UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES " CUAUTITLÁN "

SEMINARIO DE REDES DE COMPUTADORAS.
"ANÁLISIS DE LA SEGURIDAD EN INTERNET PARA EL COMERCIO ELECTRÓNICO"

TRABAJO DE SEMINARIO

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADA EN INFORMÁTICA

P R E S E N T A :

LUCERO MARÍN CARDONA

ASESOR: LIC. CARLOS PINEDA MUÑOZ

Cuautitlán Izcalli, Edo de México, 1997

VNIVERSIDAD NACIONAL
AVPNOMA DE
MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN
UNIDAD DE LA ADMINISTRACION ESCOLAR
DEPARTAMENTO DE EXAMENES PROFESIONALES

U. N. A. M.
FACULTAD DE ESTUDIOS
SUPERIORES-CUAUTITLAN

DEPARTAMENTO DE
EXAMENES PROFESIONALES

DR. JAIME KELLER TORRES
DIRECTOR DE LA FES-CUAUTITLAN
P R E S E N T E .

AT'N: ING. RAFAEL RODRIGUEZ CEBALLOS
Jefe del Departamento de Exámenes
Profesionales de la FES-C.

Con base en el art. 51 del Reglamento de Exámenes Profesionales de la FES-Cuautitlán, nos permitimos comunicar a usted que revisamos el Trabajo de Seminario:

Redes de Computadoras. Análisis de la Seguridad en Internet para el Comercio Electrónico.

que presenta la pasante: Lucero Marín Cardona,
con número de cuenta: 8906828-9 **para obtener el Título de:**
Licenciado en Informática.

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXAMEN PROFESIONAL correspondiente, otorgamos nuestro VISTO BUENO.

A T E N T A M E N T E .
"POR MI RAZA HABLARA EL ESPIRITU"
Cuautitlán Izcalli, Edo. de México, a 13 **de** Octubre **de 19** 97

MODULO:	PROFESOR:	FIRMA:
I	Lic. Carlos Pineda Muñoz	
III	M.I. Gloria Ponce Venegas	
IV	Ing. Francisco Chavéz Castañeda	

DEP/VOBOSEM

AGRADECIMIENTOS

A DIOS:

Por ser el creador de mi existencia y guía de todos los actos de mi vida.

A MIS PADRES:

Porque gracias a ellos, estoy aquí y he podido concluir mis metas.

A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Por darme la oportunidad de pertenecer a ella y de formarme profesionalmente, lo cual me hace sentir orgulloso de ser UNIVERSITARIO.

A LA FACULTAD DE ESTUDIOS SUPERIORES

Por los conocimientos adquiridos para obtener el Título de Licenciado en Informática y a la que siempre tendré gratitud.

A MIS MAESTROS

Por haber comparatido conmigo sus conocimientos y experiencias y por su ejemplo de tenacidad, profesionalismo y entrega.

A MIS ASESORES:

Por el tiempo y esfuerzo dedicado a la elaboración del presente trabajo.

A MIS AMIGOS:

Por la amistad brindada y respaldo ofrecido durante mi preparación profesional (en especial a Pablo R. E., quien me ha acompañado durante todo esta etapa).

ANÁLISIS DE LA SEGURIDAD EN INTERNET PARA EL COMERCIO ELECTRÓNICO

ÍNDICE

INTRODUCCIÓN

Hasta hace algunos años, nadie hubiese imaginado el acelerado desarrollo que alcanzó la industria de la computación; inicialmente existía una tecnología complicada, de uso casi exclusivo para especialistas, pero en menos de 40 años ha crecido dicha tecnológia de tal forma que está volviendose indispensable hasta para desempeñar actividades cotidianas. Sin duda alguna, se esta convertiendo en el elemento principal de la revolución industrial actual, ya que gracias a éste, se ha incrementado de manera inimaginable la productividad a un ritmo impresionante, constituyendose en una valiosa herramienta para lograr gran aceleración en los diferentes campos del saber humano.

La disminución en el tamaño y fácil manejo de los equipos de cómputo, ha llevado al desarrollo de una comunicación más ágil y oportuna en todos los órdenes de la vida, ya sea económico, político, social o cultural, Internet ha cobrado mucha importancia.

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

El éxito de Internet es la libertad que ofrece, ya que no existe ninguna compañía u organización que la posea, controle, censure, ni jefes, directores o accionistas. Los costos por largas distancias no existen así como el costo por tiempo de acceso; el costo solamente depende de la integración de los servicios deseados y su nivel de conexión, es decir, si el enlace es a través de una línea telefónica y un módem, o de un enlace de mayor envergadura, el costo dependerá del equipo utilizado (estaciones de trabajo, equipo de supercómputo, etc.) y del tipo de enlace necesario (satelital, fibra óptica, RDI, etc.). Cada organización, grupo o compañía que está conectado a Internet es responsable de sus propias máquinas y su sección de la línea.

Con base en lo anterior, es imprescindible tomar medidas de seguridad, ya que el acceso de Internet no tiene límites; basta con tener un módem al cual puedan llamar telefónicamente y cualquier persona podrá marcar el número de la línea y entrar a nuestra computadora, lo que expone totalmente nuestra información.

Lo mencionado en los párrafos anteriores fue la motivación del presente trabajo, el cual iniciará mostrando los adelantos que se han dado en Internet con el paso del tiempo, así como también se dará un análisis del tipo de conexión y los protocolos que se requieren para el intercambio de información.

Otros puntos que se abordarán son los relacionados con las cuestiones legales que se han tenido que establecer como consecuencia del acelerado crecimiento de usuarios; los cuales están relacionados con: el Comercio, .Leyes de Exportación, Derechos de Propiedad, Política y Privatización.

Entrando de lleno a las cuestiones de seguridad, se dará una descripción de los niveles generales de seguridad que se han establecido como norma (en los estados unidos). Aunque en nuestro país no se han implementado, son un adelanto de lo que tal vez regirá; además de ser una introducción de lo que esta realizando actualmente en el mundo.

También es importante saber que personas y de que forma pueden hacer daño a una organización, así como la forma en que podemos defendernos de ellos. Lo anterior se desarrolla ampliamente en el capítulo 3, donde se abordan: los tipos de personas dañinas o piratas de la información que pueden irrumpir en los sistema, la forma de contra atacarlos, los tipos de defensas más seguros y las herramientas con las que se cuentan como ayuda para mantener la seguridad.

Finalmente se presenta una propuesta general que muestra los conceptos más importantes que ayudan a mejorar la seguridad en la red, ya que muestra los puntos principales a considerar para salvaguardar los recursos tanto de software como de hardware de una organización.

CAPÍTULO

1

ANTECEDENTES DE INTERNET

CAPITULO 1. ANTECEDENTES DE INTERNET

1.1. Historia.

HISTORIA

Internet[1] fue creada a partir de un proyecto del departamento de defensa de los Estados Unidos llamado DARPANET (Defense Advanced Research Project Network) iniciado en 1969 y cuyo propósito principal era la investigación y desarrollo de protocolos de comunicación para redes de área amplia para ligar redes de transmisión de paquetes de diferentes tipos capaces de resistir las condiciones de operación mas difíciles y continuar funcionando aún con la pérdida de una parte de la red.

Estas investigaciones dieron como resultado el protocolo TCP/IP (Transmission Control Protocol/Internet Protocol), quien se encarga de asignar el domicilio destino de forma correcta y se asegura de que la comunicación se lleve a cabo. Durante el desarrollo de este protocolo se incrementó notablemente el número de redes locales de agencias gubernamentales y de universidades que participaban en el proyecto, dando origen así a la "***red de redes***" mas grande del mundo, las funciones militares se separaron y se permitió el acceso a la red a todo aquel que lo requiriera sin importar que país que solicitara, siempre y cuando fuera para fines académicos o de investigación (y por supuesto que pagara sus propios gastos de conexión), los usuarios pronto encontraron que la información que había en la red era por demás útil y si cada quien aportaba algo se enriqueceria aún más el acervo de información existente.

Después de que las funciones militares de la red se separaron en una sub-red de Internet, la tarea de coordinar el desarrollo de la red recayó en varios grupos, uno de ellos la **National Science Foundation** (Fundación Nacional de Ciencia)fue el que promovió bastante el uso de la red ya que se encargo de conectar cinco centros de supercómputo que podían ser accesados desde cualquier nodo de la red. Eso funcionó bien al principio, pero pronto fueron superadas las cargas de tráfico previstas, fue entonces que se dio la concesión a **Merit**

[1] Para una información más detallada sobre la Historia de INTERNET, ver el Anexo 1, que contiene datos cronológicos sobre la evolución de Internet.

Network Inc. para que administrara y actualizara la red, se mejoraron las líneas de comunicación dando un servicio mucho más rápido, pero este proceso de mejora nunca termina debido a la creciente demanda de los servicios que se encuentran en la red.

El grupo de mayor autoridad sobre el desarrollo de la red es la **Internet Society** creado en 1990 y formado por miembros voluntarios, cuyo propósito principal es promover el intercambio de información global a través de la tecnología Internet. Pero no es el único grupo que puede tomar decisiones importantes, existen otros tres grupos que tienen un rol significativo, el **IAB**[2] **(Internet Architecture Board)**, toma las decisiones acerca de los estándares de comunicaciones entre las diferentes plataformas para que puedan interactuar máquinas de diferentes fabricantes sin problemas, este grupo es responsable de cómo se deben asignar las direcciones y otros recursos en la red. Aunque no son ellos directamente quienes se encargan de hacer estas asignaciones, para esto hay otra organización llamada **NIC**[3] **(Network Information Center)** administrado por el departamento de defensa de los Estados Unidos. El tercer grupo más importante es el **IETF**[4] **(Internet Engineering Task Force)** en el cuál los usuarios de Internet expresan sus opiniones sobre cómo se deben de implementar soluciones para problemas operacionales y cómo deben de cooperar las redes para lograrlo. La dirección de Internet es en cierta manera una autocracia que funciona.

El enorme crecimiento de Internet se debe en parte a que es una red basada en fondos gubernamentales de cada pais que forma parte de Internet lo que proporciona un servicio prácticamente gratuito, pero desde 1993 Internet ha dejado de ser la red de instituciones gubernamentales y universidades para convertirse en la red pública más grande del mundo; y a principios de 1994 comenzó a darse un crecimiento explosivo de las compañías con propósitos comerciales en Internet, dando así origen a una nueva etapa en el desarrollo de la red.

---

2 El IAB, o Consejo de la Arquitectura Internet, es una organización perteneciente a la Sociedad de Internet (ISOC) que se encarga, entre otras cosas, de aprobar las normas de Internet.

3 El NIC, o Centro de Información de Red, reciben este nombre las organizaciones responsables de facilitar la información de una red.

4 El IETF, o Grupo de Ingeniería en Internet, es una organización perteneciente al IAB, cuya finalidad es discutir y dar solución a los posibles problemas técnicos que pueda tener Internet.

En pocas palabras, Internet es una gigantesca base de datos distribuida en todo el mundo, en la que se puede encontrar información y servicios de todo tipo, y que para poder ser accesada requiere de herramientas que permitan buscar rápidamente la información que uno necesita a través de máquinas localizadas en cualquier parte.

Actualmente Internet esta formada por aproximadamente veinte millones de usuarios y cuatro millones de computadoras conectadas en todo el mundo, con equipos y sistemas operativos tan diferentes como OS/2, Macintosh, Unix, y MS- DOS comunicándose transparentemente bajo el protocolo TCP/IP. Lo cual trae tanto ventajas como desventajas; siendo las ventajas de mayor peso que los incovenientes.

VENTAJAS DE INTERNET

Las ventajas que tiene Internet para los usuarios y empresas conectadas se listan a continuación:

- Intercambio de información de manera rápida y eficiente.
- Consultar a expertos y gente experimentada en miles de campos.
- Recepción de actualizaciones regulares en los temas de interés
- Acceso a la información desde muchas y muy diversas locaciones.
- Traducción y transferencia de datos de diferentes tipos de computadoras.
- Utilidad como entretenimiento, diversión y compras.

DESVENTAJAS

Entre las más importantes se encuentran.

- La saturación de los canales de transmisión.
- Falta de seguridad
- Facilidad de intercepción y fabricación de mensajes.

Las diferentes partes de Internet están conectadas por un conjunto de computadoras llamadas *enrutadores*, que interconectan a las redes. Estas redes pueden ser Ethernets, Token Rings o en ocasiones líneas telefónicas (medio a través del cual el correo va de un lugar a otro), como se muestra en la Figura 1.

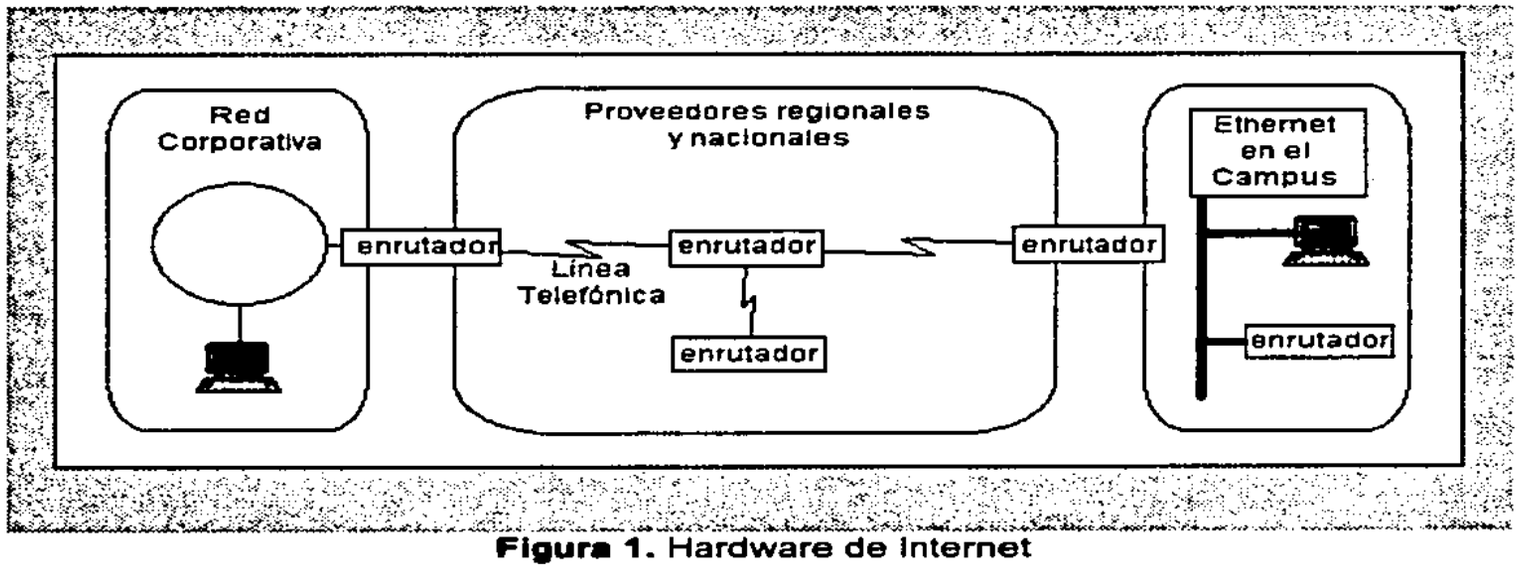


Figura 1. Hardware de Internet

Gran parte de las aplicaciones de Internet, tiene una estructura cliente- servidor. En esta estructura, la información se encuentra en el servidor y el cliente tiene la capacidad de pedir la información necesaria, interpretarla y desplegarla. De esta manera, la información se distribuye, no se centraliza, lo que permite una gran variedad de servicios al existir una diversidad de usuarios, y no hay una manera única de accesar la información, además se puede utilizar cualquier cliente que entienda el protocolo utilizado.

1.2. Descripción del modelo OSI.

Para que dos computadoras en la red puedan comunicarse, se deben considerar aspectos tan diversos, que generalmente se aplica la técnica "divide y vencerás", es decir, partiendo el problema en varias tareas, cada una encargada de resolver un punto específico de la comunicación.

De esta manera la conexión lógica entre las computadoras se divide en una serie de "capas" que, en conjunto, forman lo que se llama la arquitectura de la red, o bien la familia de protocolos de la red.

Con el fin de permitir que distintas arquitecturas diseñadas por distintos fabricantes puedan interactuar entre sí, la Organización de Estándares Internacionales (ISO, por sus siglas en inglés) inició en 1977 la definición de un modelo de referencia llamado el Modelo de Interconexión de Sistemas Abiertos (el modelo OSI), que divide la arquitectura de la red en siete capas, cada una con funciones específicas e independientes de las demás, ver el Cuadro 1.

CAPA 7	**Aplicación:** Define las reglas de comunicación entre aplicaciones y la red (correo electrónico, transferencia de archivos, bases de datos).
CAPA 6	**Presentación:** Orgánica la transferencia de datos entre sistemas para representarlos y codificarlos de una manera uniforme.
CAPA 5	**Sesión:** Se encarga de la coordinación de las comunicaciones en forma ordenada y del control de la sesión.
CAPA 4	**Transporte:** Su función es verificar la validez de la integridad de la transmisión utilizando algoritmos de corrección de errores.
CAPA 3	**Red:** Define la ruta entre las unidades de emisión y recepción de datos, haciendo las veces de conmutador.
CAPA 2	**Enlace:** Se responsabiliza de la integridad de la transmisión de datos entre dos nodos.
CAPA 1	**Física:** Configura las características físicas necesarias para la transmisión y recepción de datos en forma de bits.

Cuadro 1. Función específica de cada capa del modelo OSI.

En este modelo, la capa N en una computadora, realiza sus funciones comunicándose con la capa del mismo nivel (llamada entidad par) en otra computadora. La comunicación entre entidades pares se lleva a cabo a través de reglas bien definidas (**los protocolos**) para una arquitectura de red en particular. Las funciones de la capa N sirven para que ésta pueda ofrecer un servicio a la capa inmediatamente superior en la misma computadora. De esta manera se van agregando servicios conforme se asciende por las capas de la arquitectura hasta llegar a la capa de aplicación, en donde los procesos de los usuarios de la red, obtienen sus servicios.

El modelo OSI no define protocolos ni servicios, éstos dependen de la implementación específica a cada arquitectura de red. Lo que el modelo define es la función que debe de ser realizada en cada capa; esto es, establece los lineamientos para que el software y los dispositivos de diferentes fabricantes funcionen juntos.

1.3. Protocolo TCP/IP.

Los protocolos

Los protocolos son reglas formales de comportamiento. Teniendo un conjunto común de reglas ampliamente conocidas, se puede lograr y gobernar la comunicación entre computadoras.

En redes homogéneas, un sólo proveedor de cómputo especifica un conjunto de reglas para optimizar las capacidades de hardware y software de sus productos. Pero en redes heterogéneas, TCP/IP (es el principal protocolo utilizado actualmente) puede por ejemplo, lograr la convivencia y comunicación de máquinas de distintos proveedores, distintos sistemas operativos y distintas plataformas de hardware. Este protocolo esta conformado de dos partes: **1)** TCP y **2)** IP.

TCP: Este protocolo proporciona un flujo fiable de bytes en los dos sentidos de la conexión. Garantiza que los bytes que salen del nodo origen sean entregados en el nodo destino de una forma fiable, en su mismo orden y sin duplicarlos (TCP es un protocolo orientado a la conexión).

IP: Este protocolo fija las normas para que los paquetes alcancen su destino, pero lo que garantiza es **cuando** van a alcanzar estos paquetes su destino, **cuántos** lo van a hacer o en qué **orden**.

La Arquitectura de TCP/IP

TCP/IP es un conjunto de protocolos que no fue desarrollado en base al modelo OSI, ya que este se liberó mucho después que TCP/IP, además se basa en un modelo de cuatro capas (ver Cuadro 2), a diferencia del OSI que cuenta con 7.

CAPA 4	**Aplicación:** Consiste de programas y procesos que utilizan la red.
CAPA 3	**Transporte:** Conectividad de computadora-a-computadora en la red, ofreciendo el servicio de punto-a-punto de entrega de datos.
CAPA 2	**Red:** Define los paquetes de comunicación entre las computadoras, y maneja el ruteo de los datos. Rutear consiste en enviar la información a la computadora correspondiente en la red correspondiente.
CAPA 1	**Acceso:** Esta capa consiste en rutinas de acceso al medio de transmisión.

Cuadro 2. Función específica de cada capa del protocolo TCP/IP.

Como en el modelo OSI, los datos son transferidos entre las capas del protocolo y después es enviado por el medio físico a la red. Cada capa realiza funciones de control y transferencia al siguiente nivel. Esta información de control se le llama encabezado debido a que se posiciona al principio de los datos a ser transmitidos. Cada capa procesa la información que le llega de la capa superior y la transmite añadiéndole su encabezado, y así pasarla a la capa inferior.

Los protocolos TCP/IP en la Internet no crecieron rápidamente por el hecho de "estar ahí" como un estándar abierto. Estos protocolos satisfacieron una necesidad importante en el momento adecuado, y con varias características importantes:

- Protocolos de estándares abiertos, disponibles gratuitamente y desarrollados por varios fabricantes para plataformas específicas de hardware (actualmente se tiene software TCP/IP para prácticamente todas las plataformas de hardware existentes). TCP/IP es ideal para realizar comunicaciones entre distintas plataformas de hardware, aunque no se encuentran conectadas a Internet.
- Independencia del hardware de la red (puentes, ruteadores, tarjetas de red, etc..). Esto permite a TCP/IP integrar varios tipos de redes. TCP/IP puede correr como protocolo de comunicación en Ethernet, Token Ring, linea Telefónica, X.25, Frame Relay, ATM, y virtualmente en cualquier otro medio de transmisión.
- Un esquema de direccionamiento que permite a un dispositivo tener una dirección única dentro de toda la red, aún cuando ésta sea tan grande como la red mundial de Internet.
- Protocolos de alto nivel estandarizados para consistencia y servicios para usuarios ampliamente disponibles.

Protocolo de Transferencia de Archivos

El Protocolo de Transferencia de Archivos es el método primario de transferir archivos en Internet. Este método de transferencia normalmente requiere de una cuenta de usuario registrada en el sistema ó de una configuración realizada por el administrador del sistema para proporcionar acceso a usuarios que no cuentan con una contraseña en el sistema (anonymous login). Existen otras formas de transferir archivos entre computadoras, como son los **bbs**[5] y el **e-mail**[6]. La diferencia entre todos estos consiste en que con e-mail hay un destinatario conocido a quien se le envían los archivos, con los bbs y **ftp**[7] no existe ese

[5] BBS (Bulletin Board System), el cual un Sistema de Boletín Electrónico o un Tablón de Anuncios.
[6] E-MAIL, es un programa de Correo electrónico.
[7] FTP, es un Protocolo utilizado para la Transferencia o intercambio de Archivos.

destinatario específico, los archivos están ahí para quien esté interesada en ellos, de tal manera que puedan copiarlos a sus computadoras.

Debido al acceso anónimo con el que cuenta Internet, cualquier persona en el mundo que conozca la dirección de un servidor FTP anónimo, puede tener acceso a los recursos que éste ofrezca. Algunos sistemas han dedicado discos completos y computadoras completas a mantener una extensa variedad de archivos, documentos, programas e información.

El proceso de la conexión a estos servidores FTP, involucra que el usuario "anónimo" abra una conexión de FTP y se registre en el sistema como "anonymous", y a continuación escriba un password arbitrario (la mayoría de los sistemas pide como password la dirección de correo electrónico del usuario), como por ejemplo:

Login name (hola.com.mx): anonymous
Password: perezj@cica.com.mx

La velocidad de la transferencia depende del tipo primario de conexión, tanto del cliente (la computadora de la persona que solicita el servicio) cómo del servidor. Una computadora conectada por módem con una velocidad de 9600 bps bajo SLIP, no tendrá la misma velocidad de transferencia que un sitio que tenga un enlace de 64 kbps. Además, influyen los otros usuarios que se encuentren conectados a la red, la hora en que se realiza la transferencia (al igual que la Red telefónica existen horas pico), y el propio trabajo que se encuentre ejecutando la máquina servidora de FTP.

Para facilitar la tarea de encontrar la ubicación de algún archivo o programa en particular, existe el programa Archie, que permite hacer una búsqueda en extensas bases de datos donde se almacena información sobre los diferentes sitios que proporcionan el servicio de FTP anónimo. Las búsquedas se realizan por palabras clave, y regresa como resultado las direcciones y los directorios donde se encuentra el archivo buscado.

Finger

Es uno de los primeros protocolos (de UNIX) y de los más simples de la red. Este protocolo permite encontrar la clave de acceso de alguien (incluyendo su domicilio de correo electrónico), su nombre y también permite saber si actualmente la persona buscada tiene activa una sesión de trabajo, en la máquina investigada.

Es importante aclarar que **finger** requiere que un servidor este funcionando en la computadora destino para que atienda la solicitud de búsqueda, además de contar igualmente con un Finger. Lo anterior es considerado como una medida de seguridad, ya que al quitar al Finger del servidor, la búsqueda no se podrá realizar aunque este activo éste.

1.4. INTERNET en México.

México ingresó a Internet en 1989, siendo la Universidad Nacional Autónoma de México (UNAM) y el Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM) las primeras instituciones en ser miembros de esta red.

Actualmente, el Tecnológico de Monterrey funge como administrador principal de la conexión a Internet de México, siendo ante el cual se registran las nuevas compañías y organizaciones que adquieren su conexión a Internet. Sin embargo, esta misión es realizada en la zona sur del país por la UNAM, que provee la información y documentación necesaria para el registro a Internet.

En 1994, CONACYT delega la administración de los servicios de información para empresas e instituciones lucrativas a una organización llamada RTN (Red Tecnológica Nacional), realizándose una actualización de la conexión de alta velocidad en México de 64 kilobits a 2 megabits, financiado por las universidades integrantes de MEXNET, organización mexicana de instituciones educativas en Internet. Actualmente, el fideicomiso llamado INFOTEC administra RTN y proporciona servicios de Internet a una gran cantidad de usuarios en México, principalmente del sector privado y empresarial.

En México, el desarrollo de Internet se había limitado al ámbito de las universidades. Pero esto ha cambiado a gran velocidad a partir de 1994, con la llegada de varias compañías que ofrecen comunicación a Internet vía SLIP o PPP, como es el caso de Internet de México, los BBS (servicios de comunicación personal vía modem = Bulletin Board System) también han evolucionado y se encuentran ofreciendo conexiones a Internet, como SPIN y Tornado BBS. Aunque se ha establecido en la Universidad de Guadalajara el servicio comercial de Mexplaza, no se ha establecido aún en México la posibilidad de hacer transacciones en línea, limitándose el uso de Internet como aparador para la comunidad Internet. Por esto mismo, el campo de desarrollo dentro de Internet en México es vasto y poco explorado, y cada vez más personas se conectan y utilizan la Red para sus propósitos personales, participando de la creciente globalización mundial.

La edad de los usuarios en México varía entre los 17 y los 25 años, y la cantidad de usuarios se encuentra actualmente cercana a los 30 mil usuarios. El sector económico al que pertenecen los usuarios es medio a medio-alto. La conexión la proporciona el mismo centro educativo al cual se encuentran inscritos, y utilizan las instalaciones de sus universidades principalmente para correo electrónico, seguido por las aplicaciones de plática (IRC, Chat, BBS) y el uso de software e información de la red. La mayoría de los usuarios de Internet son hombres, siguiendo la tendencia actual a nivel mundial.

SECTOR GOBIERNO

Es conocido también que la Presidencia de la República y gran parte de las secretarías e instituciones del gobierno mexicano (Secretaría de Comunicaciones y Transportes, Secretaría de Salud, Secretaría de Educación Pública, por mencionar algunos ejemplos), cuentan con conexión a Internet. Por ejemplo,la Secretaría de Salud ha desarrollado un servicio de información médica en Internet para acceso general, y el INEGI (Instituto Nacional de Estadística, Geografía e Informática) también ha puesto su servidor en la Red. Cabe mencionar que los gobiernos de algunos estados, como Morelos y Nuevo León también han comenzado a crear servicios dirigidos a usuarios de Internet.

1.5. Futuro de INTERNET.

El gobierno de los Estados Unidos tiene grandes planes sobre Internet, como muestra la propuesta del vicepresidente Al Gore sobre la "supercarretera de la información". La NREN (National Research & Education Network) fue aprobada por el Congreso norteamericano, con un presupuesto de 2 billones de dólares y cinco años de duración para actualizar el enlace a Internet. Cuando el proyecto concluya, la red será cincuenta veces más veloz que la red más rápida que se pueda conseguir en la actualidad, por ejemplo, permitirá la transferencia electrónica de toda la Enciclopedia Britanica en un segundo.

El crecimiento de Internet se ha enfocado principalmente hacia las interfaces gráficas, donde Netscape Communications, compañía fundada en 1994 y que cuenta con casi toda la gente que ha trabajado en WWW a nivel mundial, tiene el control del 70% del mercado. La evolución continúa por esta vía: el uso de RV (Realidad Virtual) para navegar en Internet, el surgimiento del lenguaje VRML enfocado a la creación de mundos virtuales, HotJava, que permitirá la creación de programas multimedia en tiempo real accesibles a través de la red, Internet Worlds Chat, que establece un servicio de plática en línea en 3 dimensiones, la generación de nuevos estándares para el almacenamiento de imágenes, y el mejoramiento de los protocolos existentes como por ejemplo IP+ y HTTP binario (el protocolo en que se basa W W W).

Otros planes y servicios, de los cuales ya existen las bases para su desarrollo, son el uso de Internet para comunicación telefónica (Internet Phone), y el envío de faxes a gran número de personas alrededor del mundo (TPC project).

Una de las preocupaciones en Internet es referente a la seguridad; este aspecto se ha vuelto importante a partir de la entrada de empresas a la Red, ya que para sus transacciones necesitan números de tarjetas de crédito y datos confidenciales, por lo cual se esta realizando un gran trabajo para desarrollar protocolos de seguridad, como SSL[8], que no interfieran en el rendimiento de la red.

[8] SSL, es un protocolo de seguridad que permite verificar si la persona que se firma como usuario es realmente quien dice ser.

La gran importancia que ha adquirido Internet se puede apreciar claramente en la última polémica que se ha generado: la Acta de Decencia en las Comunicaciones propuesta por el Senador Leahy en Estados Unidos, en la cual, el tema a debatir es básicamente la protección de los menores de edad de la información no apropiada que se encuentra distribuida en la red. Pero claro, la reacción de los usuarios de Internet no se hizo esperar, pidiendo que la red continuara libre, por lo que la Cámara de Representantes aprobo una propuesta alternativa que deja la responsabilidad a los padres de familia de escoger la información para sus hijos.

1.5.1. Nuevos estándares de protocolos.

En el punto 1.2. Descripción del Modelo OSI, se habló de la Organización Internacional para la estandarización y su conjunto de protocolos; el cual se ha convertido en un estándar internacional. Hoy en día muchos de los componentes de Internet permiten el uso de los protocolos OSI; aunque no hay mucha demanda. El gobierno estadounidense ha tomado la postura en la que todos sus computadoras deben ser capaces de manejar estos protocolos.

Aún no es clara la demanda que tendrá OSI ahora que cuenta con el respaldo del gobierno de los Estados Unidos. Mucha gente piensa que si el enfoque actual funciona no habrá la necesidad de cambiarlo, ya que apenas se esta disfrutando lo que se tiene. Actualmente no hay muchas ventajas para cambiarse a OSI , ya que es más complejo y menos maduro que el IP y no es tan eficaz. Ofrece algunas caracteristicas adicionales, pero para redes de gran velocidad y tamaño, aunque también se tienen los mismos problemas sufridos por IP.

La gran velocidad de crecimiento de usuarios de Internet en los últimos años presentará grandes cambios en la red, la cual, deberá adaptarse a las demandas de los mismos. TCP/IP como a se menciono en el punto 1.3, es el encargado de que los datos lleguen a su destino dentro de la red. Pero este protocolo estaba previsto para un número muy inferior de usuarios a los que hay ahora. Por esto, desde hace unos años existe una

preocupación por el hecho de que se están acabando las direcciones IP (basadas en códigos de 32 bits) a la vez que el número de usuarios de Internet aumenta.

En 1994, se culminó una investigación tendente a solucionar el problema, llegando a un modelo administrativo mucho más eficiente y a una política de encaminamiento de los mensajes muy mejorada, así como una arquitectura en la cual basar la nueva generación del protocolo IP: el **IPv6** (IP versión 6).

El IPv6 amplía las direcciones del IP actual de 32 bits a 128 bits, por lo que se podrá dar cabida no sólo a todos los ordenadores que se quiera sino, también a dispositivos que en un futuro puedan entrar a la red, como son, por ejemplo los televisores. Este cambio significa que los ordenadores, routers (sistemas encaminadores) e, incluso las aplicaciones han de ser modificadas. De todas formas, el usuario no tendrá que cambiar su dirección de correo electrónico o el URL de un Web, ya que los cambios se producen en los dominios de un sistema. Se cree que la implantación masiva del IPv6 puede comenzar en 1998.

1.5.2. Cuestiones Legales en Internet.

Hay tres áreas Legales que tienen injerencia en Internet:

- Los subsidios federales pagan grandes porciones de Internet y no incluyen dichos subsidios para el comercio en la red.
- Internet no es solamente una red de cobertura nacional, es una red global, con lo cual, cuando se transporta cualquier artículo a través de la frontera de un país, incluyendo bits, las leyes de exportación tienen injerencia y las redes locales cambian.
- Cuando se transporta software (ideas) de un lugar a otro, es necesario considerar la propiedad intelectual y los asuntos de licencia.

Investigación, educación y dinero federal.

Muchas de las redes en Internet están patrocinadas por agencias federales. Bajo la Ley federal, una agencia sólo puede gastar su presupuesto en cosas que sean de su injerencia, lo que también se aplica a la red. Un usuario puede que no tenga idea por que redes atraviesan los paquetes de información que genera, pero más vale que entren en el campo de acción de la red respaldada por la agencia correspondiente, ya que de otra forma, se estará incurriendo en un delito federal.

Comercialización

Durante mucho tiempo ha estado limitado el uso comercial de Internet, esto se debe a que la red está sostenida casi en su totalidad por fondos gubernamentales y a que su propósito era estrictamente académico. Las políticas que restringían el uso de la red han empezado a cambiar, lo cual es benéfico para los negocios pequeños que no cuentan con los recursos necesarios para mantener una red nacional privada como lo hacen las grandes corporaciones. Gradualmente se irán eliminando las políticas restrictivas, permitiendo así dar un apoyo a las industrias para que aprovechen esta ventaja, además de incrementar los servicios que se ofrecen en la red. También se reducirán los costos, y la gente común podrá comprar este servicio a precios accesibles.

Las tecnologías se mejoran para adaptarse a la enorme demanda que se espera en los próximos años, el incremento en la velocidad de transmisión y la reducción en los precios ampliarán la gama de servicios existentes y permitirán otros servicios que hoy no son factibles.

Al mismo tiempo que ocurra la comercialización se dará también la privatización (para más información, ver el punto 1.5.3.). Durante años la comunidad Internet ha solicitado a las compañías telefónicas que provean conexiones IP de la misma forma que dan líneas telefónicas, pero esto parecía no importarles, ahora que las empresas comienzan a interesarse en Internet, las compañías telefónicas han visto un gran negocio y van a presionar para que el gobierno reduzca los subsidios y sean ellas las que den el servicio. Esto significa que las instituciones comerciales o educativas tendrán que pagar la parte que les corresponde por estar en Internet y el apoyo del gobierno se retirará gradualmente. Esto es justo para las

empresas que obtengan una utilidad, pero puede ser perjudicial para las universidades que dependen de los apoyos federales (si la instalación es comercial, el tráfico será enrutado por enlaces privados, los cuales serán más caros que los de investigación y educación).

Finalmente se dará una fusión entre las tecnologías de telecomunicaciones para crear un nuevo tipo de redes que incluya a las compañías telefónicas, televisoras y de servicios informativos, para que juntas conformen a lo que se conoce como las supercarreteras de información.

Leyes de exportación

La exportación de bits está dentro de las restricciones de exportación del Departamento de Comercio; para no caer en infracciones se mencionan dos formas para evitarlo[9].

1. La exportación de cualquier cosa requiere de una licencia.

Este punto es muy claro, ya que para exportar cualquier cosa se requiere de una licencia de exportación para hacerlo. Pero existe una ***licencia general*** que permite a cualquier persona exportar lo que no esté restringido específicamente y que esté disponible en foros públicos.

2. Exportar un servicio es prácticamente igual a exportar todo lo necesario para proveer el servicio.

Este se basa, en que, por ejemplo, si la exportación de alguna pieza de hardware de una supercomputadora, no está permitida, entonces el acceso remoto a este equipo tampoco lo estará.

Derechos de propiedad

Los derechos de propiedad pueden causar problemas, ya que por ejemplo cuando se toma algún archivo cuyos derechos de copia hayan expirado en alguna parte del mundo. La exportación de este archivo en otra ciudad o país puede que se este incurriendo en una

[9] Según lo menciona Krol DE en su libro "Conéctate al Mundo de Internet".

violación a la Ley del país al que pertenece el substrayente. La Ley sobre la comunicación electrónica no ha avanzado al mismo ritmo que la tecnología.

Política e Internet

Muchos usuarios de la red ven al proceso político tanto como una bendición como un castigo. La bendición significa dinero y el castigo es que todas las acciones serán vigiladas constantemente. El apoyo a la red es muy amplio, pero relativamente frágil, ya que cualquier acto que pueda llamar la atención de los políticos puede cambiar radicalmente esta situación y probablemente será en contra.

Privatización

La privatización se desprende de la comercialización. Por mucho tiempo, la comunidad de redes ha requerido que las compañías telefónicas y otras empresas lucrativas provean conexiones IP. Es decir, que así como se ordena un conector para un teléfono en una casa, se pudiera ordenar una conexión a Internet. Pero excepto por Bolt, y Newman, de la compañía que operaba DARPANET, no hubo nadie que aceptara el reto. Las compañías telefónicas siempre han dicho "Nosotros vendemos la línea telefónica y usted puede hacer con ella lo que guste". Por esta razón el gobierno se ha mantenido en el negocio de la conectividad.

Ahora que las grandes empresas se han interesado en Internet, las compañías telefónicas han cambiado de actitud, lo que trae consigo que estas y otros proveedores dedicados a las redes con fines lucrativos se quejen del gobierno por permanecer en el negocio de las comunicaciones.

El discurso ofrecido por la administración actual denominado "National Information Infraestructure" (Infraestructura Nacional de Información) provocó que más empresas de telecomunicaciones se involucraran. Las compañías de televisión por cable se han dado cuenta de que también ellas tienen una infraestructura instalada capaz de conducir señales digitales hasta muchos hogares de Estado Unidos. Por esto, las compañías de cable se han propuesto resolver el problema de la privatización mediante la construcción de una red propia,

sin necesidad de pedir fondos al gobierno. Por sus propios medios, conectarían esta nueva red a la red de televisión por cable. Aunque hay que esperar todavía para saber qué sucederá con esta iniciativa; estas empresas ya han adoptado la religión de Internet (y cuentan con dinero suficiente para invertir). Las compañías de televisión por cable se interesan en aplicaciones que aún no se contemplan en Internet: compras interactivas desde el hogar, juegos de video, etc.

Aunque la mayor parte de la gente en la comunidad de redes cree que la privatización puede ser una buena idea, existen algunos obstáculos en el camino; ya que la mayor parte de estos obstáculos consiste en el financiamiento de las conexiones existentes. Muchas escuelas están interconectadas porque el gobierno paga una parte del costo. Si tuvieran que pagar todo por sí mismas, seguramente la mayoría decidiría gastar su dinero en otra cosa. Las instituciones de investigación avanzada probablemente se quedarían en la red, pero no las escuelas pequeñas, y para la mayoría de las secundarias sería prohibitivo (esto sin mencionar las escuelas primarias). Para muchas personas Internet no es una "necesidad" todavía. Cuando lo sea, la privatización llegará pronto.

1.6. Plan Nacional de Desarrollo en Informática.

PROGRAMA DE DESARROLLO INFORMÁTICO[10], A NIVEL NACIONAL

Redes de datos

Los avances en las telecomunicaciones que posibilitaron la conexión entre computadoras han incrementado, en forma inimaginable, los beneficios de la informática al permitir el flujo de información entre millones de computadoras en todos los rincones del mundo.

[10] Según datos proporcionados por el INEGI, que abarcan el periodo de 1995 al 2000.

La interconexión de redes de computadoras se ha comparado con una infraestructura de autopistas que se enlazan. Esta metáfora hizo surgir el término supercarretera de información, que se utiliza en forma común hoy en día.

El aspecto más importante que se le atribuye a esta tecnología es que, al posibilitar la transmisión y la consulta de información ubicada en distintos continentes, en forma casi instantánea, permite el acceso al acervo creciente de conocimientos del mundo. Por esta razón adquiere gran importancia contar con una infraestructura de redes de datos que permita satisfacer las actuales necesidades del país y nos prepare para los desafíos que traerán los avances tecnológicos que se perfilan. El Programa de Desarrollo Informático propone como uno de sus objetivos propiciar el desarrollo de esta infraestructura.

Para ello, y acorde con los planteamientos del Programa de Desarrollo del Sector Comunicaciones y Transportes 1995-2000, en el apartado correspondiente a Redes Informáticas y Carreteras de la Información, se definen las estrategias y líneas de acción para propiciar el desarrollo de la infraestructura de redes de datos.

El mercado de las telecomunicaciones ha tenido un aumento sustancial en el país, considerando la infraestructura para la transmisión de datos y los servicios de valor agregado; o sea, los que emplean una red pública de telecomunicaciones para comercializar información generada a partir de adiciones, cambios, reestructuración o almacenaje de información procedente de otra fuente.

De 1991 a 1994 el crecimiento del mercado de telecomunicaciones ha sido, en promedio, siete veces mayor que el de la economía en su conjunto. A pesar de esta mejoría, subsisten en el país importantes rezagos de infraestructura que se espera serán atenuados con la entrada al mercado de nuevos oferentes que aprovechen las oportunidades que abre la Ley Federal de Telecomunicaciones, publicada en junio de 1995.

Esta Ley incluye una serie de reformas para promover el desarrollo eficiente del sector, fomentar la sana competencia entre los participantes y mejorar la calidad, diversidad y costo de los servicios. Establece, además, las condiciones para la concesión de redes

públicas de transmisión de datos, promoviendo la adopción de criterios de diseño abiertos y planes técnicos que garanticen la interconexión entre redes para el funcionamiento de servicios de telecomunicaciones. Asimismo, se permite el libre desarrollo de las redes privadas que no utilicen bandas de frecuencia del espectro radio eléctrico, se liberan los servicios de valor agregado que únicamente requieren registro y se elimina el control de precios en todos los servicios.

Diversos permisos para redes públicas de transmisión de datos han sido otorgados, de los cuales ya están en operación: Telecomunicaciones de México, empresa para estatal que opera la red Telepac X.25 de cobertura nacional y algunos servicios satelitales; Iusanet, Cecoban, Optel, Intersys y Telnor, además de la de Teléfonos de México (Telmex).

La privatización de Telmex ha contribuido a atenuar el rezago de las telecomunicaciones. En diciembre de 1994, esta empresa tenía 8.5 millones de líneas de acceso en servicio y un índice de digitalización de 83%. Durante los últimos cuatro años, se instaló una extensa red terrestre de fibra óptica que interconecta a las 54 principales ciudades del país con el resto del mundo. Con la instalación de la tecnología digital, la telefonía ofrece ahora un potencial de valor agregado para la prestación de nuevos servicios; sin embargo, la cobertura de los servicios de transporte de datos y en consecuencia la capacidad de conexión, va comenzando.

Las deficiencias en la infraestructura pública de telecomunicaciones han motivado la proliferación de redes privadas --basadas tanto en cable de cobre y fibra óptica como en conexiones satelitales-- que, aunque ha permitido cubrir las necesidades individuales de distintas organizaciones, propicia la multiplicación de esfuerzos y recursos destinados a este fin. Actualmente existen 295 redes privadas de empresas usuarias de las bandas satelitales y 242 proveedores de servicios de valor agregado, así como 91 empresas de radiolocalización móvil de personas que ofrecen otros servicios para acceso remoto a redes privadas, en México.

Por lo que se refiere a los servicios en línea, particularmente de Internet, la demanda ha mostrado un crecimiento explosivo en los últimos años. Su alta penetración en los distintos

sectores de la sociedad mexicana se refleja en la existencia, a enero de 1996, de 158 servidores de páginas de la red mundial de computadoras distribuidos en 27 entidades federativas en alrededor de 106 instituciones, la mayoría de las cuales pertenece al sector educativo o de investigación, con una creciente participación de empresas privadas. La disponibilidad de información pública del gobierno en este medio esta aún comenzando, y requerirá reforzarse en corto plazo.

La modernización de la infraestructura de telecomunicaciones alentará aún más este tipo de servicios, fomentará la prestación de servicios públicos por medio de redes, así como la creación de empresas que ofrezcan nuevas opciones de valor agregado. Ello requiere, sin embargo, una intensa actividad de investigación y desarrollo en áreas como redes, bases de datos distribuidas y seguridad de la información, que son los temas de mayor preocupación en el mundo en este momento, dentro de las consideraciones que distintos paises están realizando para desarrollar su infraestructura de información.

Objetivos

- Promover el desarrollo de la infraestructura de redes para acceso y transmisión de datos y el desarrollo de servicios públicos y privados a través de medios electrónicos.

Estrategias

- Garantizar la interconexión e interoperabilidad con las redes informáticas globales.
- Consolidar un marco regulatorio que propicie el desarrollo de las carreteras de la información por parte del sector privado, en un ambiente de libertad de acceso y competencia.
- Promover que el Gobierno Federal se convierta en un usuario permanente de las redes informáticas, para simplificar y mejorar los servicios a la ciudadanía.
- Consolidar la infraestructura de redes académicas.

Líneas de acción

Con base en estas estrategias, se proponen acciones dentro de tres líneas: infraestructura, normas y estándares; redes para el sector público; y redes académicas. Estas acciones señalan responsabilidades para las instituciones competentes de la Administración Pública Federal, en particular, de la Secretaría de Comunicaciones y Transportes por sus atribuciones en materia de telecomunicaciones; de la Secretaría de Educación Pública por su competencia en el sector académico; de la Secretaría de Contraloría y Desarrollo Administrativo en cuanto a su ámbito de acción en el desarrollo administrativo de la Administración Pública Federal; y de la Secretaría de Comercio y Fomento Industrial por lo que se refiere a fomento de proveedores de servicios.

Infraestructura, normas y estándares

- Fomentar el desarrollo de una infraestructura pública de telecomunicaciones para redes de datos accesible, confiable, poderosa, flexible y con niveles de calidad y costos competitivos a nivel internacional, que permita una amplia conectividad y sirva de sustento para nuevas aplicaciones informáticas.
- Fomentar el uso de las carreteras de la información en el país y garantizar que sus nodos y troncales de interconexión estén correctamente dimensionados.
- Promover la creación de servicios de acceso a este tipo de redes y coordinar esfuerzos en materia educativa respecto a sus beneficios.
- Fijar el alcance de la normalización en materia de infraestructura informática, para garantizar la conectividad nacional y mundial, apoyando el surgimiento de otras opciones en materia de redes y la aparición de nuevas tecnologías.
- Promover la accesibilidad, competitividad e interoperabilidad, para evitar barreras de entrada en el establecimiento de infraestructuras y de servicios de información.
- Adoptar políticas y normas fundadas en tratados, cuando su eficacia se vincule a la cooperación y coordinación internacional.
- Alentar el establecimiento de tarifas en función de los costos y los servicios, nacionales e internacionales, con el fin de lograr una asignación eficaz de los recursos.
- Agilizar el otorgamiento de permisos para la prestación de servicios de valor agregado, como son las redes de paquetes tradicionales y las de alta velocidad.

- Fomentar la incorporación de escuelas, hospitales y oficinas de gobierno, tanto estatales como municipales, a las carreteras informáticas.
- Incorporar los avances de la evolución tecnológica y el entorno regulatorio mundial para adoptar una normatividad que permita incrementar la seguridad de las redes; garantizar que se proporcione al usuario información completa de los contenidos; y proteger la propiedad intelectual.
- Promover la investigación en las áreas de interoperabilidad de bases de datos y de técnicas para proteger la seguridad de la información contenida en redes.

Redes para el sector público

- Desarrollar la infraestructura de telecomunicaciones requerida por el sector público a nivel federal, estatal y municipal, para atender las necesidades de intercambio de información entre organizaciones, de transmisión de información de carácter público, así como la prestación de servicios a la ciudadanía.
- Promover y motivar el desarrollo e introducción de nuevas aplicaciones en servicios de información.

Redes académicas

- Apoyar el fortalecimiento y desarrollo de redes académicas que permitan extender a las instituciones educativas de todo el país el acceso a servicios de información.

Analizar la opción que representan las redes académicas para cubrir las necesidades de otros sectores, en tanto se avanza en el desarrollo de la infraestructura pública requerida.

Metas prioritarias

Para el año 2000:

- Contar con una infraestructura de redes digitales de telecomunicaciones de alta velocidad.

Meta inicial: En el segundo semestre de 1996, definir los términos de referencia para el desarrollo de la infraestructura de telecomunicaciones requerida por la red del sector público, así como para el fortalecimiento de las redes académicas.

- Contar con la normalización que permita la adecuada operación e interconexión de las redes de datos a nivel tanto nacional como internacional.

Meta inicial: En el primer semestre de 1997, realizar los estudios para el establecimiento de normas, estándares y medidas de seguridad.

DESARROLLO INFORMÁTICO A NIVEL INTERNACIONAL,

Las estadísticas realizadas por Texas Internet Consulting y The Matrix (Computer Networks and Conferencing Systems Worldwide) han revelado que hay 27 millones de personas en todo el mundo con capacidad para enviar correo electrónico a cualquier otro usuario dentro de Internet[11]. Dentro de estos 27 millones se incluyen a 7.8 millones de personas que proveen servicios de Internet con 2.5 millones de computadoras, y a 13.5 millones de personas que son consumidores potenciales, es decir, que pueden utilizar servicios como WWW. Estas estadísticas también revelan que el crecimiento de Internet ha sido exponencial en estos últimos seis años y que continúa con tal tendencia, duplicándose año con año la cantidad de gente conectada. También se muestra que el servicio más utilizado en la actualidad es WWW, que en este año ha sobrepasado en cantidad de bytes y de paquetes al tradicional FTP. Otro dato que es de notar es que la edad del 30% de los usuarios de Internet fluctúa entre los 18 y los 30 años, lo cual muestra una población joven, mayoritariamente masculina (la proporción entre hombres y mujeres en la Red es de 2 a 1).

[11] Cifras consideradas hasta Diciembre de 1994.

CAPÍTULO

2

NIVELES DE SEGURIDAD

CAPITULO 2: ANÁLISIS DE LOS NIVELES DE SEGURIDAD

Niveles

Según los estándares de seguridad en computadoras desarrollado por el Departamento de Defensa de los Estados Unidos, el criterio estándar más confiable para la evaluación de computadoras[12], maneja varios niveles de seguridad para proteger de un ataque al hardware, software y a la información almacenada.

Los niveles que a continuación se presentarán describen:

- Los diferentes tipos de seguridad física.
- La autenticación de usuarios.
- La confiabilidad del software tanto del sistema operativo como de las aplicaciones del usuario.
- También estos estándares imponen algunos límites en los diferentes tipos de sistemas que se podrían tener conectados al sistema.

2.1. Nivel D1.

Este nivel es la forma más elemental de seguridad disponible. Este estándar parte de la base que todo el sistema no es confiable. No hay protección disponible para el hardware; el sistema operativo se compromete con facilidad, y no hay autenticación con respecto a los usuarios y sus derechos para tener acceso a la información que se encuentra en la computadora. Este nivel de seguridad se refiere por lo general a los sistemas operativos como MS-DOS, MS-Windows y System 7.X de Apple Macintosh; ya que estos sistemas operativos no distinguen entre usuarios y carecen de un sistema definido para determinar quién trabaja en el teclado. Tampoco tienen control sobre la información que puede introducirse en los discos duros.

[12] De acuerdo al libro naranja de estándares emitido por el Departamento de Defensa de los Estados Unidos.

2.2. Nivel C.

El nivel C tiene dos subniveles de seguridad: C1 y C2.

Nivel C1.

El *nivel* C1, o ***sistema de protección de seguridad discrecional***, describe la seguridad disponible en un sistema típico Unix. Existe algún nivel de protección para el hardware, puesto que no puede comprometerse tan fácil, aunque todavía es posible. Los usuarios deberán identificarse a sí mismos con el sistema por medio de un nombre de registro de usuario y una contraseña. Esta combinación se utiliza para determinar qué derechos de acceso a los programas e información tiene cada usuario.

Estos derechos de usuarios son permisos para archivos y directorios. Estos *controles de acceso discrecional* habilitan al dueño del archivo o directorio, o al administrador del sistema, a evitar que algunas personas tengan acceso a los programas e información de otras personas. Sin embargo, la cuenta de la administración del sistema no está restringida a realizar cualquier actividad. En consecuencia, un administrador de sistema sin escrúpulos puede comprometer con facilidad la seguridad del sistema sin que nadie se entere.

Además, varias de las tareas cotidianas de administración del sistema sólo pueden realizarse al registrarse el usuario conocido como raíz. Con la centralización de los sistemas de computadoras de ahora, no es raro entrar a una organización y encontrar a dos o tres personas que saben la contraseña raíz; lo cual constituye un gran problema, ya que de esta forma no se pueden distinguir los errores que hizo uno u otro empleado determinado día.

Nivel C2.

Este segundo subnivel, fue diseñado para **ayudar a solucionar los problemas presentados en el subnivel anterior**, ya que junto con las características del nivel C1, el nivel C2 incluye características de seguridad adicional que crean un medio de acceso controlado. Este medio es la capacidad de reforzar las restricciones a los usuarios en su ejecución de algunos comandos o el acceso a algunos archivos basados no sólo en permisos, sino en niveles de autorización. Además, este nivel de seguridad requiere auditorías del

sistema, lo que incluye la creación de un registro de auditoría para cada evento que ocurre en el sistema.

La auditoría se utiliza para mantener los registros de todos los eventos relacionados con la seguridad, como las actividades practicadas por el administrador del sistema. La desventaja de la auditoria es que requiere un procesador adicional y recursos de disco del subsistema.

Con el uso de autorizaciones adicionales, es posible que los usuarios de un sistema C2 tengan la autorización para realizar tareas de manejo de sistema sin necesidad de una contraseña raíz; lo que mejorará el rastreo de las tareas relativas a la administración, ya que cada usuario realiza el trabajo en lugar del administrador del sistema. Estas autorizaciones específicas permiten al usuario ejecutar comandos específicos o tener acceso a las tablas de acceso restringido.

2.3. Nivel B.

Nivel B1.

Este nivel B de seguridad tiene tres niveles. El B1, o ***protección de seguridad etiquetada***, es el primer nivel que soporta seguridad de multinivel, como la secreta y la ultrasecreta. Este nivel parte del principio de que un objeto bajo de control de acceso obligatorio no puede aceptar cambios en los permisos hechos por el dueño del archivo.

Nivel B2.

Este nivel es conocido como ***protección estructurada***, requiere que se etiquete cada objeto. Los dispositivos como discos duros, cintas o terminales podrán tener asignado un nivel sencillo o múltiple de seguridad. Este es el primer nivel que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior.

Nivel B3.

Este nivel es conocido como ***nivel de dominios de seguridad***, ya que refuerza a los dominios con la instalación de hardware. Por ejemplo, el hardware de administración de memoria se usa para proteger el dominio de seguridad de un acceso no autorizado o la modificación de objetos en diferentes dominios de seguridad. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una ruta de acceso segura.

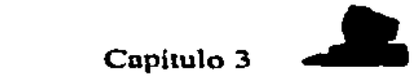
2.4. Nivel A.

Este ***nivel de diseño verificado***, es hasta ahora el nivel más elevado de seguridad. Incluye un proceso exhaustivo de diseño, control y verificación. Para lograr este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse; el diseño requiere ser verificado en forma matemática; además, es necesario realizar un análisis de los canales encubiertos y de la distribución confiable. *Distribución confiable* significa que el hardware y el software han estado protegidos durante su expedición para evitar violaciones a los sistemas de seguridad.

CAPÍTULO

3

SEGURIDAD



CAPITULO 3. SEGURIDAD.

Uno de los cambios más sorprendentes del mundo de hoy es la rapidez de las comunicaciones. Modernos sistemas permiten que el flujo de conocimientos sea independiente del lugar físico en que nos encontremos. Ya no nos sorprende la transferencia de información en tiempo real o instantáneo. Se dice que el conocimiento es poder; para adquirirlo, las empresas se han unido en grandes redes internacionales para transferir datos, sonidos e imágenes, y realizan el comercio en forma electrónica, para ser más eficientes. Pero al unirse en forma pública, se han vuelto vulnerables, pues cada sistema de computadores involucrado en la red es un blanco potencial y apetecible para obtener información.

El escenario electrónico actual es que las organizaciones están uniendo sus redes internas a la Internet, la que crece a razón de más de un 10% mensual. Al unir una red a la Internet se tiene acceso a las redes de otras organizaciones también unidas. De la misma forma en que accesamos la oficina del frente de nuestra empresa, podemos recibir información de un servidor en Australia, conectarnos a un supercomputador en Washington o revisar la literatura disponible desde Alemania. Del universo de varias decenas de millones de computadores interconectados, no es difícil pensar que puede haber más de una persona con perversas intenciones respecto de nuestra organización. Por eso, debemos tener nuestra red protegida adecuadamente.

Cada vez es más frecuente encontrar noticias referentes a que redes de importantes organizaciones han sido violadas por criminales informáticos desconocidos. A pesar de que la prensa ha publicado que tales intrusiones son solamente obra de adolescentes con propósitos de entretenerse o de jugar, ya no se trata de un incidente aislado de una desafortunada institución. A diario se reciben reportes los ataques a redes informáticas, los que se han vuelto cada vez más siniestros: los archivos son alterados subrepticiamente, los computadores se vuelven inoperativos, se ha copiado información confidencial sin autorización, se ha reemplazado el software para agregar "puertas traseras" de entrada, y miles de contraseñas han sido capturadas a usuarios inocentes.

Los administradores de sistemas gastan horas y a veces días enteros volviendo a cargar o reconfigurando sistemas comprometidos, con el objeto de recuperar la confianza en la integridad del sistema. No hay forma de saber los motivos que tuvo el intruso, y debe suponerse que sus intenciones son lo peor. Aquella gente que irrumpe en los sistemas sin autorización, aunque sea solamente para ver su estructura, causa mucho daño, incluso sin que hubieran leído la correspondencia confidencial y sin borrar ningún archivo. De acuerdo a un estudio de la firma Ernst and Young abarcando más de mil empresas, un 20% reporta pérdidas financieras como consecuencia de intrusiones en sus computadores (Technology Review, April 95, pg.33). Ya pasaron los tiempos en que la seguridad de los computadores era sólo un juego o diversión, por tal razón hay que saber quienes y como trabajan estos infractores, para poder tener una seguridad confiable.

El problema de la seguridad en Internet se centra, en dos aspectos: la protección de los sistemas locales frente a instrucciones extrañas y la seguridad del intercambio de datos.

3.1. Vándalos y contraseñas.

El término *hacker* (destructor) denotaba a alguien que era persistente, que trataba de romper cosas y averiguar cómo funcionaban. Como resultado de esta depuración, y debido a que la mayoría de la gente que hacía destrozos eran sabios de la ciencia de la computación, el término hacker desarrollo una connotación negativa (*vándalos*). Es peligroso pensar que el estereotipo de los "hackers" o quienes violan la seguridad de los sistemas computacionales son sólo brillantes estudiantes o graduados en Ciencias de la Computación, sentados en sus laboratorios en un lugar remoto del mundo. A pesar de que tales "hackers" existen, la mayoría de las violaciones a la seguridad son hechas desde dentro de las propias organizaciones.

Hay quienes diferencian entre **"hackers"** y **"crackers"**: los primeros son expertos en computación que hurgan en los sistemas, pero cuyo código de ética no los lleva a hacer daño, salvo para borrar sus huellas. Los crackers, en cambio, tratan de entrar a los sistemas a toda costa, para ganar prestigio y demostrar que el ataque es factible; o con fines económicos, dañando generalmente la información almacenada.

Cualquiera que sea la motivación, se pueden caracterizar en las siguientes categorías:

Personas dentro de una organización:

- Autorizadas para ingresar al sistema. (Ejemplo: Miembros legítimos de la empresa que acceden a cuentas corrientes o al departamento de personal)
- No están autorizadas para ingresar al sistema. (Ejemplo: Personal contratista o de aseo)

Personas fuera de la organización:

- Autorizadas para ingresar al sistema (Ejemplo: Soporte remoto de organizaciones de mantenimiento de software y equipos).
- No están autorizadas para ingresar al sistema. (Ejemplo: Usuarios Internet o de acceso remoto, sin relación con la institución)

Técnicas comunes de los Hackers

No sólo las redes conectadas a Internet son vulnerables a los ataques de los hackers.

El método más común de acceder ilegalmente a un sistema es a través de un terminal de la propia red de la organización. Cualquier persona con acceso físico a un terminal tiene la oportunidad de ingresar.

En caso de acceso remoto, por teléfono, también es posible de ingresar al sistema, aún sin conexión a Internet. Existen varios programas computacionales dedicados, telefónicos automáticos e interactivo, con los cuales se puede identificar el número de teléfono conectado a un módem, si se le da un rango de números a probar. Normalmente, dicho número es parecido al de la empresa en cuestión.

Una vez que se tiene acceso a la organización será necesario obtener una combinación válida de nombre de usuario y contraseña. Los hackers pueden intentar un ataque manual o automático para averiguar contraseñas válidas, mediante programas sencillos disponibles en Internet. Muchos sistemas guardan sus cuentas de usuario y los

passwords o contraseñas correspondientes en un archivo especial protegido por encriptación. Si un hacker accede a dicho archivo puede descifrarlo con un programa como el "Crack", en el caso de sistemas UNIX, el cual compara las palabras del diccionario, encriptadas, con el contenido de dicho archivo, hasta encontrar coincidencias.

Un hacker también puede instalar en una estación del sistema, un pequeño programa que captura la secuencia de teclas digitadas. Es el denominado Caballo de Troya, y actúa solapadamente capturando y guardando en un archivo todo lo que se digita después de ciertas palabras clave (como "login", "username", "nombre" o "password" por ejemplo). Posteriormente, el hacker revisa desde un lugar remoto el contenido del archivo que obtuvo. Esta técnica es relativamente simple, y generalmente difícil de detectar.

En el caso de redes conectadas a la Internet, los hackers pueden alterar su identidad, haciendo creer a la máquina que da acceso a una determinada institución que son computadoras "autorizadas" a ingresar o confiables (Address Spoofing).

Hay que aclarar que no todos los intentos para ingresar a un sistema son dañinos. Sin embargo, en la mayoría de los casos deberían ser tratados como si lo fueran. Sin importar las razones que hay detrás del ataque, la pieza de información más codiciada por un vándalo es el archivo /etc/passwd. Cuando el vándalo tiene una lista de nombres de cuentas de usuarios que es válida, resulta trivial crear un programa para simplemente adivinar las contraseñas. Sin embargo, muchos programas de registro modernos incluyen una demora de tiempo entre los indicadores de registro que se alargan más con cada intento frustrado. Podrán incluir también un código de programa para inhabilitar el puerto de acceso en caso de registrarse demasiados intentos fracasados.

La principal protección es utilizar /etc/shadow o la base de datos de contraseña protegida, ya que estos archivos o directorios requieren de acceso raíz para poder ser observados. Esto dificulta al vándalo obtener la información de la contraseña encriptada. Sin embargo, hay que recordar que la información de contraseña en /etc/passwd está encriptada.

Algunas formas de ataque:

Packet Sniffers

En la Internet se pueden encontrar una amplia variedad de herramientas para monitorear y analizar redes, llamadas "packet sniffers", las que actúan revisando los paquetes de información electrónica que transitan por una determinada red. Como generalmente dichos paquetes de una red no están encriptados, bastará revisar dicha información, especialmente entre las 8 y 9 AM para conocer nombres de usuarios y sus passwords.

Address Spoofing

En el caso de redes conectadas a la Internet, los hackers pueden alterar su identidad, haciendo creer al computador que da acceso a una determinada institución que son computadores "autorizados" a ingresar o confiables (Address Spoofing). Existen numerosos procedimientos, pero describirlos más ampliamente va más allá de objetivo de ilustrar del presente artículo.

LOS PHREAKERS

Estos son especialistas en telefonía, a quienes se les puede llamar ***crackers*** de los teléfonos. Sobre todo emplean sus conocimientos para poder utilizar las telecomunicaciones gratuitamente. También son perseguidos por la justicia y por las compañías telefónicas.

3.2. Encriptamiento como protección de la red.

La encriptación es, tomar una información que existe de manera legible y convertirla a tal forma que otras personas no puedan leerla ni entenderla. Por tal razón, muchos prefieren encriptar la información para brindar un nivel más alto de seguridad para el sistema y los datos, además resulta de gran interés tanto para los usuarios como para los administradores del sistema. Sin embargo hasta los datos encriptados pueden estar en riesgo sin la supervisión adecuada y el entrenamiento para los usuarios que quieran utilizar estos recursos, para explicar este subcapítulo se tomará como ejemplo el funcionamiento del sistema Unix.

3.2.1. Como encriptar las contraseñas.

Ocasionalmente, las contraseñas se guardaban en formato texto simple, y sólo el administrador y el software del sistema tenían acceso al archivo; pero esto traía varios problemas al editar el archivo de contraseña (/etc/passwds); para lo cual, generalmente se creaba un archivo temporal, el cual era el que se editaba en realidad. De tal forma, el archivo lo podían leer todos, ya que facilitaba las contraseñas para todas las cuentas.

Como resultado de lo anterior, se desarrolló un método de encriptación de contraseña que utilizaba un algoritmo de encriptación de una vía. De tal forma que los valores de encriptación se guardaban en lugar del texto.

Cuando un usuario se registra en un sistema Unix, el programa Getty pide al usuario su nombre de usuario y luego ejecuta el programa de registro. El programa de registro indica la contraseña pero no lo desencripta. En realidad, el programa encripta la contraseña y luego compara el valor encriptado reciente con el que está guardado en/etc/password. Si coinciden, entonces se considera que el usuario proporcionó el valor correcto. Este método de encriptado de contraseñas se introduce por medio de un mecanismo de kernel nombrado *crypt(3)*

El valor de la contraseña real guardado en /etc/passwd es el resultado de emplear la contraseña del usuario para encriptar un grupo de 64 bits de ceros al utilizar la llamada *crypt(3).clear text* es la contraseña del usuario, la cual es la clave para la operación de encriptación. El texto a ser encriptado es de 64 bits de ceros, y el *texto cifrado* resultante es la contraseña encriptada.

El algoritmo crypt(3) se basa en el *estándar de encriptación de datos* (DES) desarrollado por el Instituto Nacional de Estándares y Tecnología o NIST. De acuerdo con este estándar, una clave de 56 bits, como ocho caracteres de siete bits, se utiliza para encriptar el texto original, el cual es llamado texto llano, el cual es por lo general, de 64 bits de largo. Con lo que el texto cifrado resultante no puede desencriptarse con facilidad sin conocer la clave original.

La llamada crypt(3) de Unix utiliza una versión modificada de este método, al establecer que el texto llano se encripta en un grupo de ceros. Este proceso es muy complicado, ya que al tomar el texto cifrado resultante y encriptándolo nuevamente con la contraseña del usuario como clave. **¡Este proceso se realiza 25 veces!** Cuando termina, los 64 bits resultantes se dividen en 11 caracteres y luego se guardan en el archivo de contraseña. Se asegura que no hay un método conocido disponible para traducir el texto cifrado o el valor encriptado de regreso a su texto llano original.

3.2.2. Como encriptar archivos.

Como se pudo observar anteriormente, la encriptación de contraseñas mediante el uso de un mecanismo que es difícil de desencriptar, ofrece un método relativamente seguro para evitar que usuarios no autorizados tengan acceso al sistema. Además lo usuarios pueden evitar que personas no autorizadas accesen al sistema; lo anterior puede lograrse por medio del comando crypt(1). Sin embargo, éste no es un método de encriptación muy seguro; ya que, por ejemplo: Unix soporta la manipulación directa de estos archivos encriptados sin tener que desencriptarlos primero.

Si no se proporcionan argumentos en la línea de comando, entonces crypt indica la llave, lee los datos a encriptar de una entrada estándar e imprime la información encriptada en la salida estándar. La clave de encriptación utilizada es el factor principal para que la contraseña no sea descubierta, ya que mientras más larga es esta contraseña, los patrones de encriptación se toman más complejos.

Como la clave de crypt podría ser vista por curiosos que utilizan ps, crypt destruye cualquier rastro de la llave real después de hacer la entrada.

El mecanismo de encriptación no es inquebrantable y, con tiempo suficiente, puede ser averiguado. Un método para aumentar las oportunidades de proteger los datos es comprimir el archivo antes de encriptarlo.

3.2.3. Integridad de la información.

Cuando se envía un archivo a la red, hay una forma de verificar que el archivo no ha sido alterado; a lo cual se le llama integridad de la información, y se refiere al proceso que verifica que la información enviada esté completa y sin cambios desde la última vez que se verificó.

Si la información es enviada en forma electrónica por la red, una manera de asegurarse de que no ha sido modificada es utilizar ***sumas de verificación***. Cualquier modo de encriptación también ofrece integridad de la información, ya que un interceptor primero tiene que desencriptar el mensaje antes de modificarlo.

SUMAS DE VERIFICACIÓN

Las sumas de verificación (checksums) son un mecanismo muy simple y efectivo para la integridad de un archivo. Un procedimiento simple de suma de verificación puede utilizarse para calcular el valor de un archivo y después compararlo con su valor previo. Si las sumas de verificación se igualan, el archivo no ha sufrido cambios. Si las sumas no se igualan, el archivo habrá sido alterado. Muchas utilerías de comprensión y descomprensión que pueden emplearse para conservar espacios de disco y reducir los costos de transmisión de archivos, provocan que las sumas verifiquen sus algoritmos de comprensión-descomprensión.

Las sumas de verificación aritmética son fáciles de implantar. Están formadas al añadir elementos de archivo de 16 o 32 bits para llegar al número de las sumas de verificación. A pesar de que son fáciles de implantar, las sumas de verificación aritmética son débiles desde un punto de vista de seguridad, ya que un atacante puede modificar y añadir datos al archivo para que la suma de verificación aritmética se iguale al valor correcto.

La **CRC** (suma de verificación de redundancia cíclica), también se conoce como suma de ***verificación polinomial***, y es más segura que la aritmética. Su implantación es bastante simple; sin embargo al igual que la suma de verificación aritmética, podrá estar comprometida por un interceptor.

Pero aún mejor, las sumas de ***verificación criptográfica*** **(criptosellado)**. presenta mejoras sobre las de tipo aritmético y CRC, ya que los datos se dividen en grupos más pequeños y se calcula la suma de verificación CRC para cada grupo de datos. De tal forma que las CRC de todos los grupos de datos se mezclan.

Este método dificulta la alteración de los datos, ya que el interceptor no conoce el tamaño de los grupos de datos que se utilizaron. El tamaño de los grupos de datos es variable y puede calcularse mediante el uso de técnicas seudo aleatorias, que dificultan aún más, que el interceptor pueda alterar los datos.

Otro método, llamado ***código de detección de manipulación*** (MDC) o función desmenuzadora de una vía, puede utilizarse para detectar modificaciones a un archivo. Esta función se llama así porque dos entradas no pueden producir el mismo valor. Los datos en el archivo se emplean como la entrada a la función desmenuzadora de una vía para producir un valor desmenuzado. Si los datos en el archivo se modifican, tendrán un valor desmenuzado distinto. Las funciones desmenuzadoras[13] de una vía pueden implantarse con bastante eficacia y hacen posible las verificaciones irrompibles de integridad.

3.3. Virus.

Desde que surgieron por primera vez, los virus han sido una amenaza continua para el software y la información, que tanto pequeños usuarios como grandes empresas, almacenan tanto en discos duros como en flexibles. Son creados, en su mayoría, por personas que desean demostrar sus conocimientos de informática, aunque por razones obvias, suelen mantener el anonimato.

Existen virus realmente simples y totalmente inofensivos, cuya única misión o efecto es visualizar un mensaje en la pantalla del usuario en determinadas circunstancias. O mucho más complejos, capaces de atacar de forma devastadora las partes más débiles e importantes de una computadora, ocultando su existencia de forma magistral, lo que hace que sea realmente necesario protegerse lo mejor posible de ellos.

[13] Para mayor información de la función desmenuzadora de una vía, ver los RFC's 1319 y 1321.

En la actualidad, hay programas con los que cualquier usuario, sin tener ningún tipo de conocimientos de programación, puede crear su propio o propios virus, dándoles el nombre y características que desee. E incluso existen determinados Web que ofrecen esta posibilidad. Estas nuevas tecnologías facilitan la creación de una gran variedad de epidemias informáticas, por parte de programadores, inclusive novatos.

DEFINICIÓN

Un virus informático es un programa de computadora, generalmente anónimo, que lleva a cabo acciones que casi siempre resultan nocivas para el sistema informático y cuyo funcionamiento se define por ser capaz de generar copias de sí mismo de forma homogénea en un archivo distinto al que ocupa. Un virus informático modifica los programas ejecutables a los que contamina consiguiendo con esto una ejecución parasitaria, es decir, se activa de forma involuntaria por el usuario cuando ejecuta el programa contaminado[14].

TIPOS DE VIRUS.

En general hay dos tipos de virus[15]:

Virus de Programa.

Estos afectan ficheros ejecutables (extensiones EXE, COM, SYS, OVL, OVR y otros). Estos virus pueden insertarse al principio o al final del archivo, dejando generalmente intacto el cuerpo del programa que contaminan. Cuando se ejecuta un programa contaminado, el virus toma el control y se instala residente en la memoria. Después pasa el control al programa que lo porta, permitiéndole una ejecución normal. Una vez que finaliza su ejecución, si se intenta ejecutar otro programa no contaminado, el virus ejercerá su función de replicación, insertándose en el nuevo programa que se ejecuta.

[14] Según la empresa ANYWARE, especialista en seguridad en informática.
[15] El enfoque dado a estos tipos generales de virus es de Sistema Operativo.

Virus de Sector de Arranque.

Estos modifican el sector de arranque (partición del DOS del disco duro o de un disquete). Como norma general sustituyen el sector de arranque original por una versión propia para arrancar el sistema, de esta forma, cuando se inicia una sesión de trabajo se ejecuta en primer lugar la versión contaminada de arranque, con lo que consiguen cargarse en memoria y tomar el control del ordenador.

Este tipo de virus sólo se reproduce una vez en cada disco lógico localizándose en zonas muy concretas. Como el tamaño de un sector es pequeño, el virus suele ocupar varios, marcándolos como defectuosos para ocultar su presencia.

Se distinguen tres fases en la actuación de un virus:

1. El Contagio.

El contagio inicial o los contagios posteriores se realizan cuando el programa contaminado está en la memoria para su ejecución. Las vías por las que puede producirse la infección del sistema son disquetes, redes de computación o cualquier otro medio de transmisión de información. Los disquetes son por el momento, el medio de contagio más extendido en nuestro país. Estos disquetes contaminantes suelen contener programas de fácil y libre circulación y carecen de toda garantía. Este es el caso de los programas de dominio público, las copias ilegales de los programas comerciales, juegos, etc.

2. El Virus Activo.

Cuando se dice que un virus se activa significa que el virus toma el control del sistema, y a la vez que deja de funcionar normalmente a los programas que se ejecutan, realiza actividades no deseadas que pueden causar daños a los datos o a los programas.

Lo primero que suele hacer un virus es cargarse en la memoria de la computadora y modificar determinadas variables del sistema que le permiten "hacerse un hueco" e impedir que otro programa lo utilice. A esto se le conoce como "quedarse residente", con lo que queda en espera a que se den ciertas condiciones, que varían de unos virus a otros, para replicarse o atacar.

3. El Ataque.

Mientras que se van copiando en otros programas, los virus comprueban si determinada condición se ha cumplido para atacar, por ejemplo que sea 5 de enero en el caso del conocido virus Barrotes. Es importante tener en cuenta que los virus son diseñados con la intención de no ser descubiertos por el usuario y generalmente, sin programas antivirus, no son descubiertos hasta que la tercera fase del ciclo de funcionamiento del virus produce el daño con la consiguiente pérdida de información.

ACTIVACIÓN DE LOS VIRUS

Es común, que los virus se activen en una época o día determinado, como son:

Agosto

Got you: 1-31	Highlander: 29	Ital Boy: 1-31
Jerusalen (Skism): 22-29	Leprosy:10	Tormentor-Lixo-Nuke: 31,etc

Septiembre

Beware:1	Cascade: 1-31	Frogs: 5
Jerusalem June 17: 1-30	Rocko: 13,14	Violator B1: 4, etc.

Octubre

Beware: 1	Cascade: 1-31	Frodo: 1-31
Ital Boy: 1-31	Monxia: 13	Violator-C:1-31,etc.

Noviembre

AntiCad1: 1-30	Day 10: 10,20,30	Highlander: 29
Kennedy (Tiny): 22	Pinworm: 1	VCL-Miles: 3, etc.

Diciembre

Arale: 12	Chaos (Faust)	Keybug 1720:13
Nov 17th-880:1-31	TenBytes: 1-31	Witcode:24-31,etc.

No obstante, existen otro tipo de virus que no funcionan de esta forma, sino de manera aleatoria, siendo su activación independiente de la fecha del sistema, como son:

AntiCMOS	**AntiEXE**
Barrotes	**Coruña**
Doom II	**Elaine**
Flip	**Form**
Holocausto	**Junkie**
Maltese Amoeba	**Manuel**
Monkey	**Natas**
Pirate	**Quicky**
Ripper	**Stoned**
Viernes 13	

Casi seguido de la aparición de los anteriores virus se crean los antivirus que los eliminarán, ya que sea a nivel PC o en entorno de RED, y la actualización de los mismos se puede encontrar en el BBS.

3.4. COMO PROTEGER UNA RED

Existen numerosas técnicas para proteger la integridad de los sistemas. Lo primero que debemos hacer es diseñar una política de seguridad. En ella, definir quienes tienen acceso a las diferentes partes de la red, poner protecciones con contraseñas adecuadas a todas las cuentas, y preocuparse de hacerlas cambiar periódicamente (Evitar las passwords "por defecto" o demasiado obvias).

Además, se deben instalar protecciones adicionales como un buen Firewall o cortafuegos.

3.4.1. FIREWALLS (cortafuegos)

Cortafuegos es el término que se emplea para referirse a una franja de bosque que se limpia de árboles, vegetación y cualquier materia inflamable, con el fin de crear una barrera que el fuego de un posible incendio no sea capaz de atravesar.

La misión fundamental de los Firewalls o cortafuegos es proveer seguridad (se encargan de aislar la información privada de la pública), e impedir que usuarios no autorizados accedan a la información reservada de una organización. Al mismo tiempo, deben permitir transferir archivos y accesar la Internet junto con todas la funciones que se requieran de ella, como enviar y recibir correo electrónico, ver imágenes o escuchar audio, pero en forma segura y controlada. Cada aplicación constituye un desafío a la seguridad, y debe ser enfrentado eficientemente por un Firewall.

1) Se elige una máquina con capacidad de encaminar la información (por ejemplo, una PC con Linux).
2) Se le agregan dos interfaces (por ejemplo, interfaces serie, o ethernet, o de paso de testigo en anillo (Token Ring), etc.).
3) Se le deshabilita el reenvío de paquetes IP (IP forwading).
4) Se conecta una interfaz a la Internet.
5) Se conecta la otra interfaz a la red que se quiere proteger.

Con los pasos anteriores se tendrá como resultado, dos redes distintas que comparten una computadora, dicha computadora cortafuegos, puede comunicarse tanto con la red protegida como con la Internet. La red protegida no puede comunicarse con la Internet, y la Internet no puede comunicarse con la red protegida, debido a que se ha deshabilitado el reenvío IP en el único ordenador que las conecta.

Si se quisiera llegar a la Internet desde la red protegida, se tendría primero que hacer un telnet (conexión) al cortafuegos, y acceder a la Internet desde él. De la misma forma, para acceder a la red protegida desde la Internet, se debe pasar antes por el cortafuegos.

Este es un muy buen mecanismo de seguridad contra ataques desde la Internet; ya que si alguien quisiera atacar a la red protegida, primero tendría que atravesar el cortafuegos, debido a que éstos, actúan como un escudo o barrera entre la red interna y el exterior, además de proveer un nivel de seguridad más allá de la protección por contraseñas o passwords. De esta manera el ataque se divide en dos pasos, y , por lo tanto, se dificulta más la intromisión.

Comparación de algunas marcas Comerciales de Firewalls

La revista InfoWorld, Nov.11, 1996 (Vol 18, Iss. 46) publica una comparación entre los firewalls más populares, destacando a BorderWare Firewall Server como el de mejor puntaje en los test efectuados.

BorderWare es un Firewall basado en software que se destaca de sus competidores porque está basado en un sistema operativo fortalecido.

El servidor **"Firewall de BorderWare"**, de la empresa Secure Computing, distribuido en Chile por CyberCenter S.A. es una poderosa herramienta y sistema de "cortafuegos" que incorpora un alto nivel de seguridad a las redes TCP/IP conectadas a Internet, evitando los accesos indebidos a la red del usuario como también controla los accesos hacia la Internet desde el interior de la red cliente.

El Firewall de BorderWare permite efectuar traducciones de Direcciones de Red, de modo de que todo el tráfico cursado hacia Internet, aparece originado por una única dirección IP, lo cual mantiene oculto las verdaderas direcciones IP internas. Por otra parte, BorderWare permite controlar el acceso de los usuarios internos de la red, hacia los servicios que la red externa (Internet) ofrece, controlando por origen/destino, fecha, e incluso hora del día. Los eventos de intromisión a la red son notificados a través de múltiples modalidades de alarmas (reporte impreso, e-mail, detención del sistema, entre otras.) También están disponibles un conjunto de herramientas de diagnósticos de la actividad del sistema y detalle de los eventos ocurridos entre el Firewall y la Internet.

Hay diferentes técnicas usadas por los fabricantes de Firewalls para proteger un sistema. Entre ellas, están los filtros de paquetes, los proxies, application gateways y algunas más específicas como Type Enforcement, entre otras.

Los **Filtros de Paquetes** constituyen una tecnología más antigua, incorporada en algunos routers o ruteadores de información, ver Figura 2. Es un mecanismo que provee un nivel básico de seguridad a la red. Mediante tablas complejas se configuran para indicar cuales protocolos de comunicación son permitidos de entrar o salir de una red. Por ejemplo, prohibir accesos externos de aplicaciones peligrosas como telnet, o restringir ciertas direcciones IP. Muchos firewalls tienen la funcionalidad de filtro de paquetes, pero los buenos confían en otras tecnologías para mejorar el filtraje, ya que no es suficiente la protección que brindan. Las tareas del router y del cortafuegos (firewalls) las puede desempeñar un solo ordenador. En la práctica, sin embargo, suelen estar repartidas entre dos computadoras, ya que un router o cortafuegos por separado resultan más económicos y no tiene tanto riesgo de averías.

Los servidores locales representan el mundo exterior para las aplicaciones dentro de la LAN. Son ellos quienes recogen las consultas, las traducen y las ponen en el servidor de Internet al que iban destinadas. La respuesta se transmite a la aplicación y el usuario no nota que entre su aplicación e Internet hay instalado un muro de protección.

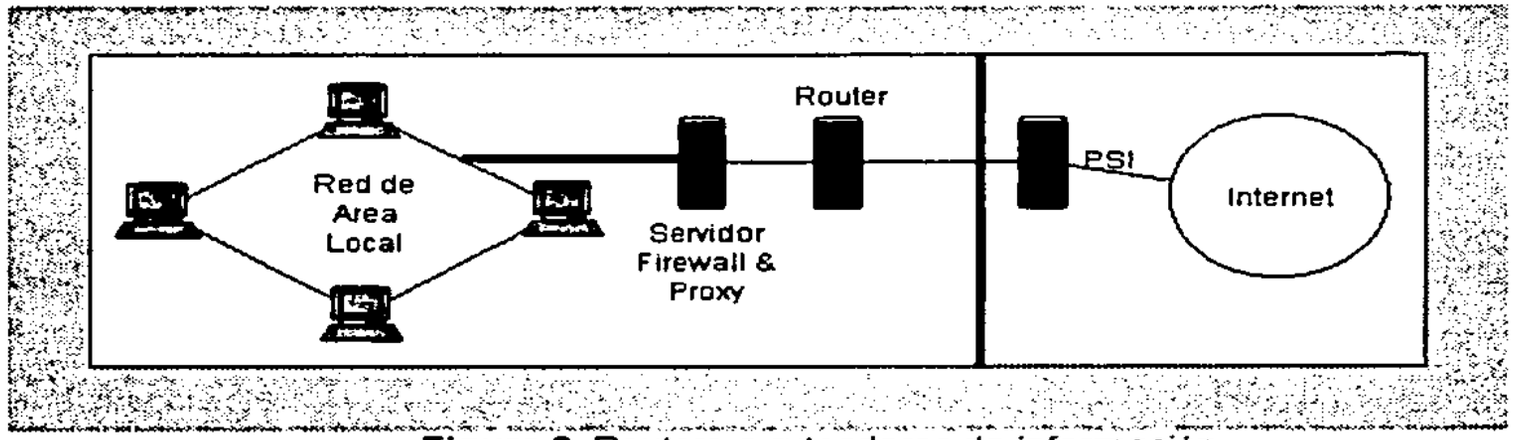


Figura 2. Routers o ruteadores de información.

Los **Proxies** son ciertos software o programas que permiten a los Firewall actuar por cuenta de otro computador al efectuar una comunicación. Por ejemplo, si un usuario de una red interna, confiable, trata de contactar a otro de una red externa, no confiable, será el proxy del Firewall quien haga dicha conexión por cuenta del computador interno, ver Figura 3. La seguridad es esta habilidad de hacer de escudo entre las máquinas internas de las externas. Para la máquina externa, le parecerá que es el Firewall con quien está conectado, no la máquina interna. Algunas marcas comerciales de firewalls proveen proxies transparentes, lo que significa que no es necesario configurar cada aplicación en forma especial, sino que el Firewall se encarga de ello.

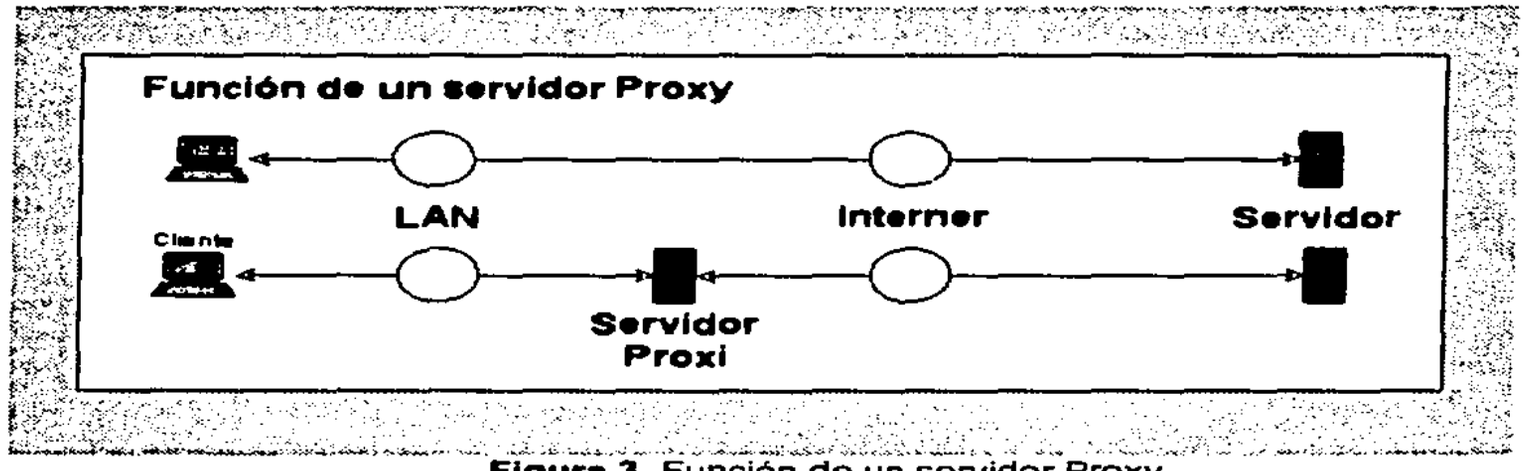


Figura 3. Función de un servidor Proxy

Debido a que los números de red internos no son accesibles desde fuera, se pueden asignar números completamente diferentes de los oficiales. En teoría, una regulación bien establecida de los cortafuegos sólo precisa números IP oficiales: uno para el servidor y otro para el router, independientemente del tamaño de la LAN que se esconda detrás.

Desventajas

- Para cada servicio a utilizar debe haber un servidor proxy, por lo que no se pueden aprovechar al cien por ciento todas las posibilidades de Internet.
- Para que la seguridad sea completa, la configuración del ordenador cortafuegos debe ser absolutamente segura. Una instalación correcta del

cortafuegos es costosa. No existen soluciones estándar y, por lo tanto, ningún cortafuegos seguro a bajo precio.

Un "**Application Gateway**" es un componente clave de un Firewall robusto. Todos los sitios Internet reciben y procesan información proveniente de otras partes de la Internet. Por ejemplo, es deseable recibir correo electrónico desde cualquier parte, y permitir que cualquiera lea la información del servidor Web. Pero desde el punto de vista de la seguridad, es peligroso permitir el acceso a máquinas internas que manejan esos servicios usando esos protocolos. Las aplicaciones tales como el correo electrónico, grupos de noticias, servidores Web, etc., se canalizan a través de gateways o puertas, las que han sido diseñadas pensando en la seguridad.

Hay Firewalls que establecen una tercera red, que no es la interna, segura, ni la externa, insegura. Es lo que se denomina una Zona Desmilitarizada o DMZ. Allí se ponen lo servicios como el servidor Web o de correo, los que pueden ser accesados tanto desde el exterior como del interior, pero con distintos privilegios. La seguridad radica en que no se compromete el resto de la red interna, en la eventualidad que se encuentren hoyos de seguridad.

Se instalan en una estación del sistema un pequeño programa que captura la secuencia de teclas digitadas, y actúa solapadamente capturando y guardando en un archivo todo lo que se digita después de ciertas palabras clave (como "login", "username", "nombre" o "password" por ejemplo). Posteriormente, el hacker revisa desde un lugar remoto el contenido del archivo que obtuvo. Esta técnica es relativamente simple, y generalmente nadie nota nada.

3.4.2. HERRAMIENTAS DE SEGURIDAD

CIFRADO Y AUTENTICACIÓN

Si los datos son sensibles, la CRIPTOGRAFÍA es el único mecanismo para asegurar que los paquetes de información enviados a través de Internet no sean interferidos por personas ajenas a la organización; garantizando la confidencialidad de los datos.

De la misma forma, la AUTENTICACIÓN permite verificar el origen de los datos que la organización recibe, firmar los datos enviados desde dentro y confirmar la identidad de los usuarios que acceden a la información privada. Existen varias herramientas para llevar a cabo la autenticación:

Anlpasswd

Es un programa de cambio de passwords que impide que el usuario escoja passwords débiles.

Crack

Es el mejor programa de "rompimiento" de passwords existente. Intenta adivinar los passwords utilizando una serie de reglas configurables.

Cracklib

Es una biblioteca de funciones que pueden utilizarse para impedir que los usuarios elijan passwords que puedan ser adivinados por ***Crack***.

Kerberos

Es un sistema de autenticación para redes físicamente inseguras, basado en el modelo de distribución de llaves presentado por Needham y Schroeder. Permite a los elementos que intervienen en una comunicación identificarse entre sí y al mismo tiempo evitar "espionaje" en la red o ataques de repetición. También proporciona integridad en el flujo de datos (detección de modificaciones) y privacidad, utilizando sistemas criptográficos como DES (Estándar de Encriptación de Datos).

Isu

Permite compartir una cuenta entre un grupo de usuarios basándose en el password del usuario y no en el password de la cuenta. Verifica que la identidad del usuario, el origen de acceso y la hora de conexión sean los especificados para cada usuario.

Npasswd

Es un programa de cambio de passwords que impide que el usuario escoja passwords débiles. Incluye soporte para los mecanismos de envejecimiento de passwords de System V Reléase 3 y NIS (Network Information Service).

Passws+

Contiene los puntos citados en Npasswd, pero con la diferencia de que el rechazo de passwords se basa en un archivo de configuración que permite la utilización de expresiones regulares, comparación con diccionarios o la ejecución de programas externos para examinar el password.

Pidentd

Es una implementación del servidor de identificación de usuario, que permite averiguar la identidad del usuario que esta solicitando un servicio remoto.

Shadow

Es un paquete que permite a cualquier sistema hacer uso de passwords shadow.

S/Key

Es un sistema que implementa passwords descartables par Unix. También incluye generadores de passwords descartables para PC's y Mac's.

Sra

Es un paquete que proporciona autenticación utilizando Secure RPC para FTP y TELNET.

La autenticación y el cifrado permiten la creación de redes privadas virtuales (VPN-Virtual Private Networks), que es la interconexión de redes de una organización o asociación que utilizan Internet como medio de comunicación entre ellas, pero que, al utilizar estos métodos de seguridad, garantizan la confidencialidad de toda la información que por ellas circulan y la veracidad de la identidad de sus usuarios.

TÉCNICAS DE CODIFICACIÓN

Básicamente se darán las diferencias entre codificación **online** y **offline**.

Offline significa que los datos se codifican antes de la transmisión, es decir, se descodifican después de la transmisión, ver Figura 4. El algoritmo de codificación puede ser de cualquier grado de complejidad.

La codificación online se da durante la transmisión, es decir, tanto la codificación como la descodificación se han de producir al tiempo de la transmisión, (como en el protocolo SSL, descrito en el punto 3.5.1.), ver la figura 4.

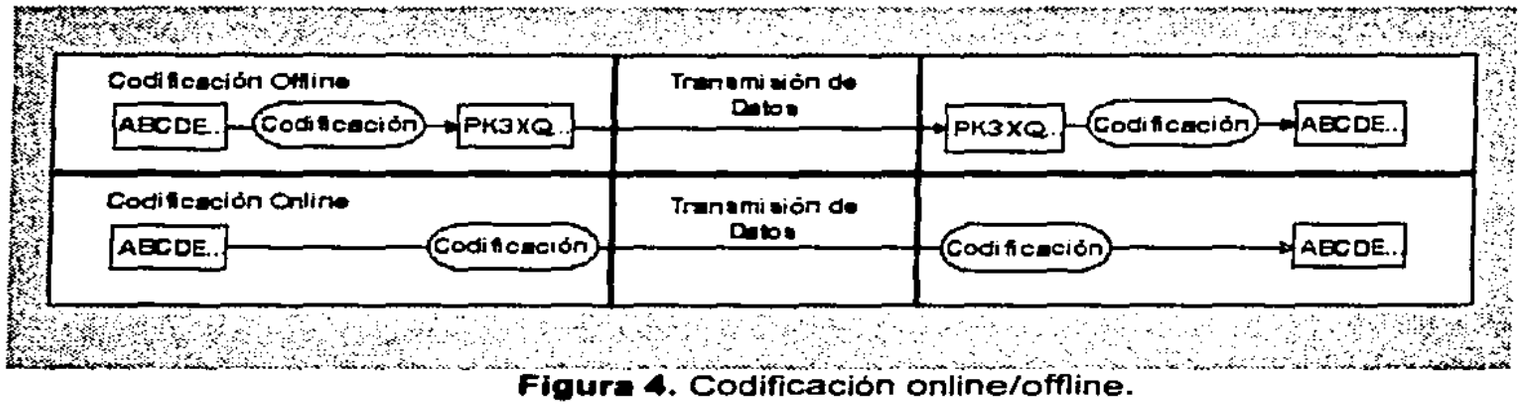


Figura 4. Codificación online/offline.

En los programas de codificación de dominio público, como SSL y PGP, hay una clave que determina el código. Aunque también hay algoritmos de codificación que funcionan sin necesidad de clave (que obviamente no son públicos).

En lo relacionado con aspectos legales, para combatir mejor la criminalidad organizada, en algunos estados es necesario un permiso especial para el uso de algoritmos de codificación y en otros está prohibido; haciendo referencia a los usuarios de Internet, estos quedan sujetos a las disposiciones legales del país desde el cual es miembro de Internet.

3.5. ESQUEMAS DE SEGURIDAD.

3.5.1. SSL (Secure Socket Layer)

El protocolo SSL, este protocolo permite la autenticación de servidores, la codificación de datos y la integridad de los mensajes. SSL está una capa por debajo de los protocolos de aplicación, tales como HTTP, SMTP, Telnet, FTP, Gopher y NNTP, y una capa por encima del protocolo de conexión TCP/IP. Esta estrategia permite a SSL operar independientemente de los protocolos de aplicación de Internet.

Con SSL tanto para el cliente como para el servidor, sus comunicaciones en Internet serán transmitidas en formato encriptado. De esta manera, puede confiar en que la información que envíe llegará de manera privada y no adulterada al servidor que usted especifique (y no a otro).

SSL emplea la tecnología de **autenticación** y **encriptación** desarrollada por RSA Data Security, Inc. Por ejemplo, la implementación de exportación de Netscape Navigator (aprobada por el gobierno de los Estados Unidos) emplea una clave de grado medio de 40 bits para el algoritmo de encriptación de flujo RC4[16]. La encriptación establecida entre usted y el servidor seguirá siendo válida para varias conexiones, aunque el esfuerzo empleado para decodificar un mensaje no puede ser empleado para decodificar el siguiente.

Para decodificar un mensaje encriptado con RC4 de 40 bits, se requeriría una media de 64 años MIPS (una PC con 64 MIPS, o millones de instrucciones por segundo, necesita un

[16] RC4 es un encriptador de flujo de caracteres con una clave de longitud variable, con operaciones orientadas a bytes, diseñado por Rivest para RSA Data Security. El algoritmo está basado en el uso de una permutación aleatoria. Esta diseñado como un drop-in (auto-remplazo).

año de procesamiento para descubrir la codificación del mensaje). La versión de alto grado de 128 bits para los Estados Unidos ofrece una protección exponencialmente mayor. El esfuerzo requerido para decodificar cualquier intercambio de información es una gran barrera contra el fraude. La autenticación de servidor emplea la CRIPTOGRAFÍA de clave pública RSA conjuntamente con los certificados digitales ISO x.509.

SSL consta de dos fases:

1ª Fase.-

El servidor en respuesta a la petición del cliente envía su certificado y sus preferencias de encriptadores; entonces, el cliente genera una llave maestra, la cual, éste encripta con la llave pública del servidor y transmite la llave maestra encriptada a el servidor. El servidor recupera la llave maestra y autentifica él mismo al cliente para poderle enviar un mensaje encriptado con la llave maestra. Subsecuentemente los datos son encriptados con las llaves derivadas de la llave maestra.

2ª Fase (opcional).-

El servidor envía un reto al cliente. El cliente autentifica al servidor para retornar su firma electrónica en el reto, así como también su llave pública certificada. Una variedad de algoritmos de encriptamiento son soportados por SSL. Después del intercambio de llaves se pueden utilizar varios encriptadores para visualizar la información (RC4, DES[17], etc.).

3.5.2. SHTTP (Secure Hyper Text Transfer Protocol).

El protocolo SHTTP, es muy utilizado como método de seguridad de la Word Wide Web. S-HTTP (Secure Hypertext Transfer Protocol) es una extensión del HTTP (Hypertext Transfer Protocol) que provee servicios de seguridad. Originalmente fue desarrollado por Enterprise Integration Technnologies, posteriormente, Terisa Systems

[17] DES es un cifrador de bloque para encripción definido y respaldado por el Gobierno de los EUA en 1977 como estándar oficial. Originalmente fue desarrollado por IBM para ser implementarlo en hardware; es el cifrador más conocido y el que tiene un uso más extenso en todo el mundo. Este algoritmo que es utilizado para comunicación (el emisor y el receptor deben conocer la misma clave secreta, para poder encriptar y desencriptar el mensaje). Puede ser usado para almacenar archivos en un disco duro en forma encriptada. Tiene una longitud de bloque de 64 bits y una llave de 56 bits durante el encriptamiento.

continuó desarrollo de éste. HTTP es el protocolo que forma la base del World Wide Web, permitiendo el intercambio de documentos multimedia en el Web. S-HTTP es diseñado para proveer confidencialidad, autenticidad, integridad y no-repudiación mientras soporta múltiples mocanismos de administración de llaves y algoritmos criptográficos a través de la opción de negociación entre las partes involucradas en cada transacción.

S-HTTP puede usar cualquiera de los cuatro métodos para intercambiar llaves de datos encriptados. Los posibles métodos son RSA[18], out-band, in-band y los Kerberos. Si RSA es usado, las llaves de los datos encriptados son intercambiados por el criptosistema de llave pública RSA. Out-band se refiere a un acuerdo de llaves externo, mientras que in-band se refiere a la llave transportada en un mensaje protegido por S-HTTP en otra sesión. En el método de los Kerberos, la llave es obtenida del servidor de Kerberos.

3.5.3. PGP (Prety Good Privacy).

El PGP, se utiliza generalmente para darle privacidad a los mensajes de correo electrónico; es muy controversial ya que ni siquiera el propio gobierno puede averiguar el código.

PGP contiene algoritmos de encriptación con dos niveles de seguridad, los cuales son:

a) una llave privada secreta y,

b) una llave complementaria pública.

[18] RSA es un criptosistema de llave pública para la encriptación y autentificación; el cual trabaja de la siguiente manera: toma dos números arbitrarios, p y q, para encontrar su producto n = pq; n es llamado "módulo". Escoge un número ,e, menor que n y un número primo relativo a (p-1)(q-1), lo cual significa que e y (p-1)(q-1) no tienen factores comunes excepto 1. Encuentra otro número d, tal que (ed-1) es divisible entre (p-1)(q-1). Los valores e y d son llamados exponentes público y privado respectivamente. La llave pública es el par (n,e); la llave privada es (n,d). Los factores p y q pueden conservarse con la llave privada o destruirse.

3.5.4. S/MIME (Secure /Multi-Purpose Internet Mail Extensions).

S/MIME es una especificación para la seguridad de mensajes electrónicos. En 1995, algunos vendedores de software se reunieron y crearon S/MIME para resolver un importante problema, la intercepción de e-mail. Datos sensiblemente protegidos en una preocupación real, especialmente en un mundo que rápidamente crece en las conexiones de red. La meta de S/MIME es hacer fácil el aseguramiento de los mensajes de aquellos que se dedican a leer correos sin permiso.

S/MIME son las siglas de Secure/Multi-purpose Internet Mail Extensions. Esta especificación fue diseñada para ser fácilmente integrada en productos de e-mail y mensajes. S/MIME construye seguridad en la parte superior del protocolo estándar de la industria de acuerdo a un conjunto de estándares criptográficos (PKCS). El hecho de que S/MIME fue creado utilizando otros estándares es importante para algunas cosas que están siendo implementadas. Por su enfoque S/MIME está siendo utilizado para software EDI, productos en Internet y servicios en línea de comercio electrónico.

3.5.5. ROT13 (Rotate 13).

El ROT13, se utiliza para darle privacidad a los mensajes de los foros o grupos de noticias. Es un sencillo esquema de criptografiado frecuentemente utilizado para mezclar mensajes fijados en los grupos de usuarios de USENET. El ROT-13 hace que un documento permanezca ilegible hasta tanto sea descifrado el texto, y a menudo se utiliza cuando un tema podría ser considerado ofensivo. Muchos lectores de noticias incorporan un comando que desencripta el texto cifrado en ROT-13 y, si lo utiliza, no se deje sorprender por lo que lea. Si uno piensa que podría resultar ofendido será mejor que no se decodifique tales mensajes.

3.5.6. CLIPPER CHIP.

El CLIPPER CHIP, es un método de codificación propuesto para el gobierno de los Estados Unidos que ha causado grandes debates, ya que sólo el gobierno conoce la clave para descodificar la información. Este permitirá que una dependencia del gobierno que cuente con una autorización pueda interferir todas las comunicaciones electrónicas.

Este CHIP permitiría a los negocios o comercios transmitir mensajes codificados, pero a la vez permite a ciertas oficinas del gobierno interceptar y decodificar los mensajes (si existe la sospecha de que puedan estar complicados en actividades de naturaleza penal). Sin necesidad de mayores explicaciones, esta proposición ha generado gran controversia, particularmente de parte de los grupos de derechos civiles que velan por el derecho de todo individuo a su intimidad y otros temas relacionados con la ética.

3.6. SEGURIDAD DE NETSCAPE

Muchas operaciones comerciales pueden realizarse a través de INTERNET, se pueden hacer compras realizando el pago con tarjetas de crédito. Sin la debida seguridad es posible interceptar estas operaciones y capturar números de tarjetas de crédito con los cuales operar en forma ilícita. Con **Nestcape** se puede garantizar la realización de operaciones seguras, como se verá a continuación.

Netscape SSLREF

Es una implementación de la recomendación del protocolo SSL, cuya finalidad es ayudar y acelerar los esfuerzos de los desarrolladores en proveer seguridad avanzada en las aplicaciones TCP/IP que utilicen SSL.SSLRef se compone de una biblioteca, cuyo fuente se distribuye en ANSI C, que puede compilarse en una amplia variedad de plataformas y sistemas operativos y puede ligarse a programas de aplicación (el cual es de libre distribución para fines no comerciales).

3.6.1. TRANSMISIÓN SEGURA:

Por ejemplo, números de tarjeta de crédito

Puede introducir su número de tarjeta de crédito en un formulario Netscape Navigator seguro (https[19]) y transmitirlo a través de Internet a un servidor seguro sin riesgo de que un intermediario obtenga la información. Las funciones de seguridad ofrecidas por Netscape Communications protegen las transacciones comerciales, así como demás comunicaciones, contra apropiación indebida y fraude que podría darse al pasar la información por las computadoras de Internet.

Las comunicaciones seguras no eliminan todas las preocupaciones de los usuarios de Internet. Por ejemplo, debe estar dispuesto a confiar el número de su tarjeta de crédito al administrador del sistema antes de poder efectuar una transacción comercial. La tecnología de seguridad protege las rutas de la comunicación en Internet, aunque no le protege contra personas descuidadas con las que pueda llevar negocios a cabo.

Los administradores de sistemas deben tomar medidas adicionales para impedir intrusiones. Con el fin de proteger su información, deberá preservar la seguridad física de los servidores y controlar el acceso a las contraseñas y claves privadas.

3.6.2. Forma en la que protege la tecnología de seguridad de Netscape

Las funciones de seguridad de Netscape Navigator protegen las comunicaciones en Internet por medio de:

- Autenticación de servidor (deteniendo a los impostores)
- Confidencialidad mediante encriptación "codificación"(deteniendo las intromisiones ilegales)
- Integridad de datos (deteniendo a los delincuentes)

[19] El protocolo S-HTTP es diseñado para proveer confidencialidad, autenticidad, integridad y no-repudiación, mientras soporta múltiples mecanismos de administración de llaves y algoritmos criptográficos a través de la opción de negociación entre las partes involucradas en cada transacción.

Sin una seguridad completa, la información transmitida a través de Internet es susceptible al fraude y a otros usos indebidos por parte de intermediarios. La información que viaja entre la PC y el servidor emplea un proceso rutinario que puede cubrir varios sistemas informáticos. Cualquiera de estos sistemas representa un intermediario con el potencial de acceder al flujo de información entre una computadora y un servidor en el que se confíe. La seguridad es necesaria para garantizar que los intermediarios no puedan hacer daño, ni "escuchar", copiar o dañar las comunicaciones (**Internet no cuenta con seguridad incorporada**).

Netscape Navigator y los servidores seguros suministran la autenticación del servidor empleando firmas digitales certificadas emitidas por organizaciones llamadas "Autoridades del certificado". Un certificado digital verifica la conexión entre la clave de un servidor público y la identificación del servidor (al igual que un permiso de conducción verifica la conexión entre su fotografía y su identificación personal). Las verificaciones criptográficas, mediante firmas digitales, garantizan que la información dentro del certificado sea de confianza.

3.6.3. FORMAS DE RECONOCER EN NETSCAPE LA SEGURIDAD

Puede saber si se tiene una conexión segura, basta ver el campo de Dirección (URL). Si el URL comienza con https:// (en lugar de por http://), el documento procede de un servidor seguro. Para conectarnos a un servidor HTTP que cuente con seguridad, deberá añadirse la letra "s" de forma que el URL comience por https://. Deberá emplearse https:// para los URL de HTTP con SSL y http:// para los URL de HTTP sin SSL. De igual manera, un URL de noticias que comience por snews: (en lugar de por news:) muestra que el documento proviene de un servidor de noticias seguro.

También puede verificarse la seguridad de un documento examinando el icono de seguridad de la esquina inferior izquierda de la pantalla de Netscape Navigator y la barra de color sobre el área de contenido. El icono consiste en una llave sobre fondo azul cuando el documento sea seguro y de una llave partida sobre fondo gris cuando no lo sea. La llave tendrá dos dientes cuando la codificación sea de alto grado, y un diente para grado medio. La

barra de color en la parte superior del área de contenido será azul para documentos seguros y gris para los no seguros.

Un documento mixto que cuente con información segura y no segura aparecerá con la información no segura reemplazada por un icono de seguridad mixta. Algunos servidores pueden permitirle el acceso a documentos de manera no segura (empleando http://) para ver por completo los documentos mixtos. La seguridad afecta a la transmisión de un documento sin afectar la capacidad de manipulación por parte del usuario.

CAPÍTULO

4

PROPUESTA
DE UNA POLÍTICA DE RED

CAPITULO 4:
PROPUESTA DE UNA POLÍTICA DE RED, PARA MEJORAR LA SEGURIDAD EN LA RED.

Es muy importante e imprescindible tener una política de seguridad de red efectiva y bien diseñada para que pueda proteger a la empresa, esto es, a sus inversiones y recursos de información con los que cuentan. Una política de seguridad para la red justifica su uso si vale la pena o es costeable proteger los recursos e información que se tiene en la red. La mayoría de las empresas tienen información sensible y secretos importantes en sus redes. Esta información debería ser protegida contra el vandalismo de la misma forma con que se aseguran otros bienes valiosos propiedad de la empresa.

Si la red actual no cuenta con ninguna medida de seguridad, entonces podrá ser más difícil adoptar una política que restrinja el acceso, ya que se deberá analizar que personas requieren tener acceso a cada parte del sistema, tomando en cuenta que no se disminuya la capacidad de la organización. Una política de red que evita que los usuarios cumplan con sus tareas de forma efectiva, traerá consecuencias desfavorables, ya que los usuarios tarde o temprano, encontraran la forma de violar dicha política, con lo cual ya no tendría efecto la misma.

Una empresa puede tener muchos sitios o lugares a proteger, y cada uno contar con sus propias redes. Si la organización es grande, hay la probablilidad que se tengan varios administradores de red, cada uno con diferentes metas y objetivos; y si estos sitios no están conectados por medio de una red interna, cada uno de ellos podrá tener sus propias políticas de seguridad de red. Sin embargo, si los sitios están conectados por una red interna, la política de red deberá agrupar las metas de todos los sitios que están interconectados.

En general, un sitio[20] es cualquier parte de una organización que posee computadoras y recursos relacionados con la red. Entre estos sitios se encuentran los siguientes:

- Estaciones de trabajo.
- Computadoras anfitrión y servidores.
- Dispositivos de interconexión: compuertas, enrutadores, puentes, repetidoras.
- Servidores de terminal.
- Software para red y aplicaciones.
- Cables de red.
- Información en archivos y bases de datos.

PLANTEAMIENTO DE LA POLÍTICA DE SEGURIDAD

El definir una política de seguridad de red significa desarrollar los procedimientos y planes que servirán para salvaguardar los recursos de la red contra pérdidas y daños. Para poder desarrollar dicha política se requiere analizar a la organización; por ejemplo con las siguientes preguntas:

- ¿Qué recursos se requieren proteger?
- ¿De qué personas necesita proteger los recursos?
- ¿Qué tan reales son las amenazas?
- ¿Qué tan importante es el recurso?
- ¿Qué medidas se pueden implantar para proteger los bienes de una forma económica y oportuna?
- Examinar con frecuencia la política de seguridad de red actual para verificar si los objetivos y circunstancias en la red han cambiado.

[20] El RFC 1244 discute la política de seguridad del sitio más detalladamente.

En la Figura 5, se encuentra una hoja de trabajo la cual podrá servir de apoyo para desarrollar el planteamiento de seguridad.

Hoja de trabajo para desarrollar un planteamiento de seguridad

Recursos de la red			Tipo de usuarios indeseables	Posibilidad de una amenaza	Medidas a implantar para proteger los recursos de la red
Número	Nombre	Importancia del recurso			

Figura 5. Hoja de trabajo para el desarrollo de un planteamiento de seguridad.

Columna 1: Número de recursos de la red. Es un número de red de identificación interna de los recursos a ser protegidos (si es que se aplica).

Columna 2: Nombre de los recursos de la red, es una descripción de los recursos disponibles de la organización.

Columna 3: La importancia del recurso de la red, puede estar en una escala numérica del cero al diez, o como bajo, alto, medio, etc.

Columna 4: Tipo de usuarios indeseables, puede calificarse como interno, externo, etc.

Columna 5: Medidas a implantar para proteger los recursos de la red. Contendrá valores como: permisos del sistema operativo (para archivos y directorios), pistas/alertas de auditoría (para servicios de red), etc.

En general, el costo de proteger las redes de una amenaza debe ser menor que el costo de la recuperación, si es que se esta afectado por la amenaza de seguridad. Si no se

tiene el conocimiento de lo que se desea proteger, y de las fuentes de amenaza, el lograr un buen nivel de seguridad será algo difícil; por lo que es muy importante involucrar a las personas adecuadas en el diseño de la política de seguridad de la red.

COMO ASEGURAR LA RESPONSABILIDAD DE UNA POLÍTICA DE SEGURIDAD.

Otro punto importante a considerar en la política de seguridad de red es el asegurarse que todos los integrantes de la organización saben cuál es su responsabilidad para mantener la seguridad. Es muy difícil para una política de seguridad de red anticiparse a todas las amenazas posibles. Pero sí, una política puede garantizar que cada tipo de problema tendrá a alguien que pueda manejarlo de forma eficiente. De la misma forma, pueden tenerse varios niveles de responsabilidad asociados con la política de seguridad de la red. Cada usuario de la red, por ejemplo, deberá ser responsable de guardar su contraseña, ya que si no lo hace de forma consciente, se pondrá en riesgo y, comprometerá a otras cuentas y recursos de la organización. Aunque por otro lado, los administradores de red y de sistemas son responsables de mantener la seguridad general de la red.

ANÁLISIS DE LOS RIEGOS

Al crear una política de seguridad de red es importante entender que la razón para crearla es, en primer lugar, asegurar que los esfuerzos invertidos en la seguridad son costeables; lo cual implica que se debe especificar cuáles recursos de la red vale la pena proteger, y que algunos recursos son más importantes que otros. También se deberá identificar la fuente de amenaza de la que se protege a los recursos. A pesar de la gran publicidad que se hace acerca de intrusos en una red, varias encuestas indican que para la

mayoría de las organizaciones, la pérdida real proviene de los propios miembros de la organización.

Un análisis de riesgos implica determinar los siguientes puntos:

- Qué necesita proteger.
- De quién debe protegerse.
- Cómo protegerlo.

Dichos riesgos se clasifican por el nivel de importancia y por la gravedad de la pérdida; ya que como se ha venido planteando, no se deberá gastar más para proteger lo que es menos valioso. En el análisis de riesgos es necesario determinar los siguientes factores:

1. Estimación del riesgo de pérdida del recurso (Ri).
2. Estimación de la importancia del recurso (Wi).

Como una forma de cuantificar el riesgo de perder un recurso, es posible asignar un valor numérico. Por ejemplo, al riesgo (*Ri*) de perder un recurso se le asigna un valor de cero a diez, donde cero indica que no hay riesgo y diez es el riesgo más alto. De una forma parecida, a la importancia de un recurso (*Wi*) también se le puede asignar un valor de cero a diez, donde cero significa que no tiene importancia y diez es la importancia más alta. El resultado de la evaluación general del riesgo será el producto numérico del valor del riesgo y su importancia (también, llamado el peso). Lo cual puede escribirse como sigue:

$$Wri = Ri \times Wi$$

Wri = Peso del riesgo del recurso "i".

Ri = Riesgo del recurso "i".

Wi = Importancia del recurso "i".

La figura 6, muestra un ejemplo de una red (simplificada) con un enrutador, un servidor y un puente. Suponiendo que la red y los administradores de sistemas han producido las estimaciones siguientes para el riesgo y la importancia de los dispositivos de la red.

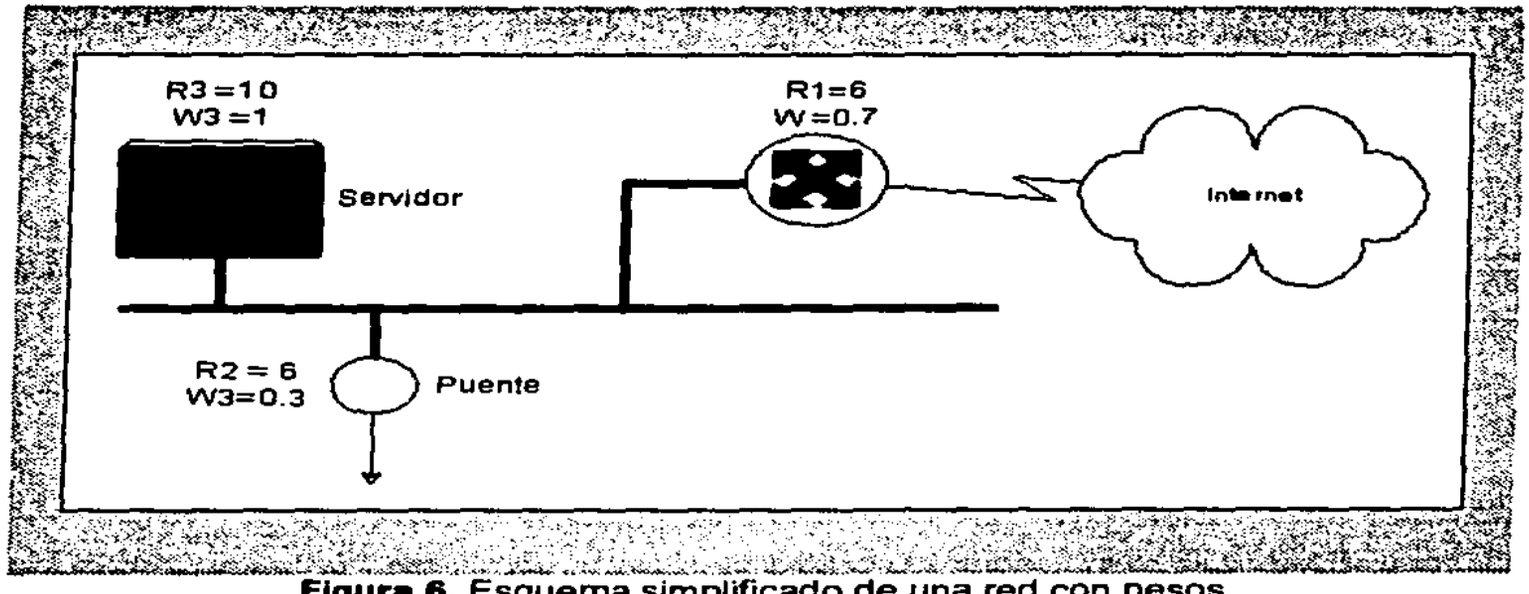


Figura 6. Esquema simplificado de una red con pesos y riesgos valorados.

Enrutador:	**Puente:**	**Servidor:**
R1 = 6	R2 = 6	R3 = 10
W1= 0.7	W2 = 0.3	W3 = 1

El cálculo de los riesgos anteriores se tienen a continuación:

Enrutador:

WR1=R1xW1= 6 x 0.7 = 4.2

Puente:

WR2 = R2 x W2 = 6 x 0.3 = 1.8

Servidor:

WR3 = R3 x W3 = 10 x 1 = 10

También es posible calcular el riesgo general de los recursos de la red, esto con la siguiente fórmula.

WR = (R1xW1 + R2xW2 + . . . + Rn x Wn) / (W1 + W2 + . . . + W n)

Para la red de ejemplo vista anteriormente se tiene el siguiente riesgo general.

WR = (R1xW1 + R2xW2 + R3xW3) / (W1 + W2 + W3)
= (4.2 + 1.2 + 10) / (0.7 + 0.3 + 1)
= (15.4 / 2)
= (7.7)

La Figura 7, muestra una hoja de trabajo de ejemplo, que servirá para registrar los cálculos obtenidos.

Hoja de trabajo para el análisis de riesgo de seguridad en la red.

Recursos de la red		Riesgo para los recursos de red (Ri)	Peso (importancia) del recurso (W i)	Riesgo evaluado (Ri x Wi)
Número	Nombre			

Figura 7. Ejemplo de una hoja de trabajo para el análisis de seguridad de la red.

Columna 1: Número de recursos en la red. Es un número para identificación interna del recurso en la red (si es que se aplica).

Columna 2: Nombre de los recursos de la red, es una descripción de los recursos disponibles de la organización.

Columna 3: Riesgos para los recursos de red (*Ri*), puede estar en una escala numérica del cero al diez, o como bajo, alto, medio, etc.

Columna 4: Importancia del recurso (*Wi*) puede estar en una escala numérica del cero al diez, o como bajo, alto, medio, etc. Pero si se utilizan valores numéricos para las columnas de riesgo y peso, puede calcularse el valor en la columna riesgo evaluado (*Ri x Wi*) como el producto de los valores riesgo y peso.

NOTA: Otros factores que se deben considerar para el análisis del riesgo de un recurso de red es la disponibilidad, su integridad y su carácter confidencial. La **disponibilidad** de un recurso es la medida de qué tan importante es tenerlo disponible todo el tiempo. La **integridad** de un recurso es la medida de qué tan importante es qué éste o los datos del mismo sean consistentes (generalmente en bases de datos). El hecho de ser **confidenciales** se aplica a los recursos, como archivos de datos, a los cuales se desea restringir el acceso.

IDENTIFICACIÓN DE RECURSOS

Al realizar el análisis de los riesgos, se deben identificar todos los recursos cuya seguridad está en riesgo de ser quebrantada. Recursos como hardware encabezan la lista, pero hay otros recursos como son los humanos o personas, quienes utilizan los sistemas y a quienes frecuentemente se ignoran. Por lo anterior es necesario identificar todos los recursos de la red que podrían ser afectados por un problema de seguridad[21]. Algunos de estos recursos se listan a continuación.

[21] El RFC 1244 lista los recursos de red a ser considerados cuando se estimen las amenazas de seguridad general.

1. **HARDWARE:** procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, servidores de terminal, enrutadores, etc.
2. **SOFTWARE:** programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicación.
3. **DATOS:** durante la ejecución, almacenados en línea, archivados fuera de línea, apoyos, bitácoras de auditoría, bases de datos, en tránsito sobre medios de comunicación.
4. **GENTE:** usuarios, personas para operar el sistema.
5. **DOCUMENTACIÓN:** sobre programas, hardware, sistemas, procedimientos administrativos locales.
6. **ACCESORIOS:** papel, formas, cintas, información grabada.

Una vez que se han identificado los recursos que requieren protección, se deberá identificar cuáles son las amenazas a tales recursos. De esta forma las amenazas podrán examinarse para determinar cual es el potencial de pérdida que representan. También se debe identificar de que amenazas de deberá proteger a los recursos, como es: el acceso no autorizado, el riesgo por divulgación de información, servicio denegado, etc.

ACCESO NO AUTORIZADO

Este puede ser de diversas formas, como utilizar la cuenta de otro usuario para obtener acceso a la red y sus recursos. En general, el uso de cualquier recurso de red sin el permiso previo se considera como acceso no autorizado.

DIVULGACIÓN DE INFORMACIÓN

La divulgación de información, ya sea voluntaria o involuntaria, es otro tipo de amenaza. Por lo cual se deberá determinar el valor o sensibilidad de la información guardada en la computadora.

SERVICIO DENEGADO

Debido a que por lo general, las redes enlazan recursos valiosos como computadoras y bases de datos, y proporcionan servicios de los cuales depende una organización, se deberá

tener cuidado de no inutilizar los servicios al grado de hacer la red inoperable y detenga los procesos.

USO Y RESPONSABILIDADES DE LA RED

Hay varios asuntos que deben contemplarse al desarrollar una política de seguridad:

1. **¿A quién se le debe permitir utilizar los recursos?**
   Esto puede realizarse de una forma general, ya que por lo general, la mayoría de los usuarios que utilizan la red se pueden dividir en grupos como usuarios de cuenta, abogados corporativos, ingenieros, etc. y otros también comunes llamados externos.

2. **¿Cuál es el uso correcto de los recursos?**
   Aquí se le proporcionará a cada clase de usuarios una guía de como utilizar los recursos y a que tienen derecho. Además deberá mencionar que no se permite entrar a cuentas ajenas por ningún motivo.

3. **¿Como determinar quién está autorizado para garantizar acceso y aprobar el uso?**
   La política de red deberá identificar quién estará autorizado a otorgar el acceso a sus servicios. Así como también deberá determinar qué tipo de acceso podrán otorgar estas personas.

4. **¿Quién debe tener privilegios de administración del sistema?**
   Deberá analizarse detalladamente quien requerirá de recursos especiales, de tal forma que no haya huecos.

5. Cuáles son los derechos y responsabilidades del usuario?

Se hará consciente a todos los usuarios del acceso que se les ha otorgado, para que no hagan mal uso del mismo ya sea filtrándose en áreas restringidas o permitiendo el acceso de personas no autorizadas,

6. ¿Cuáles son los derechos y responsabilidades del administrador del sistema frente a los usuarios?

La política de seguridad de red deberá especificar el límite de hasta dónde los administradores del sistema podrán examinar los directorios y archivos privados de los usuarios para el diagnóstico de problemas del sistema, y para investigar violaciones a la seguridad.

7. ¿Qué es lo que se hace con la información sensible?

Hay que determinar que tipo de datos delicados deben ser guardados en un sistema específico. Desde el punto de vista de seguridad, los datos extremadamente delicados son por ejemplo, la nómina, la cual debe restringirse para algunas personas

PLAN DE ACCIÓN CUANDO LA POLÍTICA DE SEGURIDAD HA SIDO VIOLADA.

Cuando es violada la política de seguridad, el sistema queda abierto a amenazas de seguridad. Si no hay cambios en la seguridad de la red después de una intromisión, entonces la política de seguridad deberá ser modificada para retirar los elementos que no están asegurados.

Cuando se detecte una violación a la política de seguridad, deberá clasificarse, dependiendo si dicha violación ocurrió por negligencia del personal, o fue causada por un accidente o error, por ignorancia de la política actual o ignorancia deliberada a la política.

COMO RESPONDER A LAS VIOLACIONES DE LA POLÍTICA

Cuando se suscita una violación, la respuesta a ella dependerá del tipo de usuario que causó la violación. Las violaciones a la política podrían ser cometidas por una amplia variedad de usuarios, tanto locales como externos. La diferencia entre ellos se basa en los límites de la red, los cuales puede ser administrativos, legales o políticos; y la respuesta a ellos puede ir desde una reprimenda verbal o advertencia hasta una carta formal o cargos legales.

Es importante definir acciones basadas en el tipo de violación. Para lo cual se requiere definir estas acciones con claridad, tomando como base el tipo de violación del usuario a la política de seguridad. Los usuario tanto internos como externos deben conocer la política de seguridad. Dicha política de seguridad también deberá incluir los procedimientos para el manejo de cada incidente de violación a la seguridad. Además deberá mantenerse y revisarse periódicamente un registro adecuado para tales violaciones de seguridad, para observar en este, las tendencias y tal vez ajustar la política de seguridad, para que se tome en cuenta cualquier tipo de amenaza que pueda surgir.

La respuesta a las violaciones de la política por parte usuarios locales, ocurre en las siguientes situaciones:

- Cuando un usuario local viola la política de seguridad del sitio local (empresa en la cual trabaja). Con esta, se podrá tener mayor control sobre el tipo de respuesta a dicha violación de seguridad.
- Cuando un usuario local viola la política de seguridad de un sitio remoto. Esta puede darse por medio de una conexión como Internet. La situación se complica porque esta implica a otra organización, y cualquier respuesta que se tome, tendrá que discutirse con la organización cuya política de seguridad fue violada

por su usuario. También se deberá consultar a los abogados de la corporación o aquellos especializados en seguridad legal de computadoras.

Hay dos tipos de estrategias de respuesta a incidentes de seguridad, las cuales son:

- **Proteger y proceder.**

La meta de esta política es proteger de manera inmediata la red y restaurarla a u estado normal para que lo usuarios puedan seguir utilizándola. Para lo cual, quizás se tendrá que interferir en forma activa con las acciones del intruso y evitar un mayor acceso; esto deberá ser seguido por un análisis de la cantidad del daño causado.

En ocasiones no es posible restaurar la red de manera inmediata a su operación normal; tal vez se tenga que aislar segmentos de la red y cerrar algunos sistemas, con el objeto de prevenir un mayor acceso no autorizado al sistema. Una desventaja de esta acción es que los intrusos se dan cuenta que han sido detectados e iniciarán acciones para evitar ser rastreados. También el intruso podrá reaccionar a la estrategia de protección mediante el ataque de sitio con una estrategia diferente; con lo cual, el intruso continuará su destrucción en otro sitio.

- **Perseguir y procesar.**

Este enfoque adopta la estrategia de que la mejor meta es permitir a los intrusos seguir con sus acciones mientras se observan sus actividades de forma sigilosa, registrando las actividades del intruso para que existan pruebas o bases para poder hacer la acusación correspondiente. Este procedimiento es recomendado por las agencias de Ley y Fiscales, porque esto genera las pruebas que serán utilizadas al procesar a los intrusos. La desventaja de esto es que el intruso continuará robando información o haciendo otros daños.

Una forma de vigilar a los intrusos sin causar daño al sistema operante es construir una **"Cárcel"**, la cual define un medio simulado para que lo utilice el intruso y en donde sus actividades puedan ser observadas. Dicho medio simulado presenta datos falsos, pero el sistema se prepara de tal forma que las actividades del intruso sean detectadas.

La Figura 8 muestra la idea general de una cárcel. Para construir una cárcel, es necesario tener acceso al código fuente del sistema operativo y gran talento por parte de un programador que pueda simular este medio. Es más seguro construir la cárcel con el uso de una máquina de sacrificio en un segmento aislado de la red para minimizar el riesgo de contaminar otros segmentos de la red y sistemas por las actividades del intruso. Aunque también es posible construir la cárcel mediante el uso de un medio simulado de software; aunque esto es mucho más difícil de implementar.

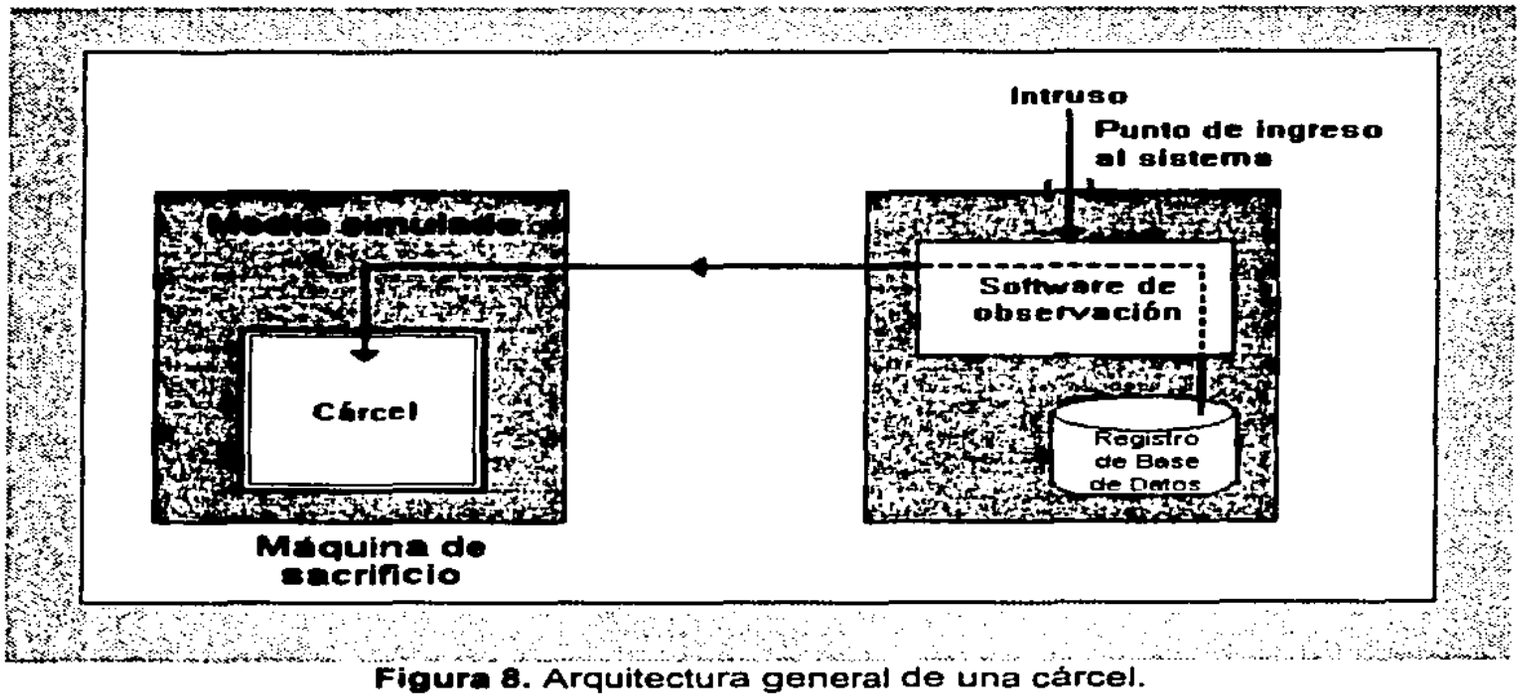


Figura 8. Arquitectura general de una cárcel.

En un sistema Unix el mecanismo ***chroot*** es muy útil para hacer una cárcel, ya que asigna de manera irrevocable un proceso para una ramificación sencilla del sistema operativo. Con fines prácticos, la raíz de este ramal del sistema de archivo aparece como la raíz del sistema de archivo al proceso. Este mecanismo evita el acceso hacia los archivos de los dispositivos y al archivo real de contraseñas (/etc/passwd).

Si no se desea que haya otros usuarios registrados en la máquina de sacrificio, se deberá actualizar de forma periódica el archivo ***utmp***, el cual contiene los datos de los

usuarios registrados para que la cárcel tenga realismo. También se deberá cancelar el acceso a las utilerías que puedan revelar que la cárcel es un medio simulado. Algunas de estas utilerías son **netstat, ps, who w.** Alternadamente se podrá ofrecer versiones falsas para hacer que este medio parezca real.

A continuación se da una guía para poder determinar cuándo un sitio deberá emplear una política de ***proteger y proceder*** o **perseguir y procesar.**

La estrategia de proteger y proceder puede utilizarse con las siguientes condiciones:

- Si los recursos de la red no están bien protegidos contra los intrusos.
- Si la continua actividad del intruso pudiera resultar de gran daño y riesgo financiero.
- Si el costo del proceso es demasiado alto o si la posibilidad o los deseos de procesar no existen.
- Si hay riesgo considerable para los usuarios existentes en la red.
- Si los tipos de usuarios de una red interna grande no se conocen en el momento del ataque.
- Si el sitio es vulnerable a acciones legales por los usuarios (para compañías de seguros, bancos etc.).

La estrategia de perseguir y procesar puede utilizarse con las siguientes condiciones:

- Si los recursos de la red y sistemas están bien protegidos.
- Si el riesgo para la red es incrementado por los disturbios causados por las intrusiones presentes y futuras potenciales.
- Si es un ataque concentrado y ha ocurrido antes.
- Si el sitio es muy visible y ha sido el blanco de ataques anteriores.
- Si no perseguir y procesar invita a nuevas intrusiones.
- Si el sitio pone en riesgo los recursos de la red al permitir al intruso continuar.
- Si el acceso del intruso puede controlarse.

- Si las herramientas para observación están bien desarrolladas para crear registros aptos y recabar evidencia para el proceso legal.
- Si se cuenta en la empresa con los programadores capacitados para construir con gran rapidez herramientas especializadas.
- Si los programadores, administradores del sistema y red son tan listos y conocedores del sistema operativo, utilerías del sistema y sistemas para que valga la pena la persecución.
- Si la gerencia desea un proceso legal.
- Si los administradores del sistema saben qué tipo de evidencia conducirían al proceso legal, y pudieran crear registros adecuados de las actividades del intruso.
- Si se tienen contactos con agencias legales conocedoras.
- Si hay un representante empapado de los asuntos legales relevantes.
- Si el sitio está preparado para una posible acción legal de sus usuarios, si los datos o sistemas se encontraran comprometidos durante la persecución.
- Si se cuenta con respaldos adecuados.

PUBLICACIÓN DE LA POLÍTICA DE SEGURIDAD

Es primordial identificar a las personas que interpretarán la política. La mejor opción es definir un comité que estará encargado de todos los asuntos concernientes, el cual se reunirá en juntas programadas o en antes si se requiere.

Implantar una política de seguridad efectiva es un trabajo colectivo. Por lo tanto, se debe permitir a los usuarios de la red comentar la política durante cierto tiempo y tal vez mantener reuniones para recabar comentarios y asegurarse de que la política ha sido entendida de manera correcta, lo anterior ayudará a pulir el lenguaje de la política y evitar ambigüedades e inconsistencias en la política.

NOTA: Si los usuarios perciben que la política reduce su productividad, se debe permitir que participen. Si fuera necesario, podrían añadirse recursos adicionales a la red para asegurar que los usuarios pueden continuar haciendo su trabajo sin pérdidas en la productividad. Para crear una política

de red efectiva, es necesario encontrar un balance entre la protección y la productividad.

Por lo general los nuevos programas se reciben con gran entusiasmo al principio, cuando todos están al tanto de la política. Pero después de cierto tiempo hay la tendencia a olvidar el contenido de la misma. Los usuarios requieren recordatorios frecuentes. También, al agregar nuevos usuarios a la red, éstos necesitan entender la política de seguridad.

Los recordatorios frecuentes (emitidos con oportunidad) y la educación continúa sobre la política, aumentarán las probabilidades de que los usuarios sigan la política de seguridad. Los nuevos usuarios deberían contar con la política incluida como parte del paquete de información de la red. Algunas organizaciones requieren de una declaración firmada por cada usuario de la red en donde afirman que han leído y entendido la política. Con lo cual, si los usuarios requieren en un futuro de una acción legal para violaciones serias de seguridad, la declaración firmada podrá ayudar a seguir la acción legal con éxito.

CONCLUSIONES

Con lo expuesto a lo largo del presente trabajo nos podemos dar cuenta que lo realizado para brindar seguridad en el intercambio de información, es vasto (aunque no sufciente) y ha tratado de cubir todos los huecos posibles que se presentan con la evolución de la computación y como respuesta a los requerimientos de los usuarios. Aunque en nuestro país no va a la vanguardia en esta área.

La necesidad de seguridad se presenta en todos los niveles de usuarios de redes: personal, organizacional, nacional e Internacional, por lo que para obtener mejores resultados se requiere concientizar a la población operante de la red, de la importancia de asegurar tanto a los recursos informáticos como, a la información perteneciente a la organización, lo cual deberá realizarse en escritos periódicos que informen a los usuarios de las políticas que se implanten, ya que sino se comienza con este primer y sencillo paso ningún esfuerzo o medida será suficiente para obtener un porcentaje aceptable de protección.

Como resultado del presente análisis realizado, sabemos que hay varias herramientas en el mercado que ayudan a tal objetivo. Algunas de estas herramientas, se encuentran disponibles en Internet o son de fácil adquisisón por distribuidores de software; y las cuales proporcionan una excelente fuente de seguridad, para cualquiera que sea la necesidad.

Para todos la información procesada en los distintos centros es muy importante, por lo que si no se tienen muchos recursos como para implantar sistemas sofisticados como cárceles, deberán tomarse otras medidas, como evitar contraseñas obvias: el nombre o las iniciales de una persona, los nombres de lugares, los números de teléfono, las fechas de nacimiento, o las palabras completas (tanto en inglés como en español). Esto se debe a que como en ambos idiomas existe un número relativamente limitado de palabras, a una computadora le resulta muy fácil intentarlas todas con relativa rapidez con la ayuda de determinados programas.

O también se puede utilizar un Kerberos como medio de autentificación, para asegurar que los usuarios están autorizados para operar en el sistema.

Con base a la experiencia, puedo asegurar que la mayoría de las áreas relacionadas con Internet no cuentan con un método o herramienta que los proteja de ataques, y sólo se conforman con el password que el sistema maneja, sin siquiera actualizarlo.

Con lo que se confirma la hipótesis planteada al inicio de esta investigación, la cual afirmaba que si los usuarios de Internet, pueden obtener de un 86% a un 90% de seguridad en la transmisión de su información, entonces, éste será un buen medio para el intercambio de Datos. Además los objetivos planteados también fueron alcanzados y cubiertos, aunque con algunas dificultades en lo referente a los esquemas de seguridad, ya que no hay mucha información sobre ellos.

En el presente trabajo se plantean una serie de políticas y procedimientos que los administradores de los centros de cómputo, deben evaluar para su posible implementación y con ello mejorar sus niveles de seguridad.

ANEXO 1

HISTORIA CRONOLÓGICA DE INTERNET

1964. La red Internet surgió de la necesidad del gobierno de los Estados Unidos de resolver un problema de estrategia militar, en el período de la Guerra Fría. ¿Cómo se podrían comunicar las autoridades después de una guerra nuclear?

RAND Corporation, una de las empresas encargadas de la estrategia militar estadounidense propuso una solución: la creación de una red de comunicaciones que no dependiera de un organismo central, integrado por nodos o puntos de enlace de igual rango y con la misma capacidad de originar, transmitir y recibir mensajes, y que, en caso de que alguno de estos nodos recibiera un ataque o dejara de funcionar, el resto de la red seguiría en operación. Los mensajes en esta red se dividirían en paquetes, cada uno con su propia dirección, originado en algún nodo en particular saltando de lado a lado y finalizando en otro nodo específico, de manera individual. La ruta de los paquetes no importa, solamente importa que lleguen. Si una ruta hubiera sido destruida, el paquete encontraría otra para llegar a su destino.

1967. La planeación de este tipo de redes se expuso durante el simposium realizado en Inglaterra sobre Principios Operativos, auspiciada por ACM (Asociation of Computer Machinery).

1968. El primer resultado en este tipo de redes se obtuvo en Gran Bretaña, utilizando un mainframe IBM

1969. ARPA (Advanced Research Projects Agency), una agencia del Pentágono surgida a partir del lanzamiento del satélite Sputnik, decide realizar un proyecto mayor sobre esta tecnología en redes en Estados Unidos. Este proyecto fue desarrollado por RAND, MIT (Massachussets Institute of Technology) y UCLA (University of California Los Angeles). El primer nodo fue instalado en UCLA. Para diciembre de ese año ya existían cuatro nodos en

ARPANET, pudiendo transmitir datos en líneas de transmisión de alta velocidad y programar remotamente computadoras en otros nodos. En 1971 había quince nodos, y para 1972, treinta y siete.

Poco a poco comenzó a expandirse el uso de ARPANET: no solamente se dedicaba a trabajos de cómputo a larga distancia, sino que se extendió a la comunicación de proyectos y trabajos entre investigadores, y al uso personalizado del correo electrónico y más humano de la comunicación persona a persona. Así también surgen las listas de interés, que son mensajes de correo electrónico retransmitidos automáticamente a los suscriptores en la red.

1973. Tuvo lugar la primera conferencia internacional de ARPANET, con una demostración entre 40 máquinas, conectadas entre sí alrededor del mundo, y sin ninguna pérdida de información, teniendo un éxito impresionante. Otra ventaja de ARPANET es que no importaba los tipos o tamaños de las máquinas en las que se estuviera trabajando, mientras cumplieran con los protocolos establecidos, funcionarían dentro de la red.

1974. El protocolo original se conoció como NCP "Network Control Protocol", el cual fue cambiado por un nuevo estándar más sofisticado, llamado TCP/IP, publicado en este año por Vint Cerf y Bob Kahn. TCP (Transmission Control Protocol) convierte mensajes en cadenas de paquetes en el nodo de origen, y los ensambla de nuevo en el punto de destino. IP (Internet Protocol) maneja el direccionamiento permitiendo que los paquetes fueran ruteados a través de diferentes nodos y hasta de diferentes redes con varios estándares, como Ethernet, FDDI y X.25.

1977. Comenzó a extenderse el uso de TCP/IP en otras redes para vincularse a ARPANET, comenzando esta red a volverse más pequeña en comparación con la gran cantidad de máquinas que comenzaron a conectarse.

A fines de los años 70 y en los años 80, personas de diferentes grupos sociales tuvieron acceso a computadoras de gran capacidad, siendo bastante fácil el conectarse a la creciente red de redes. Como el software de TCP/IP es de dominio público, y por su misma naturaleza, descentralizante y hasta anárquico, comenzó el auge de la conexión a Internet (derivado de International Networking). Fue en esta época donde surgió USENET, el boletín electrónico más grande del mundo, basándose en UUCP, tecnología desarrollada en los

laboratorios Bell de AT&T, junto con el sistema operativo UNIX, que al paso de los años, se ha convertido en el sistema operativo estándar de todos las computadoras de mediano y gran tamaño conectadas a Internet. También surgieron servicios enfocados a la diversión como el primer MUD (Multi User Dungeon, juego de rol interactivo) en la Universidad de Essex.

1981. Surgió otro punto de desarrollo de estas redes, BITNET (Because It's Time for NETwork), creado como red cooperativa, proveyendo a sus usuarios de correo electrónico, listas de interés y transferencia de información y archivos. La conexión a Internet tiene un mínimo costo, ya que cada nodo es independiente, y maneja por sí mismo sus propias necesidades técnicas y financieras. De esta manera, la red comenzó a extenderse, abarcando mayor número de gentes conectadas y de recursos. Así, la comunicación a través de la computadora comenzó a ser indispensable.

1982. El Departamento de Defensa de los Estados Unidos declara como estándar al conjunto TCP/IP, separándose de ARPANET la parte militar, MILNET, Dándose el auge por las estaciones de trabajo de escritorio, con sistema operativo Berkeley UNIX (desarrollado por la Universidad de Berkeley, en Califomia), que incluye software de red TCP/IP.

1984. NSF (National Science Foundation), a través de su Oficina de Cómputo Científico Avanzado establece un nuevo avance técnico, al integrar 5 supercomputadoras a través de enlaces más rápidos, impulsando así el desarrollo de Internet, y permitiendo una mayor cantidad de conexiones, principalmente de universidades, con finalidades académicas y de investigación. También surge el primer Freenet (acceso público a correo electrónico y servicios de Internet en forma gratuita) en Cleveland. En este punto se inició la organización de los dominios (o direcciones de Internet para las diferentes redes conectadas) por sus ubicaciones geográficas, y los seis básicos: gov, mil, edu, com, org y net, que corresponden a instituciones gubernamentales, militares, educacionales, comerciales, no comerciales, y destinados a enlaces entre redes, respectivamente.

1988. Empiezan a surgir problemas en la red, como el caso del "virus" de Internet (Internet Worm), que aprovechaba un error en el código de los programas de correo electrónico, afectando a 6,000 de los 60,000 computadoras conectadas a Internet. Por este motivo, DARPA crea el CERT (Computer Emergency Response Team), que genera

recomendaciones y alertas en caso de problemas dentro de la Red. La comunicación personal tiene mayores posibilidades con el desarrollo de IRC (International Relay Chat), que permite la conversación simultánea de varias gentes en todo el mundo conectadas a esta red.

1989. México ingresa a Internet a través de NSFNET, contando además con la red BITNET, que permite que usuarios del ITESM (Instituto Tecnológico de Monterrey) y la UNAM (Universidad Nacional Autónoma de México) tener acceso a los recursos existentes en Estados Unidos y el resto del mundo. Como ironía y muestra de la eficiencia del sistema, en la guerra del Golfo Pérsico de este mismo año, los ejércitos de Irak utilizan Internet como medio de comunicación para sus operaciones y ataques. No pueden ser detectados por las fuerzas militares estadounidenses, ya que los iraquíes utilizan direcciones piratas, y cambian constantemente de lugar el equipo y las instalaciones. La importancia de Internet comienza a revelarse, ya que es el único medio de comunicación sin censura ni restricciones que poseen los estudiantes chinos que se rebelan, pidiendo democracia en su gobierno. También juega un factor de peso en el intento de golpe de Estado realizado en la Unión Soviética, ya que algunos moscovitas poseían el enlace a Internet y conseguían de primera mano la información necesaria sobre el golpe para difundirla a nivel internacional.

1990. Debido a su propio éxito, ARPANET se volvió obsoleto y deja de existir. Por iniciativa de los usuarios, surgen las primeras organizaciones dedicadas a la protección de los derechos de las personas conectadas a Internet. Este es el caso de EFF (Electronic Frontier Foundation), y la primera organización que comercializa el acceso a Internet vía modem: The World. Se implementan herramientas que catalogan y facilitan el acceso a Internet: Archie, para la búsqueda de archivos accesibles mediante FTP (File Transfer Protocol); Hytelnet, un catálogo de recursos y bibliotecas en línea accesibles mediante telnet (terminal remota); WAIS (Wide Area Information Servers), para entregar directamente documentos al usuario, solicitándolos a través de palabras clave; Gopher, para ver la información a través de menús; PGP (Pretty Good Privacy), para dar seguridad y privacia a los mensajes de la comunidad en la red; Veronica, un sistema de búsqueda complementario a Gopher.

1991. Commercial Internet eXchange (CIX) Association, Inc., surge a partir de que NSF levanta las restricciones que existían para el uso comercial de la Red.

1992. Es un año de profundos cambios dentro de Internet. Se funda Internet Society (ISOC), para coordinar el uso de las tecnologías existentes en beneficio de todos los usuarios. Se desarrolla en el CERN la tecnología de WWW (World Wide Web), que permite un acercamiento más fácil a través de hipertexto a los recursos de Internet; también se da la primera muestra de audio y video en tiempo real a través de la Red.

1993. InterNIC es creado por NSF para proveer servicios de información, así como registros, directorios y bases de datos referentes a Internet. También el Presidente Bill Clinton, su esposa Hillary y su vicepresidente Al Gore ingresan al WWW. En este momento los medios masivos de comunicación tradicionales (televisión, radio, cine, revistas y publicaciones) toman conciencia de Internet y sus implicaciones. Entonces hay artículos en las revistas Time y Newsweek, además mereciendo reportajes en las cadenas más importantes de televisión estadounidense.

El crecimiento de la red se vuelve exponencial. Mosaic, explorador de Internet desarrollado en la Universidad de Illinois Urbane-Champagne, es el primero en aprovechar la gran capacidad del WWW, teniendo un crecimiento anual de 341,634% en número de usuarios de esta herramienta.

1994. Internet cumple 25 años de servicio. Ahora hay comunidades completas conectadas a Internet (Lexington y Cambridge, Mass., USA), el Senado de los Estados Unidos provee información y los centros comerciales llegan a la red, como Internet Shop Network y JCPenny. El auge es tal que surge servicios bancarios en la red, como First Virtual y los negocios comienzan a prosperar, como el caso de Pizza Hut.

No todo es felicidad dentro de la red y surge el caso de Canter & Siegel, que, sin respetar las reglas de cortesía de la red (conocidas como nettiquete), inundan USENET con anuncios sobre sus servicios para inmigración, teniendo una respuesta hostil por parte de los ciudadanos de la red (net.citizens).

1995. Los sistemas de servicios vía modem (Compuserve, Prodigy, Genie) comienzan a ofrecer servicios de Internet. Gran cantidad de compañías relacionadas con la

red se vuelven públicas, encabezadas por Netscape, que tiene el tercer índice de ganancias jamás conseguido en Wall Street.

Los datos antes proporcionados muestran la evolución de Internet, en la cual se señala la gran diferencia que existe entre su estado actual y sus orígenes. La red, que comenzó como un proyecto de sobrevivencia de la información ante la posibilidad de un ataque nuclear, ha derivado en una red de redes, que comunica de manera amplia y eficiente a un creciente número de personas. Alrededor de esta red se ha generado una nueva cultura, la cybercultura, con su modo de pensar, de hablar, de sentir; un mundo nuevo que aún falta mucho por explorar y que tiene un gran potencial.

ANEXO 2

GLOSARIO

ARPANET

(Advanced Research Project Agency Network: red avanzada de agencias para proyectos de investigación). Es la red precursora de la actual internet, la cual fue desarrollada en 1969 por el Departamento de defensa de los Estados Unidos.

Autenticación

Es el proceso mediante el cual se comprueba la identidad de un usuario en la red.

Cableado

Es la columna vertebral de cualquier sistema de red, ya que este, lleva la información de un nodo a otro.

Decodificador

Cualquier dispositivo de hardware o programa de software que convierte una señal codificada a su forma original.

Dirección IP

(Internet Protocol; Protocolo Internet), es la dirección única de un dispositivo de red TCP/IP, la cual consiste de cuatro números entre 0 y 255 separados por puntos (por ejemplo 200.132.5.45).

Encryption (codificación)

Proceso de codificar la información como intento de impedir el acceso no autorizado a ella. El reverso de este proceso se conoce como decodificación. Uno de los programas de codificación más populares de encryptación de programas es Pretty Good Privacy [PGP] (Muy

Buena Privacidad), escrito por Phil Zimmermann y disponible sin ningún cargo desde ciertas sitios de Internet.

FIREWALL (barrera antidifusión)

Método de impedir el acceso no autorizado a un sistema de cómputo, a menudo se encuentra en las computadoras interconectadas.

La barrera antidifusión [firewall] está diseñada para que proporcione un servicio normal a los usuarios autorizados, pero que a la vez evite que los usuarios no autorizados ganen acceso al sistema. En la realidad lo que sucede es que estas barreras casi siempre introducen algún nivel de inconveniencia para los usuarios legalmente autorizados, mientras que su habilidad para controlar el acceso ilegal puede que sea discutible. Durante mucho tiempo la comunidad de Internet ha favorecido el acceso irrestricto a la información, pero a medida que se intensifica el uso comercial de Internet, se hace más evidente la necesidad de disponer de controles cada vez más estrictos.

HACKER (pirata informático)

Un hacker describe a una persona que persigue profundizar sus conocimiento de los sistemas de cómputo por mero interés personal; es decir, alguien dispuesto a hacer correcciones profundas, inteligentes y sutiles de todos los pasos en los cuales se incurre para escribir un programa que funcione bien.

INTRUSO

Usuario no autorizado de un sistema de cómputo, por lo general se trata de una persona con intenciones malévolas.

IP

Abreviatura de Internet Protocol (Protocolo de Internet). Protocolo de comunicaciones [communications protocol] subyacente sobre el cual se basa Internet. El protocolo de Internet (IP) le permite a un paquete de información viajar a través de muchas redes antes de llegar a su destino final.

Norma para el cifrado de datos (DES).

Abreviado DES. Método estándar para codificar y decodificar los datos, desarrollado por la Oficina Nacional de Normas de E. U. La Norma para el cifrado de datos [Data Encryption Standard (DES)] es un cifrado de bloque, el cual funciona mediante una combinación de transposición y sustitución (de bits), fue desarrollado en IBM después de años de trabajo, probado rigurosamente por la Agencia Nacional de Seguridad, y aceptado finalmente como libre de cualesquiera debilidades matemáticas o estadísticas. Esto sugiere que es imposible entrar en la computadora utilizando tablas de frecuencias estadísticas o trabajar el algoritmo en forma retroactiva (hacia atrás) utilizando métodos matemáticos estándar. La utiliza el Gobierno Federal (de los EE. UU.) y la mayoría de los bancos en sus sistemas de transferencia de dinero para proteger la muy sensible información de las computadoras.

A pesar de sus muchos años de uso, esta Norma permanece vigente debido a que su método de codificación aún no ha podido ser descifrado. Se trata de un método de codificación de información completamente aleatorio, lo cual imposibilita determinar la clave de cifrado, aun cuando parte del texto original puede ser conocido.

PROGRAMA ANTIVIRUS

Programa de aplicación que se ejecuta para detectar o eliminar un virus o una infección de la computadora. Algunos programas antivirus son del tipo terminar y permanecer residente y pueden detectar actividad sospechosa en la computadora cómo y cuándo ésta ocurra, mientras que otros tienen que ser ejecutados periódicamente como parte de las actividades normales de mantenimiento (de la computadora).

El programa antivirus localiza e identifica un virus buscando patrones característicos o actividad sospechosa en la computadora, tales como el acceso inesperado al disco, o cambios poco usuales en los archivos **.EXE**. El programa antivirus reconoce el virus comparando la información del sistema contra una base de datos de virus conocidos que se mantiene en el disco. A menudo, la única cura para un virus consiste en borrar el archivo infectado y restaurar una versión anterior de ese archivo (que fue hecha mediante una copia de respaldo (o de seguridad).

PASSWORD contraseña (de acceso)

Método de seguridad de un sistema de cómputo o de una red que identifica a un usuario autorizado específico, mediante una cadena de caracteres exclusiva. Para ganar acceso a la computadora o a la red, el usuario debe teclear estos códigos de identificación.

Por lo general, las contraseñas deben ser una mezcla de letras y números, contener más de cinco caracteres (porque las contraseñas más cortas son más fáciles de adivinar por terceros); además, se deben mantener en secreto y deben ser cambiadas con frecuencia.

RECURSO

Cualquier parte de un sistema de cómputo que un programa puede utilizar a medida que se ejecuta. Los recursos incluyen la memoria, los discos duros, los discos flexibles y las impresoras.

En algunos entornos de programación, a los elementos tales como los cuadros de diálogo, mapas y tipos de letra se les considera recursos, y pueden ser utilizados por varios programas de aplicación diferentes, sin requerir ningún cambio interno en el programa.

RED

Grupo de computadoras y de dispositivos periféricos relacionados --conectados a través de un canal de comunicaciones-- los cuales son capaces de compartir archivos y otros recursos entre varios usuarios. Las redes pueden variar desde una red entre iguales (la cual conecta a un pequeño número de usuarios en una oficina o en un departamento de una compañía muy grande), pasando por una red de área local (LAN) (que conecta a muchos usuarios sobre cables permanentemente instalados y líneas conmutadas), hasta una red de área ancha (que conectan a los usuarios de varias redes esparcidas en una vasta área geográfica).

SEGURIDAD

Por lo general, la seguridad se implementa en el sistema operativo en varios niveles: seguridad de conexión y seguridad por contraseña, seguridad de cuenta, seguridad de directorio y seguridad de atributos de archivo. La mayoría de los sistemas operativos de las computadoras personales no proporcionan mayor seguridad.

SERVIDOR

Cualquier computadora que ofrece --a los usuarios de la red -- acceso a los archivos, a la impresora, a las comunicaciones y a otros servicios. En las redes grandes, un servidor puede ejecutar un sistema operativo de red especial. En las instalaciones más pequeñas, un servidor puede ejecutar un sistema operativo para computadoras personales.

TAPI

Abreviatura de Telephony API [Telefonía API]. Interfaz telefónica estándar para Microsoft Windows, desarrollada por Intel y Microsoft para permitirle a las aplicaciones configurar y controlar las llamadas. Si una llamada está en progreso, la Telefonía API o TAPI no define el método de transmisión de datos utilizado; además, es completamente independiente de la propia red telefónica.

TCP

Abreviatura de Transmission Control Protocol (Protocolo de Control de Transmisión). Protocolo de nivel de transporte orientado a la conexión, utilizado en el conjunto de protocolos de comunicaciones TCP/IP (Protocolo de control de transmisión/Protocolo de Internet.

TCP/IP

Abreviatura o acrónimo de Transmission Control Protocol/Internet Protocol (Protocolo de Control de Transmisión/ Protocolo Internet). Conjunto de protocolos de comunicaciones de computadora a computadora, desarrollado originalmente por la Administración de Proyectos Avanzados de Investigación de Defensa (DARPA), a finales de la década de los años 1970. El conjunto de protocolos TCP/IP incluye acceso a los medios de soporte, al transporte de paquetes, a las comunicaciones de la sesión, a la transferencia de archivos, al correo electrónico y a la emulación de terminal.

UDP

Abreviatura de User Datagram Protocol [Protocolo de datagrama de usuario]. Protocolo de nivel de transporte utilizado en el conjunto de protocolos de control de transmisión/Protocolo de Internet o TCP/IP [Transmission Control Protocol/Internet Protocol].

VIRUS

Programa diseñado para dañar un sistema de cómputo sin permiso ni conocimiento del usuario. Un virus puede conectarse a otro programa, a la tabla de particiones, a la pista de la carga inicial del sistema en un disco duro. Cuando ocurre cierto evento, tal como cuando llega una fecha predeterminada, o cuando se ejecuta un programa específico, el virus entra en acción. No todos los virus son dañinos, algunos sólo son molestos. El más famoso de los virus probablemente es el virus Israelí o Jerusalén, también conocido como Viernes 13, encontrado por primera vez en una computadora en la Universidad de Jerusalén, en Israel, en julio de 1987. Este virus retarda el rendimiento del sistema y dibuja cajas negras en la parte inferior izquierda de la pantalla. Si el virus está en la memoria cualquier viernes 13, cada programa que se ejecute será eliminado del disco duro.

BIBLIOGRAFÍA

CARBALLAR, A. José. Internet: el mundo en sus manos. México: ADDISON-WESLEY, 1994. -- 372 P.

BRENDAN, P. Kehoe. Internet, del arte al Zen. --México: Prentice-Hall, 1995. -- 250 P.

DE GORTARI, Eli. EL MÉTODO DE LAS CIENCIAS. Nociones Elementales. México. 7ª. 1979.-- 270 P.

ELIZONDO López, Arturo. LA INVESTIGACIÓN CONTABLE. Significación y Metodología. México: ECASA. 1992. -- 525 P.

ED, Krol. Conéctate al mundo de Internet. México: McGRAW-HILL, 1995. -- 597 P.

FERREYRA, C. GONZALO, Internet paso a paso. --México: COUMPUTEC, 1996. -- 550 P.

KARANJIT, Siyan, Internet y seguridad en redes. --México: PRENTICE HALL, 1995. -- 407 P.

MARCOMBO, Todo sobre Internet. editores --México :BOIXAREU, 1996. -- 450 P.

OLEA, Franco Francisco. Manual de técnicas de investigación documental. México: Esfinge, 1994. -- 231 P.

VAUGHAN, Steven Nichols. Inside the world wide web. --México: New Riders Publishing, 1995. -- 400 P.

TANENBAUM, Andrew S. Redes de Ordenadores. ed. 2ª --México: PRENTICE HALL, 1991. -- 759 P.

CONSULTAS ELECTRÓNICAS

http://www.cs.bbs.ncsl.nist.gov

http://www-genome.wi.mit.edu/www/faqs/www-security-faq.html

http://www.shop.internet.net

http://www.funtec.org/osi.html

http://www.funtec.org/tcpip.html

http://www.funtec.org/datos.html

http://www.infonet.com.py/nets202/seguridad.html

http://www.esegi.es/esegi/vdl.html

http://www.service.com/doccenter/home.htm

http://www.commerce.net/directories/dire

http://serpiente.dgsca.unam.mx/nicunam/servinfo/internet/acerca/historia/cronologia.html

http://dpni@dpni.inegi.gob.mx