

4 SEGURIDAD

Un ordenador seguro no existe. El único ordenador seguro es aquel que está desenchufado, guardado en una caja de seguridad cuya clave indescifrable conoce únicamente una persona que casualmente murió el año pasado. Aparte de esta situación, siempre existe algún hueco en la seguridad del sistema.

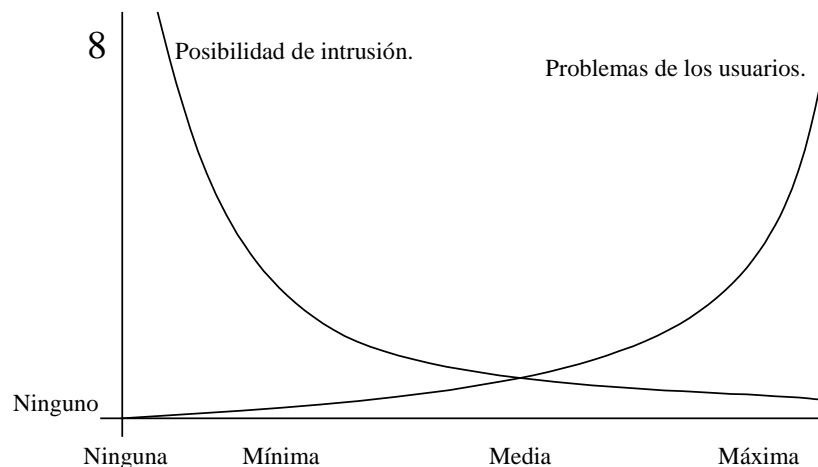
La cuestión es cuánta inseguridad se está dispuesto a aceptar en nuestro sistema.

Si un ordenador no es seguro de por sí, cuando el ordenador se conecta a una red, el número de potenciales violadores de la seguridad de nuestro sistema se multiplica ya que no es necesario sentarse delante del ordenador para acceder a él.

Se deduce que no se puede calificar un sistema como seguro o inseguro, sino que se establecen distintos niveles de seguridad que pueden cumplir o no los sistemas.

El nivel de seguridad se opone a la facilidad de uso del sistema. Cuanto mayor sea el nivel de seguridad de un sistema, más trabajo debe realizar alguno de los implicados en el sistema. Si la seguridad se basa en añadir claves de acceso a recursos, los usuarios deberán conocer esas claves y alguien se encargará de establecerlas; si el sistema tiene activada la auditoría, el usuario no lo notará, pero el sistema tendrá trabajo extra almacenando los sucesos, y el administrador deberá establecer las auditorías, controlarlas, evitar que crezcan indefinidamente, etc.

Al final se debe establecer una solución de compromiso entre las ventajas y los inconvenientes de establecer medidas de seguridad.



4.1 ELEMENTOS A PROTEGER

Básicamente hay dos cosas que se deben proteger de un sistema: los datos y los recursos.

Los datos se deben proteger para que sean privados, impidiendo que alguien no autorizado pueda conocerlos. También hay que garantizar la integridad, no se debe

permitir que personas no autorizadas modifiquen nuestra información. Si la información debe estar disponible para acceder a ella, también se debe proteger la accesibilidad.

Los recursos de los sistemas se deben utilizar para lo que se adquirieron. Si una empresa compra un disco duro para almacenar su información, y un intruso almacena información en el disco duro, está ocupando unos recursos indebidamente. O si el intruso ejecuta procesos en el ordenador, está consumiendo tiempo de CPU y energía de la empresa.

Quizá menos (o más) importante que los datos o los recursos sea la reputación. El que un usuario se haga pasar por otro y realice ciertas acciones puede dañar gravemente su reputación, además de poder meterle en líos más o menos gordos.

4.2 TIPOS DE ATAQUES

Hay muchos tipos de ataques a un sistema, y muchas formas de clasificarlos. En principio, vamos a clasificarlos en tres tipos: Intrusión, denegación de servicios y robo de información.

4.2.1.1 *Intrusión*

Es el ataque más común. Se trata de que un usuario intruso utilice el sistema. La mayor parte de las veces, se hacen pasar por usuarios legítimos.

4.2.1.2 *Denegación de servicio*

Es un tipo de ataque que consigue que el sistema no preste los servicios que se supone debe prestar. La mayoría de las veces se realiza inundando al sistema o a la red de información, de forma que no pueda realizar las tareas normalmente.

4.2.1.3 *Robo de información*

Los atacantes acceden a información reservada del sistema, muchas veces si necesidad de entrar en el sistema como usuarios. Es frecuente que los servicios que ofrece el sistema tengan algún error que se puede explotar para acceder a información restringida.

En algunas redes de ordenadores es relativamente fácil escuchar la información que circula por la red, por ejemplo, en Ethernet o Token Ring cualquier dispositivo conectado al medio puede escuchar toda la información que circula, aunque no vaya dirigida al propio dispositivo. Aunque el volumen de información sea muy grande en comparación con la información interesante, siempre se pueden escuchar los nombres de usuario y las claves de un usuario que intenta validarse en un sistema de la red.

4.3 ESTRATEGIAS DE SEGURIDAD

Referentes a la seguridad de sistemas, se pueden indicar una serie de consejos o estrategias que son válidos para todos los sistemas.

4.3.1.1 Menor privilegio

El principio fundamental de seguridad (no sólo informática sino de cualquier nivel) puede ser el de asignar siempre el menor privilegio posible. Se trata de que cualquier objeto (usuario, administrador, programa, sistema, etc.) tenga únicamente los privilegios necesarios para realizar su tarea, y ni uno más. Esto limita la exposición a posibles ataques y la gravedad de éstos si se producen.

4.3.1.2 Defensa en profundidad

Trata de que no se dependa exclusivamente de un mecanismo de seguridad por muy bueno que parezca. En su lugar, se deben establecer sistemas de seguridad que se respalden, de forma que si uno falla, actúe otro, y así sucesivamente.

Por ejemplo se puede implementar seguridad de la red (firewalls), seguridad en los ordenadores (especialmente en los bastiones) y seguridad en las personas (educación a los usuarios, administración cuidadosa, etc.). Otro ejemplo, si no se quiere que desde una máquina se envíe correo, además de filtrar los paquetes de correo, se pueden eliminar todos los programas relacionados con el correo.

4.3.1.3 Punto de choque (Choke point)

Se trata de que los atacantes deban utilizar un canal estrecho que siempre es más fácil de defender y vigilar (casa con dos puertas, mala es de guardar). De poco sirve proteger mucho el acceso a nuestro sistema por una vía, si se puede acceder sin problemas por otra.

4.3.1.4 Eslabón más débil

Una máxima fundamental de seguridad es que una cadena es tan fuerte como el más débil de sus eslabones. Siempre hay un eslabón que es el más débil, pero hay que hacerlo lo suficientemente fuerte para que resista.

4.3.1.5 Fallo seguro

Se debe tratar de que si algo falla, el sistema se quede en un estado lo más seguro posible. Por ejemplo, si falla el sistema, que no se permita entrar a ningún usuario. Esto impedirá que entren al sistema los usuarios que deben entrar, pero también impedirá que entren los atacantes.

Respecto a esta estrategia existen dos posibilidades de actuación: una que por defecto deniegue el acceso y otra que lo permita.

La opción que deniega el acceso implementa la máxima: todo lo que no está expresamente permitido, está prohibido. Desde el punto de vista de la seguridad, está claro que se debe utilizar esta estrategia.

La opción que permite el acceso: todo lo que no está expresamente prohibido, está permitido. A los usuarios seguro que les gusta más esta opción.

4.3.1.6 Participación universal

Para que una política de seguridad sea efectiva se requiere la participación de todos los implicados, o al menos, la ausencia de oposición.

Se necesita que los usuarios colaboren avisando de los sucesos extraños que descubran en los sistemas, o que no den a conocer sus claves a otras personas.

La primera forma de participación de los usuarios es que seleccionen una clave adecuada.

Es importante seleccionar una clave que no sea fácil de adivinar o de descubrir a base de hacer pruebas. En teoría las claves más seguras son una secuencia aleatoria de letras, números y signos de puntuación, pero como no son fáciles de recordar y además son difíciles de teclear, ya no son tan buenas, sobre todo si se deben apuntar en algún sitio para que no se olviden o se teclean muy despacio.

Una buena clave puede ser dos palabras aleatorias unidas por algún signo de puntuación, o las primeras letras de una frase alternando mayúsculas y minúsculas. También deben tener una longitud de 7 u 8 caracteres.

Otra característica que debe cumplir una clave es que se teclee rápidamente y se pueda teclear oculta por las manos (no se deduzca del movimiento de los dedos), para que no nos vean teclearla por encima del hombro.

En algunos sistemas se pueden imponer requerimientos mínimos que deben cumplir las claves, como número de caracteres, presencia de determinado número de caracteres no alfabéticos, y caducidad de las claves, de forma que se deban cambiar cada cierto tiempo. También se suele llevar una historia de las últimas claves utilizadas, para evitar que el usuario las repita en ciclos.

En el caso de la clave del administrador del sistema, se debe cambiar al menos cada 2 ó 3 meses, cada vez que alguien que la conocía deje la empresa (o el sistema), cuando se sospeche que alguien la ha descubierto, y todo esto un día que no se piense salir de juerga por la noche por si se olvida la clave nueva.

Lo mejor es convencer al personal de que se deben hacer bien las cosas, pero si alguien no quiere participar voluntariamente, no viene mal la ayuda de alguien que tenga el suficiente poder como para convencerles.

4.3.1.7 Diversidad de defensas

Además de defensa en profundidad se deben diversificar los tipos de medidas de seguridad. Se puede obtener más seguridad diversificando los sistemas para que si alguien conoce la forma de acceder a uno, no tenga la llave para entrar en todos. Evidentemente esto tiene el inconveniente de que se deben administrar sistemas heterogéneos.

4.3.1.8 Simplicidad

Hay dos razones por las que la simplicidad es una estrategia de seguridad. La primera es que haciendo las cosas simples, se comprenden más fácilmente. Si no se comprende una cosa, no se puede decir si es o no segura. La segunda es que cuanto más complejo sea algo, más cosas ocultas pueden ir dentro.

Los programas complejos, además, pueden tener errores indetectados, que aunque no sean problemas de seguridad, si pueden acostumar al administrador a comportamientos erráticos del sistema que podrían provenir también de ataques reales.

4.4 NIVELES DE SEGURIDAD

En 1981 el departamento de defensa formó el Computer Security Center, actualmente conocido como el National Computer Security Center (NCSC), para que fuera la organización formal gubernamental para investigar la seguridad en los ordenadores y para desarrollar métodos estándar de evaluación del nivel de seguridad ofrecido por un sistema en particular. La organización ha desarrollado un conjunto de criterios para abordar la fiabilidad de los sistemas de ordenadores. El conjunto de criterios utilizados para evaluar sistemas comerciales está disponible en una publicación titulada Trusted Computer System Evaluation Criteria, también conocida como el libro naranja (Orange book).

El libro naranja clasifica los sistemas de ordenadores en cuatro categorías D, C, B y A; siendo D la categoría menos segura y A la categoría más segura. Cada división consiste en una o más clases.

El libro naranja define seis requerimientos fundamentales:

- **Política de seguridad.** El sistema debe proveer una implementación fiable de una política de seguridad bien definida.
- **Marking.** Sistema debe proveer una implementación fiable del control de acceso a los objetos para que el sistema sea capaz de asegurar que se cumple la política de seguridad.
- **Identificación.** Cada sujeto debe ser identificado para que la política de seguridad sea capaz de forzar el control de acceso a los objetos. La información de identificación debe ser segura.
- **Auditoría.** El sistema debe proveer herramientas para auditar los sucesos relativos a la seguridad y para seleccionar el tipo sucesos que se quieren auditar.
- **Garantía.** La implementación de todas las funciones seguridad debe ser identificable claramente y estar documentada para poder evaluar y verificar que es correcta.
- **Protección continua.** El sistema de seguridad debe ser seguro en todo momento.

Los niveles de seguridad que propone el libro naranja son:

4.4.1 NIVEL D1

Es el menor nivel en la seguridad de ordenadores. El ordenador completo está sin asegurar. Es fácil infiltrarse en el sistema operativo y en el hardware. Adicionalmente, el estándar para el nivel D1, indica que no se requiere autenticación para los usuarios. Cualquiera que pueda acercarse al ordenador puede utilizarlo.

Algunos sistemas con este nivel de seguridad son: MS-DOS, MS-Windows 3.X y Windows 95 (sin grupo de trabajo) y System 7.x de Apple.

Los sistemas con este nivel de seguridad son adecuados cuando el acceso desde dichas máquinas a otros sistemas es mínimo, y los datos propios no son importantes.

4.4.2 NIVEL C1

Se le conoce como Sistema de Protección de Seguridad Discrecional (Discretionary Security Protection System). Indica que en la acceso al hardware del ordenador debe hacerse a través de algún nivel de seguridad, y que los usuarios deben validarse en el sistema antes de poder usarlo. También permite al administrador establecer permisos de acceso a ciertos programas o datos.

Algunos ejemplos de sistemas con este nivel son: Sistemas UNIX, XENIX y Novell 3.x o superior.

La seguridad de este nivel está limitada una vez que el usuario accede al nivel raíz del sistema operativo. En este nivel, puede manipular la configuración del sistema y acceder a lo que pueda acceder el administrador del sistema.

4.4.3 NIVEL C2

Este nivel tiene características que evitan los problemas del nivel anterior. Introduce la capacidad de controlar el acceso al entorno. Como está basado en algo más que los permisos de usuario, se pueden restringir a los usuarios la ejecución de ciertos comandos del sistema.

Los sistemas de nivel C2 también pueden utilizar auditoría. Mediante la auditoría se pueden almacenar los sucesos de seguridad como entradas en el sistema o realización de tareas administrativas.

Algunos sistemas que pueden obtener el nivel C2 son: Sistemas UNIX, XENIX, Novell 3.x o superior y Windows NT 3.51 y 4.0.

4.4.4 NIVEL B1

El Label Security Protection (B1) soporta seguridad multinivel. En este nivel, a los objetos bajo control de acceso obligatorio no se les pueden cambiar los permisos por el usuario propietario.

Los sistemas con este nivel de seguridad suelen estar en agencias del gobierno y del ejército.

4.4.5 NIVEL B2

También se le conoce como nivel de protección estructurada (Structured Protection). En este nivel, todos los objetos del sistema tienen etiquetas y los objetos (estaciones de trabajo, terminales, discos duros, etc.) tienen niveles de seguridad asignados.

4.4.6 NIVEL B3

Dominio de seguridad (Security Domain) obliga a que las estaciones de trabajo estén conectadas utilizando medios de comunicación seguros. Adicionalmente, se introducen sistemas de protección hardware para proteger el área de memoria de seguridad del sistema.

4.4.7 NIVEL A

Es el nivel de seguridad más alto del libro naranja. También se le conoce como Diseño verificado (Verified Design). Este nivel, como todos los niveles anteriores, incorpora las características de seguridad de los niveles menores que él. El diseño del sistema debe estar supervisado y aprobado por un equipo de individuos cualificados en seguridad. Además, todos los componentes del sistema que comprometan la seguridad del sistema, deben provenir de fuentes seguras.

4.5 SEGURIDAD EN LA RED

A principios de 1996, el departamento de defensa de Estados Unidos anunció que sus sistemas informáticos fueron atacados 250.000 veces en 1995. La mayoría de los ataques fueron contra sistemas de ordenadores que contenían información clasificada. Las dos terceras partes de los ataques se consideraron con éxito, lo que resultó en pérdida, robo, o modificación de datos.

Para evitar accesos indeseados desde la red, se recomienda la utilización de cortafuegos (*firewalls*).

4.5.1 CORTAFUEGOS (FIREWALLS)

Un *cortafuegos* es un sistema (hardware o software) que fuerza a llevar una política de control de acceso entre dos o más redes. La función básica es bloquear el tráfico no autorizado (filtrado).

La política de control de acceso se implementa básicamente de dos formas:

- Denegando el acceso a todo el tráfico excepto al tráfico autorizado.
- Autorizando el acceso a todo el tráfico excepto al tráfico denegado.

La política de control de acceso se puede aplicar en ambas direcciones, así se protege la propia red de los accesos desde la red exterior, y también se limita el acceso a Internet desde la red interna.

Originalmente había dos tipos de cortafuegos dependiendo de la capa sobre la que actuaban: a nivel de red y a nivel de aplicaciones. Actualmente los dos tipos suelen estar mezclados.

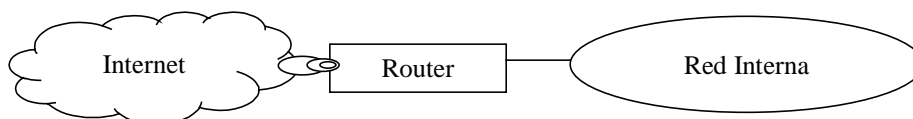
4.5.1.1 Cortafuegos a nivel de red

Operan a nivel IP. Hay cuatro tipos básicos:

- Simple router.
- Bastion host firewall.
- Screened host firewall.
- Screened subnet firewall.

4.5.1.1.1 Simple Router

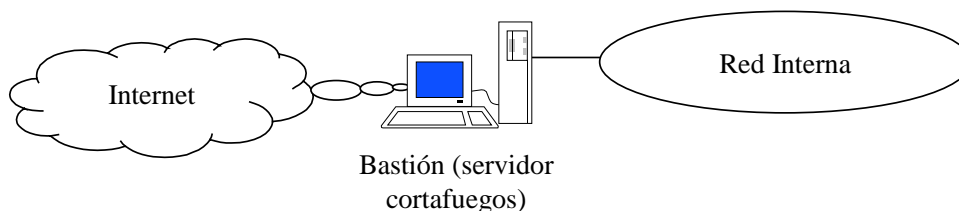
Un router especializado se puede considerar un cortafuegos. Se le asignan direcciones IP (ya que funcionan como router) y permite especificar políticas de control de acceso del tipo los host de la red 156.35.94.0 no pueden acceder a Internet.



Si le llega un paquete de un host de la red 156.35.94.0 intentando enviar información a Internet, examinaría el paquete, comprobaría la dirección origen con las políticas de acceso, vería que pertenece a una red que no puede acceder a Internet con lo que rechazaría el paquete (normalmente lo destruye) informando al host que lo envió que no lo ha enviado y posiblemente dejando grabado en algún registro el intento de acceso.

4.5.1.1.2 Dual-homed Bastion host Firewall

El término bastión se refiere al sistema central de la seguridad del sistema. Es un ordenador con al menos una conexión a la red externa (insegura) y otra conexión a la red interna (segura).



Cuando el bastión otorga permiso de acceso a un host externo, para que acceda a uno interno, se permite todo el tráfico que provenga del host externo.

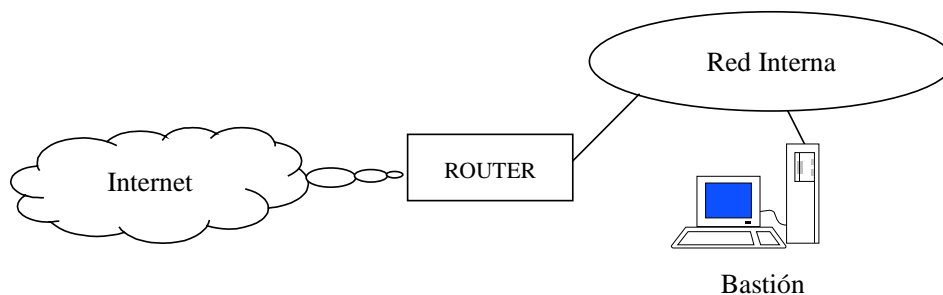
Normalmente los bastiones forman parte de sistemas más sofisticados.

Los inconvenientes de este modelo son:

- Una vez conseguido el permiso del bastión, se tiene acceso a toda la red protegida.
- La protección no es lo suficientemente avanzada para muchas aplicaciones de red.

4.5.1.1.3 Screened host firewall

Este modelo utiliza un router que apantalla al bastión encargado del cortafuegos. El router tiene una conexión a la red externa, y otra conexión con el bastión. El router filtra todo el tráfico y lo dirige al bastión. El bastión posteriormente puede realizar alguna comprobación adicional.

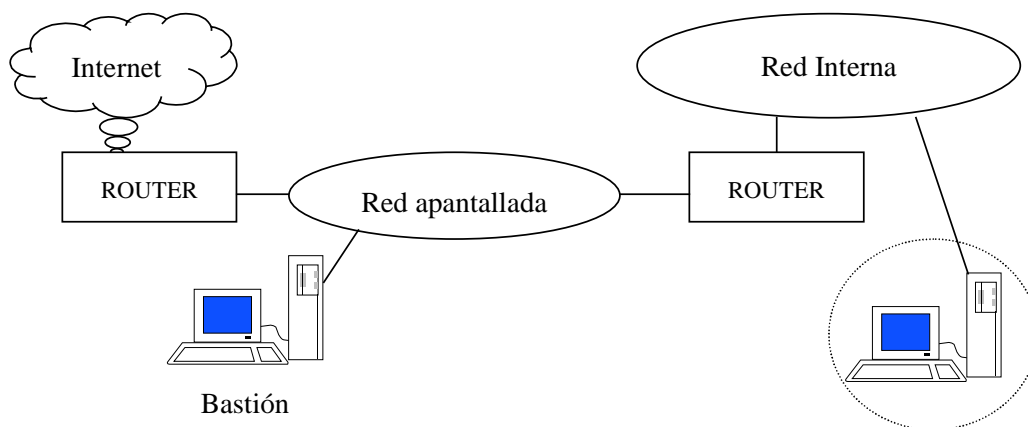


Los inconvenientes de este modelo son:

- Un único bastión apantallado puede ser un cuello de botella para el tráfico hacia la red.
- Si el bastión cae, cae toda la conexión con el exterior.

4.5.1.1.4 Screened subnet firewall

Utiliza uno o más routers y uno o más bastiones. Es una red apantallada por un lado de la red exterior por un router y un bastión y por otro lado de cada una de las subredes internas (seguras) por otro bastión y otro router.



Los inconvenientes:

- Es una implementación más cara porque tiene más dispositivos.

- La configuración es más compleja y crece exponencialmente con el número de subredes seguras internas.

4.5.1.2 Cortafuegos a nivel de aplicación

Los cortafuegos a nivel de aplicación no permiten que el tráfico pase directamente de una red a otra, además auditan y almacenan información del tráfico que procesan.

También pueden funcionar como conversores de direcciones. El tráfico que proviene de una red con una dirección de origen sale hacia la otra red con otra dirección que enmascara la dirección real.

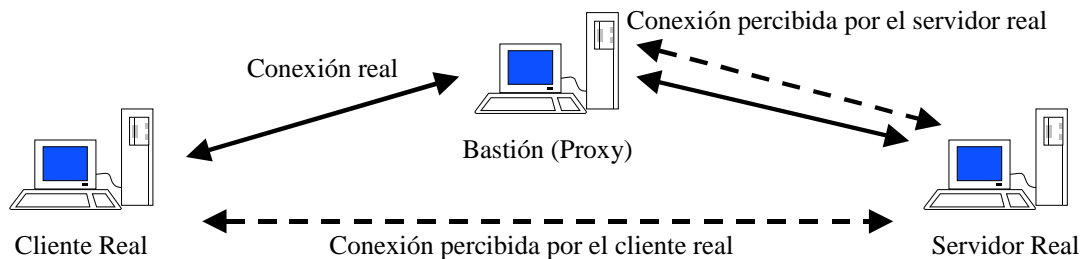
Estos cortafuegos suelen generar informes más complejos e implementar políticas de control de acceso más estrictas que los cortafuegos a nivel de red. El inconveniente es la velocidad que se pierde en la operación.

A este nivel hay tres tipos:

- Proxy server host.
- Dual-homed gateway.
- Circuit gateway.

4.5.1.2.1 Proxy server host Firewall

Desde el punto de vista del cliente, un proxy es una aplicación que sirve recursos de red emulando al verdadero servidor. Desde el punto de vista del servidor, es una aplicación cliente que emula al verdadero cliente.



Los proxies deben ser específicos para las aplicaciones que los van a utilizar.

Los inconvenientes:

- Necesita proxies específicos para cada aplicación.
- Aplicaciones proxy escritas incorrectamente pueden bloquear la salida a la red.

4.5.1.2.2 *Dual-homed gateway Firewall*

Cuando actúa como cortafuegos, no permite que el tráfico TCP/IP lo atraviese. El host sirve para almacenar datos y aplicaciones que se utilicen desde cualquiera de las redes a las que está conectado, pero no transmite información de una a otra.

Dependiendo de si se le añade un software u otro pueden ser Application forwarder, Mail forwarder o News forwarder.

Si se le añade un application forwarder funciona como un proxy proporcionando servicios.

De forma similar con un Mail forwarder o News forwarder permiten que el tráfico de correo electrónico o de news lo atraviesen.

El punto fundamental para que funcione como cortafuegos es que tenga desactivado el enrutamiento a nivel de red, lo que permitiría el tráfico independientemente de la capa de aplicación en la que debe funcionar.

Existen varios factores que pueden poner en peligro la seguridad aportada por este tipo de cortafuegos:

- Permiso de ficheros establecidos incorrectamente.
- Scripts de UNIX que pueden activar el enrutamiento.
- Que los usuarios de la red segura accedan desde la red insegura. Para evitarlo se debe evitar que existan usuarios en el gateway.
- Usuarios de la red insegura pueden llegar a conocer información sobre el sistema seguro por la información que se almacena en el gateway.

4.5.1.2.3 *Circuit Gateway Firewall*

Es un ordenador ejecutando una aplicación de gateway que facilita la comunicación entre recursos de red y aplicaciones de usuario utilizando los puertos TCP. Se envía la información a un puerto, y el circuito la cambia de puerto para que vaya a otra aplicación distinta.

4.5.2 RFC 1244 – THE SITE SECURITY HANDBOOK

The Site Security Handbook from the Internet Task Force, (RFC 1244) se conoce como la Biblia de trabajo del administrador.

Se trata de un punto de partida en cuestiones de seguridad en la red, que se debe complementar con otras fuentes locales de cada sistema particular.

4.6 TOLERANCIA A FALLOS

Existen distintas técnicas que permiten que los sistemas tengan cierto grado de tolerancia a fallos, permitiendo que el sistema siga funcionando aunque se produzca algún fallo en alguno de sus componentes. Los principales sistemas de tolerancia se orientan a la información almacenada en los discos duros del sistema.

4.6.1 RAID

El concepto de Array Redundante de Discos Baratos (Redundant Array of Inexpensive Disks) lo propusieron a finales de los ochenta unos investigadores de la Universidad de California, Berkeley. Trata de la utilización de varios discos (ahora cada vez más baratos) para distribuir la información entre ellos y proporcionar fiabilidad y mejora de la velocidad de acceso. El tema se ha tomado con mucho interés por el cuello de botella que supone el acceso a disco para los ordenadores modernos.

El concepto se basa en la técnica de *striping* que permite que bloques de datos sean entrelazados en varios dispositivos (discos) de características similares, en vez de almacenarlos en un único dispositivo. Una de las ventajas de este sistema es que permite acceder simultáneamente a los datos de más de un disco y transmitirlos en paralelo. Si se utilizan n discos, se produce un incremento de rendimiento de orden n respecto a la utilización de un único disco.

Si además se utiliza uno de los discos para mantener información de control, se puede también reconstruir la información en caso de fallo en uno sólo de los discos del RAID. Para eso, la información de control puede ser información de paridad o información XOR. El mantener información de control hace que se pierda espacio en disco pero la proporción de espacio perdido en un array de n discos es de $1/n$ del total.

Como la información de control se debe modificar cada vez que se modifica un valor cualquiera de los datos almacenados en cualquier disco, se produciría un cuello de botella en el disco que almacena la información de control. Para evitarlo, la información de control no se almacena en un único disco, sino que se distribuye entre todos los discos.

Las distintas posibilidades de utilización del *striping* dan lugar a los distintos niveles RAID.

4.6.1.1 Niveles RAID

Se distinguen seis niveles de RAID, desde el 0 hasta el 5, dependiendo de la seguridad y del fraccionamiento de la información de control.

4.6.1.1.1 RAID nivel 0

Únicamente utiliza *striping*, por lo que aumenta el rendimiento pero no mejora la fiabilidad.

4.6.1.1.2 RAID nivel 1

Proporciona *mirroring* de disco. Cada disco tiene otro que es una copia exacta. Para mejorar el rendimiento, el acceso a los datos del disco se realiza desde el disco que los proporcione antes.

Si el acceso se realiza a través de un única controladora de disco, se llama *mirroring*. Si se utilizan dos controladoras de discos, y cada disco duplicado está en una controladora distinta, se le llama *duplexing*. Con dos controladoras, se protege el sistema contra fallos en una de las controladoras además de en uno de los discos.

4.6.1.1.3 RAID nivel 2

En este nivel, el *striping* se hace a nivel de bit. Cada bit de información se guarda en un disco distinto. Los bits de control se guardan en uno de los discos.

4.6.1.1.4 RAID nivel 3

El *striping* se realiza a nivel de byte, y se reserva un disco para almacenar los bytes de control. Normalmente se le llama disco de paridad.

4.6.1.1.5 RAID nivel 4

El *striping* se realiza a nivel de bloque, siendo un bloque la cantidad de información que se puede escribir/leer por el dispositivo en una única operación. Se reserva un disco para almacenar los bloques de paridad.

4.6.1.1.6 RAID nivel 5

Es similar al nivel 4, partiendo la información en bloques, pero en vez de guardar la información de control en un solo disco, la almacena repartida por todos los discos de forma que no se tenga que acceder siempre al mismo para guardar la información de paridad.

4.6.2 SECTORES DE RESERVA

En los discos duros, el envejecimiento del medio magnético que almacena la información se suele notar en que poco a poco van apareciendo errores de lectura/escritura. Una vez que empiezan a aparecer errores, el número de ellos suele incrementarse de forma exponencial ya que indican que la vida útil del disco está terminando.

Desde que empiezan a aparecer, hasta que se generalizan todavía puede pasar un tiempo en el que se pueden seguir utilizando, pero ya pensando en la sustitución. Para permitir que se sigan utilizando, se puede dejar un grupo de sectores sin utilizar, de forma que se ocupen por la información de los sectores que empiezan a dar problemas.

El funcionamiento de este tipo de sistema de tolerancia a fallos consiste en la comprobación, en el momento de la escritura, de la igualdad de la información guardada en el disco con la que se quería guardar. Si coinciden, se puede suponer que la información se ha grabado bien y que el sector está bien. Si la comprobación falla, se almacena la información en un sector de los que se tienen reservados, indicándole al sistema dónde tiene que ir a buscar la información. El sector erróneo, se marca como tal para que no se vuelva a intentar utilizar.

4.6.3 SAI Ó UPS

El Servicio de Alimentación Ininterrumpido (SAI) (Uninterrupted Power Supply, UPS), permite que los sistemas no se apaguen como consecuencias de pérdidas de corriente.

Los más sencillos, son simples baterías que proporcionan corriente a los sistemas conectados, en caso de que falle la corriente. Tienen una duración determinada, y si el fallo de corriente supera dicha duración, se cae el sistema.

Otros más complejos mantienen cierto grado de comunicación con los dispositivos conectados, de forma que si detectan un fallo de corriente, se lo comunican a los dispositivos que tienen un margen de tiempo para almacenar la información de sus *buffers*, y para apagarse de forma adecuada y evitar pérdidas o degradaciones de información.

La forma de comunicación del SAI con los dispositivos conectados puede ser directa, normalmente a través de puerto serie, o utilizar la red para comunicar la caída de tensión, utilizando SNTP (Simple Network Management Protocol). Evidentemente, los dispositivos de red que necesiten alimentación e intervengan en la comunicación mediante SNMP (HUBS, repetidores, etc.) deben estar protegidos.

4.7 COPIAS DE SEGURIDAD

Cuando los distintos métodos de tolerancia a fallos no tienen efecto, sólo nos queda esperar a recuperar la última información que tuviéramos guardada en sitio seguro.

Lo más valioso que se tiene en un sistema informático es la información, y por eso, nos debemos encargar de minimizar las pérdidas de información. La realización de copias de seguridad implica que la información que guardamos en el sistema a disposición de los usuarios, la tenemos guardada en algún otro sitio (seguro) para recuperarla en el caso de que el sistema falle.

Las copias de seguridad son el seguro de la información. Se debe sopesar por un lado, el tiempo y dinero invertido en realizar las copias de seguridad, y por otro, el tiempo y el dinero que nos costaría recuperarnos de la pérdida de información, decremento de productividad, cambio de planificación, y demás inconvenientes que nos produciría una caída irrecuperable del sistema.

El problema de las copias de seguridad es que la información que tenemos en el sistema no es estática. Los datos cambian continuamente, y para que una copia de seguridad sea útil, debe guardar la información actualizada. Lo actualizada que esté la información guardada, depende de la estrategia de realización de copias de seguridad que implementemos.

En la planificación de la estrategia de copias de seguridad se deben tener en cuenta varios factores:

- *¿Qué ficheros se necesita copiar?*. En principio la respuesta es: *todos*. Sin embargo hay ficheros que no es necesario guardarlos, como pueden ser los ficheros del sistema operativo, que normalmente se tienen guardados en el medio desde el que lo instalamos.
- *¿Dónde están esos ficheros?*. Identifica en qué parte del sistema de ficheros están los ficheros importantes para realizar las copias de seguridad, y también

se puede ver al revés, como cuál de los sistemas de ficheros almacenan dichos ficheros.

- *¿Quién realizará las copias de seguridad?.* La respuesta depende de dónde estén los ficheros. Si los ficheros están en el servidor, el encargado puede ser el administrador, pero si los ficheros están en las estaciones de trabajo, se puede encargar a los propios usuarios realizar las copias.
- *¿Dónde, cuándo y bajo qué condiciones se deben realizar las copias de seguridad?.* El dónde se refiere a dónde está el dispositivo de copia de seguridad, que no necesariamente debe estar en el mismo sitio que el servidor. El cuando se refiere al momento de la realización. Las condiciones, indican la utilización de los ficheros. Lo ideal es un momento en el que no pueda acceder nadie al sistema, pero las condiciones no suelen ser ideales.
- *¿Con qué frecuencia se modifican los ficheros?.* Se debe tener en cuenta para decidir si hacer copia de todo o solamente de los ficheros modificados. Si se trata de un proyecto en el que se modifican muchos ficheros, se deberán copiar todos con cierta frecuencia. Si por el contrario lo único que cambia es una base de datos, la copia deberá ser frecuente (varias veces al día o a la hora) pero sólo de la base de datos.
- *¿Con qué rapidez se necesitan los datos recuperados?.* Se debe tener en cuenta la necesidad de encontrar y restaurar rápidamente los datos perdidos. Esto nos influye también en el tamaño de los datos importantes, ya que no es lo mismo guardar un fichero que contenga la licencia de una aplicación (1 KB) que una base de datos (4 GB) y ambos pueden ser imprescindibles para el funcionamiento del sistema.
- *¿En qué máquina se deben restaurar los ficheros?.* Es diferente restaurarlos en la misma máquina de la que se copiaron, que tener la posibilidad de restaurarlos en cualquier otro sitio.

Normalmente los medios donde se almacenan las copias de seguridad, son medios más baratos que los medios donde está habitualmente la información (discos duros). Se suelen utilizar cintas magnéticas, DAT, discos magneto ópticos, CDROM, etc. Algunos de los medios pueden ser reutilizables y otros no, lo que nos influirá en los métodos de almacenamiento. Otro factor a tener en cuenta, es la velocidad de transferencia de información hacia y desde los dispositivos.

Las copias de seguridad se suelen realizar en momentos en que los sistemas estén siendo poco utilizados (por la noche), por no interferir con las tareas normales de las máquinas, y por evitar la posibilidad de modificación de los datos que se guardan. El caso ideal es que las copias de seguridad se realicen cuando no haya nadie accediendo al sistema de ficheros del que se quiere hacer la copia, y la forma de asegurar esto es haciendo que no esté accesible para nadie más que para el que hace la copia de seguridad.

Lo peor de una copia de seguridad es estar esperando a que se realice. Para eso lo normal es planificar la realización de las copias de seguridad, siempre y cuando, la copia de seguridad nos quepa en el dispositivo de almacenamiento (si se debe cambiar

de cinta no nos sirve de nada). El inconveniente es que alguien acceda a la copia antes que el encargado, y la robe (si se tiene acceso al lugar físico donde está la unidad) o destruya la copia de seguridad grabando otra información accidentalmente o deliberadamente.

En los sistemas de ficheros, se suele guardar información de si se ha modificado o no la información de un fichero desde que se realizó la última copia de seguridad. Para distinguir la información modificada de la que no se ha modificado, y poder seleccionar cuáles son los ficheros que se deben copiar. Los programas que realizan las copias de seguridad, se encargan también de modificar esta información cuando realizan la copia de seguridad.

Dependiendo del grado de actualización de la información de las copias de seguridad que se quiera, y de la disposición de tiempo y de medios de almacenamiento de información, se pueden seguir distintos métodos de realización de copias de seguridad.

Los métodos más comunes son:

- Copia de seguridad completa.
- Copia de seguridad incremental.
- Copia de seguridad diferencial.
- Copia de seguridad personalizada.
- Copia de seguridad diaria.

4.7.1 COPIA DE SEGURIDAD COMPLETA

Se copia toda la información del sistema. Se marcan todos los ficheros como archivados, indicando que se han guardado independientemente de que lo estuvieran ya.

Esta estrategia es la mas completa, pero también es la más lenta por el volumen de información a almacenar. Además del tiempo de realización, tampoco es fácil de manejar, ya que para restaurar un fichero quizás se necesite buscarlo por varios de los soportes de almacenamiento (cintas, DAT, etc.).

4.7.2 COPIA DE SEGURIDAD INCREMENTAL

Solamente copia los ficheros que se han modificado desde la última copia de seguridad (completa o incremental) y se marcan como archivados.

Si se quieren recuperar los datos de una copia de seguridad incremental, se deben recuperar en primer lugar, los datos de la última copia de seguridad completa, después, recuperar los datos de las copias de seguridad incrementales que se hayan realizado posteriormente y en el mismo orden de realización.

Como sólo se guardan los ficheros modificados, las copias de seguridad incrementales son bastante rápidas, y ocupan relativamente poco espacio (siempre dependiendo del número y tamaño de los ficheros modificados).

Si se corrompe una de las copias de seguridad incrementales, se perdería la información modificada de los ficheros a no ser que se hubieran modificado posteriormente y estuviesen almacenados en otra copia incremental posterior.

4.7.3 COPIA DE SEGURIDAD DIFERENCIAL

Copia los ficheros que se han modificado desde la última copia de seguridad completa. No marca los ficheros como archivados, de forma que si se vuelve a realizar, volvería a copiar los mismos ficheros.

Para recuperar la última información almacenada, se deben recuperar en primer lugar los datos de la última copia de seguridad completa, y posteriormente, la última copia de seguridad diferencial.

Si se corrompe la última copia de seguridad diferencial, se puede intentar recuperar la anterior, con lo que sólo se perderían las modificaciones del último periodo. Si se corrompe una copia que no sea la última (y la última no se corrompe), no se pierde información.

El tamaño de las sucesivas copias diferenciales va aumentando ya que cada vez tiene que guardar más ficheros.

La copia diferencial siguiente a una copia completa, equivale a la primera copia incremental.

Si se llegan a modificar todos los ficheros, una copia diferencial sería equivalente a una copia completa. Como la mayoría de los sistemas de ficheros contienen una mezcla de ficheros de datos y programas, y los programas no suelen modificarse, es mejor utilizar diariamente una estrategia diferencial o incremental que una estrategia completa.

Teóricamente es posible mezclar copias de seguridad incrementales con copias de seguridad diferenciales, pero se pueden generar confusiones.

4.7.4 COPIA DE SEGURIDAD PERSONALIZADA

En esta estrategia, el usuario decide de qué ficheros se va a realizar la copia de seguridad y de cuáles no. Se suele utilizar cuando se quiere una copia de seguridad selectiva en un momento dado, sin tener que planificarla.

Normalmente este método no modifica la información de archivado de los ficheros, por lo que no interfiere con otros métodos que utilizan dicha información.

4.7.5 COPIA DE SEGURIDAD DIARIA

Se copian los ficheros que se han modificado en el mismo día en que se hace la copia de seguridad.

El criterio para realizar la copia de seguridad de un fichero no es la información de archivado, sino la fecha de modificación, por lo que no suelen marcar los ficheros como archivados, y no interfieren con otros métodos que utilizan dicha información.

Si se quiere recuperar la información, se debe recuperar en primer lugar la última copia de seguridad completa, y posteriormente todas las copias de seguridad diarias y en el mismo orden.

4.7.6 COPIA DE SEGURIDAD POR NIVELES

Hay sistemas que utilizan el concepto de niveles de copia de seguridad, para distinguir entre los distintos tipos. El nivel 0 siempre es equivalente a una copia de seguridad completa. Los sucesivos niveles son una copia de las modificaciones desde la última copia de seguridad del nivel inmediatamente anterior al suyo.

Con el concepto de niveles, una copia incremental sería:

1. Copia de nivel 0. Completa.
2. Copia de nivel 1. Cambios desde la anterior de nivel 0.
3. Copia de nivel 2. Cambios desde la anterior de nivel 1.
4. Copia de nivel 3. Cambios desde la anterior de nivel 2.
5. ...

Una copia diferencial sería:

1. Copia de nivel 0. Completa.
2. Copia de nivel 1. Cambios desde la anterior de nivel 0.
3. Copia de nivel 1. Cambios desde la anterior de nivel 0.
4. Copia de nivel 1. Cambios desde la anterior de nivel 0.
5. ...

Una mezcla de ambas podría ser:

1. Copia de nivel 0 Completa el primer lunes de cada mes.
2. Copia de nivel 1. Cambios desde la última de nivel 0. El resto de los lunes del mes.
3. Copia de nivel 2. Cambios desde la última de nivel 1. El resto de los días.

4.7.7 ALMACENAMIENTO DE LAS COPIAS DE SEGURIDAD

De poco sirve realizar copias de seguridad, si luego el medio en que se hicieron no está disponible.

Se deben tener en cuenta ciertos criterios para el almacenamiento de las copias de seguridad:

- *Saber dónde están las cosas.* Tener designado el sitio donde se almacenan ayuda a encontrarlas fácil y rápidamente a cualquiera de los encargados de restaurarlas. Esto se puede aplicar también a los discos de arranque, medio de instalación del sistema. Otro aspecto es conocer en qué dispositivo de copia está un fichero determinado, para no tener que ir a buscarlo cuando se necesite. Para eso se pueden generar tablas de contenido de los dispositivos.

- *Facilitar la copia y restauración.* Las copias deben estar cerca del ordenador desde el que se restauran, las cintas o medios deben estar lo suficientemente etiquetados para encontrar lo que se busca. Se pueden utilizar etiquetas de colores que ayudan a evitar errores. También es conveniente tener los suficientes medios para ir rotando con margen.
- *Proteger contra escritura.* Evita borrados accidentales. El mecanismo varía dependiendo del medio, pero todos tienen algún tipo de protección contra escritura.
- *Consideraciones del entorno.* La mayoría de los medios de almacenamiento de datos se conservan mejor en un ambiente fresco, seco y oscuro. Tampoco les va bien el polvo. Curiosamente es el mismo ambiente en el que deben estar los ordenadores, pero eso no quiere decir que tengan que estar en la misma habitación. De hecho, es mejor que algunas copias de seguridad no estén en el mismo lugar físico (off-site) para evitar que alguna desgracia acabe con el sistema y con las copias de seguridad a la vez.
- *Almacenar el medio adecuadamente.* Por ejemplo, no apilar discos unos encima de otros. Y guardar las cintas en sus cajas.
- *Tener en cuenta la duración del medio.* Si se realizan copias de seguridad que se van a almacenar mucho tiempo, se debe considerar la posibilidad de regrabarlas en medio nuevo cada cierto tiempo, antes de que se deteriore el medio y sean irrecuperables.
- *Tener en cuenta la seguridad.* El lugar donde se almacenen las copias de seguridad debe estar protegido en lo posible contra robos, vandalismo y desgracias varias.

4.7.8 PLANIFICACIÓN DE ROTACIÓN DE MEDIOS DE ALMACENAMIENTO

Es conveniente cambiar el medio de almacenamiento mediante alguna planificación. De esta forma no se utilizan siempre los mismos, y se reparte el uso, y además se aumenta el tiempo que se mantienen almacenadas las copias de seguridad antes de reutilizar el mismo medio. En los siguientes casos vamos a suponer que se utilizan cintas magnéticas, aunque podría tratarse de cualquier otro medio reutilizable.

4.7.8.1 Rotación de 2 conjuntos

Es un esquema básico en que se utilizan 2 conjuntos de cintas. Pongamos que queremos hacer copias de seguridad cinco días a la semana. En este caso se utilizarían 10 cintas en dos conjuntos de 5 cintas cada uno. Un conjunto se utiliza una semana y el otro la siguiente. A partir de la tercera semana se empiezan a reutilizar los conjuntos, pero siempre tendremos almacenadas las copias de la semana anterior.

Este método tiene el inconveniente de que almacena la información poco tiempo. Por ejemplo no nos serviría en el caso de que un virus infectase nuestros ficheros hace un mes.

4.7.8.2 Rotación abuelo-padre-hijo

El método GFS (Granfather-Fater-Son) es relativamente sencillo de manejar, y mantiene la información durante más tiempo.

Se necesitan 4 cintas para cada día de la semana excepto el viernes, 5 cintas para los viernes de cada semana del mes (la quinta es para los meses que tienen 5 viernes), y 12 cintas para cada uno de los meses.

El método consiste en hacer la copia cada día de la semana de lunes a jueves en la cinta del día correspondiente. Normalmente son diferenciales o incrementales y se reutilizan las cintas cada semana.

Las cintas de los viernes se utilizan los viernes correspondientes, y se guardan off-site al menos las dos últimas. Los meses que tengan 5 viernes se utiliza la cinta correspondiente y los que tengan 4 no se utiliza.

El último día del mes se hace la copia completa en la cinta del mes que corresponda, y se guardan off-site al menos durante un año. Si la organización necesita almacenar información durante más tiempo, se puede no reutilizar las cintas mensuales cada año, o realizar una anual.

Si alguna copia de seguridad no cabe en una única cinta, se debe considerar cada una de ellas como un conjunto de cintas.

Este método tiene el inconveniente de que hay mucha diferencia en la utilización que se hace de unas cintas y de otra, la de los lunes se usa 52 veces al año, mientras que la mensual sólo se usa 1.

4.7.8.3 Rotación de 10 medios

Este método usa un ciclo de cuatro semanas. En ellas las cintas de los lunes, martes, miércoles y jueves se reutilizan las 4 semanas y la de los viernes se va cambiando. El siguiente ciclo se desplazan una unidad las cintas y se sigue igual. La rotación empieza a repetirse cada 40 semanas.

Semanas	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V
1-4	C1	C2	C3	C4	C5	C1	C2	C3	C4	C6	C1	C2	C3	C4	C7	C1	C2	C3	C4	C8
5-8	C2	C3	C4	C5	C6	C2	C3	C4	C5	C7	C2	C3	C4	C5	C8	C2	C3	C4	C5	C9
9-12	C3	C4	C5	C6	C7	C3	C4	C5	C6	C8	C3	C4	C5	C6	C9	C3	C4	C5	C6	C10
13-16	C4	C5	C6	C7	C8	C4	C5	C6	C7	C9	C4	C5	C6	C7	C10	C4	C5	C6	C7	C1
17-20	C5	C6	C7	C8	C9	C5	C6	C7	C8	C10	C5	C6	C7	C8	C1	C5	C6	C7	C8	C2
21-24	C6	C7	C8	C9	C10	C6	C7	C8	C9	C1	C6	C7	C8	C9	C2	C6	C7	C8	C9	C3
25-28	C7	C8	C9	C10	C1	C7	C8	C9	C10	C2	C7	C8	C9	C10	C3	C7	C8	C9	C10	C4
29-32	C8	C9	C10	C1	C2	C8	C9	C10	C1	C3	C8	C9	C10	C1	C4	C8	C9	C10	C1	C5

33-36	C9	C10	C1	C2	C3	C9	C10	C1	C2	C4	C9	C10	C1	C2	C5	C9	C10	C1	C2	C6
37-40	C10	C1	C2	C3	C4	C10	C1	C2	C3	C5	C10	C1	C2	C3	C6	C10	C1	C2	C3	C7

El principal problema es la posibilidad de error en la selección de la cinta adecuada, ya que los sistemas de copia de seguridad no suelen tener implementados sistemas de rotación que avisen del orden adecuado en la utilización de cintas.

Otro inconveniente, es que sólo se tiene almacenada la información de los viernes 4 semanas. La de los otros días bastante menos.

5 APÉNDICES

5.1 BIBLIOGRAFÍA

Building Internet Firewalls.

D.Brent Chapman & Elizabeth D. Zwicky
Ed. O'Reilly & Associates, Inc. 1995.

Computer Security Basics

Deborah Russell & G.T. Gangemi, Sr.
Ed. O'Reilly & Associates, Inc. 1991.

Essential System Administration, 2ª Edition Revised & Updated

Aleen Frisch
Ed. O'Reilly & Associates, Inc. 1995.

Network and Internetworking Security.

William Stallings
Ed. Prentice Hall, 1995.

Practical UNIX and Internet Security. 2ª Edition.

Simson Garfinkel and Gene Spafford.
Ed. O'Reilly & Associates, Inc. 1996.

Windows NT Server 4. Security, Troubleshooting, and Optimization.

Wayne Dalton, Scott Fuller, Bob Kolosky, Joel Millecan Carey Nachenberg,
Karanjit S. Siyan, Lance Skok, Steve Tate.
New Riders Publishing, 1996.

Inside Windows NT Server 4. Administrator's Resource Edition.

Drew Heywood, et Al.
New Riders Publishing, 1997.

5.2 INFORMACIÓN EN LA RED

Existe gran cantidad de información en Internet, referida sobre todo a seguridad, entre ella está el RFC 1244 – The site security handbook mencionado con anterioridad, pero también en las múltiples páginas de cada sistema operativo existe información particularizada que la complementa.

También existen muchos sitios dedicados a seguridad, y aparecen muchos más a cada momento, por lo que la mejor forma de encontrarlos es utilizar cualquiera de los buscadores habituales.