho algoritmo, realizar un análisis estadístico de los criptogramas o probar todas las claves posibles del algoritmo. Este último caso se conoce como **búsqueda exhaustiva** o también como **ataque basado en fuerza bruta**.
- **Ataque mediante texto en claro conocido**: en este ataque, más ventajoso para el atacante, éste se ha hecho con pares de texto en claro y su equivalente cifrado o ha adivinado, de algún modo, el contenido del mensaje (muchos mensajes cifrados, correspondientes a protocolos normalizados, reproducen la misma estructura o poseen las mismas palabras en los mismos sitios del mensaje). Estas parejas pueden ser usadas para llevar a cabo el criptoanálisis y averiguar la clave, lo cual será útil si se usa la misma clave para posteriores comunicaciones.
- **Ataque mediante texto en claro escogido**: ataque mucho más eficaz que el anterior en el que el intruso es capaz, de algún modo, de conseguir que un texto elegido por él sea cifrado con la clave desconocida. Por tanto hay que diseñar el sistema criptográfico de modo que nunca un intruso pueda introducir mensajes propios.

- **Ataque adaptable mediante texto en claro escogido**: caso especial del anterior en el que el intruso no sólo puede elegir el texto que quiere cifrar, sino que puede tomar decisiones sobre el texto que será cifrado, basadas en resultados anteriores.
- **Ataque mediante criptogramas escogidos**: el atacante puede obtener el descifrado de diversos mensajes cifrados escogidos por él.

Aunque se pueden diseñar otros ataques criptoanalíticos, los citados son los más frecuentes. En el marco de una comunicación entre dos entidades, se puede hablar de los siguientes ataques, que pueden servir para implementar alguno de los anteriores:

- **Escucha pasiva** (*passive eavesdropping*): el intruso simplemente escucha el tráfico que circula por el canal.
- **Tercero interpuesto** (*man-in-the-middle*): el intruso, de alguna forma, se coloca entre los dos interlocutores y hace creer a cada uno de ellos que es su interlocutor.
- **Retransmisión ciega** (*replay*): el intruso intercepta un mensaje legítimo, lo almacena (sin eliminarlo) y lo reenvía un tiempo después.
- **Cortado-y-pegado** (*cut-and-paste*): dados dos mensajes cifrados con la misma clave, a veces es posible combinar partes de los dos para producir uno nuevo. El intruso no sabe lo que dice este nuevo mensaje, pero puede utilizarlo para confundir a los interlocutores legítimos e inducir a alguno de ellos a hacer algo beneficioso para el intruso.
- **Puesta a cero del reloj** (*time-resetting*): en protocolos que utilizan de alguna forma la hora actual, el intruso puede tratar de confundirnos acerca de cuál es la verdadera hora.

3.1.3 Tipos de criptografía

3.1.3.1 Criptografía de clave simétrica

Las técnicas de clave única, secreta o simétrica tienen fundamentos de complejidad diversa, pero todas usan una misma **clave k** que es conocida por el remitente de los mensajes y por el receptor, y mediante la cual se cifra y descifra el mensaje que se quiere proteger (existe una variante según la cual la clave de descifrado puede obtenerse de la de cifrado utilizando unos recursos y en un tiempo razonables).

Los cifradores simétricos pueden dividirse en dos grupos:

- **cifradores de flujo**, los cuales cifran un único bit del texto en claro cada vez.
- **cifradores de bloque**, que toman un grupo de bits (un valor típico es 64 bits) y lo cifran como si se tratase de una unidad.

Las ventajas de la utilización de criptografía de clave simétrica son la existencia de algoritmos muy rápidos y eficientes, especialmente si se implementan en *hardware*. Si k (la clave) es lo bastante larga (típicamente se usan valores de 56 a 128 bits), es imposible reventarlas usando la fuerza bruta.

3.1.3.2 Criptografía de clave asimétrica

El principal inconveniente estriba en la necesidad de que todas las partes conozcan k. Esta clave es distribuida mediante una transacción separada y diferente a la transmisión del mensaje cifrado. Es aquí, precisamente, donde se halla el punto vulnerable del mecanismo: la distribución de la clave. Si la clave es interceptada se pone en peligro todo el mecanismo. La clave debe ser transmitida por un canal que permita asegurar la eficacia del sistema criptográfico. Este canal es generalmente externo a Internet, ya que, en caso contrario, surgiría la pregunta ,Si tenemos un canal seguro, ¿para qué necesitamos criptografía?.

La solución a este problema apareció en 1976. En ese año, Whitfield Diffie y Martin Hellman demostraron la posibilidad de construir sistemas criptográficos que no

precisaban la transferencia de una clave secreta entre emisor y receptor, evitando así los problemas derivados de la búsqueda de canales seguros para tal transferencia. Se trataba de la "criptografía de clave asimétrica o pública".

Como ya hemos señalado anteriormente, el principal problema que presenta el uso práctico de la criptografía de clave simétrica es la distribución de las claves. La criptografía de clave asimétrica o pública, sin embargo, usa claves diferentes para cifrar y descifrar un mensaje. Lo único que se transmite de un usuario a otro es el mensaje cifrado.

Suponiendo un algoritmo de cifrado E y otro de descifrado D, aplicados a un mensaje M con **P clave pública y S clave privada**, debe cumplirse que:

$$D\,(E\,(M, P_i), S_i) = M$$

Suponiendo que Pepe quiere mandarle un mensaje a Manolo:

1. Pepe busca la clave pública de Manolo (P_i).
2. Pepe cifra el mensaje M con la clave pública de Manolo y le envía el resultado, C.

   $$C = E\,(M, P_i)$$
3. Manolo, al recibir el mensaje C lo descifra con su clave privada. $M = D(C, S_i)$

La seguridad de un sistema de este tipo depende de que las funciones de cifrado y descifrado, E y D, cumplan una serie de condiciones:

1. Dados el mensaje M y la clave pública P que vayamos a utilizar, el mensaje cifrado, C, debe ser fácil de calcular.
2. Dado C, el mensaje original, M, no debe ser obtenible de forma sencilla.
3. Dados C y la clave privada, S, debe ser sencillo descifrar el mensaje original.
4. Para que sea práctico el uso de criptografía de clave asimétrica, debe ser sencillo calcular parejas aleatorias de claves P y S.

Aunque Diffie y Hellman definieron los principios de la criptografía de clave asimétrica, fueron Ron Rivest, Adi Shamir y Leonard Adleman, investigadores del MIT,

los primeros que, en 1978, encontraron las funciones que satisfacían los requisitos citados. Nacía así el algoritmo RSA (Rivest-Shamir-Adleman).

La criptografía de clave asimétrica posee, sin embargo, dos inconvenientes:

- El primero se refiere a la velocidad. Los sistemas basados en clave asimétrica son notablemente más lentos que sus equivalentes de clave simétrica (por lo general y como mínimo, unos dos órdenes de magnitud). Por tanto estos sistemas no suelen ser adecuados para el cifrado masivo de datos.
- El segundo está relacionado con la validación de la clave. La discusión sobre la fortaleza de un algoritmo de clave asimétrica es irrelevante sin una discusión previa sobre el protocolo de validación de las claves.

3.1.3.2.1 Autenticación mediante criptografía de clave asimétrica

La criptografía de clave pública puede ser utilizada para identificar sin ambigüedades al remitente de un mensaje. Esto es posible teniendo en cuenta que, si el remitente cifra con su clave privada el mensaje que envía, éste solamente puede ser descifrado en destino utilizando la clave pública del remitente.

Si el mensaje no puede ser descifrado con la clave pública de quien afirma ser el remitente (si el resultado es basura), éste no ha sido el remitente del mensaje. La posibilidad de descifrar el mensaje da prueba fehaciente de la identidad del remitente.

La probabilidad de que dos personas diferentes tengan la misma combinación (clave pública/clave privada) es insignificante.

La desventaja de la utilización de cualquier algoritmo de clave pública es su lentitud, por lo que resulta poco práctico el cifrado asimétrico del mensaje entero.

Códigos de integridad

Como acabamos de señalar, resulta poco práctica la aplicación de técnicas asimétricas a un mensaje entero. En tal caso, se utilizan funciones resumen que derivan

una huella digital (o **MAC**, *Messages Authentication Code*) a partir de un cierto volumen de datos.

Las funciones resumen poseen dos interesantes propiedades. La primera es que su resultado es relativamente corto (típicamente una huella tiene entre 128 y 160 bits). Segundo y más importante, aunque sea teóricamente posible encontrar dos mensajes con idéntica huella, la probabilidad de que ésto ocurra es ínfima. Si se manipulan los datos, la huella cambia. Modificar los datos de forma tan sabia como para obtener la misma huella es algo computacionalmente inabordable.

3.1.4 Uso de funciones resumen para criptografía

3.1.4.1 Funciones resumen (o de hash)

Una función resumen o de *hash* H es una transformación que, tomando como entrada una cadena x de bits de longitud variable, produce como salida una cadena h de bits de longitud fija (h = H(x)). Para que una función de este tipo pueda usarse con propósitos criptográficos, se debe cumplir una serie de requisitos:

1. La entrada puede tener cualquier longitud. Deben proveerse mecanismos para evitar el desbordamiento (*overflow*).
2. La salida debe ser de longitud fija, independientemente de cual fuera la longitud de la entrada.
3. Para cualquier entrada, su resumen (o valor de *hash*) debe ser sencillo de calcular.
4. La función resumen debe ser de un “único sentido”, entendiendo por este concepto que, dado f(x), debe ser computacionalmente difícil encontrar un valor y (tal vez el mismo x) tal que f(y) = f(x).
5. Es difícil encontrar dos entradas x e y, tales que H(x) = H(y).

Al resumen o valor de *hash* de un mensaje *M* se le llama generalmente huella digital de M. Si la salida de la función tiene una longitud de n bits, entonces existen [$k=2^n$] salidas diferentes. Las funciones resumen son también extensivamente utilizadas como parte de los mecanismos que generan números aleatorios.

Ejemplos de funciones resumen usadas en criptografía son **MD2**, **MD4**, **MD5** o **SHA**.

3.1.4.2 Ataque de las funciones resumen

Como se desprende de las condiciones que debe presentar una función resumen, el ataque a dichas funciones puede verse desde dos puntos de vista.

Si, dado un mensaje "x" y su resumen H(x), sólo mediante una búsqueda exhaustiva es posible hallar un mensaje "y" tal que H(x) = H(y), entonces, la función resumen H se denomina **débilmente libre de colisiones**. La búsqueda exhaustiva consiste en calcular el resumen de cada entrada posible "y" hasta que se obtenga el valor H(x) conocido. Este ataque aparece en un escenario con dos actores en el cual una tercera parte intenta engañar a una de las otras calculando una entrada con un valor resumen igual al del mensaje cuyo resumen ha interceptado.

Una función resumen **fuertemente libre de colisiones** es aquella en la que no es posible hallar dos mensajes "x" e "y" tales que H(x) = H (y). En este caso es una de las dos partes implicadas la que trata de engañar a la contraria, tratando de atacar la integridad de los mensajes cuyo resumen se ha calculado.

Generalmente, el ataque a funciones resumen aparece en el primero de los escenarios, en el que se utilizan huellas digitales para firmar un mensaje. Un típico ataque es el conocido como **ataque del cumpleaños**, el cual se basa en una curiosa paradoja, que da nombre al ataque. Se trata de la **paradoja del cumpleaños**, que establece que la probabilidad de que dos o más personas de un grupo de 23 compartan la misma fecha de cumpleaños es mayor que 1/2.

Matemáticamente, suponiendo una función, alimentada con una entrada aleatoria, que produce k salidas equiprobables. Entonces, probando repetidamente diferentes entradas, esperamos obtener la misma salida después de probar $(2k)^{1/2}$ entradas y no, como cabria esperar $k^{1/2}$.

Teniendo en cuenta que $k = 2^n$ (en donde n es la longitud en bits de la salida) debemos elegir valores de n lo suficientemente grandes como para impedir este cálculo inverso.

Estos resultados no son significativos cuando se utiliza una función resumen para otros propósitos. El más usado de estos cometidos es la generación de números aleatorios. El descubrimiento de colisiones en una función no parece afectar de un modo práctico a la utilidad de estas funciones.

Generalmente, las funciones resumen tienen una estructura iterativa fundamentada sobre lo que se conoce como **función de compresión**. La función de compresión toma una entrada de longitud fija y devuelve una salida, también de longitud fija y menor longitud. De este modo, una función resumen puede definirse por medio de una aplicación repetida de la función de compresión hasta procesar el mensaje de entrada completo.

Las **pseudo-colisiones** son colisiones de la función de compresión. Aunque parece lógico que la presencia de colisiones en la función de compresión sean un punto de partida para el análisis de colisiones de las funciones resumen que se deriven de ella, eso no es normalmente posible.

3.1.4.3 Funciones resumen más comunes

MD4 y MD5

MD4 y **MD5** son funciones resumen usadas en criptografía. Su nombre proviene de *Messages Digest* (resumen de mensajes) y fueron diseñados por Ron Rivest. Se emplean fundamentalmente en la generación de huellas digitales de documentos, mensajes de correo electrónico y objetos similares. Los tres algoritmos generan huellas con una longitud de 128 bits.

MD4 fue introducida en 1990 con el objetivo fundamental de ser una función rápida. Sin embargo, ya en 1995 se demostró que era posible hallar colisiones para **MD4** en menos de un minuto utilizando un simple PC. Consecuentemente, **MD4** ya no es considerado seguro.

MD5 es una versión mejorada (aunque algo más lenta) de **MD4**, desarrollada por el propio Rivest en 1991. Su fortaleza es grande, y según su autor, Ron Rivest y dado que la longitud de la salida es 128 bits, la probabilidad de obtener dos mensajes con el

mismo resumen es de 2^{64}, en tanto que la dificultad de obtener un mensaje cuyo resumen sea igual a uno dado es de 2^{128}.

Aunque se ha avanzado en su estudio y se ha demostrado que es posible hallar colisiones para la función de compresión que utiliza el algoritmo, no se ha demostrado que puedan hallarse para el algoritmo entero. De momento es considerado seguro, aunque se recomienda que, "por lo que pudiera pasar", se actualice cualquier producto que lo utilice a otros algoritmos como SHA-1.

Hay que destacar que estos algoritmos se encuentran en el dominio público y por tanto no se ven afectados por problemas de patentes (como ocurre con el algoritmo RSA).

SHA y SHA-1

SHA (*Secure Hash Algorithm*) fue desarrollado en 1993 por NIST (*National Institute for Standards and Technology*) junto con NSA (*National Security Agency*) en EE.UU. para su uso en la norma estadounidense de firma digital, DSS (*Digital Signature Standard*). En 1994, el propio NIST publica una revisión de este último, conocida como **SHA-1**, la cual corrige un defecto no publicado de SHA.

SHA es muy similar en su modo de operación a MD5. Utilizan como entrada mensajes de menos de 2^{64} bits y generan salidas de 160 bits, más largas que las producidas por cualquier otra función resumen utilizada anteriormente. Este algoritmo es ligeramente más lento que MD5, pero la mayor longitud del resumen del mensaje lo hace más seguro frente a la búsqueda de colisiones usando la fuerza bruta.

3.1.5 Aspectos Legales

Los delitos informáticos, también denominados delitos cibernéticos, constituyen un problema tan grave que en la actualidad se realizan reuniones internacionales en las que se analizan y discuten temas tales como la defensa en internet, la seguridad de la información y las necesidades políticas para manejar los negocios en la red.

3.1.5.1 En EE.UU.

Hasta el 31 de diciembre de 1996, los productos criptográficos eran considerados como armas por la legislación de EE.UU. Como tales figuraban en la *Lista de Municiones de EE.UU.* (*U.S. Munition List*). Una serie de leyes como la *Ley de Control de Exportación de Armas*, agrupadas bajo el nombre genérico de *Regulaciones sobre Tráfico Internacional de Armas*, (*International Traffic in Arms Regulations*, ITAR) establecía estrictas limitaciones a la exportación de productos *software* o desarrollos basados en algoritmos de cifrado.

En el caso concreto de productos basados en DES (Data Encryption Standard), la clave de 56 bits se ve acortada a 40 produciéndose una sensible reducción de la seguridad que ofrece este algoritmo. Esto además repercute en el grado de seguridad que ofrece cualquier producto que incorpore este algoritmo. Similares limitaciones se establecían para cualquier otro algoritmo.

La Administración Clinton reconoció la naturaleza comercial de los productos criptográficos, transfiriendo la jurisdicción de la concesión de licencias de exportación del Departamento de Estado al Departamento (ministerio) de Comercio. Junto con esto se ofrece una relajación en las limitaciones a la exportación de productos basados en algoritmos simétricos con clave de 56 bits. Esta relajación tiene una validez de dos años. Todo ello dentro de la ofensiva del gobierno de EE.UU. en favor de sistemas de custodia de claves. De este modo, las licencias eran concedidas si la empresa en cuestión aceptaba desarrollar sistemas de recuperación de claves y apoyaba su uso.

En el caso del algoritmo RSA hay que remarcar que éste ha sido, desde la fecha de su publicación, el único sistema de criptografía de clave pública ampliamente aceptada. El principal inconveniente del sistema es la existencia de una patente sobre este algoritmo, que forza a cualquiera que quiera utilizarlo dentro de EE.UU. a pagar los correspondientes derechos a *RSA Data Security, Inc*. El tema de la exportación sigue los mismos derroteros que en el caso de algoritmos de clave simétrica. El límite en este caso son claves de 512 bits.

3.1.5.2 En Europa

La situación en España

El 8 de abril de 1998 se aprobó la nueva **Ley General de Telecomunicaciones**, regulando todo lo referente a este sector. Durante su elaboración se ha prestado mucha atención a todos los extensos artículos referentes a la televisión por cable, la televisión digital, la telefonía etc. Sin embargo, ha pasado desapercibido un vago e impreciso (y precisamente por esto, peligroso) artículo referente al uso de criptografía en las comunicaciones: el artículo 52.

En el artículo 52 de la Ley General de Telecomunicaciones de España se puede leer lo siguiente:

Artículo 52.Cifrado en las redes y servicios de telecomunicaciones.

1. Cualquier tipo de información que se transmita por redes de telecomunicaciones, podrá ser protegida mediante procedimientos de cifrado. Podrán establecerse condiciones para los procedimientos de cifrado en las normas de desarrollo de esta Ley.

2. El cifrado es un instrumento de seguridad de la información. Entre sus condiciones de uso, cuando se utilice para proteger la *confidencialidad* de la información, se podrá imponer la obligación de notificar bien a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, a efectos de su control de acuerdo con la normativa vigente. Esta obligación afectará a los fabricantes que incorporen el cifrado en sus equipos o aparatos, a los operadores que lo incluyan en las redes o dentro de los servicios que ofrezcan y, en su caso, a los usuarios que lo empleen.

3. Los operadores de redes o servicios de telecomunicaciones que utilicen cualquier procedimiento de cifrado deberán facilitar a la Administración General del Estado, sin costo alguno para ésta y a efectos de la oportuna

inspección, los aparatos decodificadores que empleen, en los términos que se establezcan reglamentariamente.

Cumpliendo con varios acuerdos internacionales, como la **Convención Europea sobre Derechos Humanos** (artículo 8) y la ley de protección de datos (**LORTAD**), la Ley de Telecomunicaciones garantiza la privacidad de las comunicaciones, e incluso el derecho a utilizar criptografía fuerte, tal y como se establece en el primer párrafo.

Sin embargo, la vaga referencia de la sección 2 que establece la posible obligatoriedad de entregar a la Administración "cualquier procedimiento" de cifrado puede ser fácilmente utilizada para autorizar la creación de una ley que establezca un sistema obligatorio de almacenamiento centralizado de claves. Es decir, todo usuario que quiera emplear cualquier software criptográfico debe entregar una copia de su clave privada a una "tercera parte de confianza" que sería un organismo gubernamental, de acuerdo con el artículo 52.

3.1.5.3 A nivel Internacional

La criptografía ha sido y es vista por muchos gobiernos como una grave amenaza a la seguridad nacional. Ello ha llevado a un deseo de controlarla y restringirla.

Una de estas primeras iniciativas fue crear en 1949 el Comité de Coordinación Multilateral para Control de Exportaciones (CoCom). CoCom estuvo formado por los países de la OTAN excepto Islandia, España (por aquel entonces país no miembro de la OTAN), Australia y Japón. La finalidad de este acuerdo era establecer una serie de restricciones que impidieran la transferencia de tecnología sofisticada, entre ella la tecnología criptográfica, a la URSS y a cualquier país de la órbita soviética.

Terminada la Guerra Fría, los países firmantes consideraron que era necesario reorganizar la situación, y tras varios años de negociaciones se llegó a la firma del **Tratado de Wassenaar**. La "renovación" consistió simplemente en admitir a nuevos países en el Tratado. En concreto, los firmantes del acuerdo son:

Alemania, Argentina, Australia, Austria, Bélgica, Bulgaria, Canadá, Corea del Sur, Dinamarca, Eslovaquia, España, Estados Unidos, Finlandia, Francia, Grecia, Holanda, Hungría, Irlanda, Italia, Japón, Luxemburgo, Noruega, Nueva Zelanda, Polonia, Portugal, Reino Unido, República Checa, Rumanía, Rusia, Suecia, Suiza, Turquía y Ucrania.

Siguiendo el Tratado de Wassenaar, sus países miembros establecen restricciones a la exportación de criptografía que pueda considerarse "material de doble uso", es decir, criptografía con uso tanto civil como militar, pero hay una gran variación de políticas. Algunos permiten la exportación bajo autorización, otros imponen restricciones al tipo de criptografía exportada y otros países, como Francia, Rusia, Estados Unidos, Nueva Zelanda y Australia van más allá de los principios recogidos en el tratado e incluyen la criptografía de uso general (programas como por ejemplo, PGP) en las restricciones (como ya hemos citado en el caso de EE.UU.).

En España, la consecuencia directa de este Tratado es el **Reglamento de Comercio Exterior de Material de Defensa y de Doble Uso**, que entró en vigor el 9 de mayo de 1998. En principio sólo regula aquella criptografía que pudiera considerarse de doble uso, sin mencionar la criptografía de uso general.

Los países firmantes del Tratado de Wassenaar se volverán a reunir en noviembre en Viena, tras un encuentro previo en septiembre de un grupo de expertos. Es de temer que debido a las constantes campañas de determinados gobiernos en contra de la criptografía, los "halcones" del Tratado consigan imponer sus puntos de vista y restringir aún más la exportación de criptografía.

3.2 Firma Digital (Electrónica) como Sistema de Seguridad

Las firmas digitales basadas sobre la criptografía asimétrica podemos encuadrarlas en un concepto más general de firma electrónica, que no presupone necesariamente la utilización de las tecnologías de cifrado asimétrico. Aunque, generalmente, varios autores hablan indistintamente de firma electrónica o de firma digital.

Tiene los mismos cometidos que la firma manuscrita, pero expresa, además de la identidad y la autoría, la autentificación, la integridad, la fecha, la hora y la recepción, a través de métodos criptográficos asimétricos de clave pública (RSA, GAMAL,PGP, DSA, LUC, etc.), técnicas de *sellamiento electrónico* y funciones Hash, lo que hace que la firma esté en función del documento que se suscribe (no es constante), pero que la hace absolutamente inimitable como no se tenga la clave privada con la que está encriptada, verdadera atribución de la identidad y autoría.

Para Y. POULLET la firma electrónica supone una serie de características añadidas al final de un documento. Es elaborada según procedimientos criptográficos, y lleva un resumen codificado del mensaje, y de la identidad del emisor y receptor.

Para DEL PESO NAVARRO es una señal digital representada por una cadena de bits que se caracteriza por ser secreta, fácil de reproducir y de reconocer, difícil de falsificar y cambiante en función del mensaje y en función del tiempo, cuya utilización obliga a la aparición de lo que denomina fedatario electrónico o telemático que será capaz de verificar la autenticidad de los documentos que circulan a través de las líneas de comunicación, al tener no solamente una formación informática, sino también jurídica.

Las firmas electrónicas o digitales consisten básicamente en la aplicación de algoritmos de encriptación a los datos, de esta forma, sólo serán reconocibles por el destinatario, el cual además podrá comprobar la identidad del remitente, la integridad del documento, la autoría y autentificación, preservando al mismo tiempo la *confidencialidad*.

La seguridad del algoritmo va en relación directa a su tipo, tamaño, tiempo de cifrado y a la no violación del secreto.

Los criptosistemas de clave pública, son los más idóneos como firma digital, además técnicamente son muy resistentes, se calcula en miles de siglos la duración media que tardaría la computadora más potente para poder romper la clave. Su mecanismo de seguridad se basa sobre todo en el absoluto secreto de las claves privadas, tanto al generarse como al guardarse y en la certificación de la clave pública por la autoridad certificadora.

Entre los objetivos de la firma electrónica está el conseguir una universalización de un estándar de firma electrónica.

3.2.1 Características De La Firma Electrónica

De las anteriores definiciones podemos destacar las siguientes características:

- Debe permitir la identificación del que firma. Entramos en el concepto de "autoría electrónica" como la forma de determinar que una persona es quien dice ser.
- No puede ser generada más que por el emisor del documento, infalsificable e inimitable.
- Las informaciones que se generen a partir de la firma electrónica deben ser suficientes para poder validarla, pero insuficientes para falsificarla.
- La posible intervención del Notario Electrónico mejora la seguridad del sistema.
- La *aposición* de una firma debe ser significativa y va unida al documento a que se refiere.
- No debe existir demora de tiempo ni de lugar entre la aceptación de quien firma y la firma.

3.2.2 Aspectos Legales

3.2.2.1 En México

En México, algunos de los artículos legales reguladores de la firma electrónica son los siguientes:

LMV Ley del Mercado de Valores (Art. 91): "…Las claves de identificación sustituirán a la firma autógrafa… y tendrán igual valor probatorio";

LIC Ley de Instituciones de Crédito (Art. 52): "…El uso de medios de identificación… en sustitución de la firma, producirá los mismos efectos que las leyes otorgan a los documentos…"

NOM El 5 de abril de 1998 se publicó en el Diario Oficial de la Federación el Programa Nacional de Normalización, que incluye el tema: "Uso de Firmas Electrónicas y Certificados Digitales".

Comité EDI Comité EDI México (Junio/'96) presidido por BANXICO, promotor de la normalización en materia del Comercio Electrónico.

3.2.2.2 En Estados Unidos

A finales de la década de los setenta, el gobierno de los Estados Unidos publicó el Data Encryption Standard (DES) para sus comunicaciones de datos sensibles pero no clasificados. El 16 de abril de 1993, el gobierno de los EE.UU. anunció una nueva iniciativa criptográfica encaminada a proporcionar a los civiles un alto nivel de seguridad en las comunicaciones: proyecto Clipper. Esta iniciativa está basada en dos elementos fundamentales:

- Un chip cifrador a prueba de cualquier tipo de análisis o manipulación (el Clipper chip o EES (Escrowed Encryption Standard) y
- Un sistema para compartir las claves secretas (KES -Key Escrow System) que, en determinadas circunstancias, otorgaría el acceso a la clave maestra de cada chip y que permite conocer las comunicaciones cifradas por él.

En EE.UU. es donde más avanzada está la legislación sobre firma electrónica, aunque el proyecto de estandarización del NIST (*The National Institute of Science and Technology*) no lo consiga. El NIST ha introducido dentro del proyecto *Capstone*, . el DSS (*Digital Signature Standard*) como estándar de firma, si bien todavía el gobierno americano no ha asumido como estándar su utilización. El NIST se ha pronunciado a favor de la equiparación de la firma manuscrita y la digital.

La ley de referencia de la firma digital, para los legisladores de los Estados Unidos, es la ABA (*American Bar Association*), Digital Signature Guidelines, de 1 de agosto de 1996.

El valor probatorio de la firma ha sido ya admitido en Utah, primer estado en dotarse de una Ley de firma digital. La firma digital de Utah (Digital Signature Act Utah de 27 de febrero de 1995, modificado en 1996) se basa en un "Criptosistema Asimétrico" definido como un algoritmo que proporciona una pareja de claves segura.

Sus objetivos son, facilitar el comercio por medio de mensajes electrónicos fiables, minimizar la incidencia de la falsificación de firmas digitales y el fraude en el comercio electrónico.

La firma digital es una transformación de un mensaje utilizando un criptosistema asimétrico, de tal forma que una persona que tenga el mensaje cifrado y la clave pública de quien lo firmó, puede determinar con precisión el mensaje en claro y si se cifró usando la clave privada que corresponde a la pública del firmante.

El Estado de Utah ha redactado un proyecto de ley (*The Act on Electronic Notarization*) en 1997.

California define la firma digital como la creación por ordenador de un identificador electrónico que incluye todas las características de una firma válida, aceptable, como:

- única
- capaz de comprobarse
- bajo un solo control
- enlazándose con los datos de tal manera que si se cambian los datos se invalide la firma
- adoptada como un stándar por las organizaciones siguientes:

    - The International Telecommunication Union.
    - The American National Standards Institute.
    - The Internet Activities Board.
    - The National Institute of Science and Technology.
    - The International Standards Organization.

Podemos hacer referencia a:

ABA, Resolution concerning the CyberNotary: an International computer-transaction specialist, de 2 de agosto de 1994.

The Electronic Signature Act Florida, de mayo de 1.996 que reconoce la equivalencia probatoria de la firma digital con la firma manual. En esta ley se usa el término de “international notary” en vez del “cybernotary” utilizado en otras leyes de EE.UU.

The Electronic Commerce Act, de 30 de mayo de 1997, que hace referencia al cybernotary.

The Massachusetts Electronic Records and Signatures Act, de 1996, que acoge todo mecanismo capaz de proporcionar las funciones de la firma manuscrita sin ceñirse a un tipo concreto de tecnología.

3.2.2.3 En Europa

La Comisión Europea está abocada a armonizar los reglamentos sobre Criptografía de todos sus estados miembros. Hasta el momento, sólo algunos países disponen de leyes sobre firma digital y/o cifrada:

En España; La legislación actual y la jurisprudencia, son suficientemente amplias para acoger bajo el concepto de firma y de escrito a la firma digital y a cualquier otro tipo de firma. Cierto es que por razones de seguridad y para ofrecer mayor confianza en los usuarios y jueces que a la postre deben juzgar sobre la firma digital, una reforma de ley cuyo objetivo fuera equiparar la firma manuscrita a cualquier otro medio de firma que cumpliera la misma finalidad , sería una medida positiva.

Bien es verdad que en España el Código de Comercio no exige, por regla general, para una eficacia del contrato o de la factura, la firma ni ningún otro signo de validez, si bien muchos ordenamientos jurídicos requieren que los documentos estén firmados en forma manuscrita -de puño y letra- en orden a solemnizar la transacción o a efectos de su consideración como un documento privado. Se cree que no existe inconveniente alguno en admitir la posibilidad de una firma electrónica.

La Circular del Banco de España 8/88 de 14 de Junio de 1988, creando el reglamento del Sistema Nacional de compensación electrónica, se convirtió en pionera y marcó un hito para la protección y seguridad necesaria en la identificación para el acceso a la información, al indicar que la información se cifrará, para que las entidades introduzcan un dato de autentificación con la información de cada comunicación, a lo que se le reconoce a este método el mismo valor que el que posee un escrito firmado por personas con bastante poder.

El artículo 45 de la Ley 30/1992 de régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común incorporó el empleo y aplicación de los medios electrónicos en la actuación administrativa, de cara a los ciudadanos.

Para su regulación, el Real Decreto 263/1996 de 16 de febrero de 1966, indica que deberán adoptarse las medidas técnicas que garanticen la identificación y la autenticidad de la voluntad declarada, pero no hace ninguna regulación legal de la "firma electrónica".

En Alemania; La ley de firma digital regula los certificados de las claves y la autoridad certificadora. Permite el seudónimo, pero preveé su identificación real por orden judicial. A la firma electrónica se le define como sello digital, con una clave privada asociada a la clave pública certificada por un certificador.

La Ley de 19 de septiembre de 1996 es el primer proyecto de ley de firma digital en Europa. (Entra en vigor el 1 de noviembre de 1997).

En Francia; La nueva Ley de Telecomunicaciones y disposiciones sobre uso interior de cifrado, es la que dispone lo relacionando a las leyes sobre firma digital y/o cifrado.

En Italia; La Ley de 15 de marzo de 1997 número 59, es la primera norma del ordenamiento jurídico italiano que recoge el principio de la plena validez de los documentos informáticos.

Y el reglamento aprobado por el Consejo de Ministros el 31 de octubre de 1997, aunque para el efectivo reconocimiento del valor jurídico de la documentación informática y de las firmas digitales será, necesario esperar a que sea operativo en

virtud de la emanación de los posteriores e indispensables reglamentos técnicos de actuación.

Se define la firma digital como el resultado del proceso informático (validación) basado en un sistema de claves asimétricas o dobles, una pública y una privada, que permite al suscriptor transmitir la clave privada y al destinatario transmitir la clave pública, respectivamente, para verificar la procedencia y la integridad de un documento informático o de un conjunto de documentos informáticos (artículo 1º apartado b) . En el reglamento la firma digital está basada exclusivamente en el empleo de sistemas de cifrado llamados asimétricos. (14)

Regulan la Ley y el Reglamento entre otras cosas: La validez del documento informático; el documento informático sin firma digital; el documento informático con firma digital; los certificadores; los certificados; autentificación de la firma digital; el "cybernotary"; los actos públicos notariales; la validación temporal; la caducidad, revocación y suspensión de las claves; la firma digital falsa; la duplicidad, copia y extractos del documento; y la transmisión del documento.

Esta basada esta normativa en soluciones extranjeras y supranacionales.

En Reino Unido; Hay un vivo debate sobre la posible reglamentación de los *Terceros de Confianza* -TC . Existe un proyecto de ley sobre firma digital y Terceros de Confianza.

En los Países Bajos; Se ha creado un organismo interministerial encargado del estudio de la firma digital.

En Dinamarca, Suiza y Bélgica; Preparan proyectos de ley sobre firma digital.

En Suecia; Organizó una audiencia pública sobre la firma digital en 1997.

En la Comunidad Europea; El artículo 6 del Acuerdo EDI de la Comisión de la Comunidades Europeas, que determina la necesidad de garantía de origen del documento electrónico, no regula la firma electrónica.

La Comisión Europea ha financiado numerosos proyectos (INFOSEC, SPRI, etc.) cuyo objetivo es la investigación de los aspectos técnicos, legales y económicos de la firma digital.

La Comisión Europea hizo pública en octubre de 1997 una Comunicación al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones titulada “Iniciativa Europea de Comercio Electrónico”, con un subtítulo de “Hacia un Marco Europeo para la Firma Digital y el Cifrado”.

En el segundo trimestre del 1998 se deberán encauzar las propuestas para nuevas medidas, una de las cuales podría ser la elaboración de una Directiva de firma digital.

Lo que pretende la Comisión Europea es encontrar un reconocimiento legal común en Europa de la firma digital, con el objeto de armonizar las diferentes legislaciones antes del año 2000, para que ésta tenga carta de naturaleza legal ante tribunales en materia penal, civil y mercantil, a efectos de prueba, apercibimiento y autenticidad.

Para conseguir esa coherencia europea se deberá, sin duda, pasar por el establecimiento de una política europea de control armónica con otras potencias económicas como EE.UU., Canadá y Japón.

3.2.2.4 A nivel internacional

En Naciones Unidas; La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI-UNCITRAL) en su 24º periodo de sesiones celebrado en el año 1991 encargó al Grupo de Trabajo denominado sobre Pagos internacionales el estudio de los problemas jurídicos del intercambio electrónico de datos (EDI: Electronic Data Interchange).

El Grupo de Trabajo dedicó su 24º periodo de sesiones, celebrado en Viena del 27 de enero al 7 de febrero de 1992, a éste tema y elaboró un informe que fue elevado a la Comisión.

Se examinó la definición de “firma” y otros medios de autenticación que se han dado en algunos convenios internacionales. Se tuvo presente la definición amplia de “firma” que se contiene en la Convención de las Naciones Unidas sobre Letra de

Cambio Internacionales y Pagarés Internacionales, que dice: “El término firma designa la firma manuscrita, su facsímil o una autenticación equivalente efectuada por otros medios”. Por el contrario, la Ley Modelo sobre Transferencias Internacionales de Crédito utiliza el concepto de “autenticación” o de “autenticación comercialmente razonable”, prescindiendo de la noción de “firma”, a fin de evitar las dificultades que ésta pueda ocasionar, tanto en la acepción tradicional de este término como en su acepción ampliada.

En su 25º período de sesiones celebrado en 1992, la Comisión examinó el informe del Grupo de Trabajo y encomendó la preparación de la reglamentación jurídica del EDI al Grupo de Trabajo, ahora denominado sobre Intercambio Electrónico de Datos.

El Grupo de Trabajo sobre Intercambio Electrónico de Datos, celebró su 25º periodo de sesiones en Nueva York del 4 al 15 de enero de 1993 en el que se trató de la autenticación de los mensajes EDI, con miras a establecer un equivalente funcional con la “firma”.

El Plenario de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI-UNCITRAL), el 14 de Junio de 1996 en su 29º periodo de sesiones celebrado en Nueva York, examinó y aprobó el proyecto de Ley Modelo sobre aspectos jurídicos de EDI bajo la denominación de Ley Modelo sobre el comercio electrónico. (Resolución General de la Asamblea 51/162 de 16 de diciembre de 1996). El artículo 7 de la Ley Modelo recoge el concepto de firma.

La Comisión encomendó al Grupo de Trabajo, “sobre Comercio Electrónico” que se ocupara de examinar las cuestiones jurídicas relativas a las firmas digitales y a las autoridades de certificación.

La Comisión pidió a la Secretaría que preparara un estudio de antecedentes sobre cuestiones relativas a las firmas digitales. El estudio de la Secretaría quedó recogido en el documento A/CN.9/WG.IV/WP.71 de 31 de diciembre de 1996.

El Grupo de Trabajo sobre Comercio Electrónico celebró su 31º periodo de sesiones en Nueva York del 18 al 28 de febrero de 1997 que trató de fijar las directrices sobre firmas digitales publicadas por la American Bar Association.

El Plenario de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional que celebró su 30º periodo de sesiones en Viena del 12 al 30 de mayo de 1997, examinó el informe del Grupo de Trabajo, hizo suyas las conclusiones y le encomendó la preparación de un régimen uniforme sobre las cuestiones jurídicas de la firma numérica y de las entidades certificadoras.

El artículo 7 de la Ley Modelo sobre Comercio Electrónico (LMCE) regula el equivalente funcional de firma, estableciendo los requisitos de admisibilidad de una firma producida por medios electrónicos, que nos da un concepto amplio de firma electrónica, indicando “cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos: a) si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y b) si ese método es tan fiable como sea apropiado para los fines para los que se creó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acto pertinente”.

El apartado 3 del proyecto de articulo A del WP.71 indica que “una firma digital adherida a un mensaje de datos se considera autorizada si se puede verificar de conformidad con los procedimientos establecidos por una autoridad certificadora”.

3.2.2.5 En la O.C.D.E.

La Recomendación de la OCDE (*Organización para la Cooperación y Desarrollo Económico*) sobre la utilización de criptografía (Guidelines for Cryptography Policy) fue aprobada el 27 de marzo de 1997. Esta recomendación no tiene fuerza vinculante y señala una serie de reglas que los gobiernos debieran tener en cuenta al adoptar legislación sobre firma digital y terceros de confianza, con el fin de impedir la adopción de diferentes reglas nacionales que podrían dificultar el comercio electrónico y la sociedad de la información en general.

En la Organización Internacional de Normas ISO

La norma ISO/IEC 7498-2 (Arquitectura de Seguridad de OSI) sobre la que descansan todos los desarrollos normativos posteriores, regula los servicios de

seguridad sobre *confidencialidad*, integridad, autenticidad, control de accesos y no repudio.

A través de su subcomité 27, SC 27, trabaja en una norma de firma digital.

3.2.3 Uso de la Firma Digital

En general, la forma en que se usa la firma digital en el comercio electrónico, es la siguiente:

1. Se tiene un documento a firmar.
2. Se tiene una clave privada.
3. Se genera un documento firmado.
4. Y con la clave pública y el documento firmado, el receptor del mensaje verifica la autenticidad y la Integridad del documento.

3.2.4 Legalidad De Los Documentos Con Firma Digital

Se plantea el problema de que algunas legislaciones imponen requisitos de escrito y de firma manuscrita como condición de validez o como condición de pruebas de ciertos contratos y actos jurídicos. En consecuencia, para que desde un punto de vista legal estos contratos sean plausibles, o bien la jurisprudencia debe interpretar el término firma y escrito de forma suficientemente amplia para acoger la firma digital, o bien debe modificarse la ley tratando de asimilar la firma digital a la firma manuscrita.

Todavía no se ha probado la validez legal de la firma digital en ninguna vista ante los tribunales de justicia, no existiendo por ello las garantías jurídicas plenas para su uso. No obstante, en entornos criptográficos se considera la firma digital con capacidad superior a la manuscrita, ya que no sólo comporta la autenticidad del documento firmado, sino su integridad; o lo que es lo mismo, la certidumbre de que no ha sido alterado en ninguna de sus partes. Actualmente no existe problema legal para el uso de la firma digital por un grupo de usuarios, siempre que éstos firmen “manualmente” un

acuerdo previo acerca de su uso en sus transacciones comerciales, así como el método de firma y los tamaños (y valores) de las claves públicas a emplear.

3.3 Certificado Digital como Sistema de Seguridad

El grado de seguridad de una red es mayor cuando ésta se controla mediante mecanismos centralizados que cuando se hace de forma distribuida, aunque estos no son aplicables en Internet debido a su naturaleza "anárquica". La solución actualmente empleada se basa en métodos criptográficos asimétricos gestionados por Terceras Partes Confiables (TTP, Trusted Third Parties). Estas entidades permiten garantizar los servicios de *confidencialidad* e integridad de los datos y el no repudio de origen y destino.

Una arquitectura de gestión de certificados ha de proporcionar un conjunto de mecanismos para que la autenticación de emisores y recipientes sea simple, automática y uniforme, independientemente de las políticas de certificación empleadas.

3.3.1 Generación y Distribución de Certificados

Las Autoridades Certificadoras tienen como misión la gestión de los denominados certificados (de clave pública). Un certificado está compuesto básicamente por la identidad de un usuario (subject), su clave pública, la identidad y la clave pública de la Autoridad Certificadora emisora (issuer) del certificado en cuestión, su periodo de validez y la firma digital del propio certificado. Esta firma, realizada por la Autoridad Certificadora emisora, permite que aquellas entidades que deseen realizar comunicaciones con la persona poseedora del certificado, puedan comprobar que la información que éste contiene es auténtica (suponiendo que confíen en la Autoridad Certificadora emisora). Una vez que los certificados han sido firmados, se pueden

almacenar en servidores de directorios o transmitidos por cualquier medio (seguro o no) para que estén disponibles públicamente.

3.3.2 Validación de certificados

Antes de enviar un mensaje encriptado mediante un método asimétrico, el emisor ha de obtener y verificar los certificados de los recipientes de dicho mensaje. La validación de un certificado se realiza verificando la firma digital en él incluida mediante el empleo de la clave pública de su signatario, que a su vez ha de ser validada usando el certificado correspondiente, y así sucesivamente hasta llegar a la raíz de la jerarquía de certificación.

En el proceso de verificación se ha de comprobar el periodo de validez de cada certificado y que ninguno de los certificados de la cadena haya sido revocado, para lo que se utilizan las CRLs (Certificate Revocation Lists), las cuales se explicarán mas adelante.

El esquema global de validación se muestra en la figura 3.1, donde CERT representa el certificado de la raíz de la jerarquía de certificación, firmado por ella misma y que se supone confiable.

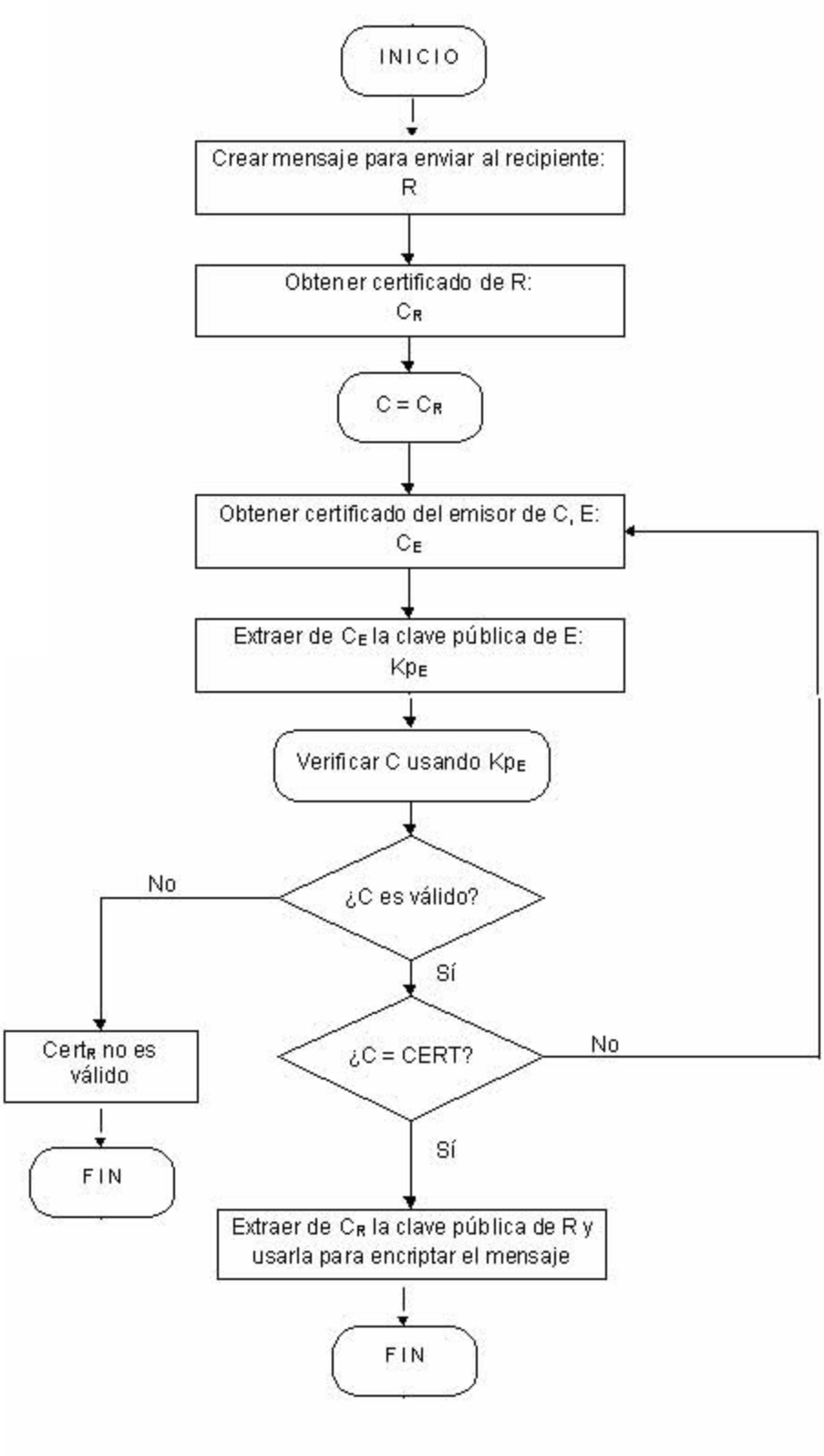


Figura 3.1 - Validación de la cadena de certificados.

Una vez validado el certificado del recipiente, se puede extraer de él la clave pública que será utilizada para realizar la encriptación.

3.3.3 Revocación

Los certificados tienen un periodo de vida limitado, el cual está especificado en el propio certificado y que viene determinado por la política de la Autoridad Certificadora emisora. Sin embargo, en algunas ocasiones especiales la seguridad de la clave privada asociada puede haberse visto comprometida, por lo que la utilización de la correspondiente clave pública ha de ser evitada. En tal caso, la Autoridad Certificadora emisora puede revocar el certificado para prevenir su uso.

3.3.3.1 CRLs

La forma en que las Autoridades Certificadoras indican que un certificado ha sido revocado es generalmente mediante su inclusión en una estructura de datos denominada Lista de Revocación de Certificados (CRL, Certificate Revocation List) [X509]. Estas listas son publicadas cada cierto periodo de tiempo por las Autoridades Certificadoras, firmadas digitalmente por ellas e indican cuales de los certificados que ellas han emitido han sido revocados.

Al igual que ocurre con los certificados y debido a que una CRL está firmada digitalmente por la Autoridad Certificadora emisora, para su distribución por Internet se pueden emplear medios no seguros, ya que antes de utilizarla se ha de realizar un proceso de validación análogo al descrito en el caso de los certificados.

3.3.4 El formato X.509

Describiendo brevemente la estructura de los certificados X.509 versión 3, esta estructura de certificación se basó en la especificación de los certificados X.509 versión 1 y 2; los cuales se consideran deficientes por lo siguiente:

Versión 1, La estructura jerárquica definida requiere que todas las cadenas de certificación comiencen a partir de la raíz, lo que implica que se ha de llegar a ésta cada vez que se realice la validación de un certificado. Esto es demasiado restrictivo, pues generalmente es suficiente (e incluso puede ser más fiable) con que la cadena de certificación comience en una Autoridad Certificadora del dominio local, hecho que facilita también la generación y actualización de claves, certificados y CRLs.
Versión 2, El uso del concepto de PCA (intervención del usuario) requiere del conocimiento del usuario para poder construir la lógica de verificación de las cadenas de certificados, lo que dificulta la automatización de dicho proceso (serio problema en los entornos del comercio electrónico).

Con la versión 3, no hace falta aplicar restricciones sobre la estructura de las Autoridades Certificadoras gracias a la definición de las extensiones de certificados. Se permite que una Organización pueda definir sus propias extensiones para contener información específica dentro de su entorno de operación. Este tipo de certificados es el que usa el protocolo de comercio electrónico SET.

Las extensiones se pueden dividir en críticas y no críticas. Los sistemas que usan los certificados X.509 deben:

- Poder reconocerlos independientemente de su número de versión,
- Determinar si tienen extensiones críticas, y
- Aceptar aquellos que no las tengan, aunque no reconozcan las posibles extensiones no críticas que puedan portar. En el caso de que un certificado posea extensiones críticas que el sistema no reconoce, éste ha de ser rechazado.

3.4 Autoridad o Entidad de Certificación de las claves

La creciente interconexión de los sistemas de información, posibilitada por la general aceptación de los sistemas abiertos, y las cada vez mayores prestaciones de las actuales redes de telecomunicación, obtenidas principalmente de la digitalización, están potenciando formas de intercambio de información impensables hace pocos años.

A su vez, ello está conduciendo a una avalancha de nuevos servicios y aplicaciones telemáticas, con un enorme poder de penetración en las emergentes sociedades de la información. Así, el teletrabajo, la teleadministración, el comercio electrónico, etc., están modificando revolucionariamente las relaciones económicas, administrativas y laborales de tal forma que en pocos años serán radicalmente distintas de como son ahora.

Todos estos nuevos servicios y aplicaciones no podrán desarrollarse en plenitud a no ser que se les dote de unos servicios y mecanismos de seguridad fiables.

Dentro del sistema de seguridad que indicamos, para que cualquier usuario pueda confiar en otro usuario se deben establecer ciertos protocolos. Los protocolos sólo especifican las reglas de comportamiento a seguir.

Existen diferentes tipos de protocolos en los que intervienen terceras partes confiables (Trusted Third Party, TTP, en la terminología inglesa):

- **Los protocolos arbitrados.** En ellos una TPC o Autoridad de Certificación participa en la transacción para asegurar que ambos lados actúan según las pautas marcadas por el protocolo.

- **Los protocolos notariales.** En este caso la TPC, además de garantizar la correcta operación, también permite juzgar si ambas partes actuarán por derecho según la evidencia presentada a través de los documentos aportados por los participantes e incluidos dentro del protocolo notarial. En estos casos, se añade la firma (digital) del notario a la transacción, pudiendo éste testificar, posteriormente, en caso de disputa.

- **Los protocolos autoverificables.** En estos protocolos cada una de las partes puede darse cuenta si la otra actúa deshonestamente, durante el transcurso de la operación.

La firma digital en sí, es un elemento básico de los protocolos autoverificables, ya que no precisa de la intervención de una Autoridad de Certificación para determinar la validez de una firma.

La Autoridad o Entidad de Certificación debe reunir los requisitos que determine la ley, conocimientos técnicos y experiencia necesaria, de forma que ofrezca confianza, fiabilidad y seguridad. Se debería preveer el caso de desaparición del organismo certificador y crear algún registro general de certificación tanto nacional como internacional, que a su vez audite a las entidades encargadas y garantice su funcionamiento. Pues aún se carece de normas que regulen la autoridad o entidad de certificación. Para una certificación de naturaleza pública, el Notario, en el momento de suscribir los acuerdos de intercambio y de validación de prueba, puede generar y entregar con absoluta *confidencialidad* la clave privada.

3.4.1 Criterios que debe seguir la Autoridad o Entidad de Certificación de las claves

El documento WP.71 del 31 de diciembre de 1996 de la Secretaría de las Naciones Unidas indica en su párrafo 44 que las entidades certificadoras deben seguir los siguientes criterios:

- Independencia
- Recursos y capacidad financieros para asumir la responsabilidad por el riesgo de pérdida
- Experiencia en tecnologías de clave pública y familiaridad con procedimientos de seguridad apropiados
- Longevidad
- Aprobación del equipo y los programas
- Mantenimiento de un registro de auditoria y realización de auditorias por una entidad independiente
- Existencia de un plan para casos de emergencia (programas de recuperación en casos de desastres o depósitos de claves)
- Selección y administración del personal
- Disposiciones para proteger su propia clave privada

- Seguridad interna
- Disposiciones para suspender las operaciones, incluida la notificación a los usuarios
- Garantías y representaciones (otorgadas o excluidas)
- Limitación de la responsabilidad
- Seguros
- Capacidad para intercambiar datos con otras autoridades certificadoras
- Procedimientos de revocación (en caso de que la clave criptográfica se haya perdido o haya quedado expuesta)

3.4.2 Tipos de Certificados que emite

Las autoridades de Certificación pueden emitir diferentes tipos de certificados:

- Los certificados de Identidad, que son los más utilizados actualmente dentro de los criptosistemas de clave pública y ligan una identidad personal (usuario) o digital (equipo, software, etc.) a una clave pública.
- Los certificados de Autorización o potestad que son aquellos que certifican otro tipo de atributos del usuario distintos a la identidad.
- Los Certificados Transaccionales son aquellos que atestiguan que algún hecho o formalidad acaeció o fue presenciada por un tercero.
- Los Certificados de Tiempo o estampillado digital de tiempo permiten dar fe de que un documento existía en un instante determinado de tiempo.

El Sector de autoridades de certificación, hasta la fecha, está dominado por entidades privadas americanas, aunque ya existen iniciativas propias de la Unión Europea que se circunscriben a las fronteras de sus países de origen, es decir, sin salir a otros Estados miembros.

El término TTP (Tercera Parte Confiable) al que antes nos referíamos nos indican aquellas asociaciones que suministran un amplio margen de servicios, frecuentemente asociados con el acceso legal a claves criptográficas. Aunque no se descarta que las TTP actúen como Autoridades de Certificación (AC), las funciones de ambas se van

considerando progresivamente diferentes; descartándose la expresión AC para las organizaciones que garantizan la asociación de una clave pública a una cierta entidad, lo que debería excluir el conocimiento por parte de dicha Autoridad de la clave privada; que es justamente lo que se supone debería conocer una TTP.

3.4.3 Uso de la Entidad de Certificaciòn

1. El Usuario genera en su computadora su par de claves (pública y privada) y lleva su Clave Pública a Certificar con un Agente Certificador.
2. El Agente Certificador da fe de que un usuario es realmente quién dice ser y que acepta como suya una clave pública.
3. La Agencia Certificadora se encarga de emitir los certificados definitivos, respecto a sus agentes certificadores y los envía a registrar.
4. La Agencia Registradora mantiene el registro de los certificados emitidos por la Agencia Certificadora y publica la lista de certificados revocados.
5. La Autoridad Registradora Central es el ente regulador del sistema además de mantener un registro central de todas las Claves Públicas emitidas por los participantes.

3.5 EDI (Electronic Data Interchange)

El EDI, o Intercambio Electrónico de Datos, es un procedimiento por el que se busca facilitar el intercambio de datos entre empresas que mantienen una relación comercial, y consiste básicamente en automatizar todo el proceso comercial, de forma que los clásicos papeles como pedidos o facturas ceden su lugar a una serie de archivos codificados que las empresas intercambian entre sí.

De esta forma, se consigue una relación comercial más limpia, eficaz y controlada, ya que el siguiente paso suele ser la integración del sistema EDI con los propios sistemas de producción de la empresa. Como es de suponer, son las empresas de cierto tamaño las que más han apoyado esta forma de intercambio electrónico

(dadas las numerosas ventajas que conlleva: a grandes rasgos, resulta más sencillo, económico y automático), pero poco a poco comienza a notarse un creciente interés por parte de las PYME´s: pequeñas y medianas empresas.

Y es que EDI pretendía -y de hecho lo está consiguiendo-, convertirse en el estándar a seguir en este tipo de comercio. Buena prueba de ello es que las grandes empresas comerciales, para estimular a sus pequeños proveedores, llegan en algunos casos incluso a ofrecer pequeños descuentos a quienes en su interrelación comercial utilicen facturación electrónica EDI, frente a la clásica basada en papel.

3.5.1 Historia

Los principios del EDI se remontan a unos cuantos años atrás, cuando varios grupos de empresas, con relaciones comerciales entre sí, comenzaron a realizar sus pedidos de forma informatizada, en vez de recurrir a la clásica utilización de papel o fax. Se perseguía con ello, una mayor eficacia de los sistemas de comercio y producción, al integrarlos con el resto de los sistemas de información de la empresa.

Desde aquel momento se puede decir que se empezó a hacer EDI, aunque no existía aún un estándar claramente definido, de modo que cada grupo de empresas recurría a utilizar su propio sistema de intercambio de datos. Pero, dicha falta de estandarización se convirtió en un problema a corto plazo, puesto que cada vez era más frecuente que las distintas empresas trabajasen con más de un cliente EDI a la vez, lo que obligaba a soportar simultáneamente los diferentes tipos de comunicación existentes.

Se hizo evidente entonces la necesidad de un organismo internacional, como EAN (iniciales aleatorias), que normalizara los estándares que regulan todo este intercambio comercial, independientemente de la plataforma o aplicación utilizada por cada empresa. Fundada en 1977, EAN INTERNATIONAL es una asociación empresarial de alcance mundial, preocupado por satisfacer la necesidad de un estándar multisectorial de identificación de productos, servicios y ubicaciones, teniendo como base un lenguaje común aceptado internacionalmente.

En España, la asociación que desde el principio ha tomado las riendas del estándar EDI ha sido AECOC (*Asociación Española de COdificación Comercial*), una de las encargadas de gestionar la implantación del estándar en todas las herramientas, sirviendo de entidad certificadora de que las aplicaciones cumplen el estándar EDI.

Aunque sí es la que más se ha preocupado de aspectos tales como calidad y certificación, AECOC no es la única que se ha encargado de gestionar la implantación del EDI, ya que por ejemplo Odette (que depende de la Asociación Nacional de Fabricantes de Automóviles y Camiones, ANFAC) se encarga de normalizar para el sector de automoción.

3.5.2 Funcionamiento de EDI

La mejor forma de explicar y comprender el funcionamiento del EDI, es la utilización de un ejemplo práctico.

Suponiendo que una gran superficie comercial, como un supermercado o unos grandes almacenes, decide comenzar a utilizar el intercambio electrónico de datos. Para ello, informatiza toda su empresa, llevando en sus computadoras un control de stock, de modo que en todo momento se sepa la cantidad de unidades de cada producto, que quedan en el almacén.

Cada vez que un cliente adquiere un producto y pasa por caja, automáticamente se da de baja dicho producto en el control de stock. La aplicación, cuando detecte que quedan pocas unidades de cierto producto, también automáticamente dará la orden para realizar un pedido de nuevas unidades de dicho producto. Hasta aquí, ningún cambio con un sistema de gestión, control de stocks y facturación «clásico». Ahora bien, dependiendo del producto, el pedido se realizará a un proveedor u otro, controlando la aplicación, en todo momento, a quién pedir cada cosa. Es en este momento cuando entra en juego el EDI.

Antiguamente, para la realización del pedido, la aplicación «avisaba» al encargado del departamento, quien a su vez se encargaba de ponerse en contacto, por carta o fax, con la empresa proveedora. Sin embargo, con EDI, es la propia aplicación informática la que se encargará de realizar el pedido al proveedor, mediante un formato estándar. El

proveedor recibirá dicho archivo EDI y, automáticamente, realizará el envío del producto reclamado, generando el correspondiente albarán. Además, la aplicación del proveedor generará automáticamente una factura electrónica, que será remitida al cliente también mediante EDI (a la vez que impresa en papel, si éste lo desea).

Como se puede observar, con la utilización de EDI se abaratan costos y se simplifica la labor de pedidos y distribución, dado que todo el proceso lo realizan las aplicaciones informáticas de forma automática, sin necesidad de hablar telefónicamente con el proveedor, o de tener que pasar por fax los pedidos y albaranes. Se pretende, de esta forma, que la información no tenga que ser procesada manualmente, sustituyendo los documentos mercantiles habituales -pedidos, facturas, etc.- por su equivalente en formato electrónico.

El anterior ejemplo nos muestra que el cliente envía al proveedor un pedido en formato EDI, el proveedor remite al cliente la factura también en formato EDI. Pero, ¿cómo se mandan? Aquí es donde entra en juego una de las partes más importantes dentro del mundo del intercambio electrónico de datos: la red. Las funciones de ésta son fundamentales en el intercambio de datos, dado que, aparte de servir como «puente» entre las empresas, también realiza labores de certificación. Una red cobra una cuota a cada empresa que maneje EDI, a cambio de servir como buzón de documentos, ya que si una empresa quiere realizar un pedido a otra, tendrá que enviarlo en ese tipo de formato. Pero, para realizar dicho envío, sería necesario que, en el momento de la transmisión, la otra empresa estuviera conectada con la primera para poder intercambiar los datos.

Como esto no es así, las redes actúan como buzones de documentos EDI, de modo que cuando enviamos un archivo EDI a una empresa, éste permanece en su buzón, a la espera de que la empresa receptora lo recoja cuando se conecte a la red. Por buscar una similitud, sería algo parecido a lo que ocurre con los mensajes de correo electrónico e-mail, salvo que en vez de mensajes escritos estamos hablando de documentos EDI.

De este modo, cada empresa que realice EDI tiene una dirección propia y única en todo el mundo, que es la que la identifica frente a las demás. Así, cuando enviemos un documento a una empresa, lo que haremos en realidad será enviar el documento a su

dirección electrónica. La red será la encargada de que el documento EDI sea enviado al buzón correcto, y almacenado hasta que el receptor se conecte y lo recoja. El protocolo utilizado mayoritariamente para el envío y recepción de archivos es el denominado OFTP, utilizado por primera vez por la industria automovilística para el intercambio de datos electrónicos.

En nuestro país las dos redes más extendidas son las de TSAI (*Telefónica Servicios Avanzados de Información*) e IBM, aunque existen otras alternativas de menor uso. Algunas aplicaciones ofrecen además la integración dentro de una red propia y privada, algo que tradicionalmente se podía considerar como un obstáculo, pero que hoy en día se supera con facilidad gracias a la existencia de «pasarelas» hacia otras redes, lo que permite de hecho una comunicación casi absoluta y de forma transparente al usuario.

3.5.3 Aspectos Legales: validación

Otra labor fundamental de las redes es la de validación. Al enviar un archivo EDI a una empresa, éste pasa necesariamente por la red, la cual, además de almacenarlo en el buzón correcto, comprueba que es válido en cuanto a estructura y, ante posibles problemas legales, certifica que ha sido almacenado en el buzón de destino.

Cuando la empresa receptora recoge el archivo EDI, automáticamente la red puede certificar que el documento se ha entregado, y esta certificación es válida ante cualquier problema de tipo legal. Es decir, el intercambio de paquetes no se limita a un mero envío de documentos, sino que existen además confirmaciones de depósito o retirada del buzón.

En este sentido, una de las ventajas que ofrece la red TSAI, frente a otras redes existentes en nuestro país, es el hecho de estar aceptada y reconocida por la Agencia Tributaria, de modo que las facturas EDI que hayan pasado a través de TSAI tienen exactamente la misma validez que las facturas en papel. De este modo, podremos presentar ante la correspondiente Delegación facturas electrónicas, del mismo modo que hasta ahora presentábamos facturas en papel.

3.5.3.1 Tipos de aplicaciones EDI

Aunque dentro del mundo EDI podemos encontrarnos con diversidad de aplicaciones, orientadas a necesidades de empresa muy diferentes y con funcionalidades muy distintas, lo cierto es que todos los programas tienen algo en común: La forma de comunicarse entre sí (lo cual es evidente, dado que éste es uno de los puntos claves de intercambio de documentos electrónicos).

De menor a mayor especialización de los programas, podemos distinguir varios grupos. **Por un lado**, nos encontramos con una serie de aplicaciones que sirven únicamente como «puente» entre aplicaciones ya existentes y el mundo EDI en general. De este modo, las aplicaciones que ciertas empresas estén utilizando, podrán ser adaptadas mediante un sencillo cambio para poder funcionar conjuntamente con programas EDI, que se encargarán de traducir los datos internos a archivos de formato EDI, de modo que puedan ser transmitidos al interlocutor.

El siguiente grupo de programas lo forman ciertas aplicaciones que, sin ser soluciones completas para empresas, sí que permiten la introducción y envío de datos a través de EDI, todo ello mediante la presentación de formularios en pantalla que facilitan su uso. Estas aplicaciones serán útiles para pequeñas empresas que necesitan hacer EDI en ciertos momentos, y a las que no les importe introducir los datos manualmente. Dentro de este grupo, se podría englobar también la solución EDI Web, donde los formularios se presentan en formato HTML y se envían a través de Internet.

Por último, existe un grupo, el más amplio, que lo conforman todas las aplicaciones que constituyen una solución completa a las necesidades EDI de una empresa. Dichas aplicaciones suelen incorporar un potente software de gestión de facturas y pedidos, a la vez que realizan las funciones de traducción a formato EDI y el posterior envío.

3.5.3.2 Evaluación

Una aplicación EDI, consta de varias partes bien diferenciadas. Por un lado, nos encontramos con la interfaz de usuario, la cual debe ser lo más clara y potente posible. Dentro de la misma, debemos tener en cuenta aspectos como la calidad de realización,

la sencillez de manejo -soporte de ratón, etc.- y la velocidad a la hora de realizar las tareas más comunes. Quizás ésta sea la parte más importante, ya no sólo de las aplicaciones EDI, sino de cualquiera en general; porque si este apartado no resulta práctico y efectivo, es el usuario final del programa el que sufre las consecuencias de la dificultad de manejo.

Las funciones soportadas son otro aspecto fundamental, por lo que hay que valorar la existencia de todo tipo de ayudas, como la inclusión de módulos para la realización de la Declaración de la Renta, de gestión automática de facturas y pedidos, etcétera. En función de estos aspectos, la aplicación nos ahorrará más o menos trabajo.

La tercera cuestión a considerar es, sin duda, la velocidad y la potencia con la que se realiza la traducción del formato de archivos interno de la aplicación, normalmente compatible con bases de datos, al formato EDI estándar. Si realizamos la traducción de pocos documentos, este aspecto será poco relevante. Pero a medida que crezca nuestro volumen de transacción de documentos EDI, podremos notar una gran diferencia entre un buen módulo traductor y uno que sea lento. Además de la velocidad, un traductor deberá ser asimismo capaz de gestionar y tener en cuenta cualquier tipo de fallos que puedan producirse en el archivo EDI o en el interno, de modo que pueda informar al usuario en todo momento de lo que está aconteciendo.

Por último, y muy importante también, nos encontramos con el apartado de comunicaciones. En este caso, deberemos fijarnos en cuestiones tales como el manejo o no de modems, envío a través de Internet o fax, y cualquier otro tipo de canal de comunicaciones. En cualquier caso, el programa deberá ser capaz de funcionar con el mayor número posible de redes, como pueden ser TSAI, IBM o BT. Además, aunque normalmente las empresas de software nos proporcionan junto con su programa la gestión de un buzón con una red en concreto, siempre es bueno saber que podremos cambiar de red cuando resulte necesario, y que nuestra aplicación sea capaz de poder soportar cualquier cambio.

3.5.3.3 EDI e Internet

EDI ha estado vinculado desde un principio a las redes de valor añadido de alto coste y de naturaleza propietaria (VAN: Value Added Network), que gestionaban las transacciones comerciales de forma electrónica, pero la insurgencia de Internet ha provocado una lógica interconexión entre ambos. Por un lado, la mayoría de los expertos consideran que el comercio electrónico basado en la Red no reemplazará a corto plazo los sistemas EDI actuales; pero por otro, los sistemas EDI ya están dando grandes pasos hacia la generación de sus sistemas y servicios a través de Internet.

Las ventajas de utilizar Internet son evidentes: universalidad, independencia del proveedor, transmisiones directas de extremo a extremo, softwares universales y, sobre todo, una importante reducción de costes y menores barreras de entrada. Pero también existen graves problemas que condicionan que EDI irrumpa definitivamente en el tráfico IP, como es la existencia de protocolos de transmisión diferentes entre Europa y Norteamérica.

En cualquier caso, muchas empresas están comenzando a utilizar Internet para ofrecer a sus socios comerciales conexiones directas a sus redes internas, eliminando así la necesidad de emplear una red de valor añadido para sus intercambios electrónicos, todo ello, a pesar de que quedan muchas cuestiones pendientes hasta que Internet se convierta en el medio ideal para el transporte EDI, como es la falta de seguridad, la incapacidad para confirmar la integridad del mensaje, la vulnerabilidad a las intromisiones, etc.

La seguridad es una preocupación constante e inevitable a la que cualquier empresa o usuario de comercio electrónico no puede dejar de sustraerse. Este es uno de los principales problemas del desarrollo EDI en Internet, porque aún a sabiendas de que una seguridad absoluta es algo imposible de conseguir, el usuario demanda evidentemente medidas objetivas y fiables de seguridad. En este sentido, tanto la industria como los organismos de seguridad y normalización trabajan constantemente.

Por otro lado, serán las grandes empresas los líderes que determinarán la línea de evolución EDI -una evolución, por otra parte, de extraordinario dinamismo y rápida evolución-, así como quienes decidirán cómo será utilizado el sistema y cuáles serán

los protocolos y los métodos de reparto considerados estándares, al mismo tiempo que impondrán a las pequeñas empresas su utilización si desean entablar relaciones comerciales habituales con ellas. En cualquier caso, son precisamente las PYME´s las entidades que mayor atractivo pueden encontrar en las soluciones EDI basadas en Internet, fundamentalmente por su bajo coste y su gran facilidad de acceso.

Según subrayan los expertos, las cuestiones tecnológicas serán resueltas, pero será así mismo indispensable aportar serios argumentos a los responsables empresariales para que decidan acometer el cambio tecnológico y el de los modelos habituales de negocio. Por el camino, probablemente habrá que asistir a una lenta transición entre el EDI habitual y el sostenido por las nuevas tecnologías web. EDI, hasta entonces, se seguirá construyendo sobre una base híbrida que intentará resolver los desafíos que presenta su normalización.

3.6 SET (Secure Electronic Transactions)

SET es un protocolo específico que pretende asegurar, mediante la encripción, todos los procesos típicos del comercio electrónico en Internet:

1.- Envíos de las órdenes de pedidos y las instrucciones de pago.
2.- Solicitud de autorización del comerciante a la institución financiera del comprador.
3.- Confirmación de la orden por parte del comerciante.
4.- Solicitud de reembolso del comerciante a la institución financiera del comprador.

Esta secuencia de procesos es el objetivo de trabajo del SET, dada la vulnerabilidad que presentan cuando se realizan a través de la Red.

3.6.1 Historia

Durante 1995, las grandes compañías mundiales de tarjetas de crédito presentaron proposiciones de comercio electrónico, con vistas a incorporar los prácticamente

universales medios de pago electrónicos al mundo de Internet. *Visa*, en colaboración con *Microsoft*, desarrolló una especificación completa, la *Secure Transactions Technology* (STT).

Por otra parte, *MasterCard*, en asociación con *IBM*, *Netscape* y *CyberCash* patrocinó una especificación conocida como *Secure Electronic Payment Protocol* (SEPP). Ambas especificaciones se basaban en el uso de criptografía de clave pública, certificados...

Ante la previsible guerra que se adivinaba, ambos gigantes, junto con los consorcios que les apoyaban, decidieron asociarse y presentaron, en febrero de 1996, una especificación abierta para conseguir la protección de los pagos hechos mediante tarjeta de crédito en cualquier red insegura y, específicamente, en Internet. *American Express* se unió al consorcio poco después de la publicación del primer borrador. Se consideró que las primeras implementaciones se desarrollarían durante el año 1997.

Esta especificación se denomina SET (*Secure Electronic Transactions*).

3.6.2 Objetivos

Los objetivos que persigue el desarrollo del protocolo **SET** son los siguientes:

- Definir un estándar único para efectuar transacciones a través de Internet, evitando la competencia entre diferentes estándares auspiciados por distintas empresas y consorcios. Este estándar debe ser similar a y compatible con los sistemas de pago, mediante tarjeta, existentes en la actualidad.
- Proveer la autenticación de todas las partes implicadas en una transacción.
- Mantener la *confidencialidad* de la información intercambiada, de forma que cada parte no tenga acceso a más información que la estrictamente necesaria para llevar a cabo su función en la transacción.
- Mantener la integridad de la información implicada en los pagos.
- Ser independiente de plataformas y navegadores.

3.6.3 Actores de la transacción

Los actores implicados en una transacción de comercio electrónico utilizando el modelo **SET** son los siguientes:

- El tenedor de la tarjeta de crédito (cliente): puede ser una persona física o jurídica. Utiliza una tarjeta de crédito emitida por la institución correspondiente. El cliente está equipado con el correspondiente navegador.
- El banco emisor: institución financiera con la que el cliente establece una cuenta y que, a su vez, emite una tarjeta a su nombre.
- El comercio: establecimiento que ofrece bienes, servicios, informaciones... a un precio. El comercio debe tener una cuenta con un banco.
- El banco del comercio: institución financiera con la que el comercio establece una cuenta. Se encarga de procesar las autorizaciones de pago y realiza el pago al comercio.
- La red de compensación: procesa la transferencia de dinero entre las instituciones financieras involucradas.
- La autoridad de certificación: avala las claves públicas de las partes, emitiendo certificados para cada una de ellas.

3.6.4 Funcionamiento

Veamos como se desarrollaría un caso práctico de comercio electrónico:

- El cliente, tenedor de una tarjeta (con un usuario imaginario, Pepe) accede al comercio y navega por él, seleccionando una serie de productos.
- Pepe rellena una orden de compra, calculándose el monto total de la operación (incluyendo los gastos de envío).
- Pepe selecciona el método de pago (tarjetas *Visa*, *MasterCard*, *American Express*...).

- Pepe envía su orden de pago con el método de pago elegido al comercio.
- El comercio solicita autorización por parte del banco de Pepe para llevar a cabo la transacción.
- El comercio le envía a Pepe la confirmación (en forma de factura pro-forma, por ejemplo) de la compra.
- El comercio envía los bienes comprados a Pepe.
- El comercio solicita a su banco el abono de los bienes comprados.

La autenticación de las partes queda encomendada al uso de certificados. Estos certificados son emitidos por las consiguientes autoridades, las cuales deben cumplir una serie de requisitos de confianza por parte de los actores de la transacción. Para cada uno de los actores debe emitirse un certificado.

La emisión y verificación de los certificados están fundamentadas en una jerarquía de confianza, con delegación de mayor a menor nivel en el que los certificadores a nivel mundial van certificando a nuevas autoridades distribuidas por zonas geopolíticas, países, etc. El seguimiento de este árbol de confianza hacia arriba permite asegurar la autenticidad de un certificado. Los mecanismos de aceptación y verificación de certificados deben ir empotrados en los programas.

El comprador obtiene sus certificados de la entidad financiera que emite la tarjeta con la que opera. El comerciante los obtiene de la entidad financiera con la que ha firmado un contrato de adhesión para aceptar las diferentes tarjetas de crédito o débito emitidas por dicha entidad.

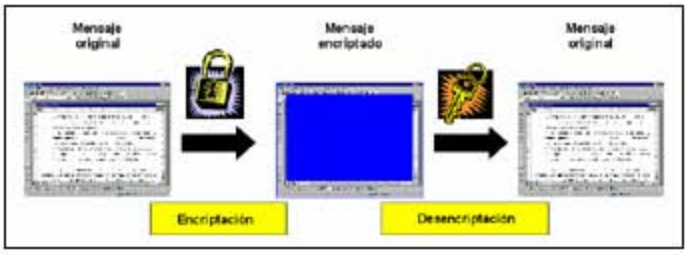
El banco o entidad financiera del comerciante debe poseer una certificación de nivel superior para operar a su vez como autoridad certificadora y emitir certificados para los comerciantes. Al igual que en el caso de la entidad financiera del comerciante, el banco del comprador debe poseer también un certificado, puesto que realiza las mismas funciones que aquel. Ambos obtendrán sus certificados de las asociaciones de medios de pago.

3.6.5 Métodos que Utiliza

SET trata de preservar la autenticación, la *confidencialidad* y la integridad de cualquier transacción de comercio electrónico para lo que utiliza los siguientes métodos:

- ***Confidencialidad*.** Mediante la encriptación de los mensajes, se pretende la no-vulnerabilidad de la información que contenga los datos necesarios para efectuar el pago, tales como el número de cuenta o tarjeta y su fecha de caducidad.
- **Integridad.** Utilizando firmas digitales se preserva la integridad de los datos conteniendo las instrucciones de pago, y garantizando que no han sido modificados a lo largo del trayecto.
- **Autenticación del comprador.** Mediante la emisión de certificados y firmas digitales se autentica al usuario legítimo de una tarjeta o cuenta sobre la que se instrumenta el pago del bien o del servicio adquirido.
- **Autenticación del comerciante.** Asimismo, a través de certificados y firmas digitales, se garantiza que el comprador mantiene una relación comercial con una institución financiera que acepta el pago mediante tarjetas.

Los algoritmos criptográficos empleados por SET para los procesos de encriptación, emisión de certificados y generación de firmas digitales son de doble naturaleza. Por un lado DES (Data Encryption Standard) algoritmo de clave privada (simétrica) que se emplea para garantizar la *confidencialidad* de los mensajes transmitidos; y RSA (iniciales aleatorias) algoritmo de clave pública (asimétrica) que se utiliza para garantizar la integridad de los datos y la autenticidad de los participantes.



Por otro lado, la fórmula de intercambio seguro de claves estriba en la utilización de certificados de autenticidad que son emitidos por las Autoridades Certificadoras (Certificate Authorities, CA), entidades de confianza para todas las partes que intervienen. Un certificado de autenticidad contiene la clave pública de la persona o entidad para la que se emite, junto con información propia, todo ello firmado electrónicamente por la CA. Estos certificados se emiten para cada uno de los agentes participantes en el SET.

El comprador obtiene sus certificados de la entidad financiera que emite las tarjetas con las que opera para realizar las transacciones de comercio electrónico.

El comerciante obtiene sus certificados de la entidad financiera con la que firma contratos de adhesión para la aceptación de tarjetas de crédito, emitidas por dicha entidad en nombre del propietario de la marca. Estos certificados vienen a sustituir a las pegatinas que habitualmente exhiben los comercios. Hay que notar que cada comerciante puede disponer de varios certificados, en correspondencia a las marcas de tarjetas que acepte como forma de pago.

La entidad financiera del comerciante (acquirer) y la entidad financiera del comprador (issuer), deben poseer certificados para poder operar como CA y además

emitir certificados para los comerciantes/compradores. Ambos obtendrán sus certificados del propietario de la marca de tarjetas.

3.7 SSL (Secure Sockets Layer)

Secure Sockets Layer (**SSL**) o capa de conexiones seguras, es un protocolo diseñado por Netscape Communications Co., que se utiliza para autentificar, codificar y enviar mensajes, dispone de un nivel seguro de transporte entre el servicio clásico de transporte en Internet (TCP) y las aplicaciones que se comunican a través de él. Proporciona conexiones seguras sobre una red insegura como es Internet con las siguientes características:

1. Conexión privada: la información se cifra utilizando criptografía de clave simétrica.
2. Autenticación: usando criptografía de clave pública.
3. Integridad: la integridad de los mensajes se asegura usando firmas digitales.
4. Además, proporciona características adicionales:
5. Extensibilidad: es capaz de soportar nuevos protocolos en el futuro.
6. Eficiencia: al utilizar compresión, minimiza el tiempo necesario para establecer la conexión.
7. Compatibilidad: productos con diferentes versiones de SSL pueden inter-operar entre sí.
8. SSL se compone de dos partes diferenciadas:
9. Handshake Protocol: Se encarga de establecer la conexión y determinar los parámetros que se van a utilizar posteriormente (fundamentalmente se trata de establecer cual va a ser la clave simétrica que se utilizará para transmitir los datos durante esa conexión).
10. Record Protocol: comprime, cifra, descifra y verifica la información que se transmite.

Este sistema es transparente para las aplicaciones finales, que simplemente saben que el canal se encarga de proporcionarles *confidencialidad* entre extremos. Por tanto, podemos situar protocolos como HTTP, FTP o Telnet.

3.7.1 Modo de funcionamiento

El denominado Handshake Protocol se compone dos fases, autenticación de servidor y autenticación de cliente, no siendo obligatoria esta última. En primer lugar, el servidor, respondiendo a una petición del cliente, le envía su certificado y las preferencias en lo que a algoritmos de cifrado se refiere. En ese momento, el cliente genera una clave maestra, la cifra con la clave pública del servidor y la transmite al servidor. El servidor recobra la clave maestra y se autentica respecto al cliente devolviendo un mensaje cifrado con la clave maestra. Los datos siguientes son cifrados con claves derivadas de esta clave maestra.

En la segunda fase opcional, el servidor envía un reto al cliente. Éste se autentica respecto al servidor retornándole el reto firmado digitalmente por el cliente, así como su certificado (el cual incluye su clave pública).

3.7.2 Algoritmos utilizados

Una gran variedad de algoritmos criptográficos son soportados por SSL. Durante la fase de acuerdo o "handshaking", se utiliza RSA (clave pública). Después del intercambio de claves, se usan unos cuantos algoritmos, entre los que se incluyen RC2, RC4, IDEA, DES y Triple-DES. Como función resumen se usa MD5 o SHA-1. Los certificados siguen el formato X.509.

3.7.3 Implementación

Los diferentes protocolos que utilizan los servicios de **SSL** usan puertos diferentes a los que les correspondería si no fuesen sobre SSL. La IANA ha reservado los siguientes puertos para su uso por **SSL**:

- 433: HTTP sobre SSL (**https**)
- 465: SMTP (correo electrónico) sobre SSL (**ssmtp**), no confirmado.
- 563: NNTP (servicio de noticias, News) sobre SSL (**snntp**), no confirmado.

El protocolo SSL está, gracias a los esfuerzos de Netscape, ampliamente extendido. La presencia de https:// en el URL de un servidor indica se trata de un servidor "seguro" y que debe utilizarse SSL en la comunicación entre dicho servidor y cliente (navegador). Los navegadores más extendidos (Netscape Navigator y Microsoft Internet Explorer) son capaces de "hablar" SSL. Esto queda indicado (en el caso de Netscape Navigator) de la siguiente forma:

- La llave de la parte inferior izquierda del navegador aparece completa, no partida como habitualmente (en los casos del MS Internet Explorer y de Netscape Communicator es un candado cerrado el que aparece en la esquina inferior izquierda).
- Aparece una línea azul en el límite superior de la línea de visualización de la pantalla del navegador.
- La información del documento alojado en el servidor seguro incluye los datos del certificado que avala al servidor seguro.

Los servidores más populares de la empresa Netscape (Commerce Server, FastTrack Server y Enterprise Server) soportan SSL, con las habituales limitaciones de exportación (clave RC4 de 40 bits para los productos vendidos fuera de EE.UU. o Canadá). El servidor más extendido a escala mundial, *Apache*, posee una versión SSL, Stronghold, con la ventaja añadida de que, al haber sido desarrollado fuera de los EE.UU., puede vender la versión "completa" de SSL con claves de 128 bits. El servidor

de Microsoft, Internet Information Server *2.0*, que viene de serie con Windows NT 4.0 no soporta SSL. Las últimas versiones (IIS 4.0) soportan plenamente el estándar (junto con protocolos propios como PCT).

3.7.4 Ventajas

A diferencia de S-HTTP, que es un protocolo substitutivo de HTTP, SSL extiende su soporte a otros protocolos habituales en Internet. Esta es una de las principales ventajas que aporta este último. Mientras que S-HTTP proporciona cifrado en el nivel de aplicación (en este caso www), SSL lo hace en el nivel de conexión, proporcionando un canal seguro en el nivel de red. Por lo demás, S-HTTP y SSL pueden convivir, utilizándose uno u otro en diferentes instantes de una transacción comercial, o incluso utilizándose simultáneamente.

El sistema es tan robusto como lo sea el menos seguro de los algoritmos que utilice. Claves públicas cortas o claves DES o RC4 de 40 bits deben utilizarse con precaución. Estos son los problemas que plantean las leyes de EE.UU.

La principal desventaja de SSL no estriba en sus fundamentos teóricos o implementación, sino, fundamentalmente, la menor protección que proporcionan las versiones exportables de los productos basados en este protocolo.

También debe tenerse especial cuidado en decidir qué autoridades de certificación y qué certificados son fiables.

3.8 Servidores y Plataformas

Un servidor conectado a Internet, ofrece servicios a todo el mundo. Esto provoca que miles de usuarios quieran saber más del servidor; para ello se esforzarán para entrar y acceder a recursos no permitidos de manera intencionada, es por eso que surge la necesidad de mantener seguro un servidor internet.

Cuando un servidor sufre un ataque, lo más probable es que no se detecte, o bien sí se detecta pero no es posible identificarlo por lo que a continuación se describe un plan con las mínimas medidas que se deben tomar para garantizar un nivel aceptable de seguridad en un servidor.

3.8.1 Servidores

Al efectuarse una compra, se rellena un formulario y se pulsa el botón enviar, se está enviando tales datos a través de la red.

Dichos datos, son transmitidos de servidor en servidor hasta llegar a su detinatario. Estos podrían ser robados en cualquiera de los servidores por los cuales pasan hasta llegar a su destino.

Un servidor seguro garantiza la privacidad de los datos transmitidos por la red. Dicha privacidad se consigue mediante el protocolo SSL.

3.8.1.1 Servidor seguro

Un servidor seguro es un servidor de páginas html, especialmente configurado para establecer una conexión transparente con el cliente, consiguiendo que la información que circule entre ellos (cliente-servidor) viaje a través de Internet encriptada mediante algoritmos que aseguran que sea inteligible sólo para el servidor y el visualizador que accede al web.

- Es la Plataforma necesaria que permite proteger la información confidencial (números de tarjetas de crédito).
- Requisito imprescindible para el establecimiento de servicios de banca electrónica o de comercio electrónico.

3.8.1.2 Funcionamiento de un Servidor Seguro

Encriptando los datos enviados mediante el sistema cifrado RSA, cuando se está ubicado en una zona segura con el navegador.

El navegador Netscape o Explorer, colaborando con el servidor seguro al que llama, encripta los datos de forma que, si algún individuo en el proceso de transmisión consigue apropiarse de éstos, no podrán ser leídos ya que no se dispone de la clave necesaria.

Esta encriptación se basa en el Secure Socket Layer, SSL , estándar desarrollado por Netscape Communications para transferir información segura a través de internet.

Un servidor seguro certificado por Verising cuenta con una clave de 128 bits, con una parte secreta de 40 bits.

Esto confirma que los intrusos que intentan descifrar los datos transmitidos con este sistema, deberán realizar 240 complicadas operaciones para descifrar estos datos, que en tiempo de computación supone miles de años en una de las maquinas más potentes del mercado.

El usuario podrá enterarse en un Servidor Seguro revisando los siguientes puntos:

- La dirección URL comienza por https:// en vez de http://
- La mayoría de los navegadores lo indican:

En Netscape se presentan las siguientes indicaciones:

- La llave de la parte inferior izquierda, que habitualmente aparece partida se ve completa
- Aparece una línea azul en el límite superior del área de visualización.

En Microsoft Internet Explorer:

- Aparece un candado cerrado.
- Si no configura lo contrario, su navegador le avisará que entra en un servidor seguro.

3.8.1.3 Plan de seguridad para un servidor

Un plan de seguridad consiste en definir los modos de uso apropiado de las redes y computadoras de la organización, al mismo tiempo se definen procedimientos para detectar y responder a los problemas de seguridad que se presenten.

La seguridad de un servidor Internet abarca una gran cantidad de aspectos a tratar. Se pueden simplificar y dividir los problemas en tres aspectos:

1. Acceso al Servidor
2. Protección de la información
3. Seguimiento de actividades

Las dos primeras partes se pueden entender como muros que se ponen a los intrusos y la última, como la vigilancia que se debe realizar de los citados muros.

El objetivo es poner el mayor número de trabas posibles y de obtener una gran cantidad de información sobre las actividades que se desarrollan en el servidor.

3.8.1.3.1 Acceso al servidor

Esta es la primera barrera con la que cualquier intruso se va a encontrar. Debe ser lo más consistente posible.

El servidor tendrá dos tipos de usuarios: internos y remotos. En este caso se tratarán las amenazas de los usuarios remotos.

El tipo de acceso que puedan hacer los usuarios remotos depende de los servicios que se estén dando. Cualquier servicio sobre TCP/IP que se ofrezca, supone interacción con un usuario remoto. Al ser esto así, cada servicio puede provocar agujeros de seguridad en el sistema. Se debe estudiar con detalle cada servicio que se ofrece y analizar minuciosamente el software servidor que maneja el servicio.

En este punto se deben distinguir dos tipos de acceso. Uno, mediante nombre de usuario y contraseña. Otro mediante problemas de configuración o errores en el software servidor. Por ejemplo:

Mediante el servicio Telnet, un intruso realiza un ataque con diccionario para averiguar una determinada contraseña. A este tipo de acceso se denomina Acceso directo.

Mediante un programa ejecutándose en un servidor web (http), se consigue acceso al servidor. Se denomina Acceso Indirecto.

Acceso directo: Nombre usuario + contraseña

Algún servicio del sistema requiere del usuario remoto la introducción de un nombre y contraseña de usuario para permitirle el acceso a recursos. Por ejemplo, el servicio Telnet, el servicio de acceso remoto, el servicio FTP, etc.

Para protegerse de estos ataques existen dos opciones. Una es no ofrecer esos servicios a usuarios remotos. Esta opción protege totalmente pero tales servicios pueden ser necesarios.

La otra forma de protegerse es implantar un buen plan de contraseñas. Se pueden llevar a cabo dos ataques bien conocidos, el ataque bruto y el de diccionario. Ambos coinciden en probar contraseñas adjuntas a un nombre de usuario fijo. El nombre de usuario suele ser uno que los sistemas o servicios establezcan por defecto y que todo el mundo conoce (root, Administrador, etc.). Los intentos consistirán en introducir el nombre de usuario prefijado para el ataque y luego una contraseña. En el ataque bruto probaremos todas las posibles contraseñas, y en el ataque de diccionario se prueban todas las contraseñas que aparecen en un archivo de texto, donde cada línea posee una palabra a probar.

Un plan de contraseñas debe especificar como mínimo los siguientes parámetros:

Longitud mínima de las contraseñas. Deben tener un mínimo de 8 caracteres. Si se pone una contraseña inferior, sería factible intentar un ataque bruto.

Caducidad de las contraseñas. Se debe poner caducidad a las contraseñas. Este parámetro limitará enormemente el posible ataque bruto.

Plazos de reutilización de contraseñas. No se debe permitir a un usuario reutilizar sus contraseñas en un plazo razonable. Si se permite que las reutilicen se está disminuyendo el valor del parámetro anterior.

Composición de las contraseñas. Las contraseñas NO deben ser una palabra que se encuentre en un diccionario (contraseña muy débil). Una recomendación es que contengan caracteres alfanuméricos y signos de puntuación mezclados o como mínimo mayúsculas y minúsculas mezcladas. En Internet se pueden encontrar diccionarios de contraseñas que utilizan los intrusos para acceder.

Bloqueo del servicio ante fallos de acceso repetitivos. Esto permitirá que sea imposible lanzar un ataque bruto o con diccionario, o por lo menos complicarlo de forma decisiva. Si por ejemplo, cada tres intentos fallidos bloquean el servicio o la cuenta del usuario que se esta probando, impedirá que se continúe probando.

Acceso Indirecto: explotar un agujero de acceso

Este tipo de acceso consiste en explotar un agujero de acceso que el software del servicio, del sistema operativo o una mala configuración del usuario, ha generado. No hay una norma común para definir como son esos agujeros, puesto que depende del software, sistema operativo, etc.

Este tipo de agujeros se explotan en el software y en los sistemas operativos más comerciales. Si se desarrolla un propio programa se deben tomar precauciones de seguridad, aunque es difícil que alguien explote un posible agujero en dicho programa. La ventaja de conocer un agujero de un software comercial (por ejemplo Internet Information Server) es que se puede utilizar en muchos sitios. Si un intruso dedica mucho tiempo para averiguar un agujero en el programa que se ha desarrollado, tan solo le permitirá entrar en el sitio y, probablemente, esto no le compense o satisfaga demasiado.

Estar al tanto de los agujeros de seguridad que un sistema puede tener es una tarea bastante laboriosa.

Los desarrolladores de sistemas operativos y software de servidor poseen sus listas de avisos y páginas dedicadas a seguridad de sus productos. Visitando dichas páginas,

se puede ver si para un determinado agujero descubierto hay algún parche o medio de solucionarlo.

3.8.1.3.2 Protección de la información

Si por algún error o por la astucia del intruso, éste ha conseguido entrar en el servidor, quiere decir que el primer muro lo ha logrado traspasar. Se deben poner todo tipo de trabas, para evitar su visita y que no la vuelva a repetir.

Siguiendo con el modelo simple se resume este aspecto en dos partes:

Protección de la información del sistema.
Protección de la información de la empresa.

Protección de la información del sistema

El sistema operativo posee información vital que se debe proteger. Esta información puede darle al intruso nuevas formas de penetrar en el servidor o de introducirse en otros sistemas conectados en red. La manera de proteger esta información dependerá del nivel de acceso que un intruso haya logrado. Normalmente todos los sistemas operativos tienen una cuenta con acceso a todos los recursos, denominada Administrador o root. Dicha cuenta posee un control absoluto sobre el sistema y, si el intruso ha conseguido entrar con los derechos del Administrador, se tienen serios problemas. Esta cuenta es la que mejor hay que proteger.

La información del sistema esta guardada en archivos del disco duro del servidor. Dicha información no se puede encriptar puesto que el propio sistema la usa. Las nuevas versiones de los sistemas operativos ya vienen con este tema un poco resuelto, aunque no del todo.

Así, se deben proteger los archivos de claves de acceso del sistema, los archivos de control del sistema y los programas que ofrecen los servicios.

Si el intruso tiene acceso a los programas del sistema puede sustituir alguno por un Caballo de Troya y asegurarse la entrada futura al sistema sin que nos hayamos dado cuenta. Si tiene acceso al archivo de claves de acceso, no hace falta decir lo que puede pasar.

En definitiva, se debe limitar el acceso a los archivos del sistema operativo. Es en estos aspectos donde los sistemas operativos se diferencian unos de otros con mayor claridad.

Protección de la información de la empresa

Se debe tener cuidado a la hora de almacenar la información. Por ejemplo, no es una buena idea almacenar la información más sensible en el servidor conectado a Internet.

Para proteger la información se debe analizar cuales son los requisitos de acceso necesarios para los usuarios remotos. Se deben eliminar todo tipo de accesos y permisos por defecto que dicha información tenga. Los sistemas operativos establecen permisos muy amplios para la información nueva que se crea en su sistema. Una vez creada se deben limitar los permisos.

Si se requiere mayor protección, se deben cifrar dicha información con algoritmos de cifrado lo más robustos posibles.

3.8.1.3.3 Seguimiento de actividades

Esta es la tercera parte del problema de la seguridad. Se deben vigilar las actividades que se desarrollan en el servidor. Mediante esta vigilancia se pueden comprobar entre otras cosas lo siguiente:

Accesos repetitivos.
Accesos a recursos no permitidos.

Uso fuera de horario de un usuario autorizado.

Cambios en archivos del sistema sospechosos.

Lo anterior, es una pequeña muestra de la valiosa información que aportará un buen seguimiento de actividades.

Algunos sistemas operativos traen sus propios sistemas de auditoria o seguimiento de actividades. Se debe comprender perfectamente todo el sistema de auditoria que posee. Además, existen muchas herramientas que permiten mejorar el sistema de auditoria propio del sistema operativo.

Dos actividades que se deben obligatoriamente auditar son: la entrada y actividad que se realiza en cada puerto TCP/IP. Esto dirá si existe alguna actividad sospechosa. La segunda es que se debe instalar un checador de integridad de los archivos del sistema. Esta utilidad debe ser obligatoria en el sistema. Permite alertar de los cambios que se produzcan en los archivos. Es la mejor forma de detectar los Caballos de Troya.

Monitoreando el sistema, se puede bloquear a un intruso antes de que haga cualquier fechoría. Hay que tener en cuenta que en algunos casos el intruso tarda tiempo en entrar.

Durante ese tiempo realiza intentos o hace operaciones que un administrador de seguridad capacitado debe analizar, detectando su actividad antes de que entre.

3.8.2 Plataformas para el Comercio Electrónico

Windows NT, Unix y MacOS, principales opciones de plataformas escogidas por la mayoría de las tiendas virtuales. La elección del sistema que da soporte a un negocio virtual tiene una gran importancia. Un fallo en la máquina o en el sistema operativo que soporta toda la tienda virtual puede originar la pérdida de confianza del posible comprador, provocando que no vuelva a visitar más el sitio web.

La elección más adecuada tiene una serie de pros y contras, en función del tipo de comercio virtual que quiera implantarse. No existe un producto ideal para todo tipo de negocios electrónicos. En ocasiones, no existe posibilidad de elegir, bien por que las

personas que deben tomar la decisión ya están habituadas a un entorno de trabajo y no desean salir de él, bien por que los sistemas dentro de la empresa están ya diseñados sobre un tipo de plataforma, bien por que la tienda se construya alquilando espacio en un servidor ya existente. En otros casos los diseñadores del comercio virtual deben implantar un servidor específico para aplicaciones de comercio electrónico, partiendo de cero, independientemente de cuál sea la red informática usada en la empresa. De hecho, muchas empresas que poseen una red principal basada en Windows NT, usan servidores web sobre Unix, por ejemplo. Normalmente la elección final recae sobre los tres principales sistemas operativos: Unix, Macintosh y Windows NT.

La decisión sobre qué plataforma elegir para satisfacer las necesidades de comercio electrónico no suele ser fácil. El paquete servidor de Macintosh, MacOSXS, por ejemplo, es una plataforma web ideal en muchos aspectos. Sin embargo el número de servidores en Internet que ofrecen servicios http (protocolo de transferencia de hipertexto) sobre servidores Mac no alcanza la cifra del 3 por ciento. La decisión es más complicada de lo que pudiera parecer a primera vista.

3.8.2.1 Plataforma Unix

Más del cincuenta por ciento de los servidores de Internet están basados en Unix. Se trata, sin duda alguna, de un auténtico peso pesado en la Red. Unix habitualmente funciona sobre máquinas de alto nivel, como Sun o Silicon Graphics. Son máquinas que pueden incorporar desde uno hasta 64 microprocesadores. Las máquinas más potentes pueden atender cientos de miles de impresiones webs con el mímino esfuerzo.

Unix soporta sistemas operativos de 64 bits, como los de Digital O Hewlett-Packard, que son capaces de manejar grandes volúmenes de información en múltiples compartimentos de disco duro. Estas características son cruciales para las tareas críticas y las necesidades de estabilidad asociadas al comercio electrónico. Permiten capacidades de clustering lo que, entre otras cosas, facilita tener abierta la tienda virtual 24 horas al día, los siete días de la semana: el clustering posibilita poner a funcionar múltiples servidores como si fueran uno sólo, compartiendo procesos y provee

seguridad de forma unitaria. HP permite soportar ocho servidores, mientras Que Sun Solaris Cluster permite manejar cuatro a la vez.

Como contrapartida, están los altísimos precios que pueden llegar a alcanzar la red de servidores. En Unix, las cifras pueden sobrepasar con holgura los diez millones de pesetas. Además, Unix requiere la atención de personal especializado con una formación específica en dichos entornos. Su sistema operativo es complejo y utiliza comandos propios. En cualquier caso, parece claro que para un emprendimiento de altos vuelos en la arena del comercio electrónico, lo más aconsejable sea pasar por Unix.

3.8.2.2. Plaforma NT

Los servidores web basados en Windows NT, ocupan aproximadamente una cuarta parte de la red Internet, y suponen el sector de mayor crecimiento. No es de extrañar, las astronómicas cifras que Microsoft está invirtiendo para liderear todos los campos, pero especialmente Internet. La versión 4.0 viene provista de ciertas utilidades de servidor web. La próxima versión, añade aún más, y promete convertirse en un duro rival en los entornos empresariales.

NT se ha convertido en un líder en entornos de baja gama en Internet e intranet por varias razones. Quizá la principal sea la fuerte presencia de mercado de Microsoft, junto a las continuas novedades en el desarrollo de herramientas de software. NT posee además algunas ventajas técnicas. Gracias a su capacidad de proceso multi-hilo, permite realizar varias tareas al mismo tiempo, lo cual es una característica deseable en la trastienda de cualquier negocio virtual.

NT Server Enterprise Edition permite manejar ocho procesadores a la vez, lo cuál no llega a desarrollar tanta potencia como las capacidades de clustering de los sistemas Unix, aunque sí supone una ventaja respetable. Como atractivo adicional, hay que señalar que existen muchas más aplicaciones de comercio electrónico diseñadas para NT que para cualquier otra plataforma, siendo sus precios bastante razonables. El equipamiento hardware necesario para NT cuesta considerablemente menos que en

caso de UNIX. Aunque es posible instalarlo sobre una PC común y corriente, es aconsejable recurrir a estaciones de trabajo más potentes, NT, además, es menos complicado de usar que Unix, aunque no llega a la facilidad de Macintosh.

Como inconveniente, las capacidades de clustering de Microsoft no soportan las capacidades escalables de los sistemas Unix. Tampoco llegan a su nivel de estabilidad, siendo más proclives a sufrir cuelgues, cosa que, se promete, no sucederá en la próxima versión.

En cualquier caso, las características de Windows NT lo convierten en una solución eficiente para entornos de negocio electrónico de bajo y medio nivel, que no manejen niveles de tráfico como Yahoo o Alta Vista, por ejemplo.

3.8.2.3 Macintosh se renueva

Para algunos emprendedores de tiendas virtuales, el principal coste del proyecto está en el tiempo que se dedica a los mismos. Los servidores y las aplicaciones que soportan deben ser constantemente vigilados. Con Macintosh estas tareas pueden realizarse con facilidad, y sin necesidad de recurrir constantemente a personal especializado.

La arquitectura Macintosh ofrece una seguridad extrema, ya que separa en distintos espacios el sistema operativo y el servidor web. Muchos servidores web han experimentado una cifra nula de errores o paradas de funcionamiento en las transferencias de información http. El sistema operativo Mac OSXS, además, ofrece la posibilidad de hacer funcionar múltiples servidores virtuales en cualquier Power Mac G3 o Mac Server G3. Los precios de Apple han experimentado sensibles bajadas, hasta casi situarse al nivel de plataformas Wintel (Windows + Intel).

3.8.3 Firewall como Mecanismo de Seguridad

La medida más importante para prevenir entradas no deseadas, cuando conectamos una red local a internet, es definir una Política de Seguridad de Red basada en un Firewall.

El Firewall funciona como pasarela entre la red privada y el resto de la red, y se basa en una serie de reglas o políticas que definen los diferentes modos de acceso a los servicios disponibles. Si se quiere acceder a Internet desde la red privada, se debe conectar primero al dispositivo que actúa de Firewall y, éste de acuerdo a sus reglas le dará o no acceso a los servicios permitidos. Para el caso en que los clientes se conecten desde Internet es similar pero lo recomendable es permitir el menor número de servicios posible ya que Internet es un gran universo y la piratería de información ha ido incrementando de acuerdo a las diferentes empresas buscando su globalización.

3.8.3.1 Tecnologías de Firewall de Internet

El Firewall asegura que todas las comunicaciones entre la red de una compañía y la Internet se adecuen a la política de seguridad de la organización, para proporcionar una seguridad real y efectiva, el firewall debe seguir y controlar el flujo de comunicaciones que pasa por él. Para poder tomar decisiones de control sobre los servicios basados en TCP/IP, un firewall debe obtener, guardar, recoger y manipular información derivada de todos los niveles de comunicación y también desde otras aplicaciones ya que no es suficiente examinar paquetes aislados.

La información de estos estados, derivada de comunicaciones anteriores y de otras aplicaciones, es un factor esencial para poder tomar la decisión de control para realizar nuevos intentos de comunicación.

Para resumir, las decisiones de control requieren que el firewall sea capaz de acceder, analizar y utilizar lo siguiente:

- Información sobre la comunicación de cada una de las capas.
- Estado derivado de comunicaciones previas, por ejemplo, se podría conservar el comando de salida de PORT de una sesión de FTP para que una conexión entrante de datos FTP pudiera ser comprobada.

Estado derivado de la aplicación, por ejemplo, se permitiría a un usuario que ya hubiese sido autenticado acceder mediante el firewall únicamente a servicios autorizados.

Manipulación de información, consiste en la evaluación de expresiones flexibles basadas en todos los factores mencionados anteriormente.

3.8.3.2 Política de Seguridad

La política de seguridad de un firewall se apoya en los términos: Base de Normas y Propiedades .La Rule Base (Base de Normas) es un conjunto ordenado de normas que se utilizan para comprobar cada comunicación. Si la fuente (SOURCE), el destino (DESTINATION) y el servicio (SERVICE) corresponden a una norma, la acción indicada (aceptar, rechazar, cifrar y cortar) se lleva a cabo; Si una comunicación no corresponde a ninguna norma, se interrumpe, de acuerdo con el principio –lo que no está permitido está prohibido-.

Protección del Consumidor en el Comercio Electrónico.

El Consejo de Europa interpela por esta resolución a la Comisión para que examine la legislación relativa a los consumidores vigente en la Unión Europea en el marco de las nuevas circunstancias derivadas de la sociedad de la información y señale posibles lagunas normativas en relación con problemas concretos en el contexto de la sociedad de la información. Esta resolución será la base sobre la que se promulguen directrices por parte de la OCDE en materia de comercio electrónico.

Vistas las Conclusiones del Consejo de 19 de mayo de 1998, Vista la Comunicación de la Comisión sobre las prioridades de la política de los consumidores 1996-1998, Vista la Declaración Ministerial de la OCDE sobre protección de los consumidores en el contexto del comercio electrónico.

1) Considerando que el continuo desarrollo de nuevas tecnologías para la transmisión y almacenamiento de información conduce a innovaciones de orden

organizativo, comercial, técnico y jurídico que están teniendo un profundo impacto en la sociedad en general.

2) Considerando que las nuevas tecnologías de la comunicación tendrán una incidencia notable en la vida cotidiana de todos los ciudadanos, tanto si adoptan una actitud activa como pasiva ante esta evolución;
3) Considerando que las nuevas tecnologías de la información y de la comunicación y el desarrollo de la sociedad de la información con ellas asociado pueden ofrecer numerosas ventajas a los consumidores pero dan también lugar a nuevos contextos comerciales con los que no están familiarizados y que pueden poner en peligro sus intereses;
4) Considerando que los consumidores están especialmente interesados en temas relacionados con:
   a) La accesibilidad
   b) La facilidad de uso de equipos y aplicaciones y las competencias necesarias para utilizarlos.
   c) La transparencia, la cantidad y la calidad de la información.
   d) La equidad de las prácticas comerciales, las ofertas y las condiciones contractuales.
   e) La protección de los niños frente al contenido inadecuado.
   f) La seguridad de los sistemas de pago, incluida la firma electrónica.
   g) El régimen jurídico aplicable a las transacciones que los consumidores efectúen en el nuevo entorno con respecto tanto a la elección del régimen jurídico como a la viabilidad de las disposiciones existentes;
   h) La atribución de responsabilidades.
   i) La intimidad y la protección de los datos personales.

5) Considerando que la confianza de los consumidores constituye un requisito indispensable para que éstos acepten la sociedad de la información y tomen parte en ella.

6) Considerando que para instaurar esta confianza es necesario que exista en las nuevas tecnologías un nivel de protección equivalente al que rige en las transacciones tradicionales de los consumidores, aplicándose a los nuevos productos y servicios que ofrece la sociedad de la información los principios vigentes en materia de política de los consumidores, especialmente:

a) La transparencia y el derecho a recibir, antes de la transacción y en su caso después de ella, información suficiente y fiable que contenga, en particular, la identidad comprobada del proveedor y la información necesaria para probar la autenticidad de cada uno de los elementos de una transacción;

b) La no-discriminación en el acceso a productos y servicios, con atención a las necesidades de los consumidores vulnerables;

c) La protección de los consumidores frente a las prácticas de comercialización no solicitadas, engañosas y desleales, incluida la publicidad, y el apoyo a que se pongan a disposición del consumidor medios fiables para filtrar el contenido de los sistemas de comunicación;

d) La protección de los intereses económicos de los consumidores, con una distribución equitativa de riesgos y responsabilidades que refleje en especial la responsabilidad del proveedor al optar por medios electrónicos de comercio y con inclusión, en particular, de las condiciones necesarias para que el consumidor pueda tomar decisiones ponderadas;

e) La protección de la salud, seguridad e intimidad de los consumidores, incluida la protección contra la utilización abusiva de datos personales;

f) La información y educación del consumidor, a fin de posibilitar la adquisición de las competencias adecuadas;

g) La consulta de los consumidores a la hora de desarrollar nuevas políticas o mecanismos reglamentarios;

h) La representación de los intereses de los consumidores en los órganos de control y vigilancia pertinentes;

7) Considerando que, a juicio del Consejo, la mejor manera de garantizar, en la Comunidad Europea, que se tengan plenamente en cuenta los intereses de los consumidores en la sociedad de la información consiste en integrar la dimensión relativa a los consumidores y, en particular, los principios antes mencionados en materia de política de los consumidores, en las correspondientes iniciativas de la Comunidad;

8) Considerando que la legislación comunitaria y las legislaciones nacionales de aplicación pertinentes son aplicables a las transacciones de los consumidores en el nuevo entorno de la sociedad de la información;

9) Considerando que en el especial la Directiva 97/7/CE del Parlamento Europeo y del consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia ya estable, entre otras cosas, una protección en el ámbito del comercio electrónico.

10) Considerando que, en el caso de las transacciones trans-fronterizas efectuadas por medio de las tecnologías de la información, los consumidores deben poder, en el marco del Derecho comunitario y de ls Convenios de Roma y Bruselas, acogerse a la protección que ofrece la legislación de su país de residencia habitual y poder acceder fácilmente a los procedimientos de recurso, en particular en su país de residencia habitual; teniendo en cuenta que la Comisión ha propuesto una Directiva relativa a la comercialización a distancia de los servicios financieros para el consumidor y ha indicado que está tomando en consideración otras posibles iniciativas de armonización de la legislación en este ámbito.

11) Considerando que la política comunitaria en este ámbito debe tener debidamente en cuenta el carácter plurilingüe y multicultural de la Comunidad;

12) Considerando que las organizaciones de consumidores y los organismos públicos competentes desempeñan un importante papel a la hora de proteger los intereses de los consumidores en este nuevo entorno así como de facilitar información y contenidos, y que deben cumplir ese cometido a través de una acción coordinada; Que las empresas también pueden desempeñar un papel importante mediante, en particular, códigos de conducta;

13) Considerando que la Comunidad debe desempeñar un papel activo a escala internacional para garantizar el cumplimiento de sus normas aceptadas de protección de los consumidores a la hora de desarrollar la sociedad de la información global.

Visto lo anterior podemos entender la importancia que tiene un software como sistema de seguridad pero es necesario definir las necesidades de seguridad, lo que se desea proteger, y con ello la solución o la tecnología a usar.

Cuando se ha definido el grado de riesgo, se debe elaborar una lista de los sistemas con las medidas preventivas que se deben tomar y las correctivas en caso de desastre, señalando la prioridad de cada uno con el objetivo de que en caso necesario se trabajen los sistemas de acuerdo a sus prioridades.

Por ejemplo:

NECESIDADES	**SOLUCIONES**
Control de Accesos al Sistema	Cortafuegos o firewall (a nivel de aplicación es más lento que el del método de filtrado, pero garantiza una mayor seguridad)
Control de Acceso de Usuarios	Técnicas de password y gestión de éstas
Autenticación, No repudio	Técnicas criptográficas para la firma digital y su infraestructura
Integridad, *Confidencialidad*	Técnicas criptográficas para el cifrado y su infraestructura

CAPITULO IV
EVALUACIÓN DE SISTEMAS DE SEGURIDAD EXISTENTES

Es importante y necesario regular el comercio electrónico, pero de modo que no obstaculice el crecimiento de esta importante herramienta. La industria electrónica debe autorregularse y contar con códigos de comportamiento y normas que sean respetados por todos los usuarios. Sin embargo el desafío radica en establecer un mercado seguro y equitativo para todos.

4.1 Evaluación de Sistemas de Seguridad por Función

A continuación se muestra una tabla en donde se indican los aspectos de seguridad más importantes que deben cubrir los sistemas de seguridad para el comercio electrónico, listando del lado izquierdo los métodos o sistemas de seguridad y del lado derecho la función para la cual fueron creados:

MÉTODO	AUTENTICACIÓN	PRIVACIDAD	INTEGRIDAD	CONTROL DE ACCESO	NO-REPUDIO
Encripción		X			
Firma Digital			X		
Certificado Digital	X				X
Protocolos	X	X	X		X
Servidor Seguro				X	

4.2 Análisis de la Encripción

La encripción proporciona un medio para identificar a los emisores, autentificando los contenidos de los mensajes, evitando que se niegue la propiedad de ellos y protegiendo su carácter privado.

Como se ha mencionado con anterioridad existen básicamente 2 tipos de encripción los cuales son el simétrico y el asimétrico, y a continuación se presenta las diferencias, ventajas y desventajas de cada uno. Los esquemas de encriptamiento simétrico también presentan un problema con la autenticidad, ya que la identidad de un originador de mensaje o un receptor no se puede probar. Si dos personas poseen la misma llave, cada una puede crear y encriptar un mensaje y decir que la otra persona lo envió. Esta ambigüedad inherente acerca de quién es el autor de un mensaje hace que no-repudiación sea imposible con las llaves secretas. El encriptamiento simétrico no puede garantizar la autenticidad ni la no-repudiación.

La forma para resolver el asunto de la no-repudiación consiste en usar lo que se denomina "criptografía de llave pública", que emplea algoritmos de encriptamiento asimétricos. Por otro lado las ventajas de la utilización de la criptografía de clave simétrica es la existencia de algoritmos muy rápidos y eficientes, especialmente si se implementan en hardware. Si la clave de cifrado es lo bastante larga, entre 56 y 128 bits, es prácticamente imposible reventarlas usando la fuerza bruta.

Mencionando las ventajas del otro tipo de encripción, el asimétrico, éste resulta un tanto mas seguro que el simétrico debido a su naturaleza de manejo de llaves públicas y privadas, en donde ya no es necesario que todo el mundo conozca nuestra clave de cifrado, sino que ahora podremos cifrar nuestro mensaje con nuestra llave pública y nuestro destinatario lo podrá descifrar con su llave privada.

Con esta técnica de cifrado se garantiza la autenticación y la no-repudiación de las partes involucradas en la transmisión del mensaje, cosa que se veía perdida con la anterior técnica.

La criptografía de clave asimétrica posee, sin embargo, dos inconvenientes:

1. Velocidad. Los sistemas basados en clave asimétrica son notablemente más lentos que sus equivalentes de clave simétrica. Por tanto estos sistemas no suelen ser adecuados para el cifrado masivo de información.
2. Validación de la clave. La discusión sobre la fortaleza de un algoritmo de clave asimétrica es irrelevante sin una discusión previa sobre el protocolo de validación de claves.

4.3 Análisis de los Certificados Digitales y las Entidades Certificadoras

En la siguiente tabla se muestra una comparación de costos de los diferentes tipos de certificados existentes en el mercado así como las principales entidades certificadoras que los emiten.

Tipo de Certificado	ipsCA	Verisign USA	Verisign Internacional	GLOBALSIGN
Servidor (SSL)				
Certificado	$ 123,7	$ 349	$ 449	$ 180,4
Renovación Certificado	$ 103,1	$ 249	$349	No disponible
Personales				
Clase 1	$ 10,3	$ 14,95	$ 14,95	No disponible
Clase 2	$ 20,6	$ 14,95	No disponible	$ 19,6
Clase 3	$ 51,5	No disponible	No disponible	$ 61,8
Firma de Código				
Certificado Netscape	$ 201	$ 400	$ 400	$ 314,4
Certificado I.E: 4,0	$ 201	$ 400	$ 400	$ 314,4
WAP				
Certificado	$ 201	No determinado	No determinado	No disponible
Renovación Certificado	$ 103,1	No determinado	No determinado	No disponible

4.4 Análisis de los Protocolos

Los protocolos cubren un aspecto muy importante en la seguridad en el comercio electrónico, como ya se ha dicho anteriormente. Estos protegen la información que circula por la red a diferentes niveles y haciendo uso de diferentes técnicas y herramientas como la encripción.

De hecho, ahora parece como si Internet hubiera ganado un exceso de riquezas en cuanto a la seguridad, con una variedad de estándares que cubren muchos niveles de redes, desde la seguridad a nivel de paquete, hasta la seguridad a nivel de aplicación. Aunque todavía se considere a Internet como un medio inseguro, debido a su naturaleza descentralizada, es importante señalar que los datos involucrados en las transacciones que usen estos protocolos pueden estar seguros.

Algunos de los estándares de seguridad para Internet se muestran en el siguiente cuadro:

STÁNDARD	FUNCIÓN	APLICACIÓN
Secure HTTP (S-HTTP)	Asegura las transacciones en el web.	Exploradores, servidores web, aplicaciones para Internet.
Secure Sockets Layer (SSL)	Asegura los paquetes de datos en la capa de la red.	Exploradores, servidores web, aplicaciones para Internet.
Secure MIME (S/MIME)	Asegura los anexos de correo electrónico en plataformas múltiples.	Paquetes de correo electrónico con encriptamiento RSA y firma digital.
Secure Wide-Area Nets (S/WAN)	Encriptamiento punto a punto entre firewalls y ruteadores	Redes virtuales privadas.
Secure Electronic Transaction (SET)	Asegura las transacciones con tarjeta de crédito.	Tarjetas inteligentes, servidores de transacción, comercio electrónico.

Los estándares pueden proporcionar seguridad de conexión y de aplicación. Los estándares cubiertos aquí se pueden clasificar de acuerdo a si proporcionan o no la seguridad de conexión o de aplicación.

Los estándares, como Secure Sockets Layer (SSL-Capa de sockets segura) y Secure Wide-Area Networks (Secure WAN o S/WAN-Redes de área grande seguras) están diseñados para mantener comunicaciones seguras en Internet, aunque SSL se usa primariamente con aplicaciones para el web. Secure HTTP (S-HTTP, HTTP Seguro) y Secure MIME (S/MIME-MIME Seguro), por el contrario, están dirigidos a proporcionar autentificación y preservar el carácter privado, es para correo electrónico y aplicaciones habilitadas para correo. SET va un paso más adelante al proporcionar seguridad únicamente para las transacciones de comercio electrónico.

La seguridad de las aplicaciones para web gira en torno a dos protocolos, Secure HTTP y Secure Sockets Layer, que proporcionan autentificación para servidores y navegadores, así como *confidencialidad* e integridad de los datos para las comunicaciones entre un servidor web y un navegador.

S-HTTP está diseñado específicamente para soportar el protocolo de transferencia de hipertexto (HTTP), proporcionando la autorización y seguridad de los documentos. SSL ofrece métodos de protección similares, pero asegura el canal de comunicaciones

al operar más abajo en la pila de red (entre la capa de la aplicación y las capas de red y transporte TCP/IP).

S-HTTP asegura los datos, mientras SSL asegura el canal de las comunicaciones. SSL se puede usar para otras transacciones, aparte de las de web, pero no está diseñado para manejar decisiones de seguridad basadas en autentificación a nivel de documento o aplicación. Esto significa que se tendrían que usar otros métodos para controlar el acceso a diferentes archivos.

En el siguiente cuadro se muestran las comparaciones del SET contra el SSL y los beneficios que tiene uno del otro cubriendo los principales aspectos de seguridad que engloban los protocolos:

	SSL (Secure Sockets Layer)	SET (Secure Electronic Transactions)
AUTENTICACION	El vendedor se autentica con un Certificado Digital emitido por una Entidad Certificadora, este documento, dado que es totalmente infalsificable, garantiza que el vendedor es quien dice ser. En este protocolo el cliente no se autentica.	Este aspecto es la base del SET, tanto el banco como el vendedor y el cliente deben estar certificados por otra entidad.
PRIVACIDAD	Haciendo uso de la encripción se garantiza que los datos enviados y recibidos no podrán ser interpretados por ninguna persona que no sea ni el emisor ni el receptor.	Igual que en el SSL, los datos van encriptados y no pueden ser interpretados alguna persona ajena a la transacción. Para el SET se aumenta la privacidad de la comunicación al impedir que el vendedor tenga acceso a los datos bancarios del cliente y que el banco no pueda acceder a los datos de la compra.
INTEGRIDAD	Se garantiza que los datos recibidos son exactamente iguales a los datos enviados, pero no se impide al receptor la posibilidad de modificar estos datos una vez recibidos.	Con el SET los datos enviados no pueden ser alterados ni durante la comunicación ni después ya que han sido firmados digitalmente.
NO-REPUDIO	Este aspecto no esta garantizado por este protocolo.	La firma digital puede servir como prueba de la transacción, por lo que ninguna de las partes puede negar haber participado en ella.

4.5 Seguridad en los servidores

Características entre determinados proveedores de servidores para comercio electrónico; en este caso haciendo énfasis en la seguridad.

Características	Zeus Web Server v3.0	Enterprise Server 3.01	Microsoft IIS 3.0
Tecnología			
Soporte HTTP/1.1	Sí	Sí	No
Arquitectura escalable para alojar miles de sitios web en una única máquina	Sí	No	No
Arranque/parada de los servidores virtuales de forma independiente	Sí	Sí	No
Configuración de los servidores remota, delegable y basada en web	Sí	No	No
Limitación del ancho de banda por servidor virtual	Sí	No	No
Estadísticas y gráficas en tiempo real accesibles vía web	Sí	No	No
Multiplataforma: UNIX y NT	Sí	Sí	No
Soporte integrado para clustering con tolerancia a fallos y balance de carga	Sí	No	No
Soporte para diversos idiomas	Sí	Sí	Sí
Formatos de registro (logs) configurables	Sí	Sí	No
Páginas de error configurables	Sí	Sí	No
Seguridad			
Soporte SSL3 para contenido estático y dinámicos	Sí	Sí	No
Seguridad SSL 128 bits en todo el mundo	Sí	No	No
Soporte para aceleradores de criptografía por hardware	Sí	Sí	No
Soporte para aplicaciones Web			
Encapsulación segura CGI/1.1	Sí	No	No
Soporte multiplataforma para extensiones y filtros ISAPI	Sí	No	No
API de generación de contenido distribuida con tolerancia a fallos y balance de carga	Sí	No	No
Soporte para Servlets Java	Sí	Sí	Software adicional
Soporte para Servlets Java distribuidos	Sí	No	No
API para autentificación distribuida	Sí	No	No
Análisis en el lado del servidor para contenido dinámico y estático	Sí	No	No
File extension application handlers	Sí	Sí	No
Administración			
Administración completa desde un browser de web, incluso en modo texto	Sí	No	No
Registro de configuración multiplataforma basado en red para configuración centralizada o distribuida	Sí	No	No
Jerarquía de configuración totalmente delegable con múltiples usuarios y control de acceso	Sí	No	No
Herramientas de configuración de línea de comandos para tareas comunes o especializadas	Sí	No	No
Administración de usuarios y grupos centralizada	Sí	Sí	No
Administración de usuarios y grupos multiplataforma	Sí	Sí	No
Creación Web y Publicación			
Soporte integrados para extensiones Microsoft Frontpage	Sí	Sí	Sí
Soporte de publicación Frontpage para miles de sitios web en un único servidor	Sí	No	No
Soporte de publicación Netscape Gold	Sí	Sí	No
Motor de búsqueda integrado	Sí	Sí	Software adicional
Servidor automático de indexación	Sí	Sí	Software adicional

4.6 Objetivos de la infraestructura de seguridad

- Definir e implementar un esquema de seguridad basado en políticas, que permitan mantener un esquema consistente en la seguridad de contenido y control de acceso, sobre cada uno de los servicios y protocolos utilizados.
- Establecer una infraestructura de seguridad completamente integrada y escalable basada en protocolos y estándares.
- Asegurar, con la plataforma instalada, que todas las comunicaciones entre las redes internas de la empresa e Internet estén conforme a lo establecido en las políticas de seguridad.
- Contar con una infraestructura de seguridad transparente para el usuario final.
- Permitir una comunicación segura, eficiente y controlada con los clientes.
- Optimizar y garantizar los tiempos de respuesta sobre las transacciones en línea a través de la red.
- Establecer un modelo de autenticación y certificación de usuarios seguro y eficiente, de fácil administración. Encriptar la información para garantizar la *confidencialidad* de los datos y firmar electrónicamente cada transacción para asegurar la integridad de los datos que viajan entre el usuario y la empresa.

4.7 Importancia de la Auditoria Informática en el comercio electrónico

La auditoría informática juega un papel primordial en un sistema de comercio electrónico, ya que tiene como función verificar que se cumplan las políticas y controles establecidos para garantizar la seguridad en el comercio electrónico, considerando los aspectos de *confidencialidad*, autenticación, integridad, no repudio, control de acceso y *disponibilidad*, además de proponer soluciones de acuerdo a las deficiencias detectadas.

Para definir el alcance de una auditoría en un sistema de comercio electrónico así como las políticas de seguridad, es necesario conocer los elementos básicos que lo integran. Por lo que se mencionan a continuación:

- Acceso a la red de Internet y un determinado software de navegación.
- Un servidor www, es decir, un equipo en el que esté funcionando el software de servidor de Internet, que entiende los protocolos fundamentales de Internet, al menos.
- Obtener un certificado de clave pública el cual acredita el número de URL.
- Software que permite crear y administrar el catálogo de productos.

Los aspectos a considerar para auditar un sistema de comercio electrónico son:

Evaluar la seguridad lógica y física del sistema de Comercio Electrónico, considerando los siguientes aspectos:

4.7.1 Control de Acceso

Revisar que el acceso a los recursos (información, capacidad de cálculo, nodos de comunicaciones, entidades físicas, etc.) sea controlado y limitado por el sistema destino, mediante el uso de contraseñas o llaves hardware, para protegerlos de usos no autorizados o manipulación.

4.7.2 Identificación y Autenticación

Identificar el origen del mensaje, asegurando que la entidad no sea falsa. Al conectarse a un servidor Web seguro como https://www.commercialplace.com le obliga al servidor que se autentifique. Esta autentificación tiene que ver con un complejo

proceso que incluye claves públicas, privadas y un certificado digital. El certificado digital confirma que una compañía independiente y con privilegios legales asegura que el servidor Web al que se ha conectado pertenece a la compañía que dice ser.

Un certificado de seguridad válido significa que se obtiene la conformidad de que se está enviando información al lugar correcto.

El certificado de seguridad para dominios en Internet que tramita el centro proveedor Interplanet está acreditado por la empresa Thawte Consulting quien opera como Notario Virtual para toda la red Internet a la vez que da fe de la autenticidad de una empresa cuando alguien se conecta a un servidor. El certificado digital que se puede obtener para un dominio registrado en Interplanet es aceptado por los fabricantes de software más importantes y en consecuencia por los siguientes navegadores o browsers de Internet:

Netscape Navigator 3.0.
Netscape Comunicator 4.0.
Microsoft Internet Explorer 3.01.
Microsoft Internet Explorer 3.02.
Microsoft Internet Explorer Suit 4.0.

4.7.3 *Confidencialidad* e Integridad

Verificar que la información sea accesible y modificada sólo por las entidades autorizadas. Al enviar los datos desde un servidor seguro, viajan de forma cifrada, por lo que si llegaran a ser interceptados, no podrían ser descifrados, lo cual garantiza que no son manipulados en el camino.

4.7.4 No repudio

Ofrecer protección a un usuario frente a otro usuario que niegue posteriormente que en realidad se realizó cierta comunicación. Esta protección se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje. Las firmas digitales constituyen el mecanismo más empleado para este fin.

4.7.5 *Disponibilidad*

Garantizar que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando los necesiten.

Es imprescindible diferenciar cuándo los usuarios se encuentran en un servidor seguro y cuándo no. Esto resulta muy sencillo, porque el navegador de Internet se encarga de avisar por diversas señales:

1. La configuración por defecto de los navegadores avisan mediante un mensaje cuando se va a acceder a un servidor seguro, solicitando la confirmación del usuario.
2. Una vez accedido el sitio seguro, se debe siempre verificar en la barra de direcciones, que la URL comience por https://, en lugar del http://
3. El pequeño icono de la llave (o candado) que aparece en la esquina inferior izquierda de la pantalla (en Netscape Navigator) se transforma: la llave se vuelve completa o el candado se cierra, y su fondo se resalta.

Cuando estas señales aparecen, se puede estar seguro de haber entrado en un servidor seguro, pero antes de capturar el número de tarjeta de crédito, es importante

asegurarse de que la computadora realmente pertenece al dominio de la empresa en cuestión. Cualquiera de los navegadores permite comprobar los detalles de seguridad de un documento.

Se debe examinar el certificado del sitio, para ver si corresponde a la empresa que se cree, comprobando, sobre todo, que la dirección o URL sea correcta y exacta (el navegador comprueba también si la dirección del certificado coincide con la del sitio). Si el certificado fue expedido por una autoridad de certificación reconocida, el navegador, sea cual sea, lo validará sin problemas. Si la autoridad certificadora es desconocida, se dará la opción de validarlo con el riesgo de efectuar transacciones inseguras.

Una empresa que implementa un sistema de comercio electrónico necesita, entre otras cosas, instalar y configurar un servidor seguro. Obteniendo su par exclusivo de claves (pública y privada), que empleará para cifrar sus comunicaciones seguras.

Una vez generadas sus claves el servidor necesita ser certificado como servidor seguro, es decir, se requiere que una tercera parte fiable verifique la implementación que ese servidor concreto hace del protocolo de seguridad, y avale digitalmente la autenticidad de la relación entre ese servidor seguro (con sus claves), y la empresa que lo posee. Las terceras partes encargadas de otorgar certificados digitales se conocen como autoridades de certificación. Una de las más aceptadas a nivel mundial es Verisign.

También los clientes necesitan certificados para intercambiar información cifrada y autentificada con los servidores seguros. Los navegadores de Internet traen incorporadas de serie las claves públicas raíz (o certificados) de las principales autoridades certificadoras. De esta forma, cuando se visita un servidor seguro acreditado por Verisign, el navegador puede iniciar con él un intercambio cifrado, pues dispone de las claves necesarias y reconoce a Verisign como una autoridad de certificación válida.

No obstante, los navegadores proporcionan al usuario control absoluto para decidir qué certificados considera fiables y cuáles no, es decir, para retirar alguno de los existentes, actualizarlo o añadir alguno nuevo.

Además de incorporar claves públicas de autoridades de certificación se pueden solicitar, e incorporar al navegador, certificados de cliente (o usuario), de mayor o menor nivel, que le acrediten ante determinados servidores que puedan requerir su identificación, algo que será imperativo cuando se implante SET.

4.8 Políticas y controles en un sistema de comercio electrónico

Una política de seguridad informática es una forma de comunicarse con los usuarios y los gerentes. Las políticas de seguridad establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos importantes de la organización. No es una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que desea proteger y el por qué de ello.

De manera general se describen las políticas y controles en un sistema de comercio electrónico:

- Todos y cada uno de los servidores de comercio electrónico deberán contar con claves de acceso para protegerlos de usuarios no autorizados.

- Los servidores deberán contar con claves públicas y privadas así como de un certificado digital para garantizar la identificación y autenticación de las partes involucradas.

- Se debe actualizar periódicamente el certificado digital para realizar transacciones válidas y seguras.

- Los servidores deben contar con mecanismos de seguridad (firmas digitales, SET, SSL, métodos de encriptación, etc) para garantizar el flujo de la transacción.

- Debe existir tecnología de alta *disponibilidad* (*cluster*s, RAID) para contar con información segura y oportuna.

- La red interna de la empresa deberá contar con mecanismos de seguridad (firewalls) para monitorear la seguridad de la red y generar alarmas en intentos de ataque.

- El servidor debe contar con una bitácora de movimientos para validar la trayectoria y movimientos de las transacciones efectuadas.

Estas son las políticas y controles que todo sistema de comercio electrónico debe considerar como fundamentales independientemente de la infraestructura que tenga cada empresa.

4.9 Soluciones de seguridad para el comercio electrónico

Cortafuegos (Check Point Firewall-1) permite la puesta en marcha de una política de seguridad centralizada, así como su distribución en numerosos puntos de la red.

Analizador de objetos (Safe Gate Complemento OPSEC) de una nueva tecnología de inspección, con el fin de protegernos de los applets Java, componentes Active/X y otros programas telecargables.

Análisis de logs (Secure It) Proporcionan abundante información sobre el uso de la red (webs visitados, costes de comunicación, intentos de intrusión, etc.)

Antivirus (Esafe Technologies) Analiza el tráfico que llega de Internet y elimina los posibles virus, applets hostiles Java, controles Active/X, etc.

Auditoria (ISS - Internet Security Systems) Protección contra los riesgos de intrusión, análisis de las debilidades de todos los equipos conectados a las redes informáticas, detección en tiempo real de las amenazas de seguridad en los entornos de red.

Autentificación dinámica (Safe Data System) Permite asegurar la autentificación de los usuarios así como su identificación contra el recurso informático al que accede.

Protección de estaciones (EZ Lock) Para garantizar que las personas que acceden a la información sean las correctas, tanto en redes locales como en ordenadores portátiles.

Redes privadas virtuales (Aventail) Permite asegurar eficientemente las comunicaciones sobre Internet, sin reducir por ello el rendimiento de la conexión.

Alta *disponibilidad* (Legato Soluciones) software de alta *disponibilidad* para sistemas de información empresariales que funcionan en entornos heterogéneos.

Seguridad para E-Business (NetSecure) Software Soluciones de seguridad para gestionar informaciones confidenciales, ofrecer un nivel de seguridad máximo en los servicios en línea, intercambios seguros de e-mail, integridad de los datos de los servidores, protección del servidor web.

4.10 Propuesta del esquema de seguridad

El esquema de seguridad propuesto debe cumplir con los siguientes puntos:

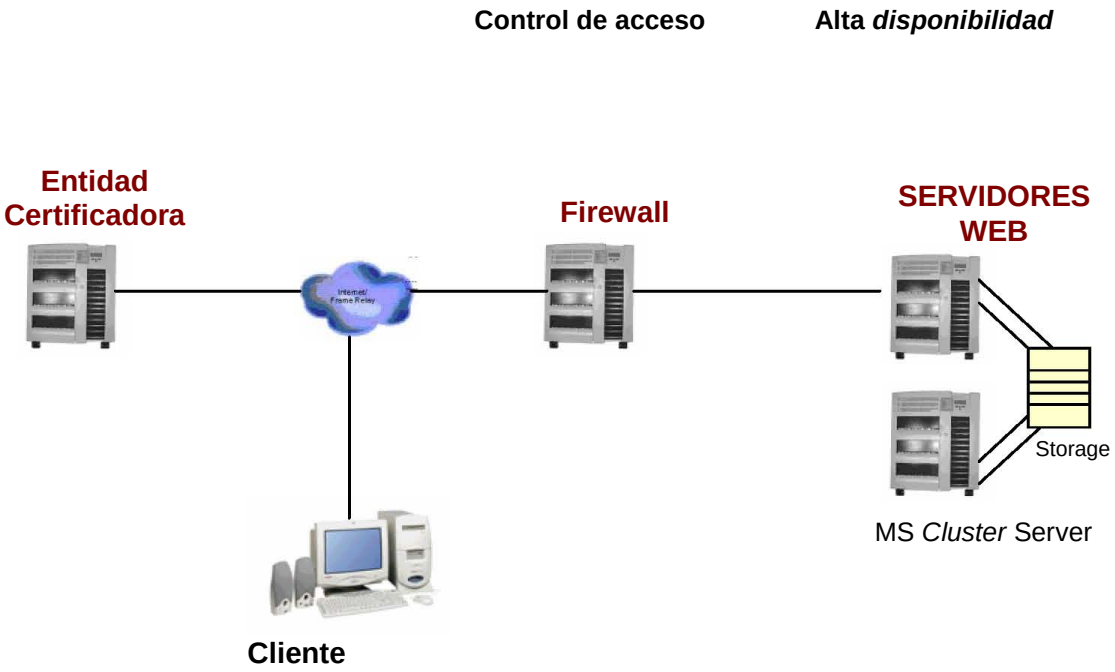
4.10.1 Implementación de un FireWall

Como filtro para el acceso a la red de la empresa:

En esta fase se instala y configura el dispositivo de FireWall, se definen las reglas o políticas de seguridad de acceso para controlar cuales entidades están autorizadas para utilizar cada uno de los servicios.

Las políticas de seguridad controlarán el acceso a la tecnología y a los sistemas de información de la empresa, los usuarios estarán restringidos en qué pueden o no hacer sobre los distintos componentes del sistema, indicando los servicios y el tipo de tráfico permitido.

Esquema de Alta *Disponibilidad* para la Seguridad



4.10.2 Autenticación, Certificación y Firma Electrónica

Es necesario proveer confianza a los clientes de la empresa y uno de los factores fundamentales para lograr esto es la validación de las entidades que intervienen en la comunicación. El cliente debe tener la certeza que la empresa es quien dice ser y viceversa. Esto proporciona un primer paso para establecer una comunicación segura y confiable. La identificación única del cliente la va a dar el certificado digital, el cual valida a cada usuario para poder utilizar los servicios. Así entonces solamente aquellos usuarios que cuenten con un certificado digital podrán tener acceso al servicio.

La propuesta debe tener...

4.10.3 Alternativas sobre los métodos de distribución de certificados

Más recomendables y seguros. Esto conlleva a las siguientes responsabilidades de la entidad certificadora:

- Generación de los certificados de los usuarios que los soliciten y que sean válidos para la empresa.
- Entrega de los certificados a los usuarios autorizados.
- Revocación de certificados a usuarios que dejen de ser válidos.

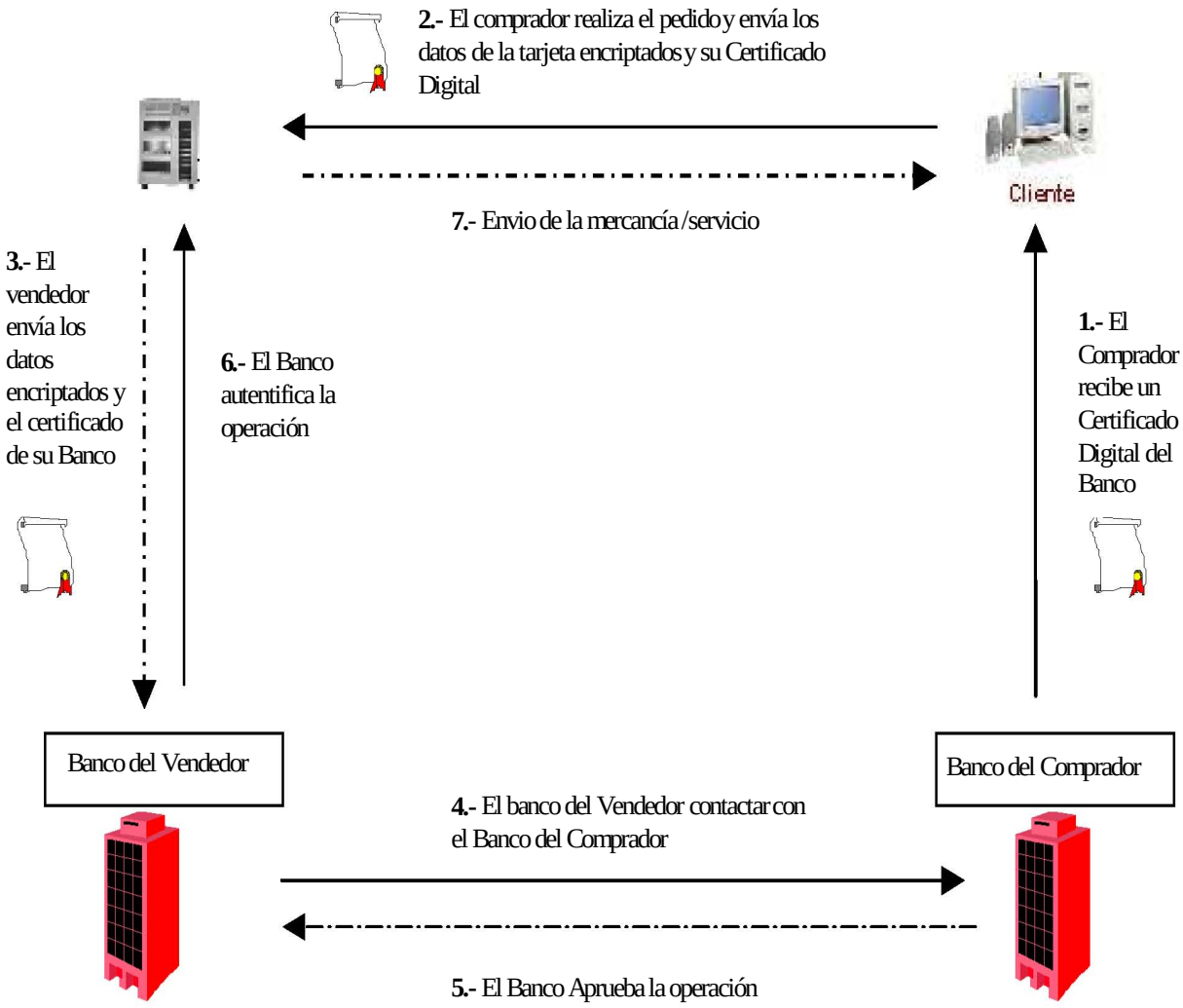
Es importante destacar que cualquier transacción realizada por un usuario con certificado lo responsabiliza directamente como autor de la operación. Evitando los posibles fraudes por la personificación de algún ente en nombre de otro, ya sea del lado del cliente como del lado de la empresa.

4.10.4 *Confidencialidad*

Este aspecto se refiere al encriptamiento de la información que viajará entre el cliente y la empresa sin importar el medio de comunicación. Es imprescindible que la comunicación se realice de una manera segura, garantizando que la información no pueda ser descifrada por entes no autorizados o no certificados

En la siguiente figura se describe el funcionamiento del protocolo SET el cual basado en la evaluación realizada anteriormente se concluye que en la actualidad es lo más completo que se tiene en cuanto a seguridad en transacciones.

Esquema de una compraventa con Protocolo SET



Los beneficios de un sistema de seguridad, bien elaborado, son inmediatos, ya que la organización trabajará sobre una plataforma confiable, que se reflejará entre otras cosas en el Aumento de clientes conformes y con ello nuevas oportunidades de negocio.

Con lo anterior se da por finalizado el Análisis de Riesgos y medidas de Seguridad que se deben tener presentes al incursionar en el Comercio Electrónico, considerando que cada vez será mayor la influencia del Comercio Electrónico en la vida diaria y se debe estar preparado para ello. Sabiendo también que cada día surgirán nuevas medidas de seguridad y con ello la oportunidad de comprar vía Internet de una forma más segura y rápida.

CONCLUSIONES

Algo de lo que se pudo ver a lo largo del desarrollo del presente trabajo es que la seguridad de las compras que se realizan por Internet es uno de los principales frenos para el despegue definitivo del comercio electrónico. El hecho de enviar información confidencial y códigos personales a través de la red, representa un freno en la decisión de compra, ya que existe cierta desconfianza y numerosas dudas acerca de la privacidad, anonimato y la confidencialidad de los datos que se envían a través de ella.

Así mismo se pudo aprender acerca de lo que es el Comercio Electrónico, los riesgos al incursionar en él, de algunos sistemas de seguridad y las opciones que se tienen para ponerla en práctica.

Aunque para algunas empresas una página web es más que nada un escaparate o medio de publicidad (por la imagen) antes que el gran negocio; si se considera como algo adicional al negocio puede ser muy bueno y además globaliza a la empresa.

Para los clientes es bueno cuando no se encuentran cerca de los negocios, cuando desde un solo lugar se puede visitar más de un sitio a la vez y si se cuenta con al menos el mínimo requerimiento de software y hardware que así lo permita. Aunque

para algunos de ellos el costo adicional en el manejo y envío hace más cara la compra, además del tiempo o contratiempos para recibir los productos.

Sin embargo, tenemos que acostumbrarnos, enfrentar y solucionar la inseguridad y los riesgos al involucrarnos con el Comercio Electrónico, como lo hacemos al contratar una tarjeta de crédito o al salir de nuestro domicilio a realizar nuestras actividades diarias.

En los últimos 5 años, millones de personas en México compraron y vendieron exitosamente a través del Comercio Electrónico, Más de 700.000 visitas únicas a diario en diferentes sitios y no siempre es necesario tener tarjeta de crédito.

Es de suma importancia incursionar en el comercio electrónico para formar parte del mundo actual tan lleno de prisa y a destiempo, el comercio electrónico cada vez es más seguro y es una manera fácil y rápida de hacer las compras desde un lugar favorito.

BIBLIOGRAFÍA

Libros

1. CONÉCTATE AL MUNDO DE INTERNET
Krol Ed
Edit. Mc Graw Hill
México 1994
597 pp.

2. APRENDA RÁPIDO INTERNET
E. Potter James
Edit. Alfaomega Grupo Editor, S.A. de C.V.
Segunda Edición, México D.F. 1996
160 pp.

3. INTERNET Y DERECHO EN MÉXICO
Barrios Garrido Gabriela, Muñoz de Alba M. Marcia, Pérez Bustillo Camilo
Edit. Mc Graw Hill,
México D.F.
421 pp.

4. COMERCIO ELECTRÓNICO
Boen Oelkers Dotty
Edit. Thomson
México D.F.
168 pp.

5. EL LIBRO DE LA JUNGLA DE INTERNET
Kretschmer Bernd
Edit. Marcombo y Data Becker Edition,
Barcelona 1996
187 pp.

Paginas de Internet:

http://www.tscm.com/compcrim-computer crime squad- FBI
http://www.onnet.es/bsa-BSA
http://www.bsa.org- BSA Estados Unidos
http://www.first.org- FIRST
http://mansci1.uwaterloo.ca/~msc1604/604_95w9.html- prevención de delitos
http://www.asertel.es/cs/comercio.htm
http://www.gvnfo.state.ut.us/sitc/elec-com/elec-com.htm
http://www.cc.emory.edu/bussiness/gds.html
http://www.adm.salvador.edu.ar/sistemas/teleinformatica/seguridad.htm
http://www.geocities.com/CapeCanaveral/2566/seguri/segurint.htm
http://www.anaya.es/diccionario/castellano/body_productos1.htm
http://ute.edu.ec/~mjativa/ce/seguridad.html
http://aui.es/biblio/libros/mi99/5seguridad_integral.htm
http://www.geocities.com/ResearchTriangle/System/9644/Trabajos/CS/Protoc.htm#SET
http://www.senyal.com/espanol/compra/comset.htm
http://www.visa.es/pys/nt/comercio3.html
http://www.kriptopolis.com/set.html
http://www.geocities.com/CapeCanaveral/2566/ssl/ssl.html
http://emision.uson.mx/tips/seguridad/comercio.htm
http://www.geocities.com/ResearchTriangle/System/9644/Trabajos/CS/Protoc.htm
http://www.geocities.com/SiliconValley/Vista/6664/legislac.html
http://www.geocities.com/SiliconValley/Horizon/4299/doc_4.html
http://www.pki.gov.ar/index.php?option=content&task=view&id=91&Itemid=102
http://www.tiendasvirtuales.com.mx/docs/nove099.html
http://www.fd.com.ar/manual7.html
http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node319.html
http://www.pki.gov.ar/index.php?option=content&task=view&id=91&Itemid=102
http://es.wikipedia.org/wiki/Certificado_digital
http://www.reduy.com/computacion/ms-com-electronico/technet-3.htm
http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml
http://www.dccia.ua.es/dccia/inf/asignaturas/PI/General.htm
http://www.informatica-juridica.com/trabajos/firma_digital.asp

CITAS TEXTUALES

(1) HERNÁNDEZ HERNÁNDEZ ENRIQUE, “AUDITORIA INFORMATICA”
México D.f
(2) http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml
(3) http://www.fd.com.ar/manual7.html
(4) http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node319.html
(5) http://www.pki.gov.ar/index.php?option=content&task=view&id=91&Itemid=102
(6) http://es.wikipedia.org/wiki/Certificado_digital
(7) http://www.reduy.com/computacion/ms-com-electronico/technet-3.htm
(8) http://www.reduy.com/computacion/ms-com-electronico/technet-3.htm
(9) http://www.reduy.com/computacion/ms-com-electronico/technet-3.htm
(10) http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml
(11) http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml
(12) HERNÁNDEZ HERNÁNDEZ ENRIQUE, “AUDITORIA INFORMATICA”
México D.f
(13) http://www.dccia.ua.es/dccia/inf/asignaturas/PI/General.htm
(14) http://www.informatica-juridica.com/trabajos/firma_digital.asp

GLOSARIO

A*posición:* sustantivo explicativo o específico.

Host: máquina conectada a una red de computadoras. Puede ser una computadora, un servidor de archivos, un dispositivo de almacenamiento por red, una máquina de fax, impresora, etc.

Cluster: grupo de múltiples computadoras unidos mediante una red de alta velocidad, de tal forma que el conjunto es visto como una única computadora r, más potente que las comunes de escritorio.

Rotures: computadoras encargadas de dirigir el tráfico de información también llamados enrutadores.

Multicast: representa un servicio de red en el cual un único flujo de datos, proveniente de una determinada fuente, se puede enviar simultáneamente a diversos receptores interesados.

Firewall: Es un dispositivo lógico que tiene como objetivo aislar una red privada del resto de las redes. Se activa automáticamente, con lo que sirve de ayuda para proteger el equipo frente a virus y otras amenazas de seguridad.

Upgrade: actualización de versiones

know how: contrato de licencia de know-how, es un negocio jurídico por el que una parte (transferente) se compromete a poner a disposición de la otra (adquirente o receptor) los conocimientos técnicos constitutivos de modo definitivo, se obliga a comunicar dichos conocimientos, posibilitando su explotación por un tiempo determinado, a cambio de una contraprestación (normalmente, una cantidad de dinero calculada como porcentaje sobre producción o venta).

Bulletin Board System: software corriente del sistema informático que permite que los usuarios marquen en el sistema sobre una línea telefónica y, con un programa, que realicen funciones tales como descargar software y los datos, leyendo noticias e intercambiando mensajes por otros usuarios.

Capstone : es un hardware orientado a la criptografía, un chip, que implementa la firma digital, propuesto por el National Institute of Science and Technology como un proceso de información federal.

Confidencialidad: La cual se refiere al servicio prestado para proteger la información principalmente de accesos no autorizados.

Disponibilidad: Consiste en lograr que todos los recursos del sistema informático se puedan tener o accesar en determinado momento.

Sellamiento electrónico: es el sistema de FIRMA ELECTRÓNICA O DIGITAL por medio del cual se pueden verificar los datos fechas de emisión del documento y otros datos de la persona, por medio de una autoridad certificadora.

Terceros de confianza (TC): Autoridad de certificación que Ofrece diversos servicios, pudiendo gozar de acceso legítimo a claves de cifrado. Una TC podría actuar como una Autoridad de certificación.