UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SEGURIDAD DE LA INFORMACION

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

SHEILLA ETTY GOMEZ FERNANDEZ

PROMOCIÓN

2002-I

LIMA – PERÚ

2007

SEGURIDAD DE LA INFORMACION

Dedico este trabajo a:

Mis Padres, razón de mi vida.

SUMARIO

El presente informe consta de cuatro capítulos, estructurados de la siguiente manera:

En el Capítulo I analizaremos de manera general la seguridad de la información, se define la integridad, la disponibilidad y la confidencialidad de la información.

En el Capítulo II hacemos un análisis de los sistemas de seguridad a nivel de red, se menciona sobre la criptología, se muestra diseños típicos de firewall, Proxy, así como la seguridad de las VPN y el Protocolo SSL.

En el Capítulo III hacemos un análisis de los sistemas de seguridad a nivel de comunicaciones, mencionando los servidores típicos en un sistema, como el de correo, archivo, web.

En el Capítulo IV se da detalles sobre la auditoría de información que se debe de realizar en un sistema, para la mejora del mismo.

INDICE

PROLOGO

El Presente trabajo pretende únicamente ser una introducción al mundo de la seguridad de los sistemas de información desde la perspectiva y el enfoque que proporciona una de las familias de protocolos de comunicaciones más extendidas actualmente: TCP/IP.

Hoy en día ya no cabe preguntarse si es necesaria la seguridad. Más bien debemos preguntarnos –cada cual en su caso- porqué es necesaria la seguridad. El concepto de ordenador individual casi ha desaparecido. Internet está llegando cada vez más a todos los rincones de nuestra vida, desde el ordenador al teléfono móvil e incluso la televisión.

Es una ventana al mundo, el concepto de aldea global ha pasado de una utopía a algo muy real. Pero no olvidemos que las ventanas tiene dos lados, y que bien se puede mirar la calle desde la apacible tranquilidad de tu casa, pero también se ve tu casa desde la calle. La gente pone cortinas, usa ventanas ahumadas... ¿por qué?

Porque a nadie le gusta que le invadan su intimidad. Creo que es un buen símil para poder extraer una idea intuitiva de la importancia de la seguridad. El crecimiento de las conexiones hace que la necesidad de seguridad sea imperiosa, urgida por la información que se transmite a través de las conexiones. Ya no sólo leemos el correo electrónico o visitamos determinados sitios Web.

Hoy día compramos por Internet, consultamos los movimientos bancarios a través de Internet, trabajamos a través de Internet en definitiva, la cantidad de datos "sensibles" que atraviesan nuestras líneas telefónicas ha crecido y lo seguirá haciendo día a día.

Y eso ya no es preocupación de empresas o de gurús de la informática, sino una preocupación muy real de cualquier usuario de a pie. Internet es libre, y se ha convertido en el medio de comunicación más imparcial que puede existir, gracias a su concepción descentralizada.

CAPÍTULO I
ANALISIS DE LA SEGURIDAD DE LA INFORMACIÓN

1.1 Introducción

La seguridad en los sistemas de información y de cómputo se ha convertido en uno de los problemas más grandes desde la aparición, y más aún, desde la globalización de Internet. Dada la potencialidad de esta herramienta y de sus innumerables aplicaciones, cada vez más personas y más empresas sienten la necesidad de conectarse a este mundo.

Verdaderamente, la Seguridad (denominación que se refiere a una disciplina amplísima que abarca los sistemas de protección física, la prevención de accidentes, o la prevención de actividades desleales por parte de los empleados), no es una función nueva de la empresa, ni una necesidad sobrevenida por el uso de Redes Telemáticas, pero sí es cierto que recientemente merece mayor atención por parte de los administradores de redes.

La información es un valor clave para cualquier institución ya sea pública o privada. La carencia de información o una información defectuosa pueden llevar la empresa a la ruina. Para que la empresa tenga éxito debe tener una información de calidad.

Una información es de calidad cuando satisface los requerimientos que la gestión de la empresa le pide como son:

La integridad.

La disponibilidad.

La confidencialidad.

1.2 Clasificación de la Información

Las categorías de clasificación son:

- Integridad. Se refiere a la necesidad de mantener la información exacta y completa.

- Disponibilidad. Se refiere a la necesidad de mantener acceso continuo y oportuno a la información.

- Confidencialidad. Se refiere a la necesidad de mantener la información privada. Su divulgación presentaría riesgos.

Desde el punto de vista de su **integridad**, la información se puede clasificar en:
1. Modificación Altamente Restringida. Modificación de esta información sin autorización puede causar daño significativo a EMPRESA ABC, sus clientes, vendedores, asociados o al público. Este tipo de información requiere autorización individual por el usuario dueño de la información para actividades específicas sobre archivos de datos específicos y requiere revisión y aprobación por parte de la Auditoría.

2. Modificación Restringida. Información potencial para cambios moderados a través de fraudes, robo electrónico u otras formas para obtener beneficio personal. Esta clasificación aplica a información para la cual EMPRESA ABC está disponible a otorgar derechos de modificación sobre una base restringida.

3. Modificación Controlada. Recursos de información que se le pueden dar a cualquier usuario para efectuar modificaciones bajo circunstancias debidamente controladas. Los usuarios pueden modificar directorios internos y programas relacionados. Terceros pueden tener acceso bajo esta categoría.

Desde el punto de vista de su **disponibilidad**, la información se puede clasificar en:
1. Muy crítica. Información que si no está disponible en el momento que se requiere puede causar consecuencias serias sobre el negocio. Esta categoría puede ser el 20% o menos de su información.

2. Crítica. Información necesaria para la continuidad de operaciones de EMPRESA ABC. Si no está disponible en el término de uno a dos días o durante los períodos de cierre, puede causar consecuencias sobre el negocio. Esta categoría también incluye aquellas aplicaciones y archivos que se tornan críticos periódicamente, tales como al final del mes, trimestre o año. Esta categoría de información incluye el 50% de la información del negocio.

3. Importante. La falta de disponibilidad de esta información implica que EMPRESA ABC puede operar por un término de cinco días sin estos recursos de información en particular o puede encontrar modos de procesamiento alternos (a menudo manuales) para trabajar fuera de línea.

Desde el punto de vista de su **confidencialidad**, la información se puede clasificar en:
1. Restringida. Información de la más alta confidencialidad. Se autoriza el acceso a personas que tengan una necesidad específica de conocerla o usarla para cumplir con sus funciones; no debe ser compartida a menos que exista aprobación de la Alta Gerencia.

Impacto del Uso Inapropiado: Podría causar daños financieros, legales, regulatorios o de imagen graves para EMPRESA ABC, sus accionistas, clientes, proveedores y empleados.
Ejemplos: contraseñas, claves de encriptación, planes de inversión, resultados financieros previos a su liberación, planes estratégicos a largo plazo y secretos comerciales o de negocios.

2. Confidencial. Información de uso selectivo. Su acceso se basa en la necesidad de conocerla o usarla para cumplir con su función. Esta información es compartida solamente bajo condiciones predefinidas o de acuerdo con una orden judicial o de la Gerencia.

Impacto del Uso Inapropiado: Podría tener un impacto adverso a EMPRESA ABC, sus accionistas, empleados, proveedores o clientes.
Ejemplos: Información de clientes (copias de pantallas con información de la cuenta), información personal, plan de operaciones a corto plazo, y estrategias de mercadeo y operaciones.

3. Uso Interno. Este valor se asigna a la información que se debe mantener interna. Información dirigida al uso dentro de EMPRESA ABC y normalmente no compartida con personas que no son empleados de EMPRESA ABC. Pueden existir necesidades del negocio que requieran distribuir esta información fuera de EMPRESA ABC. Tiene el potencial de causar mínimo daño a EMPRESA ABC si se divulga.

Impacto del Uso Inapropiado: Podría causar daños a la imagen de EMPRESA ABC.
Ejemplos: Procedimientos de EMPRESA ABC, directorio telefónico de EMPRESA ABC, listas de correo, manual de empleados, algunos manuales de nuestros sistemas.

4. General. Información dirigida al público. Tiene muy poco o ningún impacto para EMPRESA ABC si es divulgada, modificada o utilizada de una manera inapropiada.

Impacto del Uso Inapropiado: Ningún impacto; con la excepción de formatos de clientes en blanco. Estos formatos requieren controles específicos de distribución.
Ejemplos: La información presentada en la página WEB de EMPRESA ABC, descripción de beneficios generales a los empleados, divulgación de noticias y literatura de productos o servicios.

1.3 Tipos de Ataques y Amenazas

Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad).

La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios. Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un fichero o una región de la memoria principal, a un destino, como por ejemplo otro fichero o un usuario.

Un ataque no es más que la realización de una amenaza. Las cuatro categorías generales de amenazas o ataques son las siguientes:

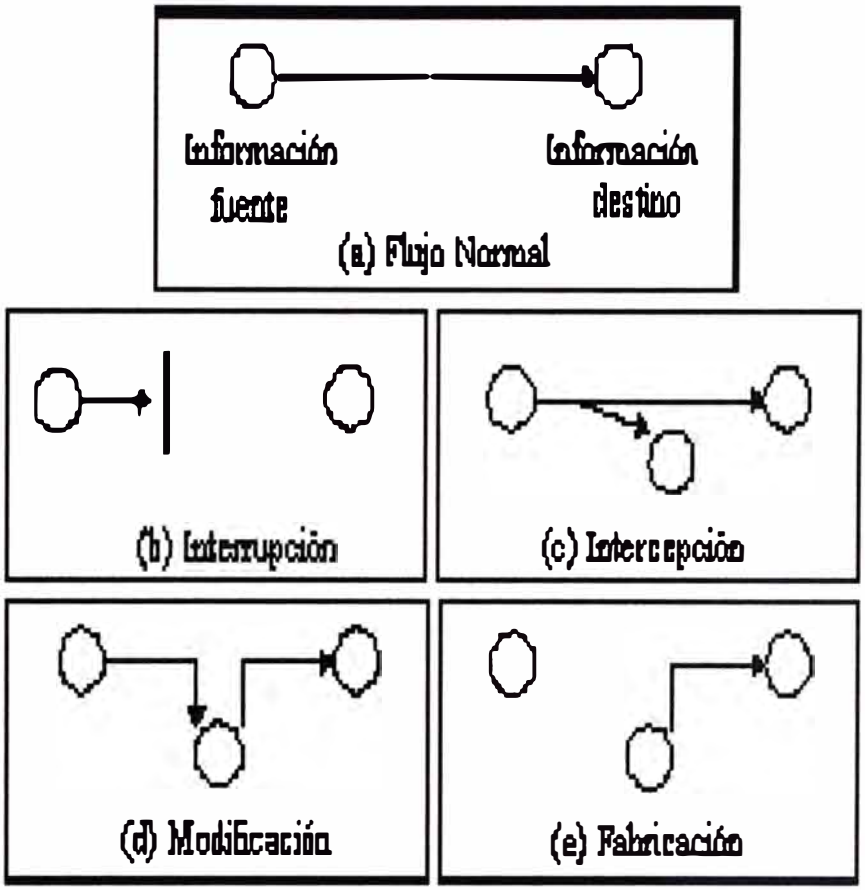


Fig. 1.1 Tipos de Ataques y Amenazas

1. Interrupción: un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

2. Intercepción: una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son interceptar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

3. Modificación: una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.
4. Fabricación: una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.

Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

1.3.1 Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

1.3.2 Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- Suplantación de identidad: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

- Reactuación: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

- Modificación de mensajes: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de soles en la cuenta A" podría ser modificado para decir "Ingresa un millón de soles en la cuenta B".

- Degradación fraudulenta del servicio: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

1.4 Ejemplo de Vulnerabilidades y Protecciones Particulares

A modo de ejemplo se ha considerado interesante presentar algunos casos de vulnerabilidades concretas existentes (o que han existido y ya han sido resueltas) en el mundo real. Estos ejemplos sirven como muestra detallada de las posibilidades asociadas a las vulnerabilidades y protecciones mencionadas en los apartados anteriores.

Ni mucho menos pretenden ofrecer una muestra exhaustiva de ejemplos reales en las implementaciones de los fabricantes de equipos con pilas TCP/IP, ya que el número de éstas se cuenta por cientos de miles y además aumenta a pasos agigantados cada día. Asimismo, los equipos, servicios o S.O. reflejados no denotan un mayor índice de vulnerabilidad, sino que simplemente se han tomado como muestra representativa de ejemplo.

Las vulnerabilidades encontradas son clasificadas con un código identificativo o CVE. Previamente a esta clasificación pueden ser contempladas con un identificador CAN, representando vulnerabilidades candidatas a ser CVEs, pero que no han sido completamente comprobadas.

El único método que puede permitir un acercamiento mayor a las vulnerabilidades existentes, así como a las nuevas que van surgiendo, y a las ya solucionadas, es la suscripción a listas de distribución, grupos de news, servidores Web (portales) de organizaciones dedicadas a la seguridad o de los propios fabricantes.

Estos sistemas son actualizados diariamente para mantener informados tanto a la comunidad de administradores de sistemas y redes en Internet, como a la comunidad de hackers. Asimismo, cuentan con grandes bases de datos en las que almacenan todas las referencias pasadas.

1.4.1 Dispositivos Cisco: puerto de identificación 1999

Los dispositivos de red Cisco ejecutando su sistema operativo IOS utilizan el puerto 1999 como puerto de identificación. En algunos documentos aparece clasificado como sigue:

tcp-id-port 1999/tcp cisco identification port
tcp-id-port 1999/udp cisco identification port

Las peticiones recibidas en dicho puerto se manejan de forma diferente a las de los otros puertos; en este caso, al recibir un paquete TCP de SYN, responden inmediatamente con

un paquete RST (en lugar de con el típico SYN-ACK), incluyendo el término "cisco" en el payload del paquete.

La implicación de este comportamiento es la sencillez a la hora de identificar dispositivos de este fabricante cuando se realiza un escaneo de puertos. Por tanto, aunque el dispositivo no permita el acceso a su puerto de telnet, es posible identificarlo.
Para protegerse de este ataque basta con impedir conexiones TCP externas al puerto en cuestión.

1.4.2 En los puertos de acceso de los routers

Los puertos de acceso o configuración de los routers, habitualmente 23, 2001, 4001, 6001 y 9001, pueden ser atacados enviando unos pocos miles de caracteres (en ocasiones basta con enviarlos un par de veces), consiguiendo que el router no proporcione servicio durante el periodo de tratamiento de esa información. La denegación del servicio lógicamente perdurará más al enviarse un mayor número de paquetes.

Algunos dispositivos solo pueden ser restaurados mediante un reset manual del equipo, mientras que otros se recuperan a los pocos minutos, horas o incluso días. Este ataque ha afectado tanto al sistema operativo IOS de los Cisco como al ComOS de 3Com.
El impacto de este ataque es que condiciona al administrador a disponer de acceso físico al sistema, condición que no siempre se cumple, debido a la comodidad de las tareas de administración remotas. Un ejemplo del ataque es el envío de varias (3-6) ráfagas de información como sigue:

```
$ perl –e ' print 0xFF x 10000 ' | telnet router.dominio.com 4001
```

Tras la desconexión, un nuevo intento de conexión al puerto generará un mensaje de "Connection refused", y el tiempo que se mantendrá el router en esta situación depende del modelo y la versión de S.O., pero puede variar entre 30 seg. y varios días.

1.4.3 NetBIOS

NetBIOS es un protocolo de transporte de datos (basado en sesiones) característico de los entornos Windows. Asimismo añade la funcionalidad de resolución de nombres en este entorno, a través del puerto UDP 137.

En Windows 2000 es posible ejecutar TCP/IP de forma nativa, pero no ocurre lo mismo en las versiones anteriores de Windows, por ejemplo NT. Las vulnerabilidades entorno ha este protocolo son numerosas.

Un ejemplo concreto se centra en la gestión de nombres. Cuando un ordenador quiere dar a conocer alguno de sus recursos a la red, para compartirlo, éste debe reservar un nombre único para que el resto de equipos sepan identificarlo. De esta manera, el protocolo envía un mensaje broadcast - a todos los ordenadores de la red - "preguntando" si la denominación que quiere reservar está o no ocupada. En el supuesto de que no esté, el nombre del nuevo recurso se almacena en una lista en este equipo que queda visible al resto de clientes de la red para su acceso. Por el contrario, en el caso de que ya esté reservado por otro cliente, éste, al recibir el mensaje de petición, responde con otro de "conflicto". De esta manera, esta denominación queda "tachado" en la lista del demandante como ya en uso.

Supóngase qué, aunque el protocolo de bajo nivel (en este caso TCP/IP) funcione correctamente, NetBIOS deje de funcionar en un sistema A. En el momento en que cualquier cliente B quiera acceder a un recurso almacenado en el sistema A, éste utiliza el nombre del recurso compartido para llegar hasta él. B envía un broadcast (en el caso de que la dirección no se encuentre en la caché del sistema) preguntando quién es A. Como este último no puede responder a la petición del nombre, B no encuentra el equipo en la red. Lo mismo ocurre cuando el ordenador A intenta acceder a otro recurso en la red. Pese a que el resto de equipos si son capaces de responder, no saben a quien hacerlo con lo que A queda completamente aislado de la red. Debe tenerse en cuenta que Windows utiliza NetBIOS no sólo para resolver nombres, sino además se emplea para establecer ciertas sesiones de autenticación y enviar los contenidos de los recursos compartidos.

El fallo descubierto, cuya demostración se encuentra en un pequeño programa del grupo hacker "Cult Of The Dead Cow", intenta eliminar el nombre de un recurso en la red. Cuando se reconoce un nuevo recurso, el equipo que quiere registrar el nombre (que tiene formato de 15 caracteres y 1 byte que determina el tipo de servicio, algo así como un puerto UDP o TCP) envía un mensaje broadcast a la red del tipo NAME REGISTRATION REQUEST. Si otra máquina ya tiene registrado este nombre en su lista interna, envía de forma inmediata un mensaje al que realiza la petición de tipo DENY. El dispositivo que realizó la petición marca este nombre como "en conflicto" y deja de responder a cualquier tipo de mensajes dirigidos a este recurso. Lo mismo ocurre cuando un equipo "libera" uno de estos nombres, ya que pasará a ser marcado o directamente borrado de esta lista interna. ¿Qué es lo que ocurre cuando cualquier cliente envía, por amor al arte, uno de estos mensajes a otro equipo DENY?

En las implementaciones de NetBIOS (afecta desde Windows NT a 2000), este mensaje es aceptado en cualquier momento, incluso cuando no se ha realizado la consulta de registro. De esta forma, el cliente acepta el mensaje y marca en su lista de nombres su recurso como "en conflicto" y deja de utilizarlo.
La solución para evitar el fallo de este mecanismo es utilizar algún tipo de autenticación. De esta forma, el equipo que envía el mensaje maligno DENY, tendría que probar que en efecto es él el que ha registrado previamente el nombre. Desgraciadamente, NetBIOS no ha sido diseñado con esta característica y es necesario aplicar otro tipo de soluciones. La forma más efectiva de evitar que NetBIOS juegue una mala pasada es desactivarlo; no obstante, muchas redes basan su infraestructura en este sistema. Otra solución sería el uso de IPSec en el servicio asociado UDP.

1.4.4 Ataque DNS cache

Las versiones de BIND 4.9.5 y 8.1.X sufrían una vulnerabilidad asociada a la recursividad que permitía cachear información falseada. Cuando un cliente realiza una petición DNS a su servidor para un dominio sobre el que éste no tiene autoridad, si la recursividad está activa, el servidor local preguntará al servidor DNS con autoridad sobre el dominio,

obtendrá la respuesta y se la reenviará al cliente solicitante. Esta información se almacenaba en caché para agilizar peticiones posteriores.

Mediante el ataque conocido como PTR record spoofing, un atacante podía insertar registros PTR en la caché del servidor a través de la recursividad, modificando la relación entre direcciones IP y nombres. Asimismo, este ataque puede implicar DoS cuando un nombre de dominio concreto se asocia a una dirección IP inexistente, negando el servicio proporcionado por ese dominio.

El servicio de DNS ha sufrido numerosas vulnerabilidades en los últimos años, algunas de ellas contempladas en el aviso del CERT con identificador "CERT Advisory CA-2001-02". Tanto las vulnerabilidades como las recomendaciones asociadas para evitarlas, principalmente mediante la configuración del servicio, pueden obtenerse del ISC.

1.4.5 Vulnerabilidades DoS en las pilas TCP/IP

El equipo de seguridad de RAZOR descubrió y documentó numerosas vulnerabilidades de las implementaciones TCP/IP. Todas ellas permiten a los atacantes consumir recursos del sistema (tiempo de CPU, ancho de banda de la red, memoria, así como recursos del kernel del S.O.: entradas de procesos, identificadores de ficheros abiertos...), y por tanto, reproducir un DoS.

Las implementaciones de TCP disponen de un número limitado de recursos al simular la máquina de estados del protocolo. Cualquier sistema que permite que ciertos recursos críticos sean consumidos, es potencialmente un candidato de un DoS.

Existe un ataque denominado Naptha, basado en un DDoS, que permite como se ha comentado, consumir la totalidad de los recursos de un sistema, empleando para ello un gasto de recursos reducido (ICMP broadcast), mantiene el anonimato del atacante (IP Spoofing), y puede llevarse a cabo de forma distribuida, DDoS. El ataque se basa en el número de conexiones que puede mantener activas la pila TCP en los diferentes estados posibles: SN RECVD, ESTABLISHED, FIN WAIT 1, FIN WAIT 2

La defensa frente a estos ataques pasa por:

Aplicar los parches específicos del fabricante de la implementación de la pila TCP/IP.

Parametrizar de forma apropiada, adecuándolo a su uso, el sistema.

Preparar previamente las medidas a realizar en el caso de producirse un DoS.

Existen protecciones frente a Naptha de fabricantes como Compaq en su Unix Tru64, FreeBSD, Microsoft, Sun.

CAPÍTULO II
SISTEMAS DE SEGURIDAD A NIVEL DE RED

Existen muchas y muy potentes herramientas de cara a la seguridad de una red informática. Por sí mismas, las aplicaciones de software y los productos de hardware que componen la red informática de una empresa no constan de política de seguridad, y, sin embargo, son elementos esenciales en el establecimiento de la seguridad de las empresas. Las herramientas que tienen como fin la protección de las redes informáticas han sufrido una continua evolución durante las dos últimas décadas, prácticamente el mismo tiempo que se lleva intentando "piratearlas" y violar las redes informáticas En la actualidad se cuenta con diversos métodos que garanticen la seguridad de nuestra información, dentro de los mas difundidos tenemos a los siguientes

2.1 Criptología

Las amenazas que sufre la información durante su proceso, almacenamiento y transmisión son crecientes y complejas. Para contrarrestarlas se han desarrollado numerosas medidas de protección, que se implementan en el equipo físico o lógico mediante los denominados mecanismos de seguridad. La lista de estos mecanismos es muy numerosa y en ella encontramos, entre otros muchos: identificación y autenticación de usuarios, control de accesos, control de flujo de información, registros de auditoría, cifrado de información, etc. De éstos, el mecanismo por excelencia es el de cifrado de la información.
La Criptología se divide en dos ciencias importantes: la Criptografía y el Criptoanálisis.

La Criptografía se puede traducir como " La manera de escribir raro " (Criptos, extraño ; Graphos, escritura). Es una ciencia que se ocupa principalmente de conseguir que nuestros mensajes sean comprensibles exclusivamente para aquellos que nosotros deseemos e inteligibles para el resto de la Humanidad, aplicando para ello procedimientos matemáticos

o claves. El texto inicial, el de partida, recibe el nombre de texto claro. El que resulta de aplicarle el algoritmo criptográfico, es el texto cifrado. Ej. Proceso de cifrado de mensajes

El Criptoanálisis es la ciencia que se dedica a quebrantar el cifrado obtenido de la Criptografía. Una de las propiedades necesarias que debe tener un algoritmo criptográfico, es que cada texto, al aplicarle el algoritmo de descifrado con la misma clave de cifrado o la clave de descifrado relacionada, debe convertirse en el mismo texto claro del que procede.

Históricamente los militares y los cuerpos diplomáticos han utilizado y han contribuido, de una manera importante, en el arte de la Criptología. Sin embargo, hoy en día su interés merece una atención especial para todos los sectores públicos o privados para los que la información es algo muy valioso. Con la introducción de las computadoras, la necesidad de herramientas automatizadas para proteger archivos y otro tipo de información almacenada en las computadoras es evidente. La implementación de sistemas distribuidos y la utilización de redes entre un usuario terminal y una computadora o entre computadoras afecta a la seguridad. Las medidas de seguridad en una red de datos son necesarias para proteger los datos durante la transmisión. Los sistemas de cifrado modernos se clasifican en:

Simétricos o de clave secreta: La clave utilizada es la misma tanto para cifrar como para descifrar. El algoritmo debe ser público, pero la clave debe ser siempre secreta.

Asimétricos o de clave pública: La clave para cifrar es pública y la de descifrar secreta, y están relacionadas entre sí. El algoritmo puede ser público o secreto. Cualquier persona que disponga de la clave pública puede cifrar el mensaje, pero solo el que ha generado las claves y tiene la clave secreta puede descifrar el mensaje.

No hay ningún algoritmo irrompible. El algoritmo puede ser más o menos duro. La dureza de un algoritmo se mide teniendo en cuenta su factor de trabajo, que es la cantidad necesaria de trabajo para descubrir las claves.

Dentro de la criptografía moderna, es decir, aquella en que los algoritmos operan en bits, dos son los algoritmos más conocidos y utilizados, el DES y el RSA

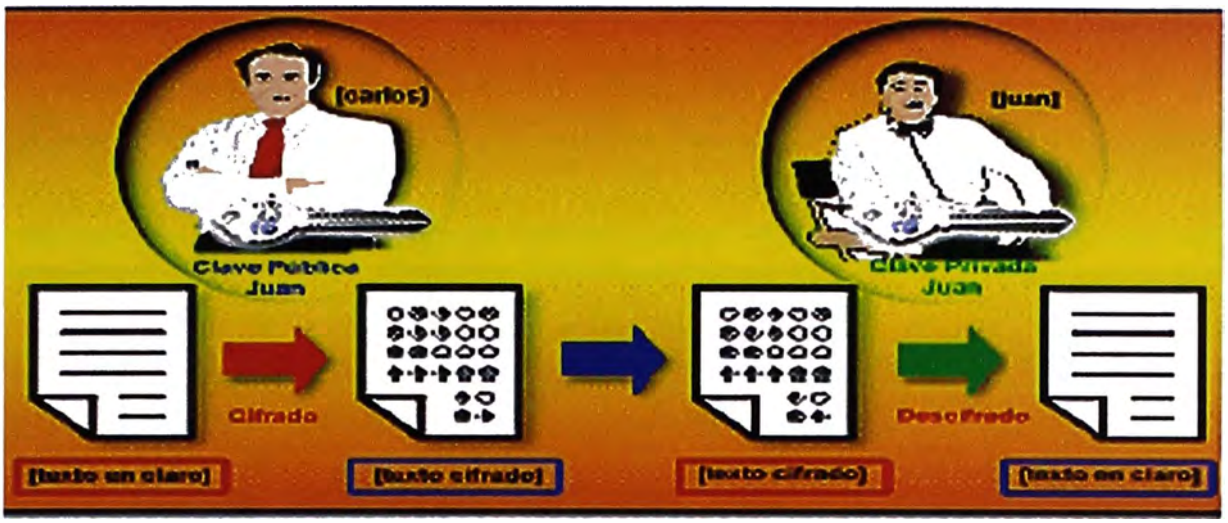


Fig. 2.1 Proceso de Filtrado de Mensaje

2.1.1 Algoritmos mas utilizados

DES

Las siglas DES corresponden a las iniciales de Data Encryption Standard. Este algoritmo se convirtió en un estándar y se utiliza en gran parte de los sistemas informáticos que precisan de un cierto grado de protección, a pesar de las restricciones que el gobierno de los Estados Unidos impuso para su comercialización fuera del país. El algoritmo consiste en un complejo sistema de operaciones matemáticas basado en sustituciones y permutaciones de bits en función de una clave. El conocimiento del algoritmo no permite descifrar la información cifrada; de hecho éste es de dominio público. El proceso de cifrado trabaja con bloques de 64 bits y una clave de otros 64 bits, siendo 56 de la clave en sí y los restantes 8 de paridad impar para detección de errores. Tras la aplicación de un algoritmo, que efectúa una serie de complejas permutaciones, sustituciones y operaciones

lógicas, los 64 bits de información se transforman en otros tantos cifrados. Dividiendo la información en bloques de este tamaño y realizando la misma operación para cada bloque, se consigue cifrar un texto completo.

Seguridad del algoritmo

Cuando el algoritmo DES se presentó existían numerosas dudas sobre si contendría "puertas traseras" que permitiesen al gobierno de los Estados Unidos descifrar todo tipo de comunicaciones. Más tarde se demostró que estas dudas no tenían fundamento; sin embargo, el tamaño de la clave utilizada hace que el algoritmo sea vulnerable y esta situación se agrave más según vaya incrementándose la potencia de los ordenadores y disminuyendo su precio. La única forma conocida de violar el algoritmo es probar a descifrar la información con todas las posibles claves. Puesto que constan de 56 bits habría que probar con 2E56, es decir, 72.057.594.037.927.936 claves distintas. Suponiendo que se dispone de un ordenador de gran potencia capaz de generar y probar un millón de claves por segundo, se requerirían unos 72.000 millones de segundos lo que, traducido a años, serían 2.285. Sin embargo, utilizando un superordenador con multitud de procesadores en paralelo se podrían generar todas las claves en tan sólo unas horas, aunque este tipo de ordenadores no está al alcance de cualquiera

RSA

El algoritmo RSA fue desarrollado en los años setenta por Rivest, Shamir y Adleman, de cuyas iniciales toma su nombre, y está basado en el problema de hallar los factores primos de grandes números. Frente a sus diversas ventajas sobre los sistemas de clave privada presenta el inconveniente de la carga que supone al sistema, puesto que se basa en operaciones que consumen mucho tiempo de proceso. Además, cada vez el tamaño de los números a emplear debe ser mayor para garantizar la inviolabilidad del sistema debido al incremento en la potencia de cálculo de los ordenadores. La encriptación RSA es un sistema de encriptación de clave pública, y se trata de una tecnología patentada en los Estados Unidos, por lo que no puede utilizarse sin licencia. Sin embargo, el algoritmo se hizo público antes de ser adjudicada la patente, lo que dio lugar a que la encriptación RSA pudiera utilizarse en Europa y Asia sin necesidad de pagar royalties. La encriptación RSA

está creciendo en popularidad, y se considera bastante segura frente a ataques de fuerza bruta.

Seguridad del algoritmo

La seguridad del algoritmo radica en el tamaño de un número n, que es el producto de los números primos. No es aconsejable trabajar con valores inferiores a 154 dígitos o lo que es lo mismo 512 bits y para aplicaciones que requieran un alto grado de seguridad 1024 bits (308 dígitos) ó incluso 2048. El algoritmo más rápido conocido para factorizar un número se debe a R. Shroeppel, que permite hacerlo con un número de operaciones definido por la expresión: ev(ln (ln n))ln n Por ejemplo con un número de 300 dígitos. Suponiendo que se dispone de un ordenador de gran potencia capaz de realizar un millón de operaciones por segundo, se requerirían 4800 billones de años para factorizar el número. Aun dividiendo el problema en partes y utilizando múltiples sistemas o un superordenador con multitud de procesadores en paralelo, con 300 dígitos la seguridad está garantizada.

2.1.2 Aplicaciones

La Criptología se utiliza también para la autentificación de mensajes y para firmas digitales. El método de la autentificación consiste en incorporar al mensaje un código llamado MAC (Modification Autentification Code), que se calcula aplicando un algoritmo de cifrado al texto entero. El receptor hace lo mismo y compara el valor que le da con el que lleva el mensaje, si es igual, el mensaje se considera autentico

Firma Digital.

Una firma digital es un bloque de caracteres que acompaña a un documento, acreditando quién es su autor ("autentificación") y que no ha existido manipulación posterior de los datos ("integridad"). El proceso de la firma digital lo realiza un software (por ejemplo PGP, Eudora, Outlook, etc) que aplica un algoritmo sobre el texto a firmar, obteniendo un extracto (número) de longitud fija, y único para ese mensaje. Este extracto cuya longitud oscila entre 176 y 160 bits se somete a continuación al cifrado (RSA o DES) mediante la clave secreta del autor, previa petición de contraseña. Para verificar la firma, el receptor

descifra la firma con la clave pública del emisor, comprime con la función hash al texto original recibido y compara el resultado de la parte descifrada con la parte comprimida, si ambas coinciden el emisor tiene garantía de que el texto no ha sido modificado. Como el emisor utiliza su clave secreta para cifrar la parte comprimida del mensaje, puede probarse ante una tercera parte, que la firma sólo ha podido ser generada por el usuario que guarda la componente secreta.

El mecanismo de firma digital soporta los servicios de integridad de datos, autenticación de origen y no repudio con prueba de origen. Para proporcionar el servicio de no repudio con prueba de entrega es necesario forzar al receptor a enviar al emisor un recibo firmado digitalmente.

Control de acceso. Este mecanismo se utiliza para autenticar las capacidades de una entidad, con el fin de asegurar los derechos de acceso a recursos que posee. El control de acceso se puede realizar en el origen o en un punto intermedio, y se encarga de asegurar si el emisor está autorizado a comunicar con el receptor y/o a usar los recursos de comunicación requeridos. Si una entidad intenta acceder a un recurso no autorizado, o intenta el acceso de forma impropia a un recurso autorizado, entonces la función de control de acceso rechazará el intento, al tiempo que puede informar del incidente, con el propósito de generar una alarma y/o registrarlo. El mecanismo de control de acceso soporta el servicio de control de acceso.

Integridad de datos. Es necesario diferenciar entre la integridad de una unidad de datos y la integridad de una secuencia de unidades de datos ya que se utilizan distintos modelos de mecanismos de seguridad para proporcionar ambos servicios de integridad. Para proporcionar la integridad de una unidad de datos la entidad emisora añade a la unidad de datos una cantidad que se calcula en función de los datos. Esta cantidad, probablemente encriptada con técnicas simétricas o asimétricas, puede ser una información suplementaria compuesta por un código de control de bloque, o un valor de control criptográfico. La entidad receptora genera la misma cantidad a partir del texto original y la compara con la recibida para determinar si los datos no se han modificado durante la transmisión. Para proporcionar integridad a una secuencia de unidades de datos se requiere, adicionalmente, alguna forma de ordenación explícita, tal como la numeración de secuencia, un sello de

tiempo o un encadenamiento criptográfico. El mecanismo de integridad de datos soporta el servicio de integridad de datos.

Intercambio de autenticación. Existen dos grados en el mecanismo de autenticación:

Autenticación simple. El emisor envía su nombre distintivo y una contraseña al receptor, el cual los comprueba.
Autenticación fuerte. Utiliza las propiedades de los criptosistemas de clave pública. Cada usuario se identifica por un nombre distintivo y por su clave secreta.

Cuando un segundo usuario desea comprobar la autenticidad de su interlocutor deberá comprobar que éste está en posesión de su clave secreta, para lo cual deberá obtener su clave pública

2.2 Firewalls

Un firewall es un sistema o un grupo de sistemas que decide que servicios pueden ser accesados desde el exterior (Internet, en este caso) de un red privada, por quienes pueden ser ejecutados estos servicios y también que servicios pueden correr los usuarios de la intranet hacia el exterior (Internet). Para realizar esta tarea todo el trafico entre las dos redes tiene que pasar a través de él.

El firewall solo deja pasar el trafico autorizado desde y hacia el exterior. No se puede confundir un firewall con un enrutador, un firewall no direcciona información (función que si realiza el enrutador), el firewall solamente filtra información.

Desde el punto de vista de política de seguridad, el firewall delimita el perímetro de defensa y seguridad de la organización. El diseño de un firewall, tiene que ser el producto de una organización conciente de los servicios que se necesitan, además hay que tener presentes los puntos vulnerables de toda red, los servicios que dispone como públicos al exterior de ella (WWW, FTP, telnet, entre otros) y conexiones por módem (dial-in módem calling).

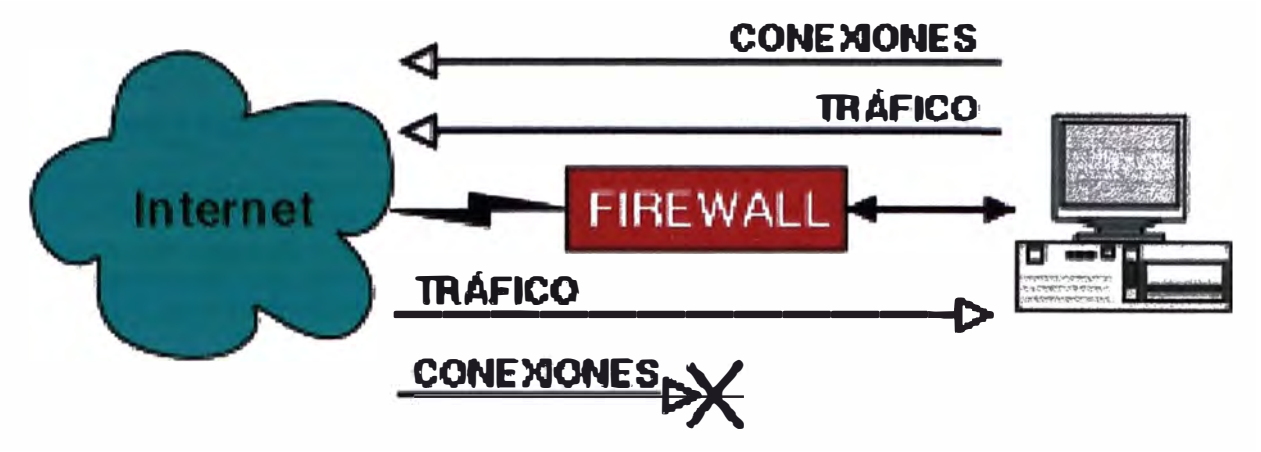


Fig. 2.2 Típica disposición de un firewall doméstico

Ello no quiere decir que la instalación de un sistema de firewall permita la relajación de la seguridad interna de las máquinas, sino que se podrá distinguir fácilmente entre el interior y el exterior, pudiendo determinar qué comportamiento general se quiere para cada servicio. Otra característica importante de estos sistemas es que permiten llegar donde los mecanismos de seguridad de los sistemas operativos a veces no pueden.

Beneficios de un firewall

Los firewalls manejan el acceso entre dos redes, si no existiera todos los hosts de la intranet estarían expuestos a ataques desde hosts remotos en Internet. Esto significa que la seguridad de toda la red, estaría dependiendo de que tan fácil fuera violar la seguridad local de cada maquina interna. El firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador de la red escogerá la decisión si revisar estas alarmas o no, la decisión tomada por este no cambiaría la manera de operar del firewall. Otra causa que ha hecho que el uso de firewalls se halla convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el numero disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones CIRD (o direcciones sin clase), las cuales salen a Internet por medio de un NAT (Network address traslator), y efectivamente el lugar ideal y seguro para alojar el NAT ha sido el firewall.

Los firewalls también han sido importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el trafico de la red, y que procesos han influido mas en ese trafico, de esta manera el administrador de la red puede restringir el uso de estos

procesos y economizar o aprovechar mejor ancho de banda. Finalmente, los firewalls también son usados para albergar los servicios WWW y FTP de la intranet, pues estos servicios se caracterizan por tener interfaces al exterior de la red privada y se ha demostrado que son puntos vulnerables.

Tipos de Firewalls

Packet filter (filtro de paquetes): Se basa en el tratamiento de los paquetes IP a los que aplica unas reglas de filtrado que le permiten discriminar el tráfico según nuestras indicaciones. Normalmente se implementa mediante un router con dos interfaces de red, uno de cara al exterior y otro al interior, aunque podría utilizarse cualquier máquina con dos placas de red y un software adecuado para filtrado de los paquetes IP. Al tratar paquetes IP, los filtros que podremos establecer serán a nivel de direcciones IP, tanto fuente como destino. Normalmente, se establece una lista de filtros por interfaz que se aplicarán a cada paquete independiente de los anteriores, o de si forma parte de una determinada comunicación para un cierto servicio. Algunos filtros de paquetes permiten establecer filtros también a nivel de puertos TCP o UDP, con lo que se podrá filtrar qué servicios se dejan pasar o no. Cortafuegos - filtro de paquetes ejemplarizado en un router. La lista de filtros se aplican secuencialmente, de forma que la primera regla que el paquete cumpla marcará la acción a realizar (descartarlo o dejarlo pasar). La aplicación de las listas de filtros se puede hacer en el momento de entrada del paquete o bien en el de salida o en ambos. Aunque no puede parecer importante lo es, pues tiene que ver con el tratamiento del 'address-spoofing' uno de los ataques utilizados con más frecuencia para saltarse la protección establecida por un cortafuegos, que como hemos descrito antes, consiste en generar paquetes IP con direcciones falsas. Los filtros de paquetes son una buena solución, pero tienen sus limitaciones a la hora de tratar los servicios como tales, pues para ellos cada paquete es independiente y no forma parte de ningún todo, por los tanto, de ningún servicio. Además, existen servicios como DNS o FTP, que dificultan realizar una configuración segura de un filtro de paquetes. Son muy pocos los sistemas de filtrado de paquetes que se basan en la propia información para aceptar o denegar un paquete. Esta posibilidad, aunque tiene un elevado coste, puede utilizarse por ejemplo, para evitar la entrada de archivos infectados con virus en una red interna. Ventajas del filtrado de paquetes: La protección centralizada es la ventaja más importante del filtrado de paquetes.

Con un único enrutador con filtrado de paquetes situado estratégicamente puede protegerse toda una red. Si sólo existe un enrutador con salida a una red insegura, independientemente del tamaño de nuestra red interna, podrá controlarse todo el tráfico en dicho enrutador.

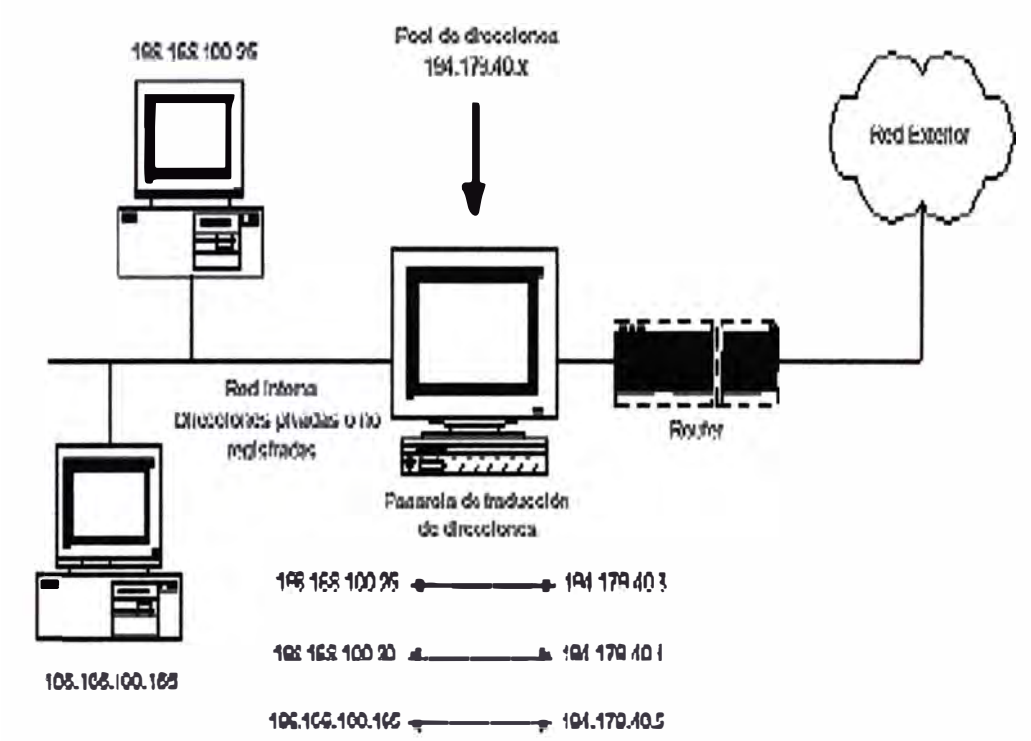


Fig. 2.3 Filtro de paquetes ejemplarizado en un router

Firewalls a nivel de aplicación: Es el extremo opuesto a los filtros de paquetes. En lugar de basarse en el filtrado del flujo de paquetes, tratan los servicios por separado, utilizando el código adecuado para cada uno. Es probablemente el sistema más seguro, ya que no necesita tratar complicadas listas de acceso y centraliza en un solo punto de gestión los servicios. Y además permitir controlar y recoger información de cada uno de los servicios por separado. Las pasarelas a nivel de aplicación son prácticamente la única solución efectiva para el tratamiento seguro de aquellos servicios que requieren permitir conexiones iniciadas desde el exterior (servicios como FTP, Telnet, Correo Electrónico). En realidad, lo que se utiliza es una puerta de acceso para cualquier servicio. Al ser esta puerta de uso obligatorio, podemos establecer en ella los criterios de control que queramos.

Atravesada la puerta, puede ocurrir que la propia pasarela de nivel de aplicación ofrezca el servicio de forma segura o que establezca una conexión con el ordenador interno que

realmente ofrece el servicio, teniendo en cuenta que éste último deber estar configurado para aceptar conexiones tan solo desde nuestra pasarela de nivel de aplicación para este servicio.

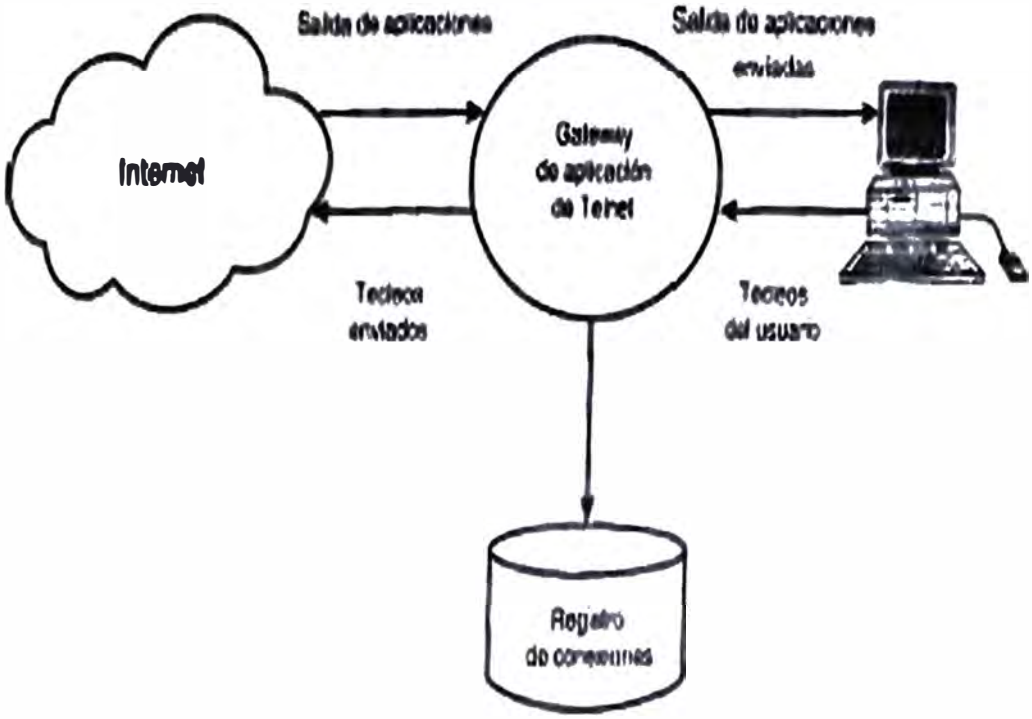


Fig. 2.4 Firewalls a nivel de aplicación

Firewalls a nivel de circuito: Se basan en el control de las conexiones TCP y actúan como si fuesen un cable de red: por un lado reciben las peticiones de conexión a un puerto TCP; y por otro, establecen la conexión con el destinatario deseado, si se han cumplido las restricciones establecidas, copiando los bytes de un puesto al otro.

Este tipo de cortafuegos suelen trabajar conjuntamente con los servidores 'proxy', utilizados para la acreditación, es decir, comprobaciones sobre máquina fuente, máquina destino, puerto a utilizar. Una acreditación positiva, significa establecer la conexión. Son el tipo de cortafuego más adecuado para el tratamiento de las conexiones salientes.

Cortafuegos basados en certificados digitales: Este tipo de cortafuegos basados en certificados digitales son extremadamente seguros y con una gran funcionalidad. Su popularidad no ha sido muy grande porque hasta hace poco tiempo no existían

distribuidores de certificados digitales universales. Actualmente este defecto está cambiando a nivel mundial.

Decisiones de diseño básicas de un firewall
Hay varias consideraciones a tener en cuenta al momento de implementar un firewall entre Internet y una intranet (red LAN) Algunas de estas consideraciones son:

- Postura del firewall

Todo lo que no es específicamente permitido se niega. Aunque es una postura radical es la más segura y la mas fácil de implementar relativamente ya que no hay necesidad de crear accesos especiales a los servicios.
Todo lo que no es específicamente negado se permite. Esta no es la postura ideal, por eso es mas que todo usado para subdividir la intranet. No es recomendable para implementar entre una LAN e Internet, ya que es muy vulnerable.

- Política de seguridad de la organización

Depende mas que todo de los servicios que esta presta y del contexto en el cual esta. No es lo mismo diseñar un firewall para una ISP o una universidad que para proteger subdivisiones dentro de una empresa.

- Costo del firewall

El costo del firewall depende del numero de servicios que se quieran filtrar y de la tecnología electrónica del mismo, además se necesita que continuamente se le preste soporte administrativo, mantenimiento general, actualizaciones de software y parches de seguridad.

- Componentes de un firewall

Los componentes típicos de un firewall son:
Un enrutador que sirva única y exclusivamente de filtro de paquetes.

Un servidor proxy o gateway a nivel de aplicación (debido al costo, implementado comúnmente en una maquina linux).
El gateway a nivel de circuito.

Configuraciones de cortafuegos

Los tipos de cortafuegos que existen se han tratado de forma independiente, no como sistema. Cuando se realiza un sistema de cortafuegos, suelen emplearse varios o todos los tipo. Se hace así porque, cada uno de ellos trata la protección a un nivel distinto, desde los paquetes de red, pasando por los puertos de conexión, hasta el servicio propiamente dicho.

Existen múltiples variaciones sobre los esquemas de configuración. Algunos de ellos aportan un nivel mayor de seguridad, pero requieren la dedicación de un número mayor de recursos del sistema, con el consiguiente coste, mientras que otras reducen gastos a costa de la seguridad, pero siendo aún plenamente funcionales. Se ha de encontrar la configuración adecuada a cada sistema, en función del nivel de seguridad que requiera la política de seguridad del sistema y el trabajo y los recursos que se quieran invertir en dicha seguridad. Esta configuración se conseguirá equilibrando esos dos factores de forma coherente

Limitaciones del firewall

La limitación mas grande que tiene un firewall sencillamente es el hueco que no se tapa y que coincidencialmente o no, es descubierto por un hacker. Los firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo dejara pasar. Pero este no es lo más peligroso, lo verdaderamente peligroso es que ese hacker deje "back doors" es decir abra un hueco diferente y borre las pruebas o indicios del ataque original. Otra limitación es que el firewall "no es contra humanos", es decir que si un hacker logra entrar a la organización y descubrir passwords o se entera de los huecos del firewall y difunde la información, el firewall no se dará cuenta. Es claro que el firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus

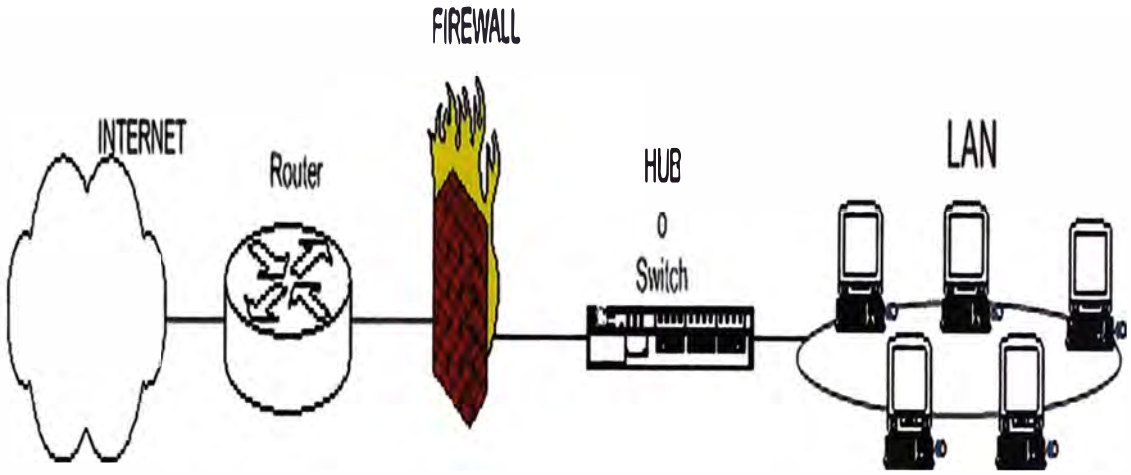


Fig. 2.5 Ubicación Típica del Firewall

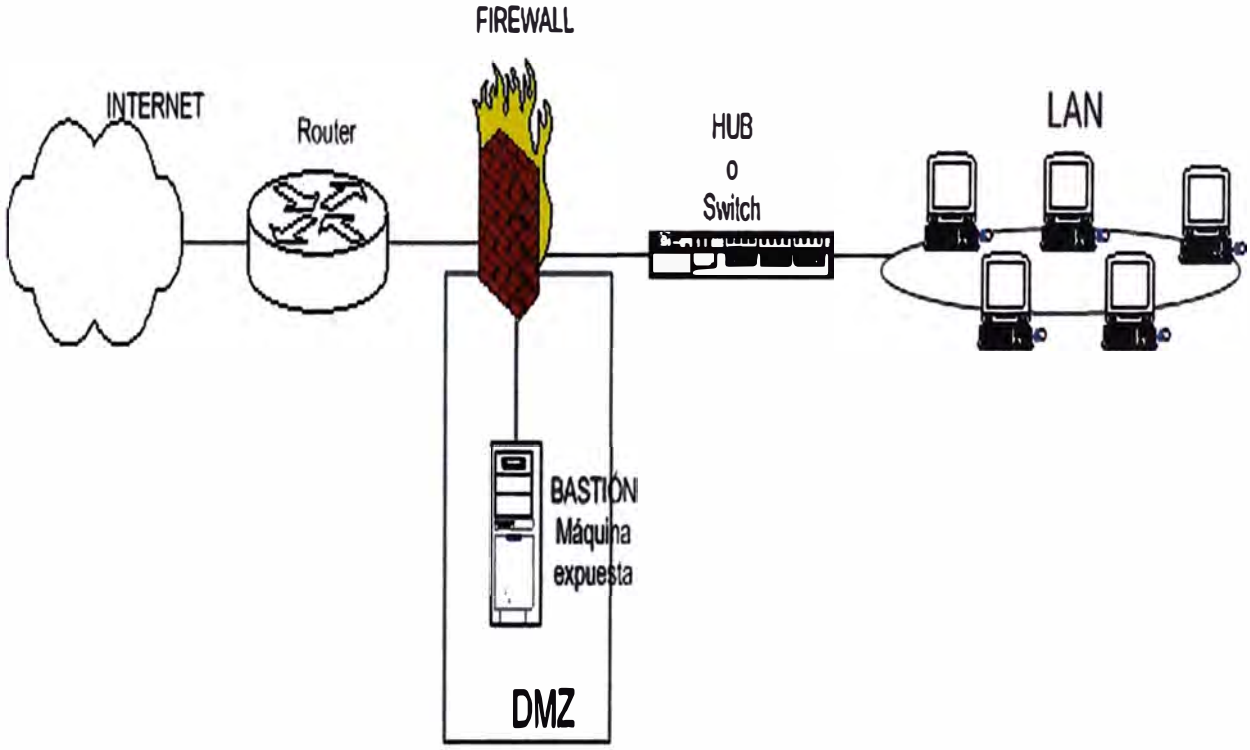


Fig. 2.6 Firewall usado para proteger un DMZ y una LAN

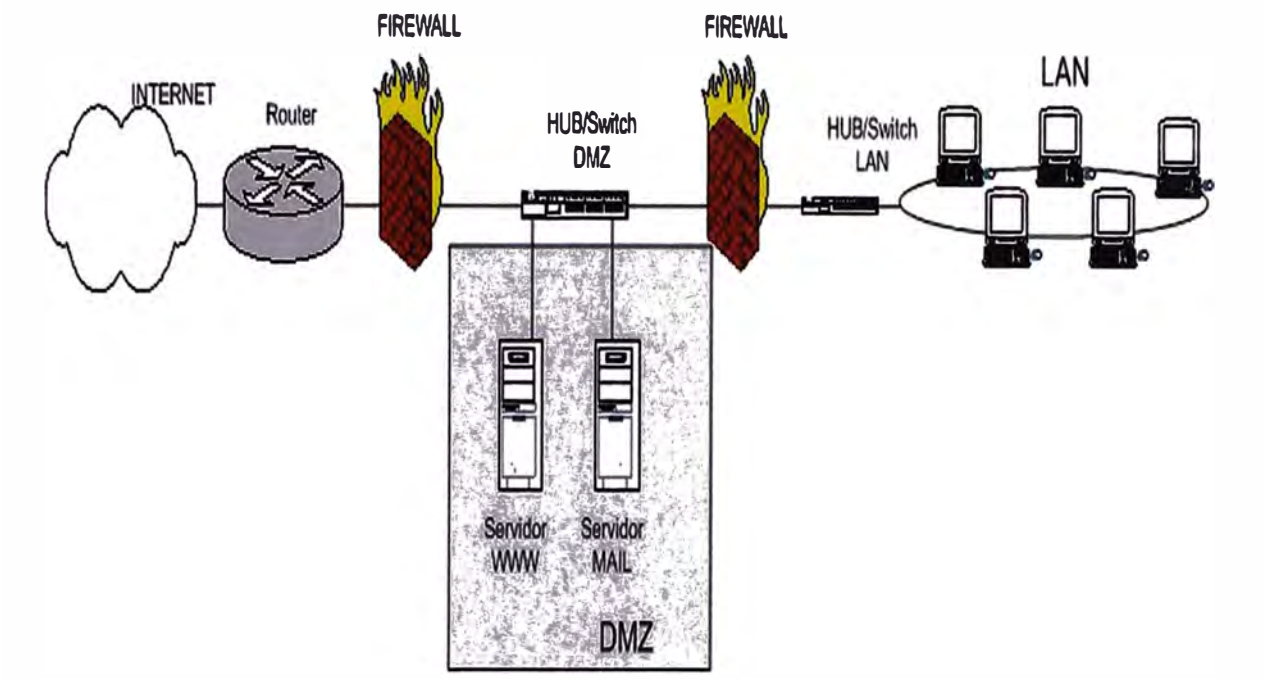
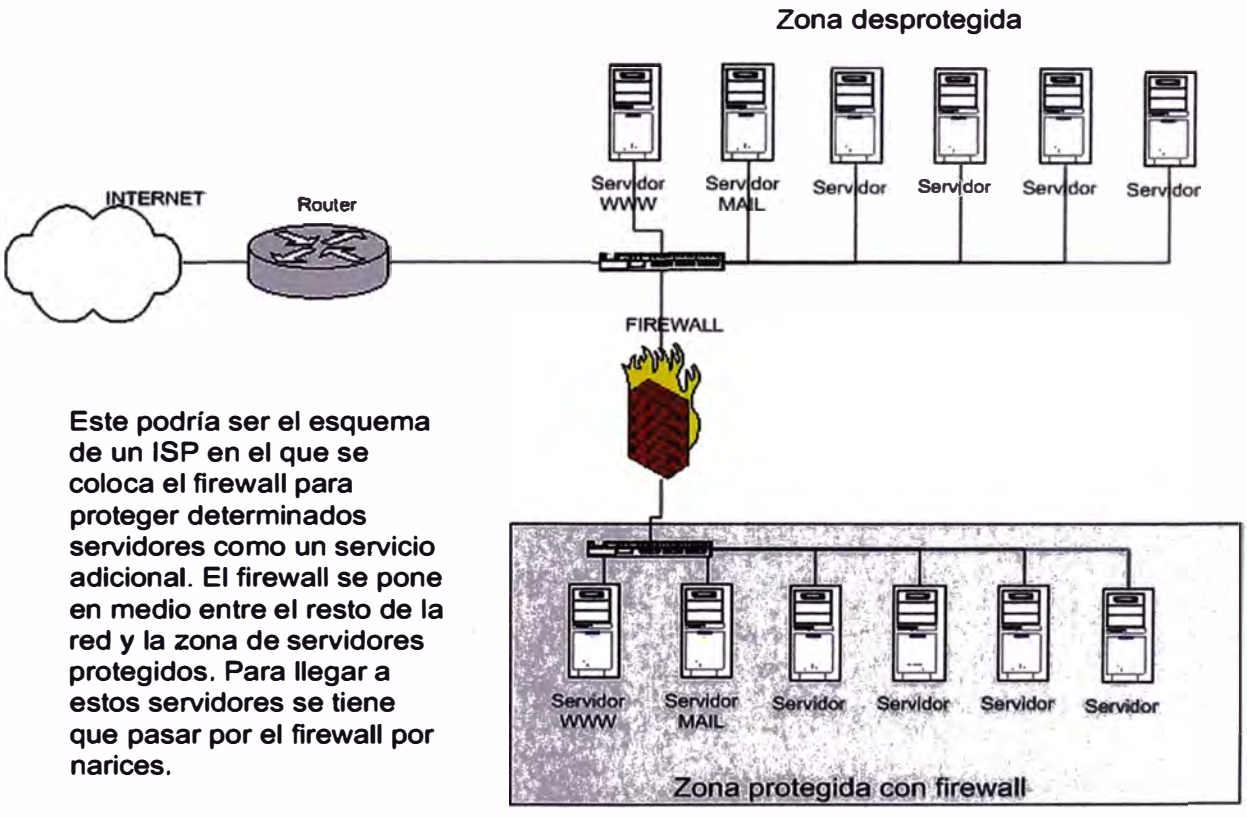


Fig. 2.7 Usando dos firewalls, uno que protege una LAN y el otro un DMZ



Este podría ser el esquema de un ISP en el que se coloca el firewall para proteger determinados servidores como un servicio adicional. El firewall se pone en medio entre el resto de la red y la zona de servidores protegidos. Para llegar a estos servidores se tiene que pasar por el firewall por narices.

Fig. 2.8 Otro posible diagrama de red.

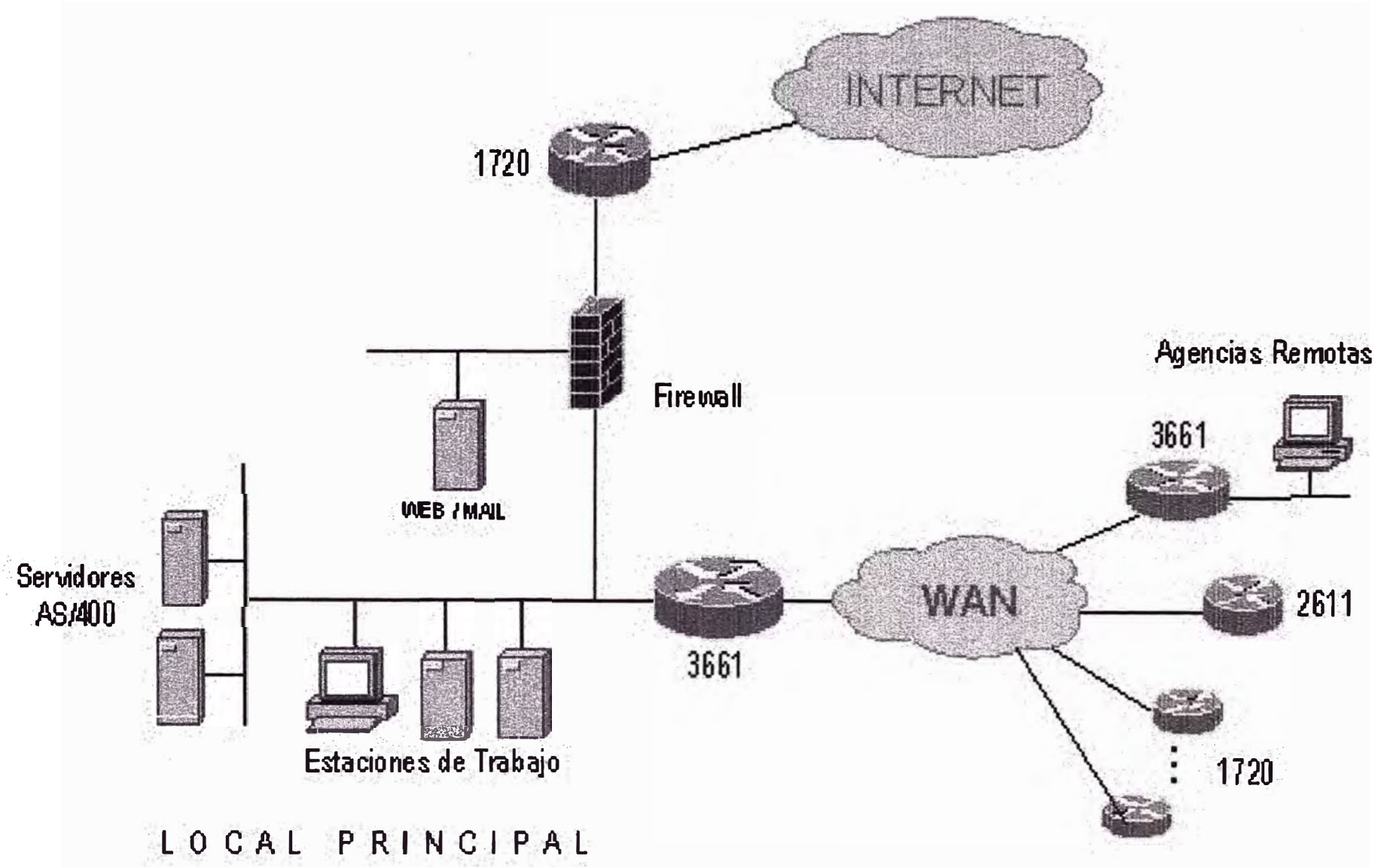


Fig. 2.9 Arquitectura de red de un Sistema Coorporativo

2.3 Proxies

Con los "Packet Filtering Firewalls" sólo es posible realizar filtrajes cuando los criterios están limitados a las direcciones y a los puertos. Una de las técnicas más usadas para resolver este problema son los proxies.

Los servidores proxy proporcionan el acceso a una red insegura para determinados protocolos de aplicación a través de un host con doble acceso. El programa del cliente se comunica con el servidor proxy en lugar de hacerlo directamente con el servidor real situado en la red insegura. El servidor proxy es el encargado de evaluar las solicitudes del cliente y decide cuáles deja pasar y cuáles no. Si una petición es aceptada, el proxy se comunica con el servidor real en nombre del cliente (el término proxy significa representante) y lleva a cabo las peticiones de servicio del cliente al verdadero servidor y transmite las respuestas de éste de nuevo al cliente. Es importante realizar las conexiones a través de un proxy junto con algún método de restricción de tráfico IP entre los clientes y los servidores en la red insegura, como un router con filtrado de paquetes o un host con doble acceso que no enrute paquetes. Si hay conectividad a nivel IP entre clientes y servidores de la red insegura, los clientes pueden saltarse el servidor proxy y producirse ataques desde el exterior.

Ventajas de los servidores proxy

Acceso directo a la red externa: Si se utiliza la arquitectura de host con doble acceso, un usuario debe iniciar una sesión con el host antes de utilizar cualquier servicio de la red exterior, algo que resulta molesto para la mayoría de usuarios. Al utilizar un servidor proxy, los usuarios pueden conectarse de una forma más o menos transparente a un servidor de la red externa de forma directa sin que se den cuenta que están pasando por una máquina intermedia, el servidor proxy. No obstante, esto requiere re-configuraciones en los programas cliente (navegador HTTP, cliente FTP, etc.).

Logging del sistema: Gracias a que los servidores proxy trabajan a nivel de aplicación resulta fácil generar logs o monitorizar las conexiones de los usuarios a cada tipo de servicio de forma cómoda sin tener que profundizar a nivel IP.

Desventajas de los servidores proxy

Disponibilidad de servidores para nuevos servicios: Debido a que es necesario un servidor proxy específico para cada tipo de servicio esto resulta bastante problemático a la hora de utilizar servicios de reciente aparición. Aunque existen servidores proxy para la gran mayoría de servicios (HTTP, Telnet, FTP, SMTP, etc.) el administrador de red puede encontrarse en la necesidad de utilizar un nuevo servicio para el cual todavía no se ha creado ningún proxy.

Dependencia del servicio: Puede ser necesario utilizar un servidor proxy exclusivo para cada protocolo. La instalación, configuración y administración de varios servidores puede requerir mucho trabajo. También existen servicios para los cuales difícilmente existirá alguna vez un servidor proxy. Son servicios como talk con interacciones complicadas y desordenadas entre cliente y servidor.

Modificaciones en los clientes: La utilización de un servidor proxy requiere la modificación o configuración de los clientes. Esto requiere tiempo y trabajo. Los navegadores HTTP de última generación incluyen la opción centralizada de configuraciones para proxy. Desde un puesto de trabajo, el administrador pueda cambiar la configuración en lo que respecta a servidores proxy de todos los clientes de forma automatizada.

Tipos de Servidores Proxy:

- Servidores proxy a nivel de aplicación y a nivel de circuito. Un proxy a nivel de aplicación conoce la aplicación o servicio específico para el cual está proporcionando los servicios de proxy, es decir, comprende e interpreta los comandos en el protocolo de aplicación. Un proxy a nivel de circuito crea un circuito entre el cliente y el servidor sin interpretar el protocolo de aplicación. Normalmente se utiliza con aplicaciones como SMTP, que implementa un protocolo de guardar y enviar. La versión más avanzada de un proxy a nivel de circuito actúan como proxy para el exterior pero como enrutador con filtrado para el interior. En general, los proxy a nivel de aplicación emplean procedimientos modificados y los proxy a nivel de circuito clientes modificados. Esto se

relaciona con los aspectos prácticos del proxy. Un proxy a nivel de aplicación obtiene la información necesaria para conectarse al servidor exterior del protocolo de aplicación. Un proxy a nivel de circuito no puede interpretar el protocolo de aplicación y necesita que le proporcione la información a través de otros medios (por ejemplo, mediante un cliente modificado que le dé al servidor la dirección de destino). La ventaja de un proxy a nivel de circuito es que proporciona servicios para una amplia gama de protocolos. La mayoría de los servidores proxy a nivel circuito también son servidores proxy genéricos; pueden adaptarse para servir casi a cualquier protocolo. No todos los protocolos pueden manejarse fácilmente por un proxy a nivel de circuito. Los protocolos como FTP, que comunican datos del puerto cliente al servidor, necesitan cierta intervención a nivel de protocolo y, por lo tanto, ciertos conocimientos a nivel de aplicación. La desventaja de un servidor proxy a nivel circuito es que proporciona muy poco control sobre lo que circula a través del proxy. Al igual que un filtro de paquetes, controla las conexiones con base en su fuente y destino y no puede determinar fácilmente si los comandos que están pasando a través de él son seguros o están en el protocolo esperado. Un proxy a nivel de circuito es fácilmente engañable por servidores instalados en los números de puerto asignados a otros servidores.

- Servidores proxy genéricos y dedicados: Un servidor proxy dedicado funciona para un único protocolo, mientras que uno genérico sirve para varios protocolos. En la práctica los servidores proxy dedicados son a nivel de aplicación y los genéricos son a nivel de circuito.

- Servidores proxy inteligentes: Se denomina servidor proxy inteligente a aquellos que son capaces de hacer algo más que transmitir peticiones como por ejemplo funciones de cache de datos (páginas web, ficheros de FTP, ...). A medida que se consoliden los servidores proxy sus habilidades se irán incrementando de forma rápida. Generalmente los servidores proxy inteligentes son dedicados a aplicación. Un servidor proxy a nivel de circuito tiene habilidades limitadas.

2.4 Redes Privadas Virtuales (VPN)

Las redes privadas virtuales crean un túnel o conducto dedicado de un sitio a otro. Los firewalls permiten una conexión segura a través de Internet. Las VPNs son una alternativa

de costo útil, para usar líneas alquiladas que conecten sucursales o para hacer negocios con clientes habituales. Los datos se encriptan y se envían a través de la conexión, protegiendo la información y el password. La tecnología de VPN proporciona un medio para usar el canal público de Internet como un canal apropiado para comunicar los datos privados. Con la tecnología de encriptación y encapsulamiento, una VPN básica, crea un pasillo privada a través de Internet. Instalando VPNs, se consigue reducir las responsabilidades de gestión de una red local.

Modo de trabajo de las VPN

Las redes privadas virtuales pueden ser relativamente nuevas, pero la tecnología de túneles está basada en estándares preestablecidos. La tecnología de túneles - Tunneling- es un modo de transferir datos entre 7 redes similares sobre una red intermedia. También se llama "encapsulación", a la tecnología de túneles que encierra un tipo de paquete de datos dentro del paquete de otro protocolo, que en este caso sería TCP/IP. La tecnología de túneles VPN, añade otra dimensión al proceso de túneles antes nombrado -encapsulación-, ya que los paquetes están encriptados de forma de los datos son ilegibles para los extraños. Los paquetes encapsulados viajan a través de Internet hasta que alcanzan su destino, entonces, los paquetes se separan y vuelven a su formato original. La tecnología de autentificación se emplea para asegurar que el cliente tiene autorización para contactar con el servidor. Los proveedores de varias firewall incluyen redes privadas virtuales como una característica segura en sus productos.

Redes privadas virtuales dinámicas - Dynamic Virtual Private Networks (DVPN)

Basadas en la tecnología de Internet, las intranets, han llegado a ser una parte esencial de los sistemas de información corporativos de hoy en día. Sin embargo, Internet no fue diseñada, originalmente, para el ámbito de los negocios. Carece de la tecnología necesaria para la seguridad en las transacciones y comunicaciones que se producen en los negocios. Se presenta, un tema peliagudo en los negocios: ¿Cómo establecer y mantener la confianza en un entorno el cual fue diseñado desde el comienzo, para permitir un acceso libre a la información? Para decirlo de otro modo: ¿Cómo conseguir seguridad en una intranet sin

chocar con los principios básicos de Internet sobre la flexibilidad, interoperatividad y facilidad de uso?.

A diferencia de una VPN tradicional que ofrece seguridad limitada e inflexible, una VPN dinámica proporciona ambos extremos, con altos niveles de seguridad, e igualmente importante es que proporciona la flexibilidad necesaria para acoplarse dinámicamente a la información que necesitan los distintos grupos de usuarios. Las VPNs dinámicas, pueden ofrecer esta flexibilidad porque están basadas en una misma arquitectura así como pueden proporcionar otras ventajas. Una VPN dinámica es una habilitadora de intranet. Habilita que una intranet ofrezca más recursos y servicios que de otra forma imposibilitaría al mundo de los negocios a hacer mayor uso de los recursos de información.

Potencial de una Red Privada Virtual Dinámica

Una VPN dinámica, permite que los negocios extiendan sus comunicaciones, y que el acceso a la información se produzca en un entorno agradable, versátil y controlado. En vez de estar diseñando engorrosas pantallas de usuario con las conocidas limitaciones y con esquemas de seguridad inflexibles, una VPN dinámica ha sido diseñada para proporciona el más alto nivel de libertad dentro de un entorno seguro, consiguiendo que el mayor número de usuarios pueda realizar su trabajo con la mayor cantidad de información posible

2.5 Protocolo SSL

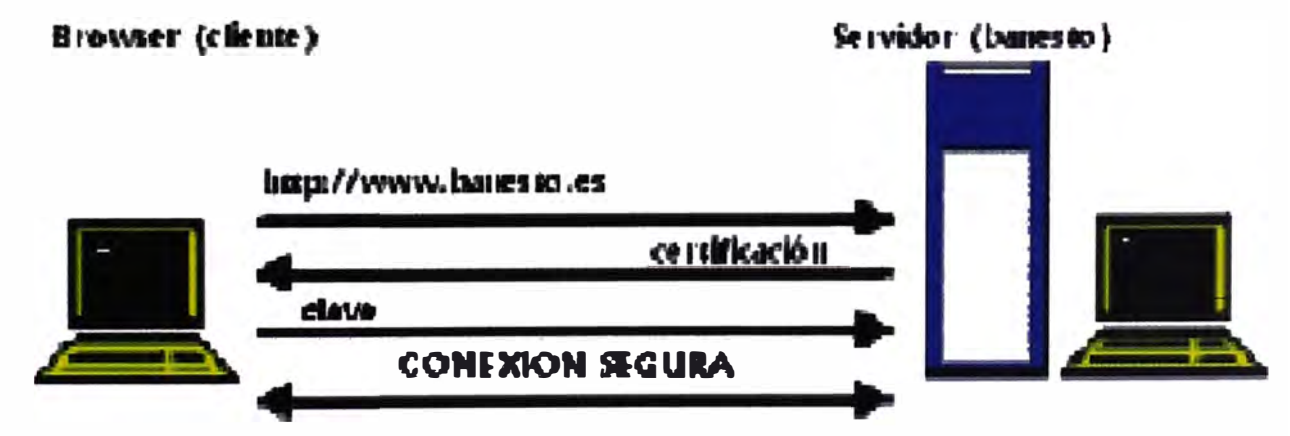


Fig. 2.10 Establecimiento de una conexión segura

Cuando transmitimos datos mediante HTTP se establece una comunicación entre un cliente y un servidor. Para realizar transacciones seguras el protocolo más utilizado hoy día es el SSL (Secure Sockets Layer) que impone la certificación del servidor, conociéndose como servidor seguro. Este protocolo encripta los datos transferidos mediante HTTP. Un servidor seguro funciona de la siguiente forma:

Un cliente accede a la dirección del web seguro a través de la URL correspondiente. Una vez establecida la conexión, el visualizador solicita una conexión segura. Si el servidor a que se accede es un servidor seguro, responderá afirmativamente a la solicitud, enviándole un certificado electrónico de tipo RSA. Tras recibir este certificado, el visualizador lo desempaquetará con la clave de la autoridad de certificación, ya integrada en el software, obteniendo de este modo la clave según el algoritmo RSA. Por último, el cliente genera una clave de encriptación simétrica según el algoritmo RC4 y se la envía encriptada al servidor (con su clave pública). A partir de este momento, tanto el cliente como el servidor pueden establecer una comunicación segura basada en esta clave simétrica, que ambos, y sólo ellos conocen. Las claves simétricas son generadas aleatoriamente en cada sesión, por lo cual no hay posibilidad de que éstas sean conocidas por eventuales hackers.

Un factor importante en la seguridad es quién tiene acceso a nuestros datos de cuentas bancarias, ya que si la tienda on-line se quedara con los números de la tarjeta de crédito podrían darse fraudes. Para evitar este fenómeno la mayoría de las tiendas dejan que la entidad bancaria realice toda la transacción, desde la captación de datos hasta la transacción en sí. Esto se consigue mediante una redirección https hacia la entidad bancaria. El proceso de compra on-line suele dividirse en dos etapas:

Introducción de datos personales no bancarios y comprobación del importe de la compra.
Introducción de datos bancarios (nº tarjeta de crédito)

La primera parte se realiza en la Web de la tienda, al principio no supone ninguna transacción crítica (aunque sería deseable que también fuera encriptada mediante SSL) y la segunda se realiza directamente en una página del banco.

TRANSACCIONES SEGURAS: SET: Los servicios financieros electrónicos: servicios de compras, de crédito, debito o prepago (monedero electrónico), gestión de activos o banca electrónica exigen transacciones seguras a través de Internet. Actualmente está en fase de pruebas el sistema SET (Secure Electronic Transaction) que regirá las transacciones a través de Internet en un futuro no muy lejano.

SET: Solucionando los problemas de SSL: Aparece una figura muy importante en el contexto de la autentificación: la autoridad certificadora, que expide certificados electrónicos que autentifican que el propietario de la tienda on-line (en general, cualquier web site segura) es quien dice ser y esta dentro del contexto legal del comercio electrónico. Además, el protocolo SSL utiliza un sistema de encriptación asimétrica y simétrica, encriptando tanto la comunicación tienda-cliente como cliente - tienda. El protocolo SSL ofrece un alto nivel de seguridad pero puede mejorarse.

El protocolo SET (Secure Electronic Transaction) ofrece mecanismos de seguridad para las transacciones con tarjetas de pago en redes abiertas, ofreciendo un nivel de seguridad superior a SSL solucionando todos sus problemas. Este protocolo ha sido desarrollado por VISA y Mastercard, con la ayuda de otras importantes compañías como IBM, Microsoft, Netscape, RSA, Terisa y Verisign, entre otros. El protocolo SET usa técnicas criptográficas a fin de ofrecer confidencialidad de la información, asegurar la integridad de los mensajes de pagos y autentificar tanto a los titulares de las tarjetas como a los vendedores. Estas son las características de SET:

Ofrece confidencialidad de la información de los medios de pago así como de la información de los pedidos mediante el cifrado de todos los mensajes intercambiados usando algoritmos de clave simétrica y asimétrica.

Garantiza la integridad de todos los datos transmitidos gracias al uso de firmas digitales.

Ofrece autentificación de que el poseedor de la tarjeta es un usuario legítimo de una cuenta asociada a dicha tarjeta de pago, usando firmas digitales y el certificado del titular de la tarjeta.

Ofrece autentificación de que un vendedor puede aceptar transacciones con tarjetas de pago gracias a su relación con una institución financiera, usando para ello firmas digitales y el certificado del vendedor.

Utiliza un protocolo que no depende de otros mecanismos de seguridad de transporte, así como tampoco evita su utilización.

Actualmente parece complicado predecir cuando funcionará SET debido que las previsiones no se cumplen, fundamentalmente por problemas técnicos, logísticos y de universalidad. Son tantos los agentes que intervienen en el proceso SET que dificulta la integración de todos ellos y por encima de todo, existe un problema fundamental: la cultura informática y de seguridad. Posiblemente para comercio electrónico empresa-empresa, SET tenga un éxito indiscutible.

CAPÍTULO III
SISTEMAS DE SEGURIDAD A NIVEL DE COMUNICACIONES

3.1 Seguridad en los Servidores Web

El web es construido desde un programa especialmente escrito llamado Web server que hace información disponible en la red. Otros programas llamados Web Browser, pueden ser usados para accesar información que es almacenada en los servidores y desplegada en las pantallas de los usuarios. La gran telaraña mundial como se le conoce al World Wide Web (WWW) fue desarrollado originalmente como un sistema para físicos e intercambio de papeles pertenecientes a sus investigaciones físicas. Otro uso de la Web hoy día involucra poner programas detrás de la páginas Web. Los programas son creados con un protocolo llamado el Common Gateway Interface (CGI). Los script de CGI pueden ser enteramente simple, por ejemplo, un contador que se incremente cada vez que una persona mira la página, o compra un libro que permita a las personas señalarlas en el sitio. O ellos pueden ser completamente sofisticados. Por ejemplo, el paquete de servicio ofrecido por FedEx permite al cliente el uso de servicios de compañías de World Wide Web (http//www.fedex.com) para trazar paquetes. Dándole al cliente acceso a estas computadoras, en esta manera simultáneamente FedEx salva dinero y da al cliente un mejor servicio. Muchas otras compañías están explotando el uso de WWW para el comercio electrónico. Los clientes despliegan catálogos de mercancías y servicios, seleccionan artículos y luego pagan por ellos sin ninguna otra cosa más que un formulario idóneo desplegado. El WWW es uno de lo más excitantes usos de la Internet. Pero así mismo posee profundos retos de seguridad. En orden de importancia, estos retos son:

1. Un atacante puede tener ventajas de cosas en el servidor Web o en los script CGI al ganar acceso no autorizado a otros archivos en su sistema, o igualmente tomar el control en su computadora.

2. La Información confidencial que está en su Servidor Web puede ser distribuida a individuos no autorizados.
3. La Información Confidencial transmitida entre el Servidor Web y el browser puede ser interceptada.

4. Algunas cosas en su Web browser (o características que usted no está informado) pueden permitir información confidencial en su Web cliente y ser obtenida desde un servidor Web malicioso.

5. Porque de la existencia de estándares y tecnología patentada, algunas organizaciones han encontrado esto necesario al pagar especialmente licencias de software.

Cada uno de estos cambios requieren de nuestra responsabilidad. Desafortunadamente, algunas de estas soluciones que son actualmente empleadas son contradictorias. Por ejemplo, el mínimo riesgo de ser detectado, en muchas organizaciones tienen que pagar seguros por el servicio de WWW, los cuales implementan una gran variedad de protocolos de encriptamiento. Pero esos servicios requieren de un certificado firmado digitalmente para operar, y el certificado debe ser renovado cada año. Consecuentemente, organizaciones que dependen de esos servicios de WWW están expuestos a una interesante negación de servicios contra ataques.

Configuración de archivos

Dentro de la configuración de directorios, el servidor tiene los siguientes archivos:

Access.conf Controla el acceso a los archivos del servidor Httpd.conf Configuración de archivos para el servidor Mime.conf Determina el mapeo de la extensión de los archivos tipo mime

Srm.conf Los recursos de mapeos del servidor. Estos archivos contienen más información de la configuración del servidor. La información en estos archivos pueden ser usados para arruinar el sistema entero del servidor, el administrador del sistema podría proteger los scripts de manera que estos puedan ser leídos y modificados por el usuario.

Configuraciones adicionales

El seteo de permiso que el administrador del sistema podría habilitar y deshabilitar las siguientes opciones:

- Listado de directorio automático: Servidor Web podría listar automáticamente un directorio si es llamado el archivo con index.html este no se presenta en el directorio. Esto puede causar problemas de seguridad y causar vulnerabilidad en su sistema.

- Siguiendo enlaces simbólicos: Algunos servidores permiten enlaces simbólicos fuera del servidor Web. Estos permite que alguien tenga acceso al árbol del servidor para hacer otros documentos en el computador habilitándolo para el acceso al Web. Alternativamente el administrador podría setear el servidor Web con la opción de los enlaces "If Owner Match".

- Lados del Servidor incluidos: Los lados del servidor incluyen directorios que pueden ser incluidos en el documento html. Los incluidos son procesados por el servidor HTML antes de que el documento sea enviado a un requerimiento del cliente.

3.2 Seguridad en el Servidor de Correo Electrónico

Se sabe que el correo electrónico al que cada vez más recurrimos, viaja por la red de forma libre y es susceptible de ser visto y manipulado durante el recorrido que hace hasta llegar a su destinatario.

El correo electrónico de Internet es un medio poco seguro y se presta a suplantación de personalidad, errores y manipulación no deseada, por lo cual: A partir de la fecha se debe tomar la firme determinación de enviar todos los mensajes de correo electrónico con firma digital por ejemplo PGP (Pretty Good Privacy). Se debe considerar fundamental esta medida para salvaguardar la identidad en la red de redes.

Fundamentos teóricos de PGP

Desde su aparición en 1991, PGP (Pretty Good Privacy) se ha convertido en una de las herramientas más utilizadas a nivel mundial para conseguir privacidad y autenticación tanto en los mensajes de correo como en los archivos almacenados en el disco duro del ordenador. A ello ha contribuido indudablemente su distribución como herramienta gratuita, así como su puesta al día en las sucesivas versiones aparecidas mejorando los algoritmos criptográficos utilizados. El PGP nos permite dos cosas:

1. Cifrado de mensajes: Para cifrar los mensajes y archivos, PGP recurre al empleo de los dos tipos de cifrado existentes: simétrico y asimétrico. El cifrado convencional de clave única o cifrado simétrico utiliza la misma clave para cifrar y para descifrar. Esto presenta el inconveniente de la distribución de esta clave a los receptores a través de un canal que consideramos inseguro. Este problema se soluciona con el cifrado de clave pública, que emplea dos claves distintas para el cifrado y el descifrado. ¿Por qué recurrir a un método combinado? El cifrado de clave pública es mucho más lento que el de clave secreta. Lo que hace mucho más eficiente emplear el procedimiento siguiente:

- Establecer una clave secreta de sesión (que será distinta cada vez).

- Cifrar el texto llano con la clave secreta.

- Cifrar la clave de sesión con la clave PÚBLICA del destinatario.

En el cifrado simétrico los algoritmos ofrecidos por PGP son CAST CAST, Triple-DES e IDEA IDEA. Todos trabajan con bloques de 64 bits de texto llano y cifrado. Las claves CAST e IDEA tienen un tamaño de 128 bits, mientras Triple-DES usa una clave de 168 bits (aunque su longitud efectiva viene a ser de 112 bits). El algoritmo por defecto en la versión 6.5 es el CAST CAST, mientras en las versiones más antiguas de PGP es el IDEA IDEA. En cuanto al cifrado asimétrico el algoritmo por defecto es el DSS, aunque esta la versión que vamos a utilizar es también compatible con el cifrado RSA, empleado en las versiones más antiguas de PGP.

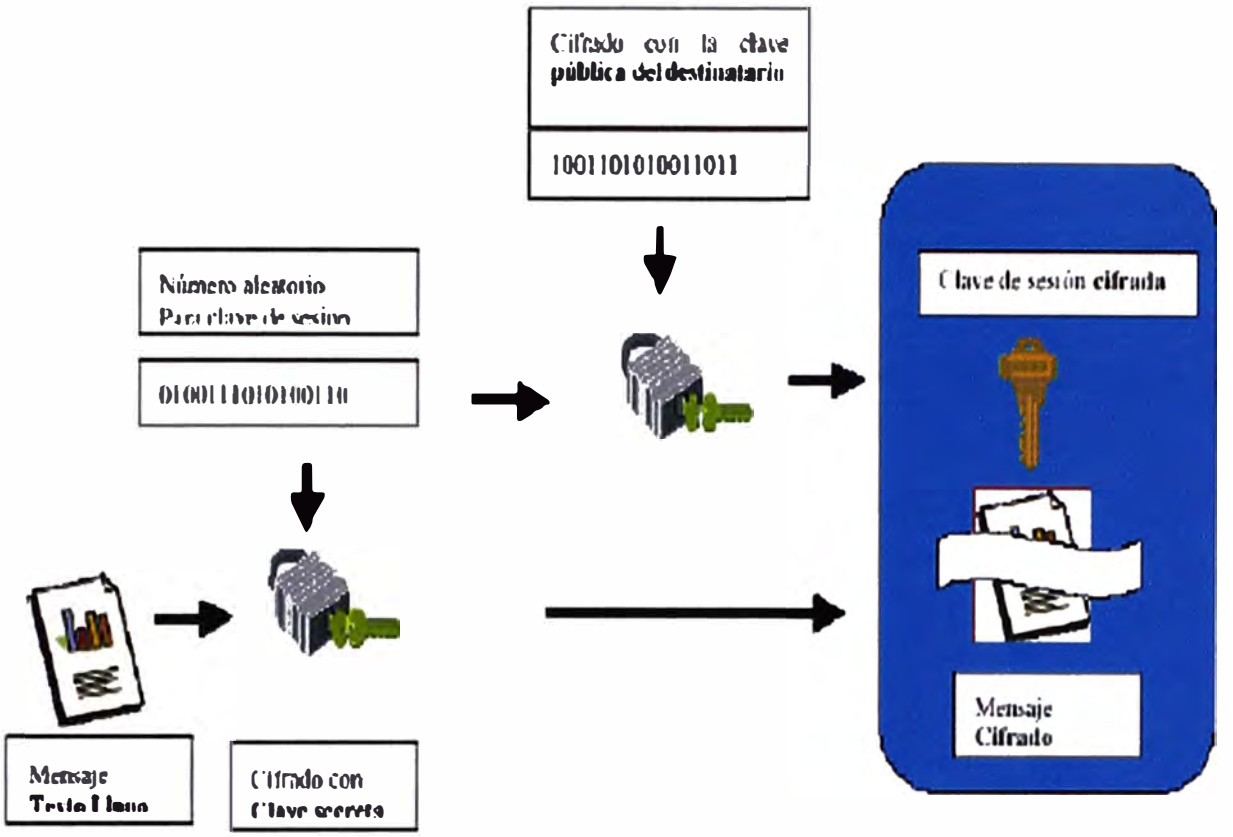


Fig. 3.1 Esquema del proceso de cifrado mediante PGP

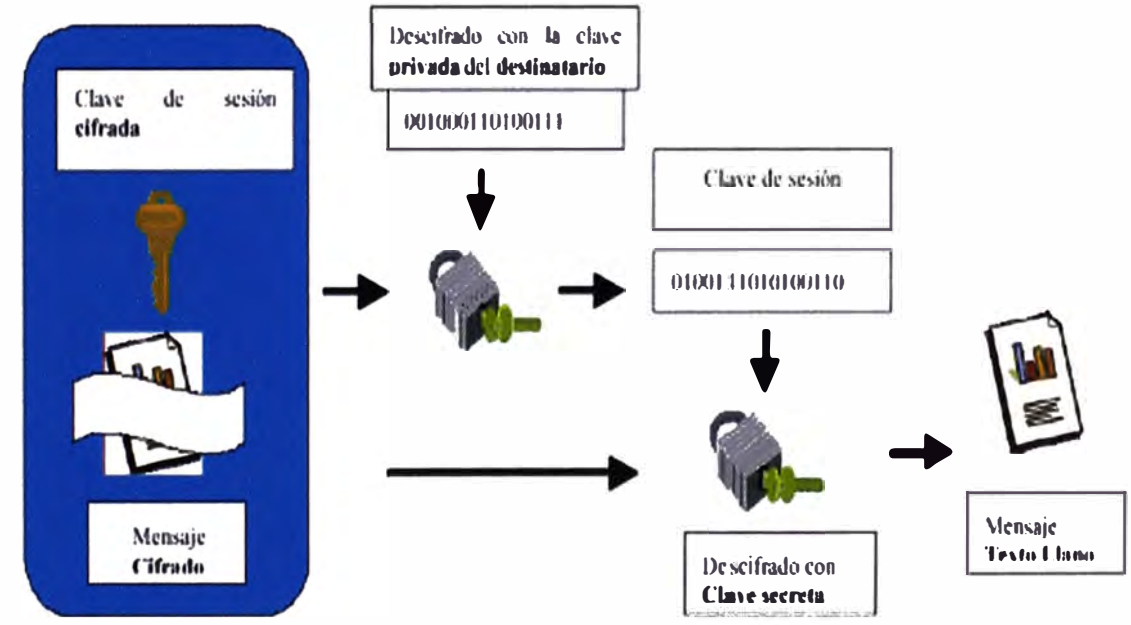


Fig. 3.2 Recuperación de la información por parte del destinatario

2. Firma digital de mensajes: Para la firma digital de un mensaje se llevan a cabo los siguientes pasos:

Obtener primero un resumen del mensaje, mediante una función de mezcla.

Cifrar el resumen del mensaje con la clave privada del firmante.

El algoritmo empleado para la función de mezcla es el SHA (Secure Hash Algorithm), que proporciona un resumen de mensaje de 160 bits, frente a versiones más antiguas de PGP que utilizaban el MD5.

3.3 Seguridad en el Servidor de Archivos.

Para proteger su información debe sentarse y analizar cuales son los requisitos de acceso necesarios para los usuarios remotos. Debe eliminar todo tipo de accesos y permisos por defecto que dicha información tenga. Los sistemas operativos establecen permisos muy amplios para la información nueva que se crea en el sistema. Una vez creada debe limitarle los permisos. Un plan de seguridad consiste en definir los modos de uso apropiado de las redes de datos de la institución, al mismo tiempo que define procedimientos para detectar y responder a los problemas de seguridad que se presenten. Es muy importante que los controles que se hagan y los procedimientos que se utilicen, dentro del plan de seguridad, sean ante todo prácticos.

Con esto quiere decir, que cualquier procedimiento o plan de seguridad que no se adapte a la forma de trabajo de la institución, es inútil. De la misma forma si obligamos a realizar engorrosos controles a los usuarios, acabarán por no realizarlos y el plan de seguridad deberemos tirarlo a la basura o lo que es peor, abriremos agujeros de seguridad nosotros mismos. Lo primero que se debe considerar es qué deseamos proteger y en que grado. Esta es posiblemente la tarea más compleja puesto que requiere tomar decisiones importantes y que afectarán de forma determinante al resto de los puntos que vamos a ver. Desgraciadamente el presupuesto influye de manera decisiva en la seguridad, y es este punto el cual se debe considerar. Una protección muy efectiva puede resultar muy costosa, y una solución más económica puede tener alguna carencia de seguridad. El objetivo es

poner el mayor número de trabas posibles y de obtener una gran cantidad de información sobre las actividades que se desarrollan en el servidor. El servidor tendrá dos tipos de usuarios: internos y remotos. En este punto debemos distinguir que el tipo de acceso al servidor es mediante nombre de usuario y contraseña.

Protección con Claves de Acceso: El sistema de autenticación comúnmente utilizado en nuestros días es a través de claves de acceso o contraseñas. Bajo este esquema, el usuario selecciona una clave de un número determinado de caracteres, lo guarda en memoria, y posteriormente lo escribe para obtener acceso a una red de computadoras. La mayoría de los sistemas suprimen los caracteres que escribe el usuario de manera que no se vea en pantalla la clave de acceso la medida que se escribe. Este esquema de protección a través de claves de acceso tiene muchas debilidades. El usuario suele elegir claves de acceso que son fáciles de recordar, tal como el nombre de su perro, un familiar o el número de las placas de su vehículo. Alguien que conozca al usuario puede intentar la entrada al sistema usando como clave los cosas que sean conocidas al propietario de la clave (el nombre de la esposa, los hijos, etc).

Las cuentas de los 'administradores' son también propensas a ser invadidas por los usuarios. Esto se debe principalmente a que una cuenta de administrador tiene casi todos los derechos y privilegios sobre la red. Muchos administradores de redes se consideran eximidos del problema de la seguridad, por lo que no ponen mayor empeño en mantener sus cuentas secretas, e inclusive la comparten con algún colega en caso de ausencia en su sitio de trabajo o para compartir tareas administrativas de la red.

¿Cómo proteger las claves de acceso? A continuación mostramos algunas reglas sencillas para proteger las claves de acceso o las contraseñas:

Requerir que todos los usuarios tengan una contraseña. Algunos administradores generan cuentas de usuario pero no le asignan una clave al mismo. Esto es bastante popular en instalaciones pequeñas donde asocian a una cuenta de usuario con un cargo dentro de la organización y no con un usuario.

No dejar las claves por defecto que poseen algunos sistemas operativos de redes, como por ejemplo, las claves del usuario GUEST (invitado). Algunos sistemas operativos de redes no poseen clave para estos usuarios.

No escribir la clave de acceso en ningún sitio, sobre todo cerca de su estación de trabajo. Muchas personas inescrupulosas buscan esas claves donde sea, inclusive debajo del teléfono.

No teclear la clave de acceso mientras hay otras personas observándolo. Muchas personas simulan haberse equivocado mientras escriben su contraseña, para escribirlo una vez mas y confundir así a cualquier observador.

Si usted supone que alguna persona ha visto su contraseña, cámbiela a la mayor brevedad posible, No compartir su clave de acceso con mas nadie, dentro o fuera de la institución.

Cómo seleccionar su contraseña: En la mayoría de los casos, la red debe ser configurado para que los usuarios puedan cambiar sus claves tantas veces como lo deseen. De no ser así, es razonable desconfiar hasta del propio administrador del sistema. Después de todo, el administrador de la red, quien es un usuario mas dentro de la organización no tiene por qué conocer las claves de todo el personal, así como un gerente de un banco no debe conocer los códigos del cajero automático de todos sus clientes. En caso de fraude, adivinen quién es el primer sospechoso.

Algunas de las reglas internacionalmente populares para elegir una buena clave de acceso son:

Evitar claves de acceso que sean nombres de personas o animales, especialmente si son de su núcleo familiar.

Elegir contraseñas que no sean palabras tomadas de un diccionario. Es muy sencillo hacer un programa que, basado en un diccionario, pruebe todas y cada una de las palabras del diccionario hasta alcanzar con la clave.

Las mejores contraseñas son aquellas que combinan letras y números, mas que aquellas conformadas solo por letras o números. Evite claves tales como números telefónicos, fechas de nacimiento y el número de la cédula de identidad.

Inventar contraseñas que sean relativamente largos, con mas de ocho (8) caracteres. Las contraseñas cortas son vulnerables a ser encontradas si se consiguen la combinación correcta. Es mas fácil conseguir la clave con las letras AB ('AB', 'BA', 'Ab', 'aB', 'Ba', 'bA', 'ab', 'ba') que con los caracteres 3D*H4$1jQE (inténtelo usted mismo)

No usar como contraseñas los nombres de las máquinas o de los servidores a los cuales se encuentra registrado.

Use una combinación de palabras cortas, caracteres especiales y números. Un ejemplo pudiera ser: KFE-LECHE, o JOATLANTA96, etc.

Evitar contraseñas sin sentido que puedan olvidarse, como por ejemplo: ^TY*ER$ME8P, la cual es sumamente segura pero bastante difícil de recordar.
Para recordar claves de acceso, utilice contracciones de palabras tales como: "Barlovento, Tierra Ardiente y del Tambor" puede ser B^TAYDT, o "Quiero ser Millonario" puede ser "IWANNAB$$"
Elegir claves de acceso que sean pronunciables, tales como: "MIAMIGO8A", o "2KTIRAS"

3.4 Seguridad en los Servidores DNS

El servicio DNS (Domain Name System), es una amplio conjunto de bases de datos distribuida usado a lo largo de la internet, proporcionando correspondencia entre los nombres de host y las direcciones de IP de los mismos. Existe la posibilidad de abusar de este servicio para poder entrar en un sistema. Suposiciones durante la fase de autentificación, pueden conllevar serias grietas de seguridad importantes. El problema de seguridad es similar al que existe en el NIS. La autentificación se lleva a cabo en muchos casos a partir del nombre o la dirección. Las aplicaciones de alto nivel, usan en la mayoría de los casos los nombres para la autentificación, puesto que las tablas de direcciones son

mucho más difíciles de crear, entender y mantener. Si por ejemplo alguien quiere suplantar una máquina por otra no tiene más que cambiar una de las entradas de la tabla que relaciona su nombre con su dirección.

Este es el problema fundamental de DNS. Para conseguir esto una máquina debe obtener primero el número ID de la petición DNS, para ello debe construir el paquete de respuesta y usar la opción de enrutamiento de fuente, para hacerlo llegar al que llevó a cabo la petición.

Seguridad en Internet:

El crecimiento espectacular de Internet y el hecho de ser una red pública y abierta, pública en el sentido que, como el teléfono, todos la pueden usar y abierta, porque todos pueden enviar mensajes de la misma manera que lo hacemos con los servicios de correo, y también podemos recibirlos. No hay condiciones ni exigencias para usar Internet. La mayoría de los servidores y servicios disponibles no saben o no se preocupan de quienes son sus usuarios. No se piden ni la identificación ni la autorización. La Internet le puede proveer recursos ilimitados, pero también facilita la oportunidad de penetrar en su Centro Corporativo. Aquellos con malas intenciones (llamados "hackers") tienen oportunidades para visualizar, alterar, corromper o borrar la información confidencial de las empresas. Consecuentemente, la seguridad es un punto muy importante a considerar al planear su conexión a Internet. Por lo tanto si queremos aprovechar al máximo los recursos de Internet, pero necesitamos mantener un alto nivel de seguridad. Se debe encontrar una solución que entrega el correcto nivel de seguridad sin necesidad de restringir o reducir los beneficios ofrecidos por Internet. Los problemas de seguridad pueden venir tanto desde fuera como desde dentro de su organización. Cerrando puertas y ordenadores, especificando contraseñas y encriptación de mensajes, puede ser una forma de asegurar sus recursos. Pero con el acceso a través de Internet, los intrusos no necesitan tener un acceso físico a sus instalaciones.

CAPÍTULO IV
AUDITORIA DE SEGURIDAD DE LA INFORMACION

4.1 Concepto

La Auditoría a la Seguridad Informática es el proceso de verificación y control mediante la investigación, análisis, comprobación y dictamen del conjunto de medidas administrativas, organizativas, físicas, técnicas, legales y educativas, dirigidas a prevenir, detectar y responder a acciones que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información que se procese, intercambie, reproduzca y conserve a través de las tecnologías de información.

El desarrollo a pasos agigantados de los medios de comunicación, nos lleva a concluir en que los Sistemas Informáticos, con el paso de los años se han constituido en herramientas muy poderosas para la organización en un nivel empresarial, materializando conceptos que son completamente vitales, los cuales conforman los Sistemas de Información de las empresas, convirtiéndose a finales del último siglo en pilares fundamentales para el desarrollo empresarial en general. La gestión empresarial cumple un rol muy importante hoy en día, estando la informática involucrada en todos los procesos que se requieren para una buena gestión, es por ello que los aspectos normativos y estándares informáticos deben encontrarse en acorde a los establecidos. El "management" o gestión de la empresa se denomina así a la forma como las organizaciones están afrontando el mercado. La informática no es quien maneja las empresas, lo que sucede es que tiene un poder de decisión, pero no decide por sí misma. Y de acuerdo a como se tome su importancia dentro del ámbito empresarial, se da la existencia de la Auditoría Informática. Pero se ha podido advertir que el término de Auditoría ha tenido un uso incorrecto frecuentemente, ya que se encasillado en el concepto de evaluación el cual está equivocado, por que se considera que tiene un solo fin y es el de detectar errores y señalar las fallas. Con esto se determina que las causas de esto se deben a que se ha tomado la frase "Tiene Auditoría" como si el

significado de esta frase quisiera decir que en dicha entidad, antes de realizarse la auditoría, ya se habían detectado fallas. Realmente Auditoría tiene una concepción mucho más amplia, por que la auditoría es un examen crítico que se lleva a cabo con la finalidad de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad, etc.

Si nos remontamos al campo de la etimología veremos que auditoría viene del latín auditorius, proviniendo de aquí la palabra auditor, la misma que significa o que se refiere a aquel que tiene la virtud de oir. La Auditoría informática puede ser definida de diversas formas, y una de las definiciones que tienen la da el diccionario Español Sopena, el cual define a la auditoría como Revisor de Cuentas colegiado. Careciendo inicialmente de una definición clara por que no se explica el objetivo fundamental, es decir no se especifica labor del auditor, la cual es evaluar la eficacia y eficiencia. Si hacemos una investigación tratando de documentarnos con respecto al rol que cumple la auditoría entonces llegaremos a concluir en que esta actividad no es sólo una actividad mecánica, donde se apliquen conocimientos y procedimientos ya establecidos, sino que también es una actividad en la que el auditor realizará un análisis crítico, en el cual no implica que ya hayan existido fallas en la entidad auditada, y que la finalidad está en que se trata de evaluar y mejorar la eficiencia y eficacia de una entidad o en todo caso la sección que se está evaluando.

El objetivo de la Auditoría a la Seguridad Informática es detectar fisuras o puntos vulnerables en el sistema informático que pongan en riesgo la seguridad de la información y de las tecnologías empleadas para su procesamiento, como base para la elaboración de un diagnóstico.

Analizar las políticas de Seguridad Informática adoptadas en la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información que en ella se procesa.
Analizar y comprobar el funcionamiento y eficacia del Sistema de Medidas de Seguridad Informática implantado en la entidad.

Detectar fisuras o puntos vulnerables en el funcionamiento del Sistema Informático y el Sistema de Medidas de Seguridad que puedan propiciar causas y condiciones para la comisión de delitos.

Valorar la factibilidad del Sistema de Medidas de Seguridad, en correspondencia con la caracterización del Sistema Informático.

El objetivo principal de la Auditoría Informática es llegar a tener un control en la actividad informática, también se rige de la normatividad que rige los parámetros establecidos por la empresa y su cumplimiento, el análisis de la eficiencia de los sistemas informáticos, supervisión de la gestión de los recursos humanos informáticos y materiales. Los sistemas de información son recursos de vital importancia para las empresas de hoy, es entonces que el auditor tiene la responsabilidad de hacer que el uso de los recursos de la empresa se lleven en buena forma y correctamente. Cabe destacar que una Auditoría bien realizada es la que toma en cuenta a todas las instituciones de forma igual e importante, debido a que un ministerio, una universidad o una entidad pública deben ser consideradas de la misma manera tomándolas en su más amplio sentido. Y es que en todas estas entidades la informática es importante pues la utilizan para realizar la gestión de negocios en forma óptima con la finalidad de obtener los beneficios económicos y de costos deseados. De acuerdo a todo esto los sistemas de información están sujetos a un control permanente y se toman en cuenta tanto como los otros órganos de la empresa o entidad a la que se está haciendo la auditoría. El hecho de realizar una auditoría informática es importante debido a que las herramientas que se utilizan pueden definir o marcar la diferencia con respecto a la competencia o al momento en que se está viviendo. Algunos de los aspectos que deben ser considerados son:

El mal diseño de los sistemas puede ser muy perjudicial, por que puede traer consecuencias desastrosas para la organización debido a que las máquinas sólo acatan órdenes recibidas de forma irrefutable, y el modelamiento de las organizaciones se encuentra supeditada al buen funcionamiento de estas mismas, las cuales materializan los sistemas de información, entonces la empresa no puede permitir que el software y el hardware presenten falta de eficiencia por que va en contra de sus propios intereses. La sofisticación en los equipos informáticos han dado pie para que los centros de control de procesos sean los puntos en el blanco para la delincuencia, el espionaje, o para manifestaciones terroristas. Para esto la seguridad en Auditoría informática es importante. Todos sabemos que hasta las computadoras pueden tener fallas en la información elaborada y arrojar resultados erróneos, pero si es que dichos datos son igualmente erróneos. Esto se da frecuentemente

cuando las instituciones pierden de vista la naturaleza y calidad de la información que ingresan a sus sistemas de consulta, con el peligro de que otros sistemas que son independientes se vean afectados por este hecho, para este hecho la Auditoría de datos es la más recomendable.

La necesidad de realizar una auditoría informática es importante para las empresas, por que les permitirá conocer la capacidad que tienen, a nivel informático para poder afrontar sus necesidades más importantes.

4.2 Etapas para la realización de la Auditoría.

En esta etapa se planificará el trabajo a desarrollar, elaborando un cronograma con todos los pasos a realizar y los objetivos a lograr. La Auditoría a la Seguridad Informática se divide a su vez en tres etapas:

Investigación Preliminar

1. Conocer los objetivos y alcances del sistema de información establecido en la entidad objeto de auditoría.

2. Obtener la información necesaria sobre la caracterización (organización, recursos, personal, documentación existente sobre el objeto social, las dependencias y otros aspectos de interés a auditar).

3. Realizar una pormenorizada revisión de los resultados de auditorías informáticas y de seguridad anteriores o controles específicos de seguridad u otras actas o documentos, con el fin de obtener la mayor información en el menor tiempo posible sobre los principales problemas que han afectado esta entidad y que evidencien debilidades en el control interno.

4. Emplear el uso de cuestionarios para la recopilación de información, con el propósito de obtener una orientación general sobre la seguridad informática de la entidad.

5. Determinar los bienes informáticos más importantes para la entidad, de acuerdo a su costo beneficio.

6. Clasificación de los activos en función de su importancia y los problemas que trae a la entidad su revelación, modificación o destrucción.

7. Confeccionar tablas que permitan determinar dentro de los activos informáticos los riesgos existentes, ya sean de carácter, administrativos, organizativos, técnicos, legales o específicamente informáticos, que determinen la vulnerabilidad de los activos.
8. Obtener los manuales de explotación y de usuario de los sistemas de las áreas o dependencias y efectuar un examen pormenorizado de éstos, para conocer el sistema y la auditabilidad para la seguridad del mismo.

Verificación de la Seguridad Informática Aplicada.

Esta etapa consiste, en la revisión y comprobación del cumplimiento de las normas y procedimientos de seguridad informática de la entidad.

Se utilizarán los cuestionarios como Herramienta de Auditoría a la Seguridad Informática, con el fin de obtener una orientación general sobre este tema.

Comprobación con el empleo de Herramientas Informáticas.

Muchos de los problemas y retos de la Auditoría de la Seguridad Informática parecen estar aún sin resolver. Según avanza la tecnología informática también tienen que cambiar y desarrollarse las técnicas de auditoría apropiadas para un determinado sistema, resultando inefectivas en otro más sofisticado.

Para el desarrollo de este enfoque, el Auditor a la Seguridad Informática necesita comprender suficientemente el sistema completo, para que le permita identificar y evaluar sus características esenciales de control.

Existe una amplia variedad de paquetes generalizados de auditoría a la seguridad que ayudan a la realización de las mismas, además de los programas generalizados disponibles.

Muchos auditores diseñan sus propios procedimientos que se adaptan a las peculiaridades del sistema auditado.

Los diversos paquetes de programas de auditoría, entre los trabajos que llevan a cabo con más frecuencia, se encuentran, las muestras estadísticas, verificaciones matemáticas, examen de los riesgos, funciones de comparación, revisión analítica, chequeo de integridad de Base de Datos, etc.

4.3 Auditoría Interna y Auditoría Externa.

Existen dos tipos de auditoría, como se ve en el titulo de este párrafo, y estas son dos La Auditoría Interna y la Auditoría Externa, de las cuales en el caso de la Auditoría Interna es realizada con recursos humanos propios de la empresa, lo mismo sucede con los recursos materiales, pues todos estos pertenecen a la empresa auditada. Considerando que los empleado que realizan esta labor reciben una remuneración económica. La Auditoría es una actividad que existe por decisión propia de la empresa, es decir, que la empresa puede decidir en el momento en que esta labor puede ser disuelta.

En el caso de la Auditoría Externa el personal que debe realizarla es un personal que debe guardar afinidad a la empresa que es auditada, este tipo de Auditoría tiene más consideración debido a que tiene una mayor objetividad por existir un mayor distanciamiento entre el personal auditor y el personal auditado.

El caso de la Auditoría informática es ventajoso en vista de que puede ser realizada periódicamente, la cual puede ser incluida en el plan anual de trabajo realizando una revisión completa de los sistemas y los equipos de cómputo, es por ello que guarda cierta ventaja con la auditoría externa.

Esto permite también al personal auditado a poder adecuarse al plan de trabajo de la auditoría, y mucho más cuando las consecuencias de las recomendaciones crean beneficio laboral.

Es tarea del personal de informática de escuchar y orientar sobre las ventajas o desventajas técnicas que puedan existir y sobre los costos que pueda demandar un sistema.

Generalmente su opinión no tiene voto en las decisiones que se toman en la empresa pero si tiene voz para dar la opinión que sea más adecuada y así poder satisfacer las necesidades más apremiantes.

Todas las empresas desean tener un control sobre sus sistemas informáticos, necesitando también que su gestión esté adecuada a los procedimientos, que todo esto implica. Es por ello que esta necesidad se ve reflejada en la imagen del auditor interno informático.

Sólo las empresas grandes pueden contar con una oficina de auditoría, debido a que es costoso contar con este servicio permanentemente, es así que las empresas pequeñas acuden a la auditoría externa.
Pero cuando la empresa adopta por tener este servicio como auditoría interna, parte del personal informático pasa a formar parte de esta actividad.

Se puede dar que una institución que cuente con una oficina de auditoría interna solicite los servicios de una auditoría externa, debido a razones que pueden ser:

- La falta de capacidad técnica, para realizar la auditoría de materia especializada en gran cantidad.

Cruzar las informaciones emitidas tanto de la auditoría interna como de la auditoría externa, sobre todo con la emisiones internas de graves recomendaciones las mismas que pueden discrepar con la opinión general de la empresa misma.

- Esto puede servir como mecanismo protector ante la posibilidad de auditorías informáticas externas que hayan sido solicitadas por la empresa.

- La oficina de auditoría interna forma parte de la misma empresa pero es independiente del Departamento de Sistemas es por ello que es recomendable solicitar los servicios de una auditoría externa, lo cual permitirá tener una visión externa de la empresa.

Tanto la auditoría externa como interna, deberán estar libres de toda influencia política, debido a que pueden afectar gravemente la estrategia y política general de la empresa. La

oficina de auditoría puede actuar por decisión propia ya que es un órgano independiente de la empresa aún estando dentro de la misma, también actúa a solicitud de la dirección o de parte del cliente.

4.4 Alcance de la Auditoría Informática.

La auditoría informática actuará dentro de parámetros establecidos, es decir que se desarrollará en un entorno y límites determinados, y es complementada con los objetivos.

Estos límites deben estar claramente estipulados en el informe final, para que quede claro hasta donde puede llegar la auditoría y no solamente eso sino que hay materias fronterizas que pueden ser omitidas. Cuando estos puntos no son bien definidos, puede implicar el que esta no tenga éxito.

4.5 Razones para determinar la necesidad de una Auditoría Informática

Cuando existen síntomas de debilidad en la empresa, éstas acuden a las auditorías externas para poder determinar en donde están las falencias. Estos síntomas se pueden agrupar de la siguiente forma:

- Cuando existe Desorganización y descoordinación:

* Los promedios conseguidos no se habitúan a los estimados, por que los parámetros de productividad no son respetados y sufren un desvío.
* Los objetivos que la empresa persigue, no coinciden con los obtenidos.
* Esto puede darse debido a un cambio masivo de personal, o también por que un área tuvo una mala reestructuración, también puede deberse a una norma importante que haya sido modificada.
* Cuando hay insatisfacción del cliente y una mala imagen
* Cuando no hay capacidad de satisfacer las necesidades del cliente.
* Las fallas en hardware no son reparadas, ni se resuelven las incidencias en plazos establecidos y razonables, ocasionando un descontento en el usuario por sentirse abandonado.

* Los resultados periódicos no son entregados en los plazos establecidos. Las pequeñas imprecisiones pueden ocasionar que la información no refleje lo real y que la actividad que ejerce el usuario se vea afectada por este motivo.

- Debilidades Económico-Financieras:

* Elevación de costos de forma repentina y desmesurada.
* Cuando se da la necesidad de justificar las inversiones informáticas.
* Cuando se dan otras prioridades en el aspecto presupuestario.

Se da una evaluación de nivel de riesgos, la que contempla los puntos siguientes:

* Seguridad Lógica.
* Seguridad Física.
* Aspectos de confidencialidad.
* La continuidad en el servicio es importante. En ocasiones se considera más importante que los aspectos de seguridad.

Por lo general las empresas deben aplicar una política de Backups, la cual puedan resguardar la información en forma diaria, estos backups deberán ser en forma doble asegurándose que uno de ellos se encuentre dentro de la empresa y otro fuera de ella. Estos backups pueden estar guardados el tiempo que la empresa lo determine, de acuerdo a la periodicidad con la que van renovando sus backups.

1° Control de Entrada de Datos

La información obtenida será analizada para su compatibilidad con los sistemas, se debe tomar en cuenta los plazos establecidos para la entrega de los datos y la correcta entrega de la información a los entornos diferentes. También se tomará en cuenta que estos procedimientos se realicen de acuerdo a las normas vigentes.

2° Planificación y Recepción de Aplicaciones

Las normas de entrega de Aplicaciones por parte de desarrollo serán auditadas, comprobando su cumplimiento y su calidad.
Una forma de evaluar la información también es escogiendo una serie de muestras representativas de la documentación de las aplicaciones en explotación. Se hará las investigaciones pertinentes a fin de determinar sobre la anticipación de contactos con desarrollo para la planificación a medio y largo plazo.

3° Centro de Control y Seguimiento de Trabajos:

La producción diaria es un procedimiento al que se realizará un análisis exhaustivo. La explotación informática dará ejecución básicamente a procesos por cadenas o lotes sucesivos (Batch), o en tiempo real(Tiempo Real). Las aplicaciones de teleproceso se encuentran en permanente actividad limitando a las funciones de Explotación a vigilar y recuperar incidencias, y mientras esto sucede el trabajo Batch absorbe una buena parte de los efectivos de Explotación. Aquí se determina el éxito de la explotación, debido a que este se considera uno de los artífices en el mantenimiento de la producción.

Batch y Tiempo Real

Aplicaciones Batch, son un tipo de aplicación que carga mucha información en el transcurso del día, durante la noche corre un proceso, el cual relaciona a la información en general, también lo que hace es calcular cosas y obtener como salida alguna acción. Entonces lo que hace es sólo recaudar información sin que sea procesada, es decir que solamente se trata de un tema Data Entry, el cual recolecta la información y corre el proceso batch(por lotes), este realiza posteriormente cálculos para comenzar a trabajar el día siguiente. En cambio lo que sucede con las aplicaciones que son Tiempo Real, es que estas procesan la información inmediatamente después de ser ingresada devolviendo el resultado en el preciso instante.

Operación, Salas de Ordenadores.

Las relaciones que unen a las personas y la conexión lógica que existe de cargos y salarios serán estudiadas, también se verá si es que la distribución de turnos es equitativa. Cada turno de trabajo estará bajo el cargo de un responsable de sala. Los Manuales de Operación son importantes, así como su utilización, también los comandos y su grado de automatización serán analizados con el fin de despejar dudas acerca de su buen funcionamiento. Los planes de formación deben ser analizados, además estos deben ser cumplidos también es importante que se cumpla el tiempo transcurrido para cada operador, desde le tiempo en que recibió el último curso. Se verificarán los montajes diarios y por horas de cintas o cartuchos, luego el tiempo que transcurre a solicitud de montaje por parte del sistema hasta el montaje real. Serán verificadas las líneas de papel impresas día a día y en las horas de impresión, así también la manipulación de papel que este implica.

Control de Red y Control de Diagnosis

Existe un centro de control de red, el cual se encuentra siempre ubicado dentro del área de producción Explotación.

Este centro dedica sus funciones exclusivamente al entorno de las comunicaciones, se relaciona mucho con el Software de Comunicaciones de Técnicas de Sistemas.

La fluidez en cuanto a la relación y el grado de coordinación entre ambos debe ser analizado. La existencia de un punto equidistante será estudiada, desde donde sean perceptibles todas las líneas que se encuentren asociadas al sistema.

En cuanto al Centro de Diagnosis, aquí se atienden llamadas de los usuarios clientes, quienes se ha averiado o han sufrido alguna incidencia, tanto en Software como en Hardware. Este centro es para informáticos grandes con usuarios dispersos en un territorio amplio. El Centro de Diagnosis es uno de los que más ayuda a disponer la configuración de la imagen de la informática de la empresa. La auditoría debe tomar este punto de vista. Desde el punto de eficacia y eficiencia del usuario en cuanto al servicio que recibe. La verificación de la eficiencia técnica del centro no es suficiente, por que será necesario un análisis simultáneo, en el entorno del usuario.

CONCLUSIONES

1. La seguridad de las redes de comunicaciones, y concretamente de Internet, evoluciona a pasos agigantados cada minuto que transcurre. Nuevas vulnerabilidades y utilidades, tanto para explotarlas como para combatirlas, son distribuidas públicamente en la red. La información disponible al respecto es inmanejable, por lo que el diseño de un sistema de seguridad debe basarse en la fortaleza de las tecnologías empleadas, y no en la ocultación de las mismas: "security through obscurity".

2. El protocolo TCP/IP sufre algunos problemas de seguridad por las características intrínsecas de su diseño, los cuales han sido ampliamente analizados a lo largo de los últimos años. La nueva versión de IP, versión 6, se diseño con la seguridad en mente, de ahí la aparición del estándar IPSec, que junto a otras tecnologías, como las infraestructuras de clave pública, PKIs, permiten controlan y disolver muchas de las vulnerabilidades presentadas a lo largo del presente trabajo.

3. Asimismo, se puede concluir que la seguridad de una red no se basa en una única técnica exclusivamente, como promulga la idea errónea de securizar una red mediante un firewall, sino que viene reforzada por la utilización de multitud de tecnologías que permiten monitorizar y gestionar cada uno de los aspectos críticos de la red: encriptación, IDSs, firewalls, software específico de seguridad, protocolos seguros (SSL, SSH, IPSec), PKIs...

4. Lo que es más, mediante el uso exclusivo de las tecnologías mencionadas no es posible asegurar la seguridad de la red. Para ello es necesario a su vez disponer de procedimientos y políticas adecuadas que permitan concienciar a los usuarios y administradores de los sistemas informáticos, así como facilitar la aplicación de análisis y controles exhaustivos en la propia red y los elementos que la componen. Es por tanto necesario dedicar tiempo y esfuerzo a evolucionar la red hacia un entorno seguro, siendo necesario mantenerse actualizado (preferiblemente de forma automática, por ejemplo,

mediante listas de distribución) de los avances que se realizan en este campo, así como de los nuevos avisos, vulnerabilidades y tecnologías que salen a la luz.

5. El objetivo final es asegurar ciertas características en las comunicaciones, como son, la autenticidad, la integridad de la información, la privacidad o confidencialidad, el no repudio, el control de acceso a la información

6. Finalmente, cabe concluir con una reflexión al respecto de la seguridad: el esfuerzo dedicado a la protección de un entorno debe ser directamente proporcional al valor de su contenido. Debido a que toda vulnerabilidad posee, más tarde o más temprano, su correspondiente protección, la vertiginosa carrera en la que la seguridad de las redes se debate actualmente, se centra en el mantenimiento constante y actualizado de las protecciones necesarias para evitar las vulnerabilidades existentes y ya conocidas.

ANEXO A

Seguridad de la Información - ISO17799

Es organizado en diez secciones mayores, cada uno que cubre un tema diferente o área:

1. Planificación de Continuidad del Negocio.

Neutralizar las interrupciones a las actividades comerciales y a los procesos del negocio críticos de los efectos de fracasos mayores o desastres.

2. Control de Acceso al Sistema.

Controlar el acceso a la información. Prevenir el acceso desautorizado a la información del sistema. Asegurar la protección de servicios conectados a una red de computadoras. Prevenir el acceso desautorizado a la computadora. Descubrir las actividades desautorizadas. Asegurar la seguridad de información al usar informática móvil y los medios tele-conectando una red de computadoras.

3. Desarrollo y Mantenimiento del Sistema.

Asegurar la seguridad en la construcción de los sistemas operacionales. Prevenir la pérdida, modificación o mal uso de datos del usuario en los sistemas de la aplicación. Proteger la confidencialidad, autenticidad e integridad de información. Asegurar los proyectos y dirigir las actividades de apoyo de una manera segura. Mantener la seguridad de software de sistema de aplicación y datos.

4. Seguridad Física y Medioambiental

Prevenir acceso desautorizado, daño e interferencia a las premisas comerciales e información. Prevenir la pérdida, daño o compromiso de recursos e interrupción a las actividades comerciales. Prevenir compromiso o robo de información e información que procesan los medios.

5. Cumplimiento.

Evitar las brechas de cualquier delictivo o derecho civil, las obligaciones estatutarias, regulador o contractuales y de cualquier seguridad requisitos. Asegurar el cumplimiento de sistemas con las políticas de seguridad orgánicas y normas. Aumentar al máximo la efectividad y minimizar el to/from de la interferencia el proceso de auditoría de sistema.

6. Seguridad del Personal

Reducir riesgos de error humano, robo, fraude o mal uso de medios. Asegurar que los usuarios son conscientes de amenazas de seguridad de información y preocupaciones, y se equipa para apoyar la política de seguridad corporativa en el curso de su trabajo normal. Minimizar el daño de las casualidades de seguridad y funcionamientos defectuosos y aprender de las tales casualidades.

7. Seguridad Organizacional

Manejar la seguridad de información dentro de la Compañía. Mantener la seguridad de información orgánica que procesa medios y recursos de información accedida por terceras partes. Mantener la seguridad de información cuando la responsabilidad por la información procesar ha sido el outsourced a otra organización.

8. La computadora y la Dirección de los Funcionamientos

Asegurar el funcionamiento correcto y seguro de información que procesa los medios. Minimizar el riesgo de fracasos de los sistemas. Proteger la integridad de software e información. Mantener la integridad y disponibilidad de información que procesa y comunicación. Asegurar la salvaguarda de información en las redes y la protección de la infraestructura de apoyo. Prevenir el daño a los recursos e interrupciones a las actividades comerciales. Prevenir la pérdida, modificación o mal uso de información intercambiados entre las organizaciones.

9. Clasificación del Recurso y Mando

Mantener protección apropiada de recursos corporativos y asegurar esos recursos de información reciben un nivel apropiado de protección.

10. La Política de Seguridad

Proporcionar la dirección de dirección y apoyar para la seguridad de información.

BIBLIOGRAFÍA

1. Marcus Goncalves, "Manual de Firewalls", Mc Graw Hill.

2. Andrew S. Tanenbaum, "Redes de Computadoras", Prentice Hall.

3. http://www.microsoft.com/technet/security/topics/networksecurity/secmod155.mspx/

4. http://www.pgpi.org/

5. http://www.microsoft.com/spain/servidores/isaserver/info/trial.aspx

6. http://www.mslatam.com/latam/technet/cso/Html-ES/home.asp

7. http://www.elhacker.net/

8. http://www.microsoft.com/latam/technet/articulos/windows2k/msppna/

9. http://www.iso-17799.com/