9.3 Identificación de procedimientos de seguridad

Una situación crítica. Las políticas de estos planes se deben actualizar constantemente para que reflejen las amenazas más recientes que afectan a las redes. Todo técnico debe seguir un plan de seguridad con procedimientos claros. Estos planes deben revisarse de forma anual.

Como parte del proceso de garantizar la seguridad, deben realizarse pruebas para identificar aquellas áreas con niveles bajos de seguridad. Las pruebas deben llevarse a cabo periódicamente. Todos los días aparecen nuevas amenazas. Las pruebas periódicas proporcionan detalles acerca de cualquier posible debilidad del plan de seguridad actual que deba atenderse.

Existen varias capas de seguridad en una red: física, inalámbrica y de datos. Cada capa está expuesta a ataques de seguridad. El técnico debe comprender cómo implementar procedimientos de seguridad para proteger tanto los equipos como los datos.

9.3.1 Explicación de los requisitos de una política de seguridad local básica

Si bien las políticas de seguridad local pueden diferir de una organización a otra, hay preguntas que todas las organizaciones deben formularse:

- ¿Qué activos deben protegerse?
- ¿Cuáles son las amenazas posibles?
- ¿Qué debe hacerse en caso de que haya una brecha en la seguridad?

NOTA: Es probable que se haga referencia a la computadora en sí como unidad central de proceso o CPU. A los efectos de este curso, usaremos el término CPU sólo para aludir al chip microprocesador.

Una política de seguridad debe describir el método utilizado por la empresa para atender los problemas de seguridad:

- Definir un proceso para la gestión de incidentes relacionados con la seguridad de la red.
- Definir un proceso para la auditoría de la seguridad actual de la red.
- Definir un marco de seguridad general para la implementación de seguridad en la red.
- Definir qué conductas están permitidas.
- Definir qué conductas están prohibidas.
- Describir qué se debe registrar y cómo deben almacenarse los registros: visor de sucesos, archivos de registro del sistema o archivos de registro de seguridad.
- Definir el acceso de red a los recursos mediante permisos de cuenta.
- Definir tecnologías de autenticación para acceder a cierta información: nombres de usuario, contraseñas, biometría, tarjetas inteligentes.

9.3.2 Explicación de las tareas necesarias para proteger los equipos físicos

La seguridad física es tan importante como la seguridad de los datos. Al robarse una computadora, se llevan también los datos.

Hay diversas maneras de proteger la integridad física de las computadoras, como se ilustra en las figuras 1 y 2:

- Controlar el acceso a las instalaciones.
- Utilizar candados de cable en los equipos.
- Mantener los cuartos de telecomunicaciones cerrados con llave.
- Colocar tornillos de seguridad en los equipos.
- Colocar los equipos dentro de estructuras de seguridad.
- Rotular los equipos e instalar sensores, como etiquetas de identificación por radiofrecuencia (RFID).

Figura 1.

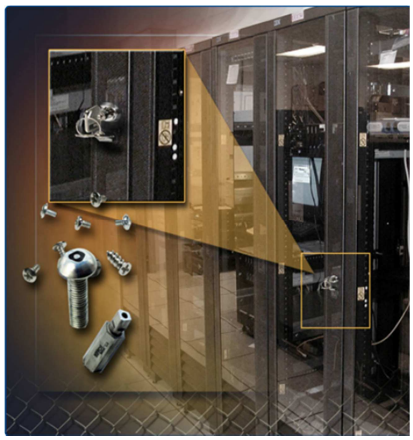


Figura 2.

Con respecto al acceso a las instalaciones, existen varias opciones de protección:

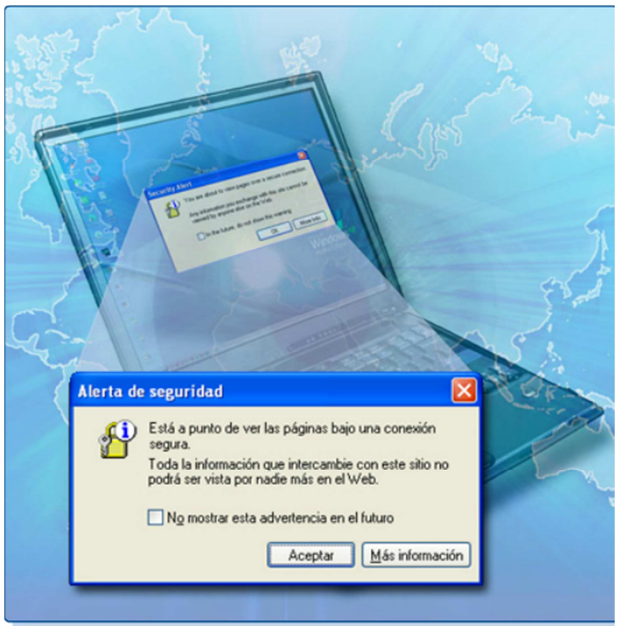
- Tarjetas magnéticas que almacenan los datos del usuario, incluso el nivel de acceso.
- Conectores Berg para la conexión a unidades de disquete.
- Sensores biométricos que identifican características físicas del usuario, como huellas digitales o retinas.
- Contratación de personal de seguridad.
- Sensores, como etiquetas de RFID, para controlar los equipos.

9.3.3 Descripción de formas de proteger los datos

Por lo general, el valor de los equipos físicos es inferior al de la información que contienen. La pérdida de datos confidenciales de una empresa en favor de la competencia o de delincuentes puede resultar costosa. Dicha pérdida puede ocasionar una falta de confianza en la empresa y el despido de los técnicos en computación a cargo de las tareas de seguridad informática. La seguridad de los datos se puede proteger mediante diversos métodos.

Protección mediante contraseña

La protección mediante contraseña puede impedir el acceso no autorizado a los datos, como se muestra en la Figura 1. La información desprotegida es vulnerable al acceso de los atacantes. Todas las computadoras se deben proteger mediante contraseña. Se recomienda utilizar dos niveles de protección mediante contraseña:



- BIOS: impide la modificación de la configuración del BIOS sin la contraseña correspondiente.
- Inicio de sesión: impide el acceso no autorizado a la red.

El inicio de sesión en la red permite registrar toda la actividad realizada en la red y autorizar o prohibir el acceso a los recursos. Esto permite identificar qué recursos se están utilizando. Por lo general, el administrador del sistema define una convención de denominación para los nombres de usuarios al crear conexiones de red. Un ejemplo típico de nombre de usuario es la inicial del primer nombre de la persona y el apellido completo. Se

recomienda emplear una convención de denominación simple para que los usuarios puedan recordar sus credenciales con facilidad.

Al asignar contraseñas, el nivel de control de contraseña debe coincidir con el nivel de protección requerido. Debe aplicarse estrictamente una política de seguridad eficaz que incluya ciertas reglas, entre ellas:

- Las contraseñas deben caducar al cabo de cierto tiempo.
- Las contraseñas deben contener una combinación de letras y números, de modo que no puedan violarse fácilmente.
- Los estándares de contraseñas deben evitar que los usuarios anoten las contraseñas y las dejen a la vista del público.
- Deben definirse reglas sobre la caducidad y el bloqueo de contraseñas. Las reglas de bloqueo se aplican cuando se realizan intentos infructuosos para acceder al sistema o cuando se detecta una modificación en la configuración del sistema.

Para simplificar el proceso de administración de la seguridad, los usuarios suelen ser asignados a grupos; y éstos, a su vez, a recursos. De esta forma, se permite modificar el acceso de los usuarios a la red de manera sencilla mediante la asignación del usuario a diversos grupos o su eliminación de éstos. Ello resulta útil cuando se deben crear cuentas temporales para trabajadores o consultores que visitan la empresa, ya que permite limitar el acceso a los recursos.

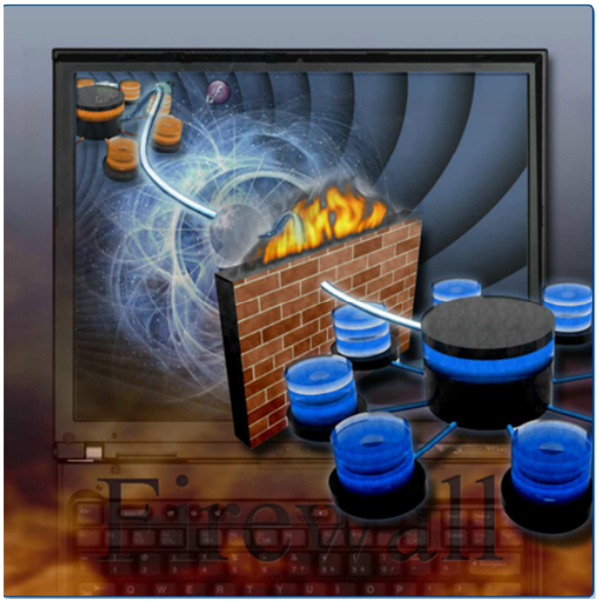
Encriptación de datos

La encriptación de datos utiliza códigos y claves. Es posible implementar la encriptación para proteger el tráfico entre los recursos y las computadoras de la red contra las actividades de los atacantes para controlar o registrar las transacciones. De esta forma, quizás no sea posible descifrar los datos capturados a tiempo para utilizarlos.

Las redes privadas virtuales (VPN) protegen los datos mediante encriptación. Una conexión de VPN permite al usuario remoto acceder de manera segura a los recursos como si la computadora se encontrase conectada físicamente a la red local.

Protección de puertos

Cada una de las comunicaciones que emplean TCP/IP se encuentra asociada a un número de puerto. HTTPS, por ejemplo, usa el puerto 443 por defecto. El uso de un firewall, como se muestra en la Figura 2, es una forma de proteger la computadora del ingreso de intrusos a través de los puertos. El usuario puede controlar el tipo de información que se envía a una computadora seleccionando los puertos que se abrirán y los que se protegerán. El transporte de datos en una red se denomina tráfico.



Copias de seguridad de datos

En un plan de seguridad, deben incluirse procedimientos para la realización de copias de seguridad de datos. En ciertos casos, como robos, fallas de equipos o desastres, como un incendio o una inundación, pueden perderse o dañarse los datos. La realización de copias de seguridad es una de las formas más eficaces de protegerse contra pérdidas de datos. A continuación, se ofrecen algunas pautas con respecto a las copias de seguridad:

- **Frecuencia de las copias de seguridad**: la realización de copias de seguridad puede llevar mucho tiempo. A veces, es más fácil realizar una copia de seguridad completa mensual o semanalmente y, luego, copias de seguridad parciales frecuentes de los datos que se hayan modificado desde la última copia de seguridad completa. Sin embargo, cuanto mayor sea la cantidad de copias de seguridad realizadas, mayor será el tiempo que tomará restaurar los datos.

- **Almacenamiento de las copias de seguridad**: las copias de seguridad deben trasladarse a un depósito externo aprobado para asegurar mayor protección. Los medios que contienen la copia de seguridad más reciente se trasladan a la ubicación externa de forma diaria, semanal o mensual, según lo exija la organización local.

- **Protección de las copias de seguridad**: las copias de seguridad pueden protegerse mediante contraseñas. Estas contraseñas se deben introducir a fin de restaurar los datos almacenados en los medios de copias de seguridad.

Seguridad del sistema de archivo

Todos los sistemas de archivos mantienen un registro de los recursos, pero sólo los que cuentan con diarios pueden registrar el acceso por usuario, fecha y hora. El sistema de archivos FAT 32 (Figura 3), que se utiliza en algunas versiones de Windows, no incluye funciones de registro por diario ni encriptación. Como consecuencia, cuando se requiere un alto nivel de seguridad, suele emplearse un sistema de archivos como NTFS, incluido en Windows 2000 y Windows XP. Si se necesita contar con un nivel de seguridad mayor, el sistema de archivos FAT 32 puede convertirse a NTFS mediante ciertas utilidades, como CONVERT. El proceso de conversión no es reversible. Por eso, antes de realizar el cambio, es importante definir claramente los objetivos.

	FAT32	NTFS
Seguridad	Seguridad baja	Encriptación y permisos de acceso a archivos y carpetas.
Compatibilidad	Compatible con Windows 95/98/ME. Se puede leer/escribir en Linux y Mac.	Solamente es compatible con Windows (NT, 2000, XP, Vista); Linux/Unix sólo lectura.
Tamaño de archivo	Límite de 4 GB en archivos y 32 GB en volúmenes.	Límite de 16 terabytes en archivos y de 256 terabytes en volúmenes.
Archivos por volumen	4,17 millones	4290 millones (4 294 967 295)
Eficacia de tamaño de archivo	Los clúster grandes consumen bastante espacio.	Los clúster más pequeños ocupan más espacio de lo disponible; la compresión integrada optimaliza espacio.
Confiabilidad	Las tablas de asignación de archivos (FAT) no llevan registro de transf. de archivos para uso posterior en la restauración tras errores.	El sistema de archivos de nueva tecnología (NTFS) incluye la función de registro para restauración tras errores.