UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

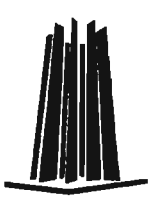
FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

"INTRODUCCIÓN AL COMERCIO ELECTRÓNICO Y SU SITUACIÓN EN MÉXICO"

T R A B A J O E S C R I T O
EN LA MODALIDAD DE EXAMEN GENERAL DE CONOCIMIENTOS
QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN
P R E S E N T A :

MARCO ANTONIO LÓPEZ RABADAN

ASESOR: M. EN C. MARCELO PÉREZ MEDEL



MÉXICO, 2005.

ÍNDICE

Capítulo 1

Objetivo

Este trabajo muestra un panorama de lo que es el comercio electrónico y los elementos que hacen posible que éste se lleva a cabo, considerando los peligros que éste implica, las soluciones que se han obtenido para poderlo explotar y los avances tecnológicos que se han desarrollado.

Introducción

El crecimiento de la tecnología en los últimos años ha generado avances y cambios en todos los aspectos. La evolución de la Internet ha sido uno de estos grandes cambios.

Internet, una red basada en millones de computadoras llamadas servidores e interconectados entre sí por todo el mundo, mediante distintos mecanismos, ha influido en nuestras vidas y en nuestras costumbres, en nuestra forma de buscar información, de entretenernos, de comunicarnos y por supuesto han aparecido nuevas formas de comprar y vender bienes. Una de las características más importantes de la Internet es que funcionan las 24 horas, los 365 días del año, y sin las tradicionales fronteras físicas creadas entre los Estados. De esta forma, ha venido a cambiar por completo la utilización de los medios de comunicación en todo el mundo.

Estos cambios traen grandes beneficios, por ejemplo hoy en día las personas se comunican desde dos puntos muy distantes del planeta, ya sea a través del teléfono o de algunos de los medios que ofrece la Internet; así mismo, las empresas han encontrado grandes oportunidades en los desarrollos de las comunicaciones, destacando que los costos de las comunicaciones se reducen y que estas tecnologías están al alcance tanto de grandes como de pequeñas empresas.

No hay ningún otro medio de comunicación que tenga la fuerza y potencia que ofrece la Internet, ya que permite la difusión de información a precios muy bajos, inclusive, inferiores a los impuestos por los medios telefónicos tradicionales. De esta forma la Internet está al alcance de todo el mundo. Los estudiantes la utilizan para obtener información y educación en línea. Profesionales como arquitectos, ingenieros, abogados y hasta doctores, ofrecen sus servicios en lugares insólitos a miles de kilómetros de distancia. Personas de todos los países y creencias encuentran un lugar para manifestar sus ideas y buscar apoyo; los niños encuentran entretenimiento y diversión; amas de casa encuentran recomendaciones sobre cómo mantener un hogar. En fin, cualquier persona es capaz de encontrar alguna utilidad o beneficio por medio de la Internet.

El hecho de que la Internet tenga el potencial de alcanzar a numerosas personas, ha centrado el interés de numerosas organizaciones y empresas relacionadas con diferentes tipos de negocios. El gran mercado potencial que representa la Internet ha traído nuevas oportunidades para aquellos negocios que permiten establecer recursos informáticos accesibles en cualquier lugar del mundo, para consumidores y socios.

La Internet es un factor que está provocando una transformación en los métodos de producción, está desapareciendo la producción en cadena y está siendo sustituida por pedidos, sin la necesidad de tener productos almacenados. Ahora aparece la empresa virtual, la empresa se convierte en un receptor de nuestro pedido vía Internet que lo rebota al fabricante quien de manera rápida le da respuesta y el cliente obtiene así el producto en poco tiempo.

En resumen, este trabajo se encuentra estructurado en siete capítulos. En el capítulo dos se hablará sobre cómo nació la Internet y se dará un vistazo a los diferentes elementos que hacen posible que éste funcione. Los elementos que se verán son: dominio, DNS, ISP, WWW, TCP/IP, HTML, URL, HTTP y páginas Web.

En el capítulo tres se da una breve explicación sobre la que son las redes virtuales privadas (VPN) que son una opción más para realizar negocios por Internet y brindan mucha seguridad en el envío de información.

En el capítulo cuatro se hablará sobre comercio electrónico, las ventajas y las desventajas que se tienen al realizar negocios por Internet. También se mostrarán algunas de las diferentes clasificaciones que se han hecho en el e-bussines. Se explicará qué es una tienda virtual, sus elementos, políticas y cómo realizar una compra.

En el capítulo cinco se hablará sobre la seguridad en el comercio electrónico que es la base principal para poder tener negocios por Internet.

En el capítulo seis se hablará sobre la legislación en materia de la Informática en México, que se encuentra un poco rezagada, pero lo que se ha legislado sirve de mucho. Se mostrarán algunos delitos que se encuentran legislados.

En el capítulo siete se darán las conclusiones del trabajo y también se incluirá la bibliografía.

Capítulo 2

Conceptos generales

Para poder entender mejor cómo funciona el comercio electrónico vamos a hablar sobre los elementos que hacen posible que éste se lleve a cabo y cómo han ido evolucionando algunos de ellos.

Internet

La Internet se define como una "red de redes", es decir, una red que no sólo interconecta computadoras, sino que interconecta redes de computadoras entre sí.

Internet nació alrededor de 1960 como un proyecto de la Advanced Research Projects Agency (ARPA) del Departamento de Defensa de los EEUU. Sus inventores lo llamaron ARPAnet. Consistía en generar una red de investigación en los ámbitos militares y científicos. Su principal finalidad, en un ámbito militar, era que un mensaje pudiera llegar a su destino sin que fuera interceptado y sin perder parte de su contenido. Esta red debía ser capaz de soportar destrozos parciales y garantizar la compatibilidad entre equipos distintos, esto en caso de un posible conflicto bélico. Esto se logró, y hoy en día la Internet ofrece mucha flexibilidad para agregar o eliminar redes en cualquier lugar del mundo sin detener la operación normal de ésta.

En sus comienzos, en 1969, la Internet constaba de cuatro computadoras interconectadas y ubicadas en El Stanford Research Institute (SRI), la Universidad de California Los Angeles (UCLA), la Universidad de California Santa Barbara (UCSB) y la Universidad de Utah (ver figura 2.1). Para 1972 y luego de que comenzara a utilizarse el protocolo[1] NCP[2] y se haya escrito el primer programa de

[1] Un protocolo es un conjunto de convenciones que determinan cómo se realiza el intercambio de datos entre dos ordenadores o programas. De forma llana se puede decir que un protocolo es un conjunto de normas que determinan cómo se realiza una acción.

correo electrónico para una red distribuida, habían pasado a ser 37 nodos en la red, 100 para 1985, 500 para 1989 y 25,000 para 1994. En enero de 1995 habían 35,000 redes interconectadas, el número de hosts conectados era de unos 4,800,000 y el número de usuarios estaba entre los 3 y los 30 millones. De esta manera Internet ha ido creciendo de manera exponencial.

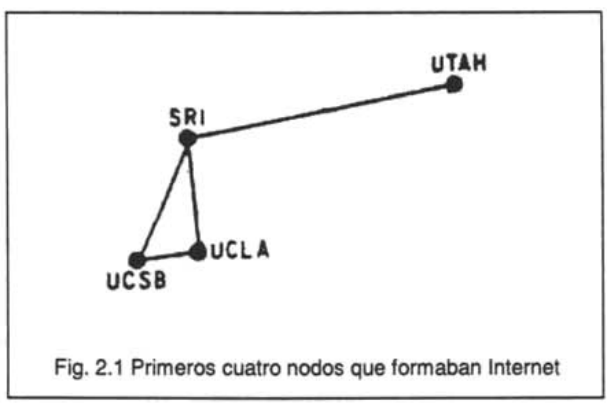


Fig. 2.1 Primeros cuatro nodos que formaban Internet

En la década de los 80, Internet se convirtió en una red básicamente de desarrollo científico, especialmente dentro de las comunidades universitarias. Aparecen las redes locales y estaciones de trabajo con UNIX[3] y TCP/IP. A lo largo de esta década se produce una gran expansión de la red, se conectan a la Internet las primeras redes europeas y también japonesas, con lo que la red ya es de ámbito verdaderamente mundial, pero como frecuentemente ocurre, el uso que más se le dio no fue por el cual fue creada originalmente (Investigación), sino la utilización de un servicio subvalorado en un principio: el correo electrónico o e-mail.

---

[2]NCP (Netwok Control Protocol o Protcolo de Control de Red). ARPANET comenzó utilizando este protocolo ya que utilizaba técnicas de conmutación de paquetes. Este protocolo fue rápidamente reemplazado por el protocolo TCP/IP (Transmission Control Protocol/Internetwork Protocol). El 1°. de Enero de 1983 se abandona definitivamente el protocolo NCP, utilizándose exclusivamente TCP/IP que ya había sido aceptado como sustituto oficial del primitivo NCP.

[3] UNIX es un complejo y potente sistema operativo multiproceso/multitarea y multiusuario orientado a comunicaciones. Fue desarrollado en 1969 por Ken Thompson y Dennis Ritchie de los laboratorios Bell, empresa norteamericana.

A finales de los ochenta se producen grandes cambios, aparecen los primeros "crackers[4]" y "hackers[5]", aparecen los primeros virus[6], la agencia ARPA se retira de la red y sobre todo aparece la World Wide Web (la Telaraña Global). También aparece el protocolo de transmisión HTTP y el lenguaje HTML en que se basa la "Web".

El acceso al público llegó a comienzos de 1990, cuando varias compañías comenzaron a ofrecer el acceso a la red a usuarios particulares en sus casas. Esto permitió que cualquier persona que tuviera en su casa un módem y un ordenador, pudiera tener acceso a Internet.

La historia de la Internet en México empieza en el año de 1989 con la conexión del ITESM (Instituto Tecnológico y de Estudios Superiores de Monterrey, en el Campus Monterrey) hacia la UTSA (Universidad de Texas en San Antonio), específicamente a la escuela de Medicina. Una línea privada analógica de 4 hilos a 9,600 bits por segundo fue el enlace.

Sin embargo, antes de que el ITESM se conectara a Internet, casi a finales de los 80's, recibía tráfico de BITNET[7] por la misma línea privada. El ITESM era participe de BITNET desde 1986. Y la UNAM se conectó a BITNET en octubre de 1987.

El primer nodo en México conectado a Internet fue el ITESM, campus Monterrey, y pasó a ser el primer Name Server para el dominio .mx. Esto fue Febrero de 1989.

---

[4] Cracker es aquella persona que rompe la seguridad de un sistema remoto con el fin de causar un daño, robando información, destruyéndola o realizando otra actividad que cause un daño.

[5] Hacker es una persona experta en informática que entra en sistemas ajenos para mostrar la baja seguridad de los mismos. Regularmente no entran a otros sistemas para hacer daño alguno, sólo por diversión.

[6] El primer virus de Internet fue el 2 de Noviembre de 1988, el llamado "Gusano de Internet de 1988". Robert Tappan Morris, estudiante de la universidad de Cornell que entonces tenía 23 años, fue el creador de este programa que no hacía otra cosa que reproducirse indefinidamente. A Robert le condenaron a tres años y después fundó la empresa Viaweb Inc a que más tarde compraría Yahoo! inc.

[7] La Red Bitnet es una de las primeras redes académicas y de investigación que se estableció a nivel mundial. El sistema tuvo un crecimiento muy importante en la década de los 80 y llegó a su apogeo al final de esta década con 3500 nodos en 46 países alrededor del mundo.

El segundo nodo fue la UNAM, en el Instituto de Astronomía en la Ciudad de México. Esto mediante una conexión vía satélite de 56 Kbps, con el Centro Nacional de Investigación Atmosférica (NCAR) de Boulder, Colorado, en los Estados Unidos de Norteamérica.

Después de esto, lo que proseguía era una interconexión entre la UNAM y el ITESM (Campus Monterrey), esto se hizo usando líneas privadas analógicas de 9600 bps.

Después el ITESM, en su Campus Estado de México, se conecta a través del Centro de Investigación Atmosférica (NCAR) a Internet. Como la UNAM, obtiene una conexión satelital de 56 kbps, es decir, enlace digital. La función de este enlace es dar servicio a los demás ITESM, diseminados a través de todo el país.

El ITESM promovió y logró que la Universidad e las Américas (UDLAP) en Puebla y el Instituto Tecnológico de Estudios Superiores de Occidente (ITESO) en Guadalajara se enlazaran a Internet por medio del mismo ITESM. Aunque esto fue con enlaces de baja velocidad, de 9600 bps.

Así varias universidades del país fueron obteniendo enlaces para conectarse a Internet por medio del ITESM, de la UNAM o de alguna universidad de los Estados Unidos.

En enero de 1992, en la Universidad de Guadalajara y por iniciativa de varias universidades (ITESM, Universidad de Guadalajara, Universidad de las Américas, ITESO, Colegio de Postgraduados, LANIA, CIQA, Universidad de Guanajuato, Universidad Veracruzana, Instituto de Ecología, Universidad Iberoamericana e Instituto Tecnológico de Mexicali), se creó un organismo para coordinar a las Universidades interesadas en contribuir al desarrollo de la Internet en México: MEXnet.

En junio de 1992, MEXnet estableció una salida digital de 56 kbps al Backbone de Internet. Ese mismo año otras instituciones educativas también se integraron a MEXnet, entre ellas el Instituto Politécnico Nacional (IPN), la Universidad Autónoma Metropolitana (UAM), la Universidad Panamericana (UP) y la Universidad Autónoma de San Luis Potosí (UASLP). En 1993 también se incorporaron la Universidad Autónoma de Nuevo León (UANL) y la Universidad Autónoma de Puebla (UAP).

En 1994 con la plena consolidación mundial a la WWW dieron inicio las actividades comerciales a través de Internet.

Definitivamente Internet ha dejado atrás a todas las demás tecnologías. Al radio le tomó casi 40 años poder llegar a una audiencia de 50 millones de personas, a la televisión 13 años, a la Internet en menos de 4 años ya alcanzaba esa audiencia.

Dispuestos a alcanzar a todos estos usuarios, la mayoría de las grandes empresas crearon sus propios sitios en el WWW para vender o informar acerca de sus productos. Para el 2003 el número de usuarios ascendió a 675 millones y se espera que para finales del 2005 esta cifra crezca a 1,000 millones de usuarios.

Algunos usos de los más comunes que se le dan a la Internet son los siguientes:

- **Correo Electrónico (e-mail).** Sirve para enviar y recibir mensajes a otros usuarios, por este medio se pueden enviar gráficos, textos, programas ejecutable, etc. Es tal vez el principal servicio de la Internet, y sin duda el de mayor importancia histórica.
- **Chat (Conversación), Messenger (Mensajería).** Esto facilita mucho las cosas ya que por este medio los usuarios se pueden comunicar mediante el teclado o un micrófono, se puede localizar a otro usuario que se encuentre en línea (conectado), e intercambiar archivos.
- **Investigación.** Esta ocupa hoy en día el segundo lugar en el orden de trabajo de la red. Universidades, museos, bibliotecas, agencias,

fundaciones, grupos de investigación, etc., han puesto en la red una inmensa cantidad de información que puede ser consultada.

- **Grupos de debate.** Es una manera de usar la Internet como foro de discusión para personas interesadas en debatir sobre un mismo tema sin importar la distancia física que los separa.
- **Noticias.** Es un servicio que ofrece la Internet para intercambiar diariamente grandes cantidades de información divida por temas. Cada noticia consta de una cabecera (información técnica dividida hasta en 20 apartados), cuerpo (el texto en sí) y signatura o firma (información sobre el usuario que envío la noticia).
- **Comercio**. Este servicio está creciendo cada vez más, y está logrando ser más aceptado. Trata de la compra - venta de servicios y/o productos a través Internet.
- **Transferencia de ficheros (FTP)**. FTP son las iniciales de File Transfer Protocol (Protocolo de Transferencia de Ficheros). Con esta herramienta conseguimos bajar a nuestro ordenador ficheros almacenados en otros ordenadores remotos y también subir ficheros desde el nuestro propio.

Dominio

Debido a que es muy difícil recordar todas las direcciones IP[8] a las que se requiere acceder, y debido a que en ocasiones las direcciones IP necesitan cambiar, se utilizan nombres más significativos y fáciles de recordar que representan direcciones IP, y que no cambian aunque ésta tenga que cambiar. A estos nombres se les ha llamado nombres de dominios.

Un nombre de dominio es una secuencia de nombres separados por el carácter punto. Por ejemplo: www.fi.upm.mx. Esta máquina pertenece al dominio fi que a su vez pertenece al dominio upm y éste a su vez, al dominio mx (México).

[8] Una dirección IP es un número de 32 bits que normalmente se escribe como cuatro números entre 0 y 255 separados por puntos (192.11.36.5). Esta dirección permite encontrar un computador en una red.

Los dominios se organizan en una estructura jerárquica con forma de árbol que los clasifica en niveles tal como se muestra en la figura 2.2.

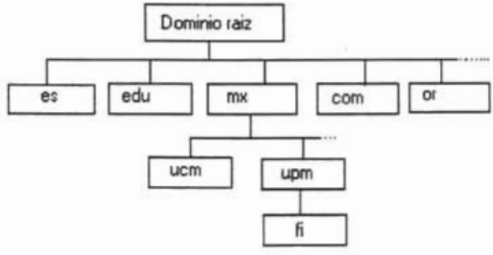


Fig. 2.2 Estructura jerárquica de los dominios en forma de árbol

El punto más alto de la jerarquía es el dominio raíz. Los dominios de primer nivel (es, edu, mx, com, etc.) parten del dominio raíz y los dominios de segundo nivel (upm, ucm, etc.) de un dominio de primer nivel; y así sucesivamente. Cada uno de los dominios puede contener tanto hosts como más subdominios.

Los nombres de los dominios son asignados por InterNIC, que es la organización mundial que actúa como autoridad máxima en la asignación para garantizar una única dirección para cada dominio. InterNIC delega a otras organizaciones la tarea de registrar aquellos dominios propios de cada país. En México es el "NIC-México" quien mantiene el sistema de nombres de dominio para todo el país.

El NIC-México nace el 1º de Febrero de 1989 cuando el ITESM, Campus Monterrey establece conexión directa a Internet. Se conectó bajo el dominio dns.mty.itesm.mx con la dirección IP 131.181.1.1.

Para 1992 había sólo 45 dominios bajo .mx, de los cuales 40 eran académicos y 5 eran comerciales.

DNS (Domain Name System)

Originalmente cuando la Internet inicio, el número de sistemas en la red era muy pequeño, y entonces cada sistema disponía de una lista completa con los nombres de dominio y direcciones IP existentes, pero con el crecimiento de la Internet, los archivos que tenía esta lista de nombres se volvió muy grande, de cientos de ordenadores, y era muy difícil de manejar esta lista. Aún más, cuando se agregaba un sistema a la red era necesario actualizar la lista de nombres e IP en todos los sistemas de la red.

Entonces se optó por tener la tabla con los nombres de dominio y direcciones IP en un único ordenador con el nombre de HOSTS.TXT. El resto de ordenadores debían consultarle a éste cada vez que tenían que resolver un nombre. Esto funcionaba bien ya que la lista sólo se actualizaba una o dos veces por semana y con esto ya no era necesario actualizar la lista en todos los ordenadores conectados a la red.

Sin embargo, a medida que se fueron conectando más ordenadores a la red comenzaron los problemas, el fichero HOSTS.TXT comenzó a ser demasiado extenso, el mantenimiento se hizo difícil ya que requería más de una actualización diaria y el tráfico de la red hacia que este ordenador se saturara.

Es por ello que fue necesario diseñar un nuevo sistema de resolución de nombres que distribuyese el trabajo entre distintos servidores. Se ideó entonces un sistema conocido como DNS (*Domain Name System*, sistema de resolución de nombres).

Este sistema utiliza un modelo cliente/servidor, en el cual los servidores DNS (servidores de nombres) contienen información acerca de la base de datos DNS y la ponen a disposición de sus clientes.

La forma en la que funciona este sistema de resolución de nombres es la siguiente: un cliente DNS envía una petición de resolución de nombres a un servidor DNS. Este servidor busca en sus bases de datos y si tiene la información da respuesta, pero sino tiene la información en su base de datos entonces reenvía

la petición a otro servidor DNS de nivel superior que le puede responder con la dirección IP solicitada o con la dirección de otro servidor DNS de un nivel superior.

Por ejemplo, en la resolución de la dirección del servidor www.fi.upm.mx ocurriría lo siguiente:

1. Nuestra computadora (cliente DNS) formula una pregunta a nuestro servidor DNS local (generalmente el proveedor de Internet).
2. El servidor local es el responsable de resolver la pregunta, aunque para ello tenga que reenviar la pregunta a otros servidores. Suponemos que no conoce la dirección IP asociada a www.fi.upm.mx; entonces formulará la pregunta a uno de los servidores de dominio raíz.
3. El servidor del dominio raíz no conoce la dirección IP solicitada, pero devuelve una referencia de los servidores de nombres encargados del dominio DNS *mx*.
4. El servidor local reenvía la pregunta iterativa a uno de los servidores de dominio DNS mx, especificados en el punto anterior.
5. El servidor del dominio mx tampoco conoce la dirección IP preguntada, aunque sí conoce la dirección de los servidores de nombres encargados del dominio DNS upm, por lo que devuelve una referencia de éstos.
6. El servidor local reenvía la pregunta iterativa a uno de los servidores de dominio DNS upm, especificados en el punto anterior.
7. El servidor del dominio upm conoce la dirección IP de www.fi.upm.mx y devuelve esta dirección al servidor local.
8. El servidor local al encontrar la respuesta se la reenvía a nuestra computadora

ISP (Internet Service Provider)

Un proveedor de servicios de Internet o ISP es una empresa que conecta sus ordenadores a Internet de forma permanente y permite que otros usuarios o clientes se conecten a la Red accediendo a través de éstos.

Básicamente los ISP son puertas por las que se puede entrar a Internet. Un usuario o cliente, marca un número de teléfono asignado al ISP, el cual, mediante una clave previamente acordada, permitirá que dicho cliente acceda a la red.

Los ISP se conectan al esqueleto de la Internet para formar "espinas dorsales" (backbones), que son redes de alta velocidad en fibra óptica que manipulan toda la información digital, formando redes centrales, a las que se conectan las redes nacionales y locales. Los backbones están conectados alrededor del mundo mediante grandes estructuras de cableado, fibra óptica, cables submarinos o conexiones satelitales. Aquí en México existen tres backbones oficiales, dos de Avantel y uno de Telnor (Telmex).

Los proveedores (ISP) de nivel 1 mantienen un enlace directo a los backbones de la Internet. Conectados a estos proveedores de nivel 1 se pueden conectar otros ISP de menor tamaño, otras redes, compañías o usuarios finales. La figura 2.3 ilustra esto.

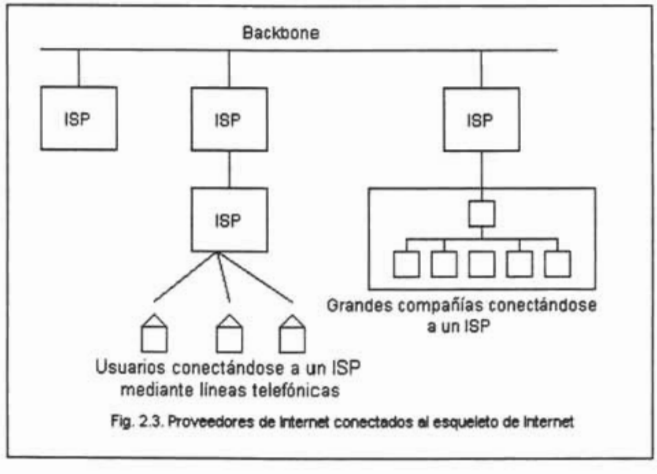


Fig. 2.3. Proveedores de Internet conectados al esqueleto de Internet

Cabe mencionar que en México, entre 1989 y 1993, las universidades operaron como los únicos proveedores de acceso a la Internet

World Wide Web

La World Wide Web (del inglés, La Gran Telaraña Mundial), la Web o WWW, es el servicio más utilizado en la actualidad por los usuarios de la Internet, junto al tan conocido e-mail.

La WWW fue creada en el Laboratorio Europeo de Física de Partículas (CERN) en Ginebra en 1991 por Tim Berners Lee, quién utilizó tres nuevos recursos: HTML (Hypertext Markup Language), HTTP (Hypertext Transfer Protocol) y un programa cliente, llamado Web Browser. Recién creada la WWW era difícil utilizarla, los usuarios debían ser verdaderos especialistas para moverse de un lugar a otro. Hasta que apareció Mosaic[9], el primer buscador de gran difusión utilizado para navegar en la red, desarrollado por Marc Andreseen, fundador luego de la empresa Netscape.

La World Wide Web es una inmensa colección de documentos multimedia (esto quiere decir que pueden incluir texto, video, animación y sonido) relacionados entre sí a través de vínculos de hipertexto[10]. De esta manera, ir de un documento a otro en la Web se vuelve algo fácil y rápido.

La empresa norteamericana CERN definió la WWW como *"un sistema capaz de saltar de un sitio a otro de una forma automática, presentando una diversidad de datos que de otra forma no estarían disponibles"*. Se predispuso que los recursos disponibles en distintas conexiones fuesen disponibles para cada investigador desde su computadora, de una forma transparente y exenta de dificultades.

---

[9] El Mosaic, no fue el primer navegador, ni siquiera el primera navegador gráfico, pero si fue considerado por la mayoría de la gente el navegador más fácil de usar. Se instalaba fácilmente, permitía navegar con toda facilidad por la WWW y funcionaba en diferentes plataformas. Era fácil de utilizar inclusive para un principiante, de ahí su gran difusión y éxito.

[10] Hipertexto son datos que contienen enlaces (links) a otros datos o documentos.

El sistema WWW fue el sucesor de Gopher[11], un servicio de Internet que organizaba la información y permitía acceder a ella en forma sencilla. El éxito del WWW se debió a que integra en una sola interfaz los múltiples servicios utilizados en las distintas redes (ftp, mailito, news, gopher, etc.), de manera que permite una interacción eficiente y sencilla con los usuarios.

Junto con la WWW fue creado el lenguaje HTML, que permite escribir documentos con hipertexto, y el protocolo HTTP, que define las reglas para poder acceder a estos documentos. De esta manera se empezó a explotar de mejor manera el uso de la WWW.

[11] Gopher organizaba la información en menús y documentos de texto sencillos, brindando una interfaz amigable para acceder a los recursos de Internet. Permitía localizar información en Internet, pero no tenía las posibilidades reales de hipertexto o gráficos en línea

TCP/IP

El protocolo de comunicación que se utilizó inicialmente, cuando surgió ARPANET, fue el NCP. Éste tenía algunos inconvenientes: no tenía la capacidad de direccionar redes (y máquinas) más lejos que un destino IMP[12] en el ARPANET, lo que sería equivalente hoy en día a, no direccionar más allá de un ruteador. Además no tenía control de errores, ya que como era tan fiable no se requería ningún control, y si algún paquete se perdía, el protocolo (y cualquier aplicación que éste soportara) se estancarían.

Estos inconvenientes ameritaban un cambio en el protocolo. Por lo que en 1978 se publicaron las especificaciones del Protocolo de Control de Transmisión (TCP - Transmission Control Protocol) y el Protocolo de Internet (IP - Internet Protocol). Los dos protocolos a la vez facilitaron los medios para transmitir paquetes de forma segura a cualquier host de la red y la comunicación entre terminales mediante una multitud de redes diversas. El 1º de enero de 1983 el protocolo NCP fue sustituido por el TCP/IP.

Estos dos protocolos, TCP/IP, permiten la comunicación en la Internet. No forman un único protocolo sino que son protocolos separados, pero sin embargo están estrechamente relacionados para permitir una comunicación más eficiente.

Ellos dividen los datos en secciones denominadas paquetes, entregan estos paquetes a su sitio de destino en la Intranet o Internet y les devuelven a estos paquetes su forma original para que se puedan visualizar y utilizar.

El TCP tiene como misión dividir los datos en paquetes pequeños que serán enviados a otro hosts, y reensamblar los paquetes que vaya recibiendo. Durante este proceso proporciona a cada uno de estos paquetes una cabecera que

contiene diversa información, como un número de secuencia, el cual permitirá poner en orden los paquetes para reensamblar la información nuevamente, también permite saber si falta algún paquete y en dado caso solicitarlo. Otro dato importante que se incluye es el denominado checksum o *suma de comprobación*, que coincide con el número total de datos que contiene el paquete. Esta suma sirve para averiguar en el punto de destino si se ha producido alguna pérdida de información.

El protocolo IP es encargado de hacer llegar cada uno de los paquetes a su destino. Para esto, a cada paquete le agrega una cabecera con cierta información como la dirección destino, dirección del remitente, tiempo de vida del paquete antes de ser descartado, etc. A este nuevo paquete se le llama datagrama.

Los datagramas son enviados a los ruteadores, que deciden en cada momento cuál es el camino más adecuado para llegar a su destino. Dado que la carga de Internet varía constantemente, los paquetes pueden ser enviados por distintas rutas, llegando entonces de forma desordenada.

Con la llegada de los paquetes a su destino, se activa de nuevo el protocolo TCP, que realiza una nueva suma de comprobación y la compara con la suma original. Si alguna de ellas no coincide, detectándose así pérdida de información en el trayecto, se solicita de nuevo el envío del paquete desde el origen. Por fin, cuando se ha comprobado la validez de todos los paquetes, el TCP los une formado el mensaje inicial.

A esta forma de enviar la información en paquetes se le denomina "Conmutación de paquetes"

---

[12] IMP – Interface Message Processor, Procesador de mensajes de Interfaz. Posibilitaba a varios hosts interconectarse mediante una red de computadores intermediarios, éstos son los antecesores de los actuales ruteadores. Bajo esta interfaz trabajaba ARPANET inicialmente para poder comunicar los diferentes hosts entre si. IMP no da la capacidad de comunicación entre terminales de diversas redes, este es un motivo por el cual fue reemplazado por el TCP/IP.

URL

El protocolo HTTP, que será explicado a continuación, emplea localizadores uniformes de recursos (URL) para localizar datos en la Internet. Si se conoce el URL de archivos HTML disponibles para el público en cualquier punto de la World Wide Web, se puede acceder a esos datos a través de HTTP.

La URL es básicamente es una extensión de la ruta que define a un fichero. Un URL añade un prefijo que identifica el método de recuperación de la información que ha de emplearse (http, ftp, gopher, telnet, news, etc.), así como un nombre de dominio o dirección IP que indica el servidor que almacena la información y por último aparece la ruta de acceso al fichero. Ver figura 2.4.

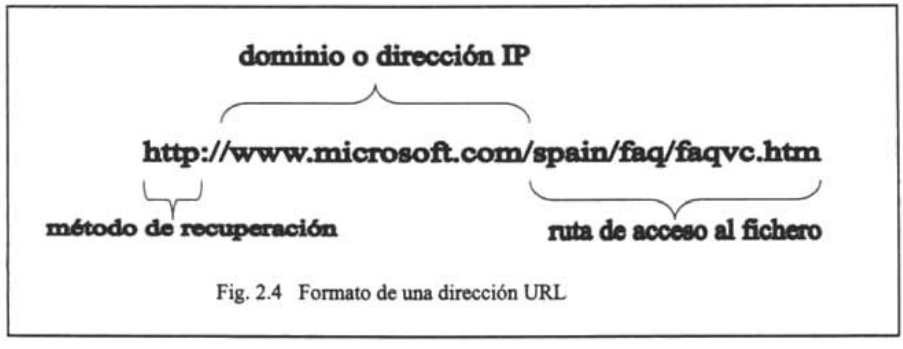


Fig. 2.4 Formato de una dirección URL

HTTP

El protocolo HTTP (HyperText Transfer Protocol, es un protocolo de transferencia de hipertexto) que constituye la base de la World Wide Web, es un sencillo protocolo cliente/servidor que permite a los clientes Web y los servidores HTTP intercambiar información. Utiliza el protocolo TCP para hacer las conexiones, y funciona de la misma forma que el resto de los servicios comunes de los entornos UNIX. Un proceso servidor escucha en un puerto de comunicaciones TCP (por defecto el 80), y espera las solicitudes de conexión de los clientes Web. Una vez

que se establece la conexión, el protocolo TCP se encarga de mantener la comunicación y garantizar un intercambio de datos.

El protocolo HTTP se basa en sencillas operaciones de solicitud/respuesta. Un cliente establece una conexión con un servidor y envía un mensaje con los datos de la solicitud. El servidor responde con un mensaje similar, que contiene el estado de la operación y su resultado. Todas las operaciones pueden adjuntar un objeto o recurso sobre el que actúan (documento HTML, fichero multimedia o aplicación CGI) que es conocido por su URL. En este protocolo es siempre el cliente quien inicia la transacción estableciendo una conexión y enviando una petición HTTP y la conexión la puede terminar en cualquier momento el cliente o el servidor como se muestra en la figura 2.5.

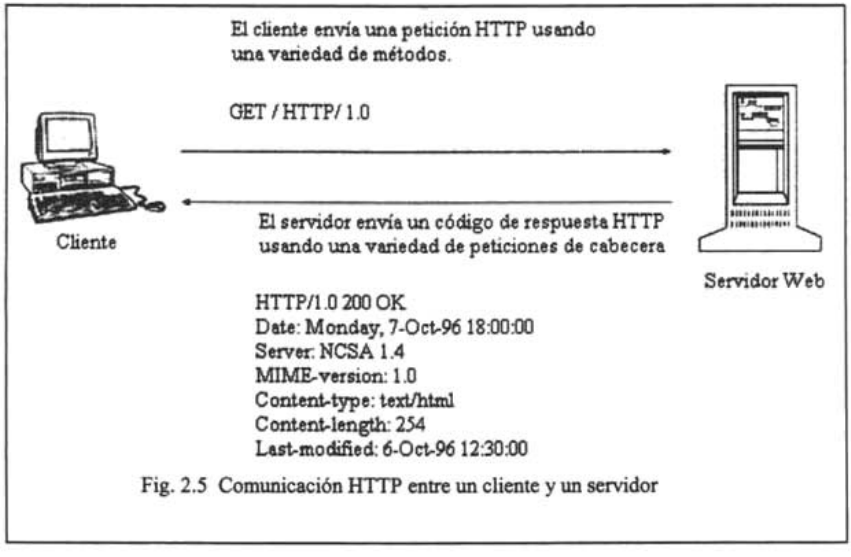


Fig. 2.5 Comunicación HTTP entre un cliente y un servidor

Cada vez que un cliente realiza una petición a un servidor, se ejecutan los siguientes pasos:

1. Un usuario accede a una URL, seleccionando un enlace de un documento HTML o introduciéndola directamente en el campo Location del cliente Web.
2. El cliente Web decodifica la URL, separando sus diferentes partes. Así identifica el protocolo de acceso, la dirección DNS o IP del servidor, el posible puerto opcional (el valor por defecto es 80) y el objeto requerido del servidor.
3. Se abre una conexión TCP/IP con el servidor, llamando al puerto TCP correspondiente.
4. Se realiza la petición. Para ello, se envía el método de petición (GET, POST, HEAD, etc.), la dirección del objeto requerido (el contenido de la URL que sigue a la dirección del servidor), la versión del protocolo HTTP empleada y un conjunto variable de información, que incluye datos sobre las capacidades del browser, datos opcionales para el servidor, etc.
5. El servidor devuelve la respuesta al cliente. Consiste en un código de estado seguido de la propia información.
6. Se cierra la conexión TCP.

Anteriormente este proceso se repetía en cada acceso al servidor HTTP. Por ejemplo, en la solicitud de un documento HTML en cuyo interior están insertadas cuatro imágenes, el proceso anterior tenía que repetirse cinco veces, una para el documento HTML y cuatro para las imágenes.

En la actualidad se ha mejorado este procedimiento, permitiendo que una misma conexión se mantenga activa durante un cierto periodo de tiempo, de forma que sea utilizada en sucesivas transacciones. Este mecanismo, denominado HTTP Keep Alive, es empleado por la mayoría de los clientes y servidores hoy en día.

Esta mejora es imprescindible en una Internet saturada, en la que el establecimiento de cada nueva conexión es un proceso lento y costoso.

Existen diferentes métodos de petición HTTP. La tabla 2.1 muestra algunos de estos[13]:

Método	Descripción
GET	Es el más simple y probablemente el más usado. Simplemente regresa la información identificada por el URL. Si el URL hace referencia a un script (CGI, servlets, etc), entonces regresa la información producida por el script.
HEAD	Provee la misma funcionalidad que GET, sólo que HEAD no regresa el archivo solicitado, éste regresa meta-información como código de respuesta del servidor, fecha del archivo, encabezados del archivo, etc., sin el cuerpo del documento.
POST	Es usado en las formas de HTML, sirve para transferir bloques de información al servidor como respuesta a los formularios.
OPTIONS	Es usado para consultar al servidor acerca de sus capacidades y funciones.
PUT	Es similar al put del ftp. Almacena una entidad en la localidad especificada.
DELETE	Es usado para borrar un documento del servidor.
TRACE	Es similar que la herramienta traceroute, sirve para detectar problemas en la red. Traza la ruta entre el cliente y el servidor..

Tabla 2.1 Algunos métodos de petición HTTP

El servidor tiene cuatro formas de responder ante estas peticiones: Exitosa, Redirección, Error del cliente o Error del servidor. La tabla 2.2 muestra estas respuestas.

Código de respuesta	Descripción
Respuesta exitosa 2xx	
200 OK	La petición ha sido exitosa.
Redirección 3xx	
301 Movido permanentemente	El servidor ha sido movido a una nueva URL de forma permanente.
302 Movido temporalmente	El servidor ha sido movido a una nueva URL de forma temporal.
Error de cliente 4xx	

[13] Hay que tomar en cuenta que la versión 1.0 de http sólo incluía los métodos GET, HEAD y POST.

400 Mala petición	La petición no fue entendida por el servidor.
401 Sin autorización	El recurso requiere autenticación por parte del usuario.
403 Prohibido	El servidor entiende la petición pero se rehúsa a responder. Con el método GET no se obtendrá mucha información con esta respuesta, pero con HEAD se puede tener más detalle al respecto.
404 No encontrado	El recurso no fue encontrado.
Error del servidor	
500 Error interno del servidor	El servidor encuentra un error interno el procesamiento de la petición.
501 No implementado	El servidor no soporta la petición.
503 Servicio no disponible	El servidor no es capaz de responder a la petición porque se encuentra saturado.

Tabla 2.2 Respuestas a las peticiones HTTP

Veamos el proceso con un ejemplo:

1. Desde un cliente se solicita la URL http://www.unican.es/invest/default.html
2. Se abre una conexión TCP/IP con el puerto 80 del sistema www.unican.es.
3. El cliente realiza la solicitud, enviando algo similar a esto:

```
GET /invest/default.html HTTP/1.0        Operación solicitada + objeto + versión de HTTP
Accept: text/plain                       Lista de tipos MIME[14] que acepta o entiende el cliente
Accept: text/html
Accept: audio/*
Accept: video/mpeg
.. .. ..
Accept: */*                              Indica que acepta otros posibles tipos MIME el cliente
User-Agent: Mozilla/3.0 (WinNT; I)       Información sobre el tipo de cliente
Línea en blanco, indica el final de la petición
```

[14] El tipo MIME especifica el tipo de dato (texto plano, texto html, imagen, sonido, etc,) que contiene la información que se transfieren un cliente y un servidor.

4. El servidor responde con la siguiente información:

HTTP/1.0 200 OK	Status de la operación; en este caso, correcto
Date: Monday, 7-Oct-96 18:00:00	Fecha de la operación
Server: NCSA 1.4	Tipo y versión del servidor
MIME-version: 1.0	Versión de MIME que maneja
Content-type: text/html	Definición MIME del tipo de datos a devolver
Content-length: 254	Longitud de los datos que siguen
Last-modified: 6-Oct-96 12:30:00	Fecha de modificación de los datos
Línea en blanco	
<HTML>	Comienzo de los datos

<HEAD><TITLE>Recursos de investigación en UNICAN</TITLE></HEAD>
<BODY>
.. .. ..
.. .. ..
</HTML>

5. Se cierra la conexión.

HTML "Hypertext Markup Language "

HTML es un lenguaje que se utiliza en la construcción de páginas HTTP, sitios y otras aplicaciones basadas en la Web. El HTML utiliza una serie de etiquetas especiales intercaladas en un documento. Dichas son posteriormente interpretadas por los navegadores (Internet Explorer, Netscape Navigator o cualquier otro) encargados de visualizar la página con el fin de establecer el formato. Por medio de estas etiquetas se puede definir la apariencia de los documentos (colores, tamaño, formas, tipos de letras, etc), es decir, la forma en que se mostrará la información en el navegador.

Básicamente, HTML sólo es suficiente para visualizar documentos, imágenes, sonido, hacer enlaces entre páginas, incluir formas y otros elementos multimedia.

HTML realmente no es un lenguaje de programación, ya que no implementa algunas funciones básicas de cualquier lenguajes de programación como acceso a bases de datos, funciones de edición de gráficos, sentencias de control (while, for, if, case), etc., Además no es necesario compilar el código que se escriba con este lenguaje como se hace comúnmente con otros lenguajes de programación. El HTML es un lenguaje de marcado que indica al browser como desplegar los

diferentes elementos que este maneja, por lo tanto no se considera un lenguaje de programación. Cuando se encuentra un error de sintaxis el browser simplemente lo ignora y despliega lo que puede interpretar.

Páginas Web

No es lo mismo hablar de la Web o WWW que hablar de una página Web. La Web o WWW es la gran telaraña mundial, mientras que una página Web es un archivo de texto que contiene lenguaje de marcas de hipertexto (HTML), etiquetas de formato y vínculos a archivos, gráficos y a otras páginas Web.

El archivo de texto se almacena en un servidor de Web al que pueden acceder otras computadoras conectadas a ese servidor, vía Internet o una LAN. Al archivo se puede acceder utilizando exploradores Web que no hacen otra cosa que efectuar una transferencia de archivos e interpretación de las etiquetas y vínculos, y muestran el resultado en el monitor.

Cuando se utiliza un hipervínculo para ir de una página a otra, por medio del URL, se localiza la dirección de la página a la que se desea acceder y por medio del protocolo HTTP es transferida la nueva página a través de la WWW.

Una sitio Web está formado por una serie de páginas, éstas pueden ser estáticas o dinámicas.

Páginas Estáticas.

Son aquellas que se muestran siempre con la misma información, cada que los visitantes soliciten una página, verán siempre lo mismo. Si se desea actualizarla o modificarla se deberá modificar el código fuente de la página. Este tipo de páginas regularmente sólo están escritas en HTML que no permite crear efectos o funcionalidades más allá de los enlaces.

Estas páginas son muy sencillas de crear, aunque ofrecen pocas ventajas tanto a los desarrolladores como a los visitantes, ya que sólo se pueden presentar textos planos acompañados de imágenes y a lo sumo contenidos multimedia como pueden ser videos o sonidos

Páginas Dinámicas

Una página es dinámica cuando realiza efectos especiales o implementa alguna funcionalidad o interactividad. Estas páginas pueden ser actualizadas mientras se visualizan. Una vez creada y puesta en línea no se necesitará modificar el código fuente para actualizarlas, estas pueden tener un control total o parcial de la información.

Para programar una página dinámica es necesario utilizar otros lenguajes y/o herramientas aparte del HTML. Estas páginas son creadas al momento que el usuario hace solicitud de la página o cuando llena el formulario de una página y envía esta información al servidor, entonces éste crea un página y se la envía al usuario. Un ejemplo son las páginas resultantes de las búsquedas en Altavista, Google, o cualquier sitio similar.

Existen muchas formas de crear páginas dinámicas. A continuación se muestran algunas de ellas.

- CGI (Common Gateway Interface) fue de las primeras formas utilizadas para dar dinamismo a las páginas. Esta interfaz permite escribir pequeños programas que se ejecutan en el servidor para aportar un contenido dinámico. El resultado de estos programas es un código HTML que se incluye en la página Web justo antes de ser enviada al cliente. La desventaja es que el programa basado en esta interfaz debe ser cargado para ser ejecutado cada vez que ser requiera, lo que provoca largos tiempo de espera, y además si el número de usuarios es elevado, la memoria del servidor también deberá ser elevada para poder cargar y ejecutar todos los procesos demandados.

Algunos de los lenguajes más comunes para programar con CGI son: C y PERL.

- Una alternativa a la CGI fue ISAPI (Internet Server Application Programming Interface). Esta API[15] proporciona la funcionalidad necesaria para construir una aplicación servidora de Internet. A diferencia de CGI que trabaja sobre ejecutables, ISAPI trabaja sobre DLL[16]. Esta diferencia hace que ISAPI sea un sistema más rápido, ya que por tratarse de una biblioteca dinámica sólo será cargada una vez y podrá ser compartida por múltiples procesos, lo que supone pocos requerimientos de memoria.

- Las técnicas anteriores fueron sustituidas por la incorporación de secuencias de órdenes (scripts) ejecutadas directamente en el interior de la página HTML. Esto es, en lugar de hacer una petición al servidor, el explorador puede procesar las secuencias de órdenes a medida que carga la página HTML, de esta manera se le quita carga al servidor. Los lenguajes más comunes para la escritura de secuencias de órdenes son VBScript y JavaScript.

- PHP inició como una modificación de Perl, y es uno de los lenguajes más utilizados para darle dinamismo a las páginas Web. Una de sus características más potentes es su soporte para acceder a gran cantidad de Bases de Datos de una forma muy sencilla. Es multiplataforma, funciona tanto para Unix (con Apache) como para Windows (con Microsoft Internet Information Server) de forma que el código que se haya creado para una de ellas no tiene por qué modificarse al pasar a la otra. La sintaxis que utiliza, la toma de otros lenguajes muy extendidos como C y Perl. Las ventajas de PHP son

[15] Una API es un conjunto de funciones que se pueden utilizar para trabajar con un componente, una aplicación o un sistema operativo. Normalmente una API está formada por varias DLL que proporcionan alguna funcionalidad específica.

principalmente su velocidad de ejecución, que es gratuito y que es multiplataforma. El programa PHP es ejecutado en el servidor y el resultado enviado al navegador. El resultado es normalmente una página HTML. PHP es un lenguaje independiente del navegador, pero sin embargo para que sus páginas PHP funcionen, el servidor donde están alojadas debe soportar PHP.

- Java es un lenguaje de programación diseñado como una mejora de C++ desarrollado por Sun Microsystems. Las características principales que tiene Java son: es orientado a objetos, robusto, tiene librerías para acceder e interactuar con protocolos como HTTP y FTP, es un lenguaje interpretado, portable, seguro y multitarea. Se pueden hacer las páginas dinámicas por medio de Java utilizando algunos de sus componentes como servlets y JSP.

[16] DLL es un acrónimo de Dynamic-Link Library que puede traducirse como librerías para vinculación dinámica. Una DLL es un componente de software que realiza ciertas funciones y que una aplicación utiliza en tiempo de ejecución. La DLL nos ahorra espacio, ya que sólo tiene que ser cargada una vez y puede ser utilizada por los procesos que la requieran. Ahorra memoria al utilizar una técnica de memoria compartida llamada "mapeo de memoria", que carga las DLL's en una zona de memoria global común y mapea el rango de direcciones de la DLL en el espacio de direcciones de cada aplicación que hace la carga de dicha DLL.

Capítulo 3

Redes Privadas Virtuales

Una Red Privada Virtual (VPN - Virtual Private Network) es un sistema para simular una red privada sobre una red pública, por ejemplo, Internet. Este sistema entra dentro de la modalidad B2B y B2E. Es B2E ya que puede permite a los empleados conectarse con la red de su empresa por Internet, y B2B porque puede ser que una empresa le quiera dar acceso a otras empresas a conectarse a su red también por Internet.

Como inconveniente tenemos el alto costo del uso de las líneas telefónicas (pues se utiliza Internet), ya que se suele cobrar un abono mensual más una tarifa por el uso, en el que se tiene en cuenta la duración de las llamadas o cantidad de tráfico enviado y la distancia hacia donde se hacen.

Pero como beneficio, las VPN son una alternativa a la conexión WAN mediante líneas telefónicas, bajando los costos de éstos y brindando los mismos servicios, mediante el uso de la autenticación, cifrado y el uso de túneles para tener conexiones seguras.

Como se muestra en la figura 3.1, la idea es que la red pública sea "vista" desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.

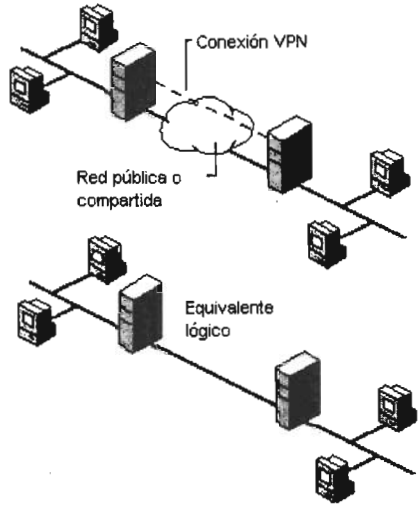


Fig. 3.1 VPN a través de una red pública

Las VPN permiten la conexión de usuarios móviles a la red privada, tal como si estuvieran en una LAN dentro de una oficina de la empresa donde se implementa la VPN. Esto resulta muy conveniente para el personal que no tiene lugar fijo de trabajo dentro de la empresa, como podrían ser vendedores, ejecutivos que viajan, personal que realiza trabajo desde el hogar, etc.

La forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo túneles virtuales entre dos puntos para los cuales se negocian esquemas de cifrado y autentificación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública.

La tecnología de túneles ("Tunneling") es un modo de transferir datos en la que se encapsula un tipo de paquete de datos dentro del paquete de datos de algún protocolo. Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan cifrados.

Las técnicas de autenticación son esenciales en las VPN, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autenticación en VPN es conceptualmente parecido al

logeo en un sistema como nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas de autenticación usados en VPN están basados en un sistema de claves compartidas.

La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no haya algún tercer participante que se haya intrometido en la conversación. Los datos son procesados con un algoritmo de hashing[17] para derivar un valor incluido en el mensaje como checksum[18]. Cualquier desviación en el checksum indica que los datos fueron corruptos en la transmisión o interceptados y modificados en el camino.

Las VPN utilizan como método de cifrado el de clave secreta, o privada, y cifrado de clave pública, que serán explicadas más adelante.

[17] El Hashing es el proceso por el cual se transforma una cadena de caracteres de longitud variable en una cadena de un longitud fija. Es una manera de obtener una huella digital de los datos. Si se necesita verificar si un archivo pertenece a cierta persona, se manda un valor de hashing para comprobarlo.

[18] El checksum es un numero obtenido tomando un mensaje, dividiendolo en bloques de longitud fija, y sumando sus complementos a uno y al resultado se le saca su complemento a uno. El resultado se envia con el mensaje. El receptor divide el mensaje en bloques del mismo tamaño realiza la misma operación y compara ambos resultados. De esta manera se pueden detectar errores en el envío o modificaciones de los datos.

Capítulo 4

Comercio electrónico

Consiste en la utilización de las redes de comunicación electrónica, donde la principal es la Internet, para que las empresas o personas transmitan y reciban información a través de diversos medios con finalidad comercial.

El comercio electrónico permite la creación de un mercado electrónico (es decir, operado por computadoras y a distancia) de todo tipo de productos, servicios, tecnologías y bienes.

El comercio electrónico hoy en día ha dejado de ser un medio cerrado y limitado a unos cuantos, para convertirse en una impresionante red de actividades comerciales mundiales, entre un número cada vez más grande de participantes, ya sean empresas o particulares; y abierta a personas y organizaciones en todo el mundo.

Según estudios realizados por AOL[19], el comercio electrónico está llegando a ser la principal actividad de los usuarios de la Internet. Cada vez más y más los usuarios de la Internet se atreven a comprar en la red.

El comercio electrónico nació en la década de los 70's, cuando las empresas comenzaron a utilizarlo con la introducción del Intercambio Electrónico de Datos

[19] AOL es una de las principales compañías de marketing de Alemania, cuyo principal objetivo es brindar a los consumidores acceso al contenido, a los foros electrónicos y a las tiendas en línea que les interesan.

(EDI)[20] entre firmas comerciales. Esta aplicación les permitía enviar y recibir información sobre sus pedidos y pagos.

El comercio electrónico orientado directamente al consumidor tampoco es algo nuevo, ya que los cajeros automáticos y las tarjetas de crédito son los primeros ejemplos de la aplicación de la tecnología informática y las redes para hacer más eficiente la forma de trabajar.

E-business vs. E-commerce

Muchas veces se presenta confusión entre los términos e-commerce (comercio electrónico) y e-business (negocios electrónicos), tratándolos como sinónimos y esto no es así. Aunque existe una relación entre ambos no podemos decir que son los mismos términos. Veamos cuáles son las principales diferencias entre ellos.

El e-commerce comprende la compra, venta, marketing, y servicios para productos o servicios por medio de redes de computadores

El e-business se refiere a todas las transacciones, negocios y operaciones comerciales que se realizan usando las Tecnologías de Información y Comunicación (TIC[21]); integra todos los procesos del negocio soportados por aplicaciones basadas en sistemas automatizados. Estos procesos se encuentran integrados de tal forma que si un cliente realiza un pedido por Internet, la tienda virtual interactúa con los sistemas de ventas, control de inventarios, cobranza,

---

[20] EDI es el intercambio, mediante computadores, de datos y documentos tales como órdenes de compra, facturas y notificaciones de cobro, en un formato estándar universalmente aceptado, que se realiza entre una empresa y sus asociados comerciales (fundamentalmente clientes y proveedores). El EDI toma la información directamente de las aplicaciones y transmite los documentos. Al recibir un documento de negocios, los sistemas computarizados de sus asociados comerciales cargan directa y automáticamente los datos de dicho documento, los procesan e interactúan con los sistemas de aplicación que los requieren como entrada. Todo esto se ejecuta en pocos minutos, sin necesidad de reingresar los datos recibidos ni de procesar manualmente los documentos.

[21] Las TIC (Tecnologías de Información y Comunicación) son aquellos dispositivos que capturan, transmiten y despliegan información electrónica. Se desprenden de cualquier herramienta basada en computadora que la gente utiliza para trabajar con información y procesarla. Dentro de las TIC tenemos a las computadoras personales, Internet, teléfonos móviles, asistentes personales digitales y todo aquel dispositivo similar.

mensajería y contabilidad, para mantener actualizado el registro de operaciones del negocio.

En el e-business la información puede utilizarse para transacciones comerciales, para suministrar noticias, comunicar normativas, etc., casos en los que los objetivos no son sólo establecer relaciones comerciales, sino también administrar valor a la empresa frente a sus trabajadores, proveedores y socios.

Dentro del e-commerce tenemos varias acciones que podemos realizar como son: la transferencia electrónica de fondos, manejo de la cadena de producción, el e-marketing (marketing orientado a Internet), y el procesamiento de transacciones en línea. Estos son algunos de los elementos que pueden estar comprendidos dentro del e-commerce, no es necesario implementar todos ellos para hablar de e-commerce. Quizás el tipo de comercio electrónico más difundido es el carrito de compras, en el cual el cliente selecciona los productos que quiere comprar, ingresa sus datos, y envía el pedido.

El comercio electrónico forma parte del negocio en línea, y no comprende todo el e-business. Es por esto que no podemos decir que el e-business es igual al e-commerce, sino que el e-commerce es un componente más del e-business.

El e-business está conformado por varios elementos como: e-commerce, Comunicación y colaboración empresarial, y Sistemas Internos de negocios. Por lo que e-commerce sólo es un subconjunto del e-business. La figura 4.1 ilustra esto.

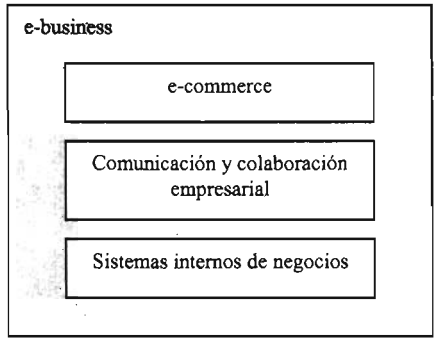


Fig. 4.1 Elementos que conforman el e-business

La Comunicación y colaboración empresarial se ocupa de mejorar los procesos de comunicación para lograr una mejor integración de los sistemas y mayor eficiencia. A su vez podemos enumerar algunas de las funciones que pueden ser incorporadas en esta parte: e-mail, mail de voz, foros de discusión, sistemas de chat, video conferencias, y sistemas de colaboración.

Quizás los Sistemas internos de negocio sean una de las partes menos visibles del e-business, pero no por ello la menos importante. Dependiendo de la escala de nuestro negocio, debemos tener una estructura de información que nos de soporte para poder tomar decisiones y realizar las acciones necesarias. Debemos poder delegar en los sistemas informáticos la mayor cantidad de procesos posibles, para poder dedicarnos verdaderamente a nuestro negocio, y no perder tiempo en procesos que no hacen al negocio. Dentro de los sistemas internos de negocio podemos enumerar algunos de ellos: sistemas para el manejo de conocimiento, sistemas para el manejo de la documentación, control de procesos, Manejo de Relaciones con el Cliente, Planeamiento de los Recursos de la Empresa.

Ventajas del comercio electrónico.

Una adecuada implantación de un sistema de comercio electrónico puede traer importantes beneficios:

- La proyección de la empresa en el ámbito mundial. Podrán tener acceso a la página en diferentes partes del mundo ya que las fronteras desaparecen y se expande la cobertura geográfica, permitiendo así captar nuevos clientes (claro, sí se tiene la suficiente difusión y conocimiento de la página).
- Reducción de costes. Internet es un medio económico ya que se pueden reducir o ahorrar muchos gastos, como teléfono, fax, vendedores, renta de un local, etc. Esto da mayor posibilidad de ingresar al mercado a aquellos que así lo desean y tienen algunos obstáculos como necesidad de espacio físico, una buena ubicación, publicidad, etc. Se puede decir que el comercio electrónico amplía los mercados existentes al crear ámbitos comercialmente nuevos.
- Reducción de tiempos de producción. Debido a que la comunicación a través de la Internet es más rápida, esto hace posible minimizar los tiempos de espera, acelerando el proceso productivo en cualquiera de sus etapas.
- Incremento de la fuerza de ventas. Las ventas aumentan gracias a que más personas tienen acceso al contacto con la empresa.
- Vendedores virtuales las 24 horas. Estos vendedores no necesitan descanso, no piden vacaciones ni días de incapacidad, trabajan todo el día y toda la noche, están al servicio de los clientes a la hora que los necesitan, la única desventaja es que el trato humano es muchas veces lo que termina de convencer a un comprador.

- Atención rápida. Los clientes no tienen que hacer largas colas para esperar a ser atendidos, pues los clientes obtienen la atención en el instante que lo necesiten.
- Comodidad. Los clientes pueden visitar varias tiendas de diferentes partes del mundo en poco tiempo y llevar a cabo sus compras cómodamente sentados frente a su computadora.
- Reducción de inventarios. No se tienen que tener todos los productos que ofrece la tienda en un lugar físico, sino que como los van solicitando los clientes, entonces se le solicitan a su vez al fabricante.

Desventajas del comercio electrónico

A pesar de las grandes ventajas que ofrece el comercio electrónico también hay desventajas que se deben considerar:

- Desconocimiento de la empresa. No conocer a la empresa que vende es un riesgo del comercio electrónico que trae incertidumbre a los clientes, ya que no se conoce la solvencia de los proveedores, la veracidad de los datos, ni su ubicación, ésta puede estar en otro país o en el mismo, pero en muchos casos las "empresas" que ofrecen sus productos o servicios por Internet ni siquiera están constituidas legalmente en su país y no se trata mas que de gente que esta "probando suerte en la Internet".
- Forma de Pago. Aunque ha avanzado mucho el comercio electrónico, todavía no hay una transmisión de datos segura al 100%. Y esto es un problema pues pocos se animan a dar los datos de su tarjeta de crédito o información confidencial a través de la Internet. Sin embargo es importante destacar que han mejorado mucho los aspectos de seguridad.
- Intangibilidad. Mirar y tocar aunque no sea sinónimo de compra, siempre ayuda a realizar una compra.

- Cambio de mercancía. Regularmente no se tiene una dirección a dónde poder ir a reclamar mercancía defectuosa o cambiarla por otra similar como en una tienda normal.
- Es susceptible de fraude. Ya que no sabemos si la persona que registra una transacción realmente es quien dice ser. Aunque también esto se puede evitar, todo depende de la forma de pago y del servicio que ofrezca la empresa.
- Página en otro idioma. Muchas veces las páginas que requerimos están en otro idioma y esto dificulta un entendimiento total.

Clasificación del e-bussines.

Existen diferentes clasificaciones y modalidades del comercio electrónico desde el punto de vista del medio de distribución de productos y servicios, y desde el punto de vista del mercado (los agentes que intervienen).

Clasificación de acuerdo a los agentes que intervienen en las transacciones

Los agentes que intervienen en el comercio electrónico son: las empresas (B - Business), los clientes (C - Customer), los empleados (E – Employee), los sectores públicos (A – Administration), etc. De acuerdo a estos elementos podemos clasificar al comercio electrónico en B2B, B2C, C2C, C2B, B2E, B2A, etc. A continuación se explican los más importantes.

B2B "Business to Business" (Empresa a Empresa)

El comercio electrónico entre empresas tiene como principal finalidad el aprovisionamiento de bienes y servicio por parte de una de ellas. Se refiere a una empresa que hace uso de una red para hacer órdenes de compra a sus proveedores, recibir facturas y realizar los pagos correspondientes. Esta categoría ha sido utilizada por muchos años, particularmente haciendo uso del intercambio electrónico de datos (EDI).

Dentro de los nuevos conceptos que están apareciendo dentro del mundo B2B comienza a surgir con fuerza el concepto de e-purchasing, el cual se define como el conjunto de procesos orientados a integrar la función de compras mediante la tecnología relacionada con Internet, con el objetivo de optimizar los flujos de información y reducir los costes de adquisición de bienes y servicios.

Un ejemplo de esta modalidad puede ser la venta de tiempo aire para teléfonos celulares de Telcel que se a través de Walmart.

B2C "Business to Customer" (Empresa a Cliente)

Es el comercio que se da entre una empresa y un particular, es decir, una empresa crea un sitio Web, por ejemplo, una tienda virtual en la que presenta sus artículos y los clientes pueden realizar sus compras en este espacio. Las nuevas tecnologías permiten que las empresas puedan presentar sus productos de una manera totalmente novedosa, cómoda, rápida y personalizada. Se le considera un "Piso Virtual", pues en esta sección los consumidores finales podrán visualizar las características generales y específicas de los productos ofrecidos, así como los servicios que se ofrecen.

C2C "Customer to Customer" (Cliente a Cliente)

Es la relación comercial entre dos clientes finales, donde no hay intermediación de ninguna empresa entre ambos. El ejemplo más característico de este modelo son las páginas de subastas y de compra/venta, donde un usuario (cliente) es quien ofrece algún producto para vender o subastar y otro usuario interesado en el producto, será quien lo compre. En este caso el trato será entre ambos usuarios sin requerir la intervención de alguna empresa. Otro ejemplo de esta modalidad son los foros de discusión.

C2B "Customer to Business" (Cliente a Empresa)

Es la relación comercial entre un cliente final y una compañía, en la que es el cliente el que origina dicha relación. Internet ha permitido la aparición de negocios que se ajustan a este modelo. Un ejemplo de esta modalidad es el caso del teletrabajo, donde es el cliente quien ofrece sus servicios a las empresas subiendo su información curricular a una página, así de una manera fácil y rápida las empresas que requieran personal podrán escoger de entre muchísimas personas a aquellos que cumplan con ciertos requisitos, y hasta encontrar personas con los conocimientos necesarios y que no soliciten un gran sueldo. Esto podría beneficiar mucho a las pequeñas empresas o a empresas que van naciendo.

B2E "Business to Employee" (Empresa a Empleado)

En esta relación se trata de rentabilizar al máximo la eficiencia y el rendimiento del empleado, reduciendo al mismo tiempo la complejidad de sus tareas diarias. Los empleados son activos críticos de la empresa, y la mejora en sus relaciones con la empresa es un factor de vital importancia para la productividad.

Dentro de esta modalidad se encuentran las redes privadas virtuales, que permiten a los trabajadores a distancia, empleados móviles, sucursales y socios de negocios conectarse entre sí o a las redes corporativas. También incluye sitios de Internet destinados a ser usados sólo por miembros de una organización. Esto requiere de una buena implementación de seguridad.

B2A "Business to Administration" (Empresa a Administración)

Es la utilización de Internet como canal de comunicación entre las empresas y las organizaciones gubernamentales. Esta modalidad es muy importante ya que se piensa que a través de ella se podrá promover la calidad, la seriedad y el crecimiento del comercio electrónico. Está enfocado a realizar trámites entre la administración (organizaciones gubernamentales), empresas y particulares. Busca la agilización de los trámites y el acceso a los mismos desde un único punto. El

desarrollo de esta modalidad puede conducir a la adopción de sistemas de comercio electrónico de forma obligatoria.

Clasificación de acuerdo al medio de distribución de los productos y servicios

De acuerdo a la forma de distribución o entrega de la mercancía se puede dividir el comercio electrónico en directo e indirecto.

Indirecto

Cuando la transacción consiste en un pedido electrónico de bienes materiales, mismos que deberán ser entregados físicamente, utilizando los canales tradicionales, como el correo. Desde este punto de vista, el comercio electrónico pudiera asemejarse, hasta cierto punto, a las ventas por catálogo.

Actualmente, los principales ejemplos de bienes que se venden por medio de pedidos electrónicos, pero que son entregados por los métodos tradicionales, pudieran ser los libros, las flores, juguetes, y artículos de ropa.

Directo

Cuando la transacción completa se realiza a través de la Internet. Esto significa que tanto el pedido, el pago, y hasta el suministro del bien, es por medio de la Internet.

Las transacciones de comercio electrónico directo pueden referir a bienes y servicios inmateriales, como software, información, música y videos.

Tiendas virtuales

El término *virtual*, según el diccionario de la Real Academia Española, representa algo que tiene existencia aparente y no real. En tal sentido, se utiliza en el ámbito de la tecnología informática cuando hablamos, por ejemplo, de realidad virtual o memoria virtual.

Sin embargo, el término virtual se ha popularizado para referirse a las empresas que operan a través de Internet (empresas "punto com" o "clic"), para diferenciarlas de las empresas que operan en el mundo físico (empresas de "cemento y ladrillos"). Aunque en realidad estas empresas son reales y no aparentes.

Una tienda virtual es un sistema completo capaz de gestionar y coordinar ventas y/o pedidos a través de la Internet tal como lo haría una tienda física en el "mundo real". También permite llevar a cabo diferentes funciones administrativas de la tienda como agregar, quitar, actualizar productos, obtener estadísticas de ventas, etc. Las tiendas virtuales conforman una de las principales actividades dentro del comercio electrónico en Internet.

Políticas

Las políticas que se observan regularmente para el funcionamiento de una tienda virtual son:

1. Todo cliente que realiza una compra en la tienda virtual se compromete a reconocer el pedido generado a la tienda virtual y a realizar el pago del mismo con el mecanismo de pago que maneja la tienda virtual al momento de efectuar la compra. De no ser así el pedido será cancelado y el cliente podrá ser dado de baja del sistema.

2. Cuando el cliente elige la opción de pago con efectivo. El pago se realizará con base en las políticas de cobro especificadas por la tienda virtual dentro de su sitio Web en la sección de políticas.
3. El pago se puede realizar con depósito bancario. El cliente recibirá un correo electrónico solicitando que realice el depósito a la cuenta y referencia bancaria especificada en dicho correo electrónico.
4. Si después de x días del plazo de pago que este será dependiendo de el tipo de tienda consultada, el cliente no efectúa el depósito correspondiente por su compra, el pedido quedará cancelado.
5. Cargos por los servicios de entrega. Los cargos causados por servicios de entrega serán pagados por el cliente o por la tienda virtual según las condiciones establecidas en el sitio Web de la tienda virtual donde se realiza la compra. El importe de los gastos de envío se calcula automáticamente por el sistema, según las condiciones de compra seleccionadas por el cliente.
6. Facturación. La tienda virtual en la que realizó la compra de su producto es responsable de emitir la factura del producto la cual deberá ser entregada en el domicilio del cliente que realiza la compra. Cuando el pago se realice con depósito bancario, los cargos de envío serán facturados.
7. Garantías. Las garantías con relación a la exactitud, veracidad y características de los productos y/o servicios comprados en la tienda virtual del asociado de que se trate son entera responsabilidad de la misma. La tienda se deslinda de toda reclamación proveniente de los clientes.
8. Devoluciones. La política de devoluciones aplica según el procedimiento establecido por la tienda virtual en la que el cliente realice su compra.

Cómo realizar una compra a través de la Internet

Una tienda virtual consta regularmente de una serie de páginas Web (estáticas o dinámicas) que tienen información de los productos de la tienda, una serie de programas y una Base de datos.

El cliente recibe la página Web en su navegador y por medio de formularios HTML envía información. Una serie de programas que componen la tienda virtual recogen esta información y la gestionan dando como resultado otra página Web que se le mostrará al usuario. Estos programas pueden realizar acceso a Bases de Datos e implementar funcionalidades muy complejas.

Una tienda virtual tiene un programa que se suele denominarse "*carrito de compra*", mediante el cual, el cliente por medio de formularios puede efectuar sus pedidos. A través de este programa el comprador escogerá la forma de pago y de envío del producto o productos que haya escogido. Los pedidos quedarán almacenados en el servidor o se notificarán por correo electrónico a una dirección elegida. Así se podrán gestionar los envíos de los productos y los cobros.

Hay varias maneras en las que se pueden llevar a cabo los pagos por los servicios o productos, los más importantes son:

- *Pago contrareembolso*. El cliente hace el pedido en Internet y paga cuando se le entrega el producto en su casa.
- *Pago bancario*. El cliente genera el pedido en Internet, paga en el banco a una cuenta en especial y en cuanto el banco notifique a la empresa que el pago ha sido realizado, entonces se le envía el producto al cliente.
- *Pago con tarjeta de crédito o débito*. El cliente proporciona los datos de la tarjeta de crédito y el cobro se realiza de forma automática mediante un sistema concertado previamente con un banco. El problema de este

sistema es que el banco o la institución financiera cobrará un porcentaje de la operación.

Hay un miedo generalizado con respecto a los medios de pago utilizados vía Internet, y esta percepción es en ciertos casos justificada. Esto no es como hacer una llamada telefónica o enviar un fax. La información enviada por el cliente hacia el servidor Web puede pasar a través de múltiples etapas antes de ser definitivamente entregada. La información se encuentra en un formato digital, y en cualquier etapa puede ser interceptada.

Para todas las operaciones de cobro tenemos que asegurarnos que la tienda va a disponer de transmisiones seguras a través de protocolos como el SSL. De esta forma, tendremos la certeza que nadie va a enterarse de los datos de las tarjetas o cuentas de nuestros clientes.

La seguridad es muy importante y casi se podría decir que es el corazón del comercio electrónico. No hay que olvidar que la relación de los proveedores con los posibles clientes se basa en la confianza, ya que ellos no van a ver a los proveedores, sino que se van a encomendar a un sistema informático anónimo para realizar sus compras.

Capítulo 5

Seguridad en el comercio electrónico

La seguridad en el comercio electrónico y específicamente en las transacciones comerciales es un aspecto de suma importancia. Para ello es necesario disponer de un servidor seguro que brinde confianza tanto a proveedores como a compradores que hacen del comercio electrónico su forma habitual de negocios.

Al igual que en el comercio tradicional existe un riesgo en el comercio electrónico, al realizar una transacción por Internet, el comprador teme por la posibilidad de que sus datos personales (nombre, dirección, número de tarjeta de crédito, etc.) sean interceptados por alguien, y suplante así su identidad; de igual forma el vendedor necesita asegurarse de que los datos enviados sean, de quien dice ser.

Un servidor seguro establece una conexión con el cliente, de manera que la información circula cifrada a través de la Internet. El cifrado de la información se realiza mediante algoritmos que aseguran que sea inteligible.

Es sencillo saber si nos hemos conectado con un servidor seguro. En primer lugar, la dirección de URL comienza por https:// (http seguro) en vez de http:// Además, en la mayoría de los visualizadores tendremos una indicación de que la conexión segura se ha establecido.

Se han desarrollado sistemas de seguridad para transacciones a través de la Internet que garantizan la confidencialidad, integridad y autenticidad de la información transmitida como el uso de los algoritmos DES, 3 DES, firmas digitales y firewalls.

Cifrado

Es el conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas. El objetivo del cifrado es convertir cualquier texto legible en algo que no se puede leer y por lo tanto comprender.

El cifrado está basado en dos componentes: un algoritmo y una clave. Un algoritmo es una transformación matemática que coge texto plano y lo cambia a datos ilegibles cifrados. Para cifrar un texto plano, se utiliza una clave como entrada para el algoritmo anteriormente citado. Un ejemplo sencillo de una clave puede ser el reemplazar cada letra con la próxima letra del alfabeto. Así la palabra UNAM se convertiría en VOBN. Para descifrar el mensaje o revertir el cifrado, el que lo recibe necesita conocer la clave secreta.

El número de claves posibles que puede utilizar un algoritmo depende de la longitud de la clave con la que trabaje. Una clave admite 2 a la n combinaciones, donde n es el número de bits de la clave, por ejemplo, una clave de 40bits, tiene 2 a la 40 = 1.099.511.627.776 posibles combinaciones.

Un algoritmo de cifrado se considera seguro si su seguridad depende exclusivamente de la longitud de su clave. Si esto es así, la única forma de atacar estos algoritmos es la "fuerza bruta", es decir probar todas las posibles combinaciones de claves hasta obtener el texto original, y así cuando se haya encontrado la clave, si es que se llegara a encontrar, podría ser demasiado tarde para ocuparla. De esta forma cuando la longitud de la clave se elige de forma conveniente puede que haga el ataque imposible.

Existen dos tipos principales de criptografía de uso común hoy en día. Criptografía de "clave sencilla" o de "clave secreta", y criptografía de clave pública.

Cifrado de la Clave Secreta o Privada

La codificación o cifrado de la clave secreta resulta útil en muchos casos, aunque tiene limitaciones significativas. Todas las partes deben conocerse y confiar totalmente la una en la otra. Cada una de ellas debe poseer una copia de la clave, una copia que haya sido protegida y mantenida fuera del alcance de los demás.

Por sí solo, este tipo de cifrado no es suficiente para desarrollar el pleno potencial del comercio electrónico, el cual debe vincular a un número ilimitado de compradores y vendedores de todas partes del mundo, ya que resulta poco práctico que una gran corporación intercambie claves con miles o incluso millones de clientes o, peor todavía, con posibles clientes con los que nunca ha tratado.

Cifrado de la clave pública

La solución a la seguridad en toda red abierta es una forma de codificación más novedosa y sofisticada, desarrollada por matemáticos del MIT en los años setenta, y conocida como "clave pública". En este tipo de enfoque, cada participante crea dos claves o "llaves" únicas.

Por ejemplo, una empresa dispone de su propia "clave pública", que publica en un tipo de directorio al que el público en general tiene acceso. Además dispone de su clave o "llave privada", que mantiene en secreto.

Las dos claves funcionan conjuntamente como un curioso dúo. Cualquier tipo de datos o información que una de las claves cierre, sólo podrá abrirse con la otra. De forma que, digamos, el servidor A desea enviar un mensaje importante al servidor B por Internet sin que nadie más pueda leerlo. Simplemente, el servidor A busca la clave pública del servidor B y la utiliza para realizar el cifrado del texto. Luego, cuando el servidor B recibe el mensaje, utiliza su clave privada para revertir el cifrado del mensaje y aparece el mensaje en forma de texto normal y corriente. Si

un intruso interceptara este mensaje, no podría descifrarlo porque no tendría la clave privada del servidor B.

Estas claves dan lugar a otra revolución en el campo de las transacciones seguras en el ciberespacio, las firmas digitales.

Firma Digital

Evita que la transacción sea alterada por terceras personas sin saberlo. Este certificado, que es emitido por un tercero, garantiza la identidad de las partes.

Cuando se recibe un mensaje en el ciberespacio, ¿cómo saber que lo envió la persona que dice haberlo enviado y no un delincuente que se hace pasar por él? ¿Y cómo sabe un comerciante si la orden que recibió es la suya o la de alguien que se propone estafarle una buena suma de dinero?

El sistema de clave pública puede resolver este problema en una forma sencilla. Digamos, por ejemplo, que X está hablando con Y, en el ciberespacio, y Y desea probar la identidad de X. Sólo tiene Y que guardar un mensaje codificado con la llave privada de X. Entonces Y puede abrir el texto con su clave pública, tomada del certificado digital de X, lo que prueba que X es el único que pudo haber cifrado ese mensaje en primer lugar.

Este proceso crea lo que los criptógrafos denominan la "firma digital". Una firma digital ofrece una forma de asociar el mensaje con la entidad que lo envía, y es la forma en la que se puede "firmar" al efectuar una compra en el ciberespacio. De esta manera, sólo el dueño de la tarjeta de crédito podrá utilizarla.

El método de la firma digital no sólo proporciona autenticidad al mensaje enviado por X, si no que también asegura el no repudio, ya que sólo el dueño de una llave privada puede cifrar un documento de tal forma que se pueda descifrar con su llave pública, lo que garantiza que ha sido X y no otro el que ha enviado dicho documento.

Tanta es la fuerza que posee éste sistema que a nivel legal la firma electrónica constituye en la mayoría de los casos una prueba indudable de quién envío de un documento electrónico, semejante a la firma tradicional de puño y letra.

Un alegato que podría dar X para negar el envío de un documento cifrado con su clave privada sería el echo de haber perdido dicha llave o que se la hayan robado, pero entonces hay que tener en cuenta que X es el único responsable del buen uso de su llave privada, por lo que está obligado a comunicar inmediatamente a la autoridad correspondiente cualquier circunstancia que ponga en peligro la seguridad de la misma.

Esto es análogo a lo que ocurre con las tarjetas de débito o crédito, siendo siempre en último extremo responsable del uso indebido de las mismas el dueño de la tarjeta si no ha avisado a tiempo a su entidad financiera o banco de la pérdida o sustracción.

Para un documento extenso puede llegar a ser muy tardado el cifrado con la llave pública. Para reducir esto aparece la función hash que mediante funciones matemáticas realiza un resumen del documento a firmar comprimiendo el documento en un único bloque de longitud fija cuyo contenido es ilegible. Este bloque de código es irreversible, o sea, a partir del bloque comprimido no se puede obtener el bloque sin comprimir.

Entonces, para certificar que un mensaje en realidad lo envió X, y que permanece inalterado, se comprime el mensaje a través de un proceso llamado "Hashing" en un código numérico único para el texto de dicho mensaje. Un mensaje comprimido con este procedimiento garantiza la integridad del mensaje, ya que cualquier modificación que se hiciera en el texto original, por más pequeña que fuera, generaría un código completamente distinto si se aplicare nuevamente al mensaje el procedimiento de hashing, consecuentemente cambiando el resultado final.

Así, una vez que X tiene el código de hash correspondiente a su mensaje, lo codifica con su llave privada, y lo anexa a su mensaje original que será cifrado con

la lave pública de Y. A esto es a lo que se le denomina firma digital, al mensaje resumido mediante la función hash y cifrado con su llave privada.

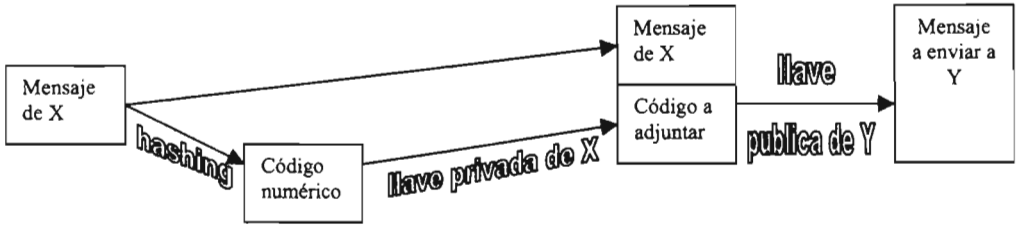


Fig. 5.1 Envío de información firmada electrónicamente

Cuando Y recibe el mensaje y lo decodifica con su propia llave privada, puede proceder ahora él a aplicarle al mensaje el mismo proceso de hashing, obteniendo el código correspondiente. Después, Y decodifica el código anexado al mensaje, utilizando la llave pública de X. cerciorándose así que en realidad proviene de X. Por último, Y deberá comparar el código enviado por X, con el código que le resulto a él después de haber aplicado el procedimiento de hashing. Si el mensaje se mantuvo inalterado, los códigos serán idénticos.

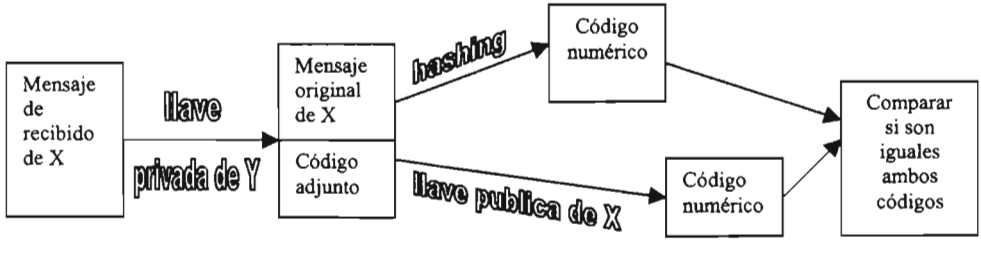


Fig. 5.2 Comprobación de la firma digital

SSL (Secure Socket Layer)

Es esencial que el tráfico de la información entre el usuario y el sitio Web sea cifrado y el protocolo estándar para ello es el SSL, desarrollado por Netscape Communications Corporation, el cual se ha impuesto debido a que provee un elevado nivel de protección a un costo reducido.

Los browsers que soportan esta tecnología indican que una sesión segura se está desarrollando mediante un mensaje: en el caso de Netscape, mostrando una llave azul al pie de la pantalla; en el caso de Microsoft Explorer, mostrando un candado cerrado.

Para establecer una comunicación segura utilizando SSL se tienen que seguir una serie de pasos. Primero se debe hacer una solicitud de seguridad. Después de haberla hecho, se deben establecer los parámetros que se utilizarán para SSL. Esta parte se conoce como SSL Handshake. Una vez se haya establecido una comunicación segura, se deben hacer verificaciones periódicas para garantizar que la comunicación sigue siendo segura a medida que se transmiten datos. Tras finalizar la transacción se termina SSL.

Solicitud de SSL

Antes de que se establezca SSL, se debe hacer una solicitud. Típicamente esto implica un cliente haciendo una solicitud de un URL a un servidor que soporte SSL. Una vez se ha hecho la solicitud, el cliente y el servidor empiezan a negociar la conexión SSL, es decir, hacen el SSL Handshake.

SSL Handshake

Durante el Handshake se cumplen varios propósitos. Se hace autenticación del servidor y opcionalmente del cliente, se determina que algoritmos de criptografía serán utilizados y se genera una llave secreta para ser utilizada durante el intercambio de mensajes subsiguientes durante la comunicación SSL. Los pasos que ocurren después son los siguientes:

- Client Hello: El "saludo de cliente" tiene por objetivo informar al servidor que algoritmos de criptografía puede utilizar y solicita una verificación de la identidad del servidor. El cliente envía el conjunto de algoritmos de criptografía y compresión que soporta y un número aleatorio. El propósito del número aleatorio es para que en caso de que el servidor no posea un certificado para comprobar su identidad, aún se pueda establecer una comunicación segura utilizando un conjunto distinto de algoritmos. Dentro de los protocolos de criptografía hay un protocolo de intercambio de llave que define cómo el cliente y servidor van a intercambiar la información, los algoritmos de llave secreta que definen qué métodos pueden utilizar y un algoritmo de Hash. Hasta ahora no se ha intercambiado información secreta, solo una lista de opciones.
- Server Hello: El servidor responde enviando su identificador digital el cual incluye su llave pública, el conjunto de algoritmos criptográficos y de compresión y otro número aleatorio. La decisión de que algoritmos serán utilizados está basada en el más fuerte que tanto cliente como servidor soporten. En algunas situaciones el servidor también puede solicitar al cliente que se identifique solicitando un identificador digital.
- Aprobación del Cliente: El cliente verifica la validez del identificador digital o certificado enviado por el servidor. Esto se lleva a cabo descifrando el certificado utilizando la llave pública del emisor y determinando si este proviene de una entidad certificadora de confianza. Después se hace una serie de verificaciones sobre el certificado, tales como fecha, URL del servidor, etc. Una vez se ha verificado la autenticidad de la identidad del servidor. El cliente genera una llave aleatoria y la cifra utilizando la llave pública del servidor y el algoritmo criptográfico y de compresión seleccionado anteriormente. Esta llave se le envía al servidor y en caso de que el Handshake tenga éxito será utilizada en el envío de futuros mensajes durante la sesión.

- Verificación: Se hace una última verificación para comprobar si la información transmitida hasta el momento no ha sido alterada. Ambas partes se envían una copia de las anteriores transacciones cifradas con la llave secreta. Si ambas partes confirman la validez de las transacciones el Handshake se completa, de otra forma se reinicia el proceso.

  Ahora ambas partes están listas para intercambiar información de manera segura utilizando la llave secreta acordada y los algoritmos criptográficos y de compresión. El handshake se realiza solo una vez y se utiliza una llave secreta por sesión.

- Intercambio de datos: Ahora que se ha establecido un canal de transmisión seguro SSL, es posible el intercambio de datos. Cuando el servidor o el cliente desea enviar un mensaje al otro, se genera un código utiliza un algoritmo de hash (acordado durante el handshake), se cifra el mensaje y se envía, cada mensaje es verificado de forma inversa.

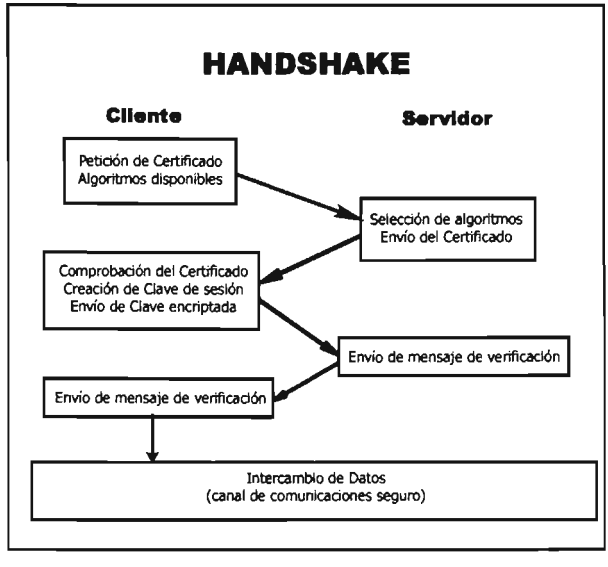


Fig. 5.3 Proceso de Handshake

- Terminación de una sesión SSL: Cuando el cliente deja una sesión SSL, generalmente la aplicación presenta un mensaje advirtiendo que la comunicación no es segura y confirma que el cliente efectivamente desea abandonar la sesión SSL.

En la figura 5.3 se muestra un diagrama que ilustra los pasos mencionados anteriormente.

Firewall (Barrera de fuego)

Esta palabra proviene de la industria del automóvil. En los automóviles modernos, existe una barrera entre el motor y el habitáculo de los pasajeros que evita la extensión de un incendio hacia zonas vulnerables.

En la industria informática, una barrera de protección lleva a cabo una función similar separando componentes vulnerables. Se sitúa entre la red y el servidor Web, o entre éste y la Internet pública.

Una barrera de protección resulta de la combinación de hardware y software, y actúa como un guardia electrónico. Comprueba qué y quién está intentando entrar y salir de la red impidiendo el acceso a servicios no deseables, tomando nota de cada conexión y, hallando el punto de origen.

Las barreras de fuego tienen las siguientes limitantes:

- Pueden parecer muy celosamente protectoras, impidiendo el acceso a algunos servicios deseables para la empresa.
- No puede prevenir problemas en el interior de la red.
- Puede provocar cuellos de botella debido a un alto volumen de tráfico o cuando se utilicen programas anti-virus.

Hay más de 150 tipos diferentes de barreras de protección en el mercado hoy en día. Sus cometidos son esencialmente los mismos: detienen cada llamada, la vetan y la dejan pasar sólo si cumple con requisitos preestablecidos.

Capítulo 6

Legislación Informática en México

El Derecho surge como un medio efectivo para regular la conducta del hombre en la sociedad. Pero la sociedad no es la misma en cada uno de los lugares del planeta ni en cada momento de la historia. La sociedad evoluciona y cambia; los cambios trascendentales se han dado a través del avance de la ciencia y de la tecnología.

En los últimos años, las Tecnologías de la Información y la Comunicación (TIC) han revolucionado la vida social en numerosos aspectos: científicos, comerciales, laborales, profesionales y escolares.

Ciertamente resulta imposible que el Derecho vaya a la par que la tecnología, regulando cuanto fenómeno o conducta lícita o ilícita infiere en el ámbito jurídico, empezando porque es evidente que estas conductas tienen que manifestarse primero, ya que las leyes no pueden regular lo que aún no existe.

Si a esto le sumamos el carácter formal, escrito de nuestro sistema jurídico, las particularidades del proceso legislativo, la necesidad de que personas con formación de abogados comprendan lo necesario sobre tópicos técnicos y tecnológicos, hace que el Derecho Mexicano tenga rezagos en materias tecnológicas y que sea rebasado. Lo que exige una atención inmediata y efectiva. A pesar de esto, se ha hecho un esfuerzo en México por llevar a cabo la legislación informática en el país, que ha servido de mucho.

La estructura de la Internet, absolutamente descentralizada, que interconecta millones de computadoras hace que los delitos informáticos sean, en muchos casos, difíciles de detectar y por lo tanto resulte extremadamente complicado localizar y castigar a sus responsables.

Delitos informáticos

Se trata de delitos íntimamente ligados a la informática o a bienes jurídicos relacionados con las tecnologías de la información tales como datos, programas, documentos electrónicos y dinero electrónico, donde se llevan a cabo conductas que lesionan o dañan bienes, intereses o derechos de personas físicas o morales.

De entre estos delitos podríamos destacar: fraude mediante el uso de la computadora y manipulación de la información que ésta contenga, el acceso no autorizado a sistemas o servicios, la destrucción de datos o programas, la violación de los derechos de autor, uso no autorizado de programas y datos, la interceptación del correo electrónico, las estafas electrónicas, etc.

Vamos a analizar algunos de los delitos antes mencionados.

- Fraude mediante el uso de la computadora y manipulación de la información que ésta contenga. El artículo 230 del Código Penal para el Distrito Federal dice: *"Al que por medio del engaño o aprovechando el error en que otro se halle, se haga ilícitamente de alguna cosa u obtenga un lucro indebido en beneficio propio o de un tercero, se le impondrán..."*, más adelante en el artículo 231: *"Se impondrán las previstas en el articulo anterior, a quien para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la institución."*

- Violación de derechos de autor. Regulada en la Ley Federal del Derecho de Autor, el artículo 11 establece el reconocimiento del Estado al creador de obras literarias o artísticas, entre las que, conforme al artículo 13 fracción XI, están los programas de cómputo, los cuales, al igual que las bases de datos, quedan protegidos por las disposiciones de la Ley de la misma forma que las obras literarias, en el sentido de que los autores tienen los derechos patrimoniales y

morales sobre sus obras (explotación, reproducción, publicación, exhibición, acceso, distribución, divulgación, reconocimiento de la calidad de autor, modificación y respeto a la obra) así como la facultad de transmitir esos derechos. En su Capítulo IV (artículos 101 al 114) la Ley amplía la protección a los programas tanto operativos como aplicativos y deja fuera a los que tienen por objeto causar efectos nocivos.

La ley prohíbe la importación, fabricación, distribución y utilización de aparatos o prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espejo electromagnético y de redes de telecomunicaciones. La violación a las anteriores disposiciones constituyen una infracción, que son sancionadas por el Instituto Mexicano de la Propiedad Intelectual con multa, que va desde 500 hasta 5000 días de salario dependiendo del tipo de infracción, además de poder efectuar visitas, pedir información y aplicar las medidas precautorias que estime convenientes.

Asimismo, el Código Penal Federa multa al que use en forma dolosa y con fines de lucro las obras protegidas por la Ley Federal del Derecho de Autor; al que produzca o reproduzca (entre otros actos) sin autorización y con fin de lucro obras protegidas por la Ley Federal de Derecho de Autor, así como a aquel que fabrique con fines de lucro, dispositivos o sistemas diseñados para desactivar los dispositivos electrónicos de protección de un programa de cómputo; al que fabrique, importe o venda algún sistema o dispositivo destinado a descifrar señales cifradas de satélite que contengan programas o realice con fin de lucro cualquier acto destinado al mismo efecto, sin autorización del distribuidor de la señal.

- Uso no autorizado de programas y de datos. La Ley Federal del Derecho de Autor, en sus artículos 107 al 110, protege como compilaciones a las bases de datos legibles por medio de máquinas que por razones de disposición de su contenido constituyan obras intelectuales, otorgándole a su organizador el uso exclusivo por cinco años; asimismo, exceptuando las investigaciones de

autoridades, la información privada de las personas contenida en bases de datos no podrá ser divulgada, transmitida ni reproducida salvo con el consentimiento de la persona de que se trate. Sanciona las infracciones con una multa que va de las 50 a las 10,000 unidades de salario y en su caso, con la suspensión o cancelación de la operación de la base de datos cuando afecte a un grupo importante de interesados.

- Intervención de correo electrónico.- Éste delito, que atenta contra la privacidad como derecho fundamental de las personas, se asemeja con el de violación de correspondencia que sanciona tanto en el Código Penal Federal, (art.173) como en el local del D.F. (art. 333) "... *al que abra o intercepte una comunicación escrita que no esté dirigida a él ...*". Sin embargo, en estricto sentido esto aplica para la correspondencia postal solamente, por lo que en la Iniciativa de reformas y adiciones sobre diversas disposiciones del Código Penal para el Distrito federal en materia del fuero común y para toda la República en materia del fuero federal del 22 de marzo del 2000, se proponía una redacción que incluyera el acceso de las comunicaciones a través de medios electrónicos, electromagnéticos u ópticos.

Además, el artículo 167 fr.VI del Código Penal Federal sanciona con uno a cinco años de prisión y 100 a 10,000 días de multa al que dolosamente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos. En ésta fracción podría encuadrar entonces la acción de interceptar correos electrónicos antes de que lleguen a su destinatario, pero no el leer la correspondencia electrónica de otra persona.

- Obtención de información que pasa por el medio.- Este tipo de conductas, que se refiere a interceptar datos que las personas envían a través de la red (cuando hacen una compra por la Internet, por ejemplo, enviando datos

personales y de crédito) se tipifican en el artículo 167 fr. VI del Código Penal Federal que fue hecho referencia en el punto anterior.

Capítulo 7

Conclusiones

La base principal del comercio electrónico es su seguridad. Hoy en día se tienen muchos protocolos realmente buenos que han hecho que realmente se pueda confiar en que la información que se envía a través de Internet no podrá ser utilizada de manera maliciosa, pues es casi imposible que se descifre esta información. Cabe mencionar que hoy en día los principales ataques no son descifrando esta información que viaja cifrada por Internet sino buscando hoyos, debilidades en los sitios y para esto regularmente un hacker lo hace a través de un browser. Por eso es muy importante tener un completo conocimiento de todos los elementos que están relacionados con nuestro sitio Web por muy simples que parezcan.

En contraste con la seguridad informática, se puede decir que la Ley llena parcialmente un vacío legislativo en una materia de mucha importancia. Sin embargo, múltiples deficiencias, así como diversas lagunas la hacen insuficiente, por lo que es necesario hacer una revisión exhaustiva en el Código Penal.

Bibliografía

"Aprendiendo TCP/IP en 14 días", Timothy Parker, Edit. Prentice Hall, 2a. edición.

"*Aplicaciones de negocios en JAVA. Haga trabajar la Red, ponga en práctica sus conocimientos"*, Jorge Bourdette, Edit. Colección compumagazine mp ediciones.

"Building Web Applications with UML Second Edition", Jim Conallen, Edit. Addison Wesley.

"*Web Hacking: Attacks and Defense"*, Stuart McClure, Saumil Shah, Shreeraj Shah, Edit. Addison Wesley.

"XML for real programmers", Reaz Hoque, Edit. Morgan Kaufmann.

Referencias

Barry M. *Leiner, A brief history of the Internet.* V. 3.32. Ultima revisión 10 Diciembre 2005. <http://www.isoc.org/internet/history/brief.shtml> [Consulta 20 Junio 2005]

Coria David Marcelo. Internet. Publicado el 6 Agosto 2003. <http://www.ilustrados.com/publicaciones/EpypElVkAytwjKMMdG.php> [Consulta 15 Junio 2005]

Grez Reddick. *Internet Basics.* <http://www.xoc.net/works/jigsaw/internetbasics.asp> [Consulta 25 Junio 2005]

Mariano Hevia. *Virtual Private Networks (VPN).* Publicado 9 Octubre 2003. <http://ilustrados.com/publicaciones/EpyVZEuyZyvcuQWbzR.php> [Consulta 13 Junio]

Oscar Robles. *Historia de Internet en México.* <www.banderas.com.mx/hist__de_internet.htm> [Consulta 21 Junio 2005]

Saulo Barajas. Curso de protocolos TCP/IP. Última actualización 8 Diciembre 2001 <http://www.saulo.net/pub/tcpip/b.htm> [Consulta 10 Junio 2005]

SmartSol. *Diferencias entre E-commerce y E-Business* <http://www.smartsol.com.ar/articulos/diferencias-ecommerce-ebusiness> [Consulta 1 Junio]

Solange Barteloot Grisel. *Las aplicaciones de negocios en Internet.* <http://lidti.unsa.edu.ar/danny/seminario/DisenoWeb.doc> [Consulta 15 Junio 2005]

V. Batis Álvarez. *Legislación informática en México.* <http://seguridad.internet2.ulsa.mx/congresos/2003/cudi2/legislacion_full.pdf> [Consulta 17 Mayo]