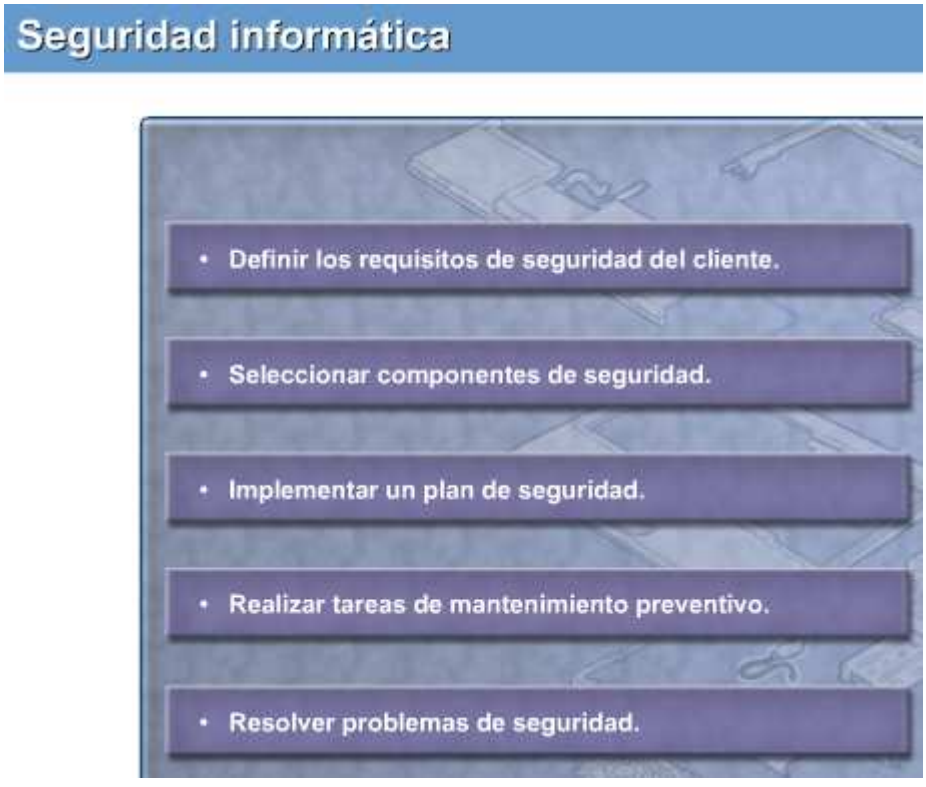
16.0 Introducción

Este capítulo analiza los tipos de ataques que amenazan la seguridad de las computadoras y los datos que éstas contienen. Un técnico es responsable de la seguridad de los datos y las computadoras de una organización. El capítulo describe cómo trabajar con los clientes para garantizar la instalación de la mejor protección posible.

Los riesgos para las computadoras y los equipos en red provienen de fuentes tanto internas como externas. Entre ellos se incluyen amenazas físicas, tales como robo de los equipos o daño de éstos, y amenazas sobre los datos, tales como pérdida o corrupción de datos.

Al completar este capítulo, alcanzará los siguientes objetivos:

- Crear un esquema de los requisitos de seguridad según las necesidades del cliente.
- Seleccionar los componentes de seguridad según las necesidades del cliente.
- Implementar una política de seguridad del cliente.
- Realizar el mantenimiento preventivo de la seguridad.
- Solucionar problemas de seguridad.



16.1 Creación de un esquema de los requisitos de seguridad según las necesidades del cliente

Una organización debe luchar para alcanzar la mejor y más accesible protección de seguridad contra la pérdida de datos o el daño de software y equipos. Los técnicos de redes y la gerencia de la organización deben trabajar en conjunto para elaborar una política de seguridad que asegure que los datos y equipos estén protegidos contra todas las amenazas contra la seguridad. Una política de seguridad incluye un plan integral sobre el nivel de seguridad necesario y la manera en que se pretende lograr esta seguridad.

Es posible que deba participar en la elaboración de una política de seguridad para un cliente o una organización. Al crear una política de seguridad, debe realizar las siguientes preguntas para determinar los factores de seguridad:

- ¿La computadora se encuentra en un domicilio particular o en una empresa?
  En general, las computadoras domésticas son más vulnerables a la intrusión inalámbrica que las computadoras de las empresas. Las computadoras de las empresas están más expuestas a amenazas de intrusión en la red, debido a que los usuarios abusan de los privilegios de acceso.
- ¿Hay acceso a Internet de tiempo completo?
  Cuanto más está expuesta una computadora a Internet, mayor es la probabilidad de ataques desde otras computadoras infectadas. Una computadora con acceso a Internet debe incluir soluciones firewall y antivirus.
- ¿La computadora es de tipo portátil?
  La seguridad física es un problema de las computadoras portátiles. Existen medidas para asegurar las computadoras portátiles; por ejemplo, candados de cable.

Al completar esta sección, alcanzará los siguientes objetivos:

- Crear una política de seguridad local.
- Explicar cuándo y cómo usar el hardware de seguridad.
- Explicar cuándo y cómo usar el software de seguridad de aplicaciones.

Política de seguridad local

16.1 Creación de un esquema de los requisitos de seguridad según las necesidades del cliente

16.1.1 Creación de una política de seguridad local

Una política de seguridad es un conjunto de reglas, pautas y listas de verificación. Los técnicos y administradores de redes de una organización trabajan en conjunto para establecer las reglas y pautas de las necesidades de seguridad de las computadoras. Una política de seguridad incluye los siguientes elementos:

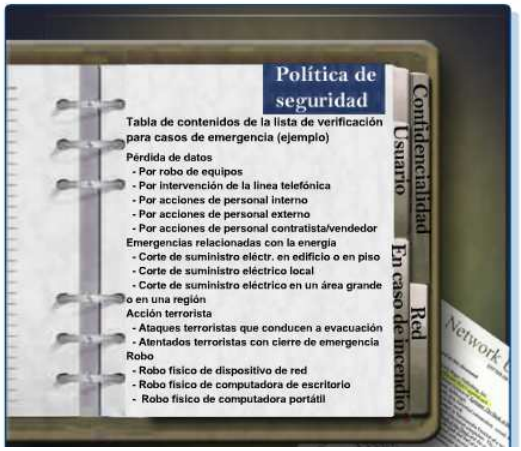
- Define un plan sobre el uso aceptable de computadoras en una organización.
- Identifica a las personas autorizadas para usar las computadoras de una organización.
- Identifica los dispositivos cuya instalación está permitida en una red y también las condiciones de la instalación. Los módems y los puntos de acceso inalámbricos son ejemplos de herramientas de hardware que podrían exponer la red a ataques.
- Define los requisitos necesarios para que los datos de una red sean confidenciales.
- Determina un proceso para que los empleados obtengan acceso a equipos y datos. Este proceso puede exigir que el empleado firme un acuerdo en relación con las reglas de la compañía. También enumera las consecuencias de los incumplimientos.

La política de seguridad también debe proveer información detallada sobre los siguientes temas en caso de emergencia:

- Ante una brecha de seguridad, es necesario:
- Saber a quién contactar ante una emergencia.
- Saber qué información se puede compartir con los clientes, los proveedores y los medios de comunicación.
- Saber qué ubicaciones secundarias se deben utilizar en una evacuación.
- Saber qué medidas tomar después que ha pasado la emergencia, incluida la prioridad de los servicios que se deben restaurar.

PRECAUCIÓN: Una política de seguridad debe ser implementada y cumplida por todos los empleados para que sea eficaz.

Lista para emergencias de la política de seguridad



16.1 Creación de un esquema de los requisitos de seguridad según las necesidades del cliente

16.1.2 Explicación de cuándo y cómo usar el hardware de seguridad

La política de seguridad debe identificar el hardware y los equipos que pueden usarse para prevenir robos, sabotaje y pérdida de datos. Existen cuatro aspectos interrelacionados con la seguridad física, que son el acceso, los datos, la infraestructura y la computadora, como ilustra la Figura 1.

Restrinja el acceso a las instalaciones mediante:

- Barreras de seguridad
- Hardware de seguridad

Proteja la infraestructura de red, como el cableado, los equipos de telecomunicación y los dispositivos de red mediante:

- Seguridad en las salas de telecomunicaciones
- Detección inalámbrica de puntos de acceso no autorizados
- Firewalls de hardware
- Sistema de administración de redes que detecte los cambios en el cableado y los paneles de conexión

Proteja las computadoras individuales mediante:

- Candados de cable
- Candados de seguridad para estaciones de acoplamiento de computadoras portátiles
- Chasis que se puedan bloquear
- Jaulas de seguridad para los chasis de escritorio

Proteja los datos mediante hardware que impida el acceso no autorizado o el robo de medios:

- Portadoras HD que se puedan bloquear
- Almacenamiento y transporte seguro de los medios de copias de seguridad
- Llaves de seguridad USB

Los factores de seguridad apropiados
Los factores que determinan los equipos de seguridad más efectivos que deben utilizarse para asegurar equipos y datos incluyen:

- ¿Qué uso se dará a los equipos?
- ¿Dónde está ubicada la computadora?
- ¿Qué acceso de usuario a los datos se requiere?

Por ejemplo, una computadora en un lugar público concurrido, como una biblioteca, requiere una protección adicional contra robos y sabotaje. En un centro de llamadas concurrido, es posible que un servidor deba mantenerse en una sala de equipos cerrada.

En caso de que sea necesario usar una computadora portátil en un lugar público, una llave de seguridad, como se muestra en la Figura 2, asegurará que el sistema se bloquee si el usuario se aleja de la computadora portátil.

Seguridad física

Llave de seguridad USB

16.1 Creación de un esquema de los requisitos de seguridad según las necesidades del cliente

16.1.3 Explicación de cuándo y cómo usar el software de seguridad de aplicaciones

Las aplicaciones de seguridad protegen el sistema operativo y los datos de aplicaciones de software.

Los siguientes productos y aplicaciones de software pueden usarse para proteger los dispositivos de red:

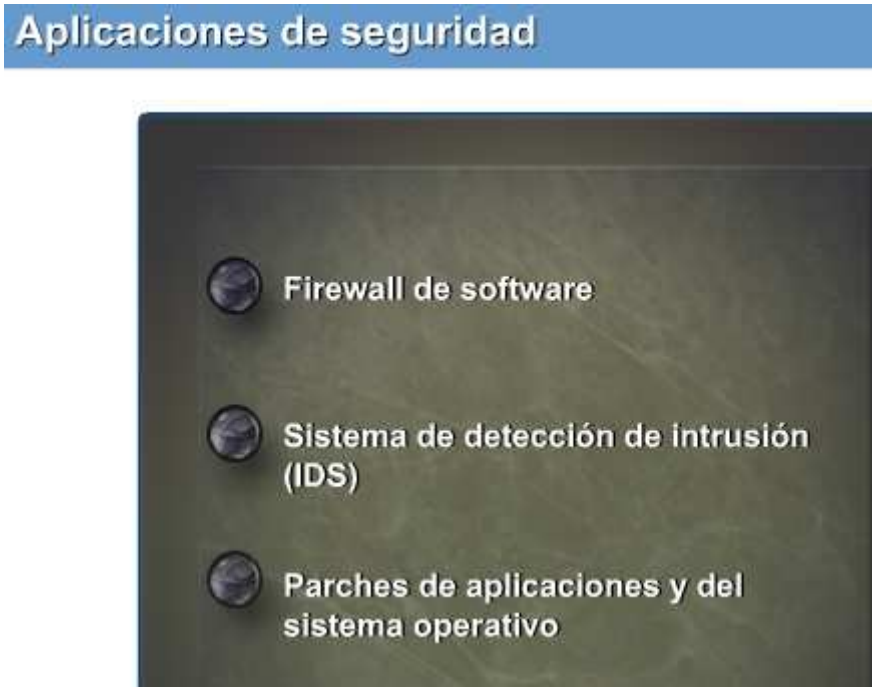
- Firewall de software: es una herramienta incorporada de Windows XP que filtra los datos entrantes.
- Sistemas de detección de intrusos (IDS, Intrusion Detection Systems): controla e informa los cambios en códigos de programa y la actividad de red inusual.
- Parches de aplicaciones y del sistema operativo: actualizan las aplicaciones y el sistema operativo para reparar los aspectos vulnerables de seguridad que se descubren.

Existen varias aplicaciones de software disponibles para proteger las computadoras contra el acceso no autorizado por medio de un código electrónico malicioso:

- Protección contra virus
- Protección contra spyware
- Protección contra adware
- Protección contra grayware

En oficinas pequeñas y hogares, las computadoras, por lo general, se conectan directamente a Internet en lugar de hacerlo a través de una LAN protegida como en las grandes organizaciones. Esto expone las computadoras sin LAN a un gran riesgo de virus y otros ataques. Como mínimo, estas computadoras deben usar antivirus y programas de protección contra malware. El software de las aplicaciones y el sistema operativo deben actualizarse con los parches más recientes. También se recomienda usar un firewall de software.

La política de seguridad debe determinar el nivel de seguridad de las aplicaciones. Cada medida que incrementa la protección implica un costo. Al establecer una política, la administración debe considerar el costo de la pérdida de datos con el gasto de protección de seguridad y determinar cuál es equilibrio aceptable.



16.2Selección de los componentes de seguridad según las necesidades del cliente

La política de seguridad ayuda a los clientes a seleccionar los componentes de seguridad necesarios para proteger los equipos y los datos. Si no existe una política de seguridad, debe discutir los asuntos de seguridad con el cliente.

Utilice su experiencia como técnico e investigue los productos de seguridad vigentes en el mercado cuando seleccione los componentes de seguridad para éste. El objetivo es brindar el sistema de seguridad que mejor se adapte a las necesidades del cliente.

Al completar esta sección, alcanzará los siguientes objetivos:

- Describir y comparar técnicas de seguridad.
- Describir y comparar dispositivos de control de acceso.
- Describir y comparar los distintos tipos de firewall.

16.2 Selección de los componentes de seguridad según las necesidades del cliente

16.2.1 Descripción y comparación de técnicas de seguridad

Un técnico debe determinar las técnicas apropiadas para proteger los equipos y datos del cliente. Según la situación, es posible que se necesite más de una técnica.

Contraseñas
Utilizar información de conexión encriptada y segura para las computadoras con acceso de red debe ser un requisito mínimo en toda organización. El software malicioso controla la red y puede registrar contraseñas de texto simple. Si las contraseñas están encriptadas, los atacantes tendrán que decodificar la encriptación para conocer las contraseñas.

Registro y auditoría
Deben activarse la auditoría y el registro de eventos para controlar la actividad en la red.

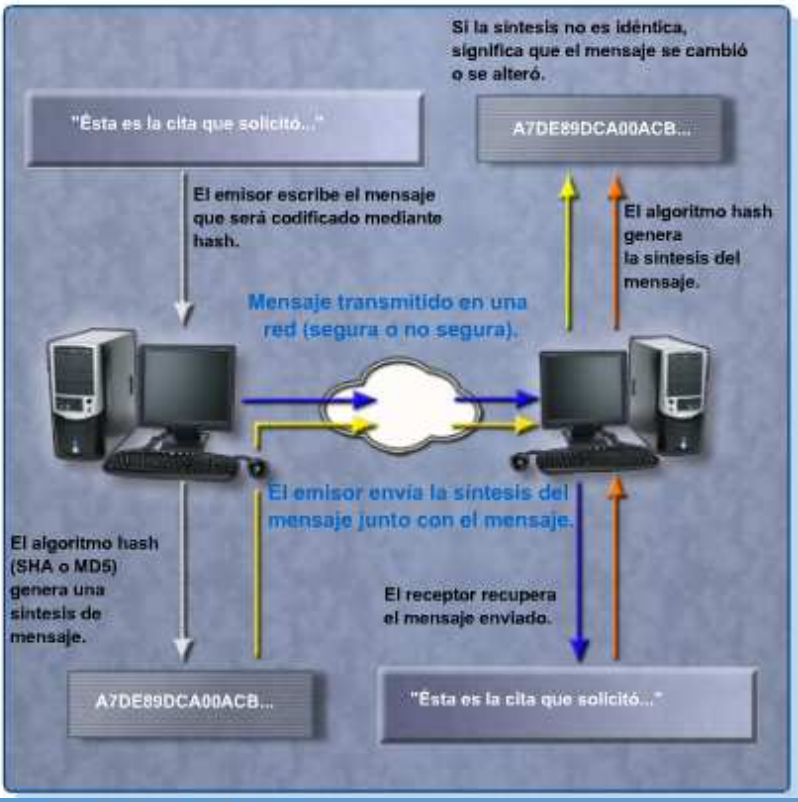
El administrador de red audita el archivo de registro de eventos para investigar el acceso a la red de usuarios no autorizados.

Configuraciones inalámbricas
Las conexiones inalámbricas son especialmente vulnerables al acceso de atacantes. La conexión de clientes con tecnología inalámbrica debe configurarse para encriptar los datos.

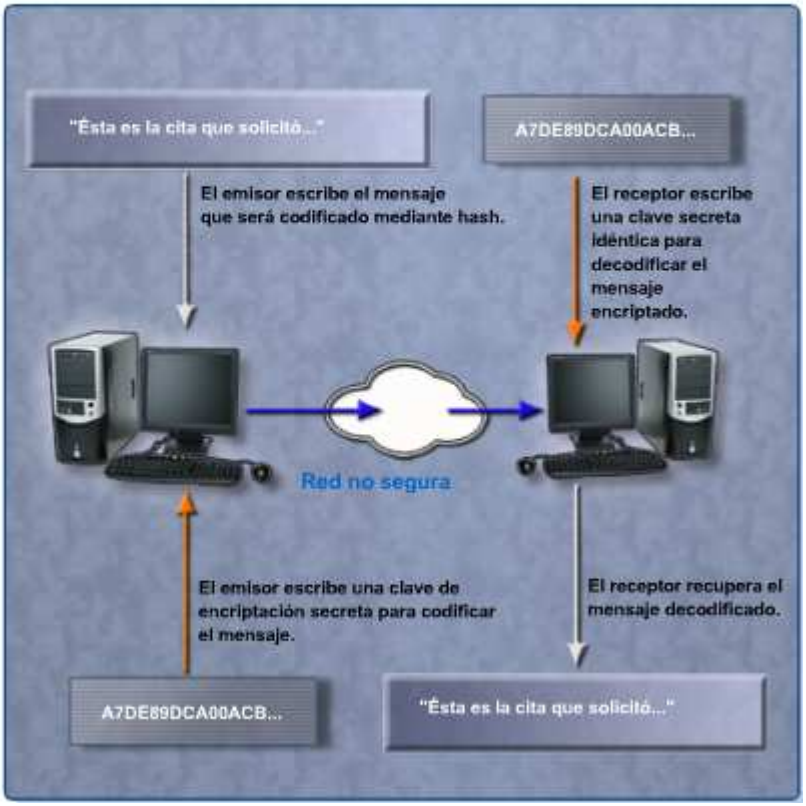
Encriptación
Las tecnologías de encriptación de datos se utilizan para codificar los datos que se transmiten en la red. Cada tecnología se utiliza para un propósito específico:

- Codificación hash: la codificación hash o hashing asegura que no se corrompan ni se adulteren los mensajes durante la transmisión. El hashing usa una función matemática para crear un valor numérico que es exclusivo de los datos. Si se cambia aunque sea un carácter, el resultado de la función, llamado message digest, no es el mismo. Sin embargo, la función es unidireccional. Conocer el message digest no permite que un atacante vuelva a crear el mensaje. Esto dificulta que alguien intercepte y cambie los mensajes. En la Figura 1, se ilustra la codificación hash. Los nombres de los algoritmos de hashing más populares son SHA y MD5.
- Encriptación simétrica: la encriptación simétrica requiere ambos aspectos de una conversación encriptada para usar una clave de encriptación con el fin de poder codificar y decodificar los datos. El emisor y el receptor deben utilizar claves idénticas. En la Figura 2, se ilustra la encriptación simétrica.
- Encriptación asimétrica: la encriptación asimétrica requiere dos claves, una privada y una pública. Se requiere una clave privada para escribir un mensaje y una clave pública para decodificarlo. La ventaja de la encriptación asimétrica es que sólo la clave privada debe ser confidencial. Las claves públicas pueden distribuirse abiertamente por correo electrónico o pueden publicarse en la Web. En la Figura 3, se ilustra la encriptación asimétrica.
- Red privada virtual (VPN): una red privada virtual utiliza la encriptación para proteger los datos como si se transmitiesen por medio de una LAN privada de una empresa, aunque los datos en realidad se envían a través de cualquier red, por ejemplo, Internet. Los canales protegidos de datos que comunican distintos puntos de la VPN se denominan "túneles seguros". El proceso se ilustra en la Figura 4.

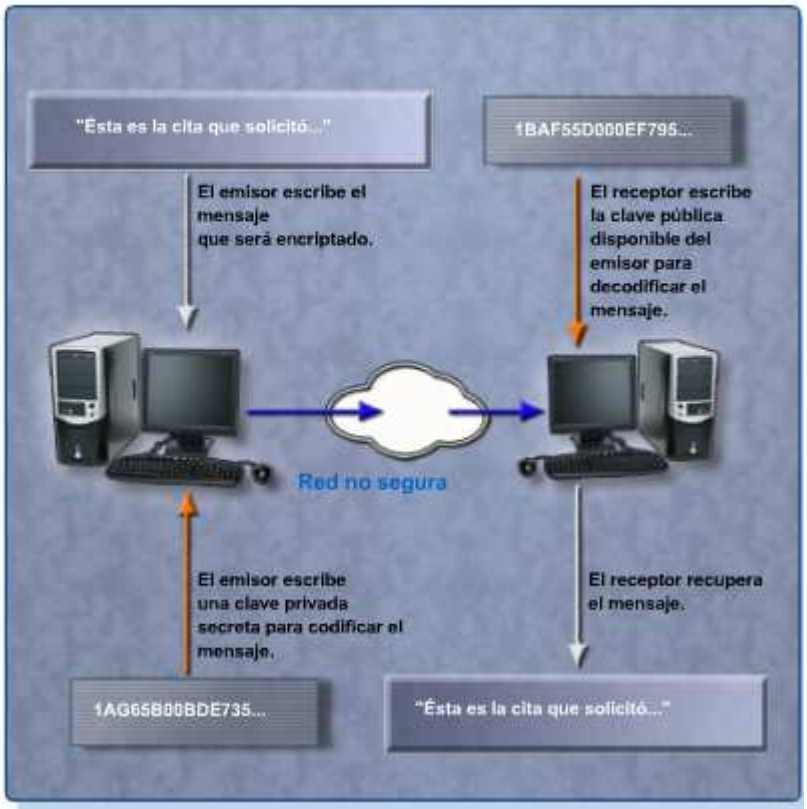
Codificación hash



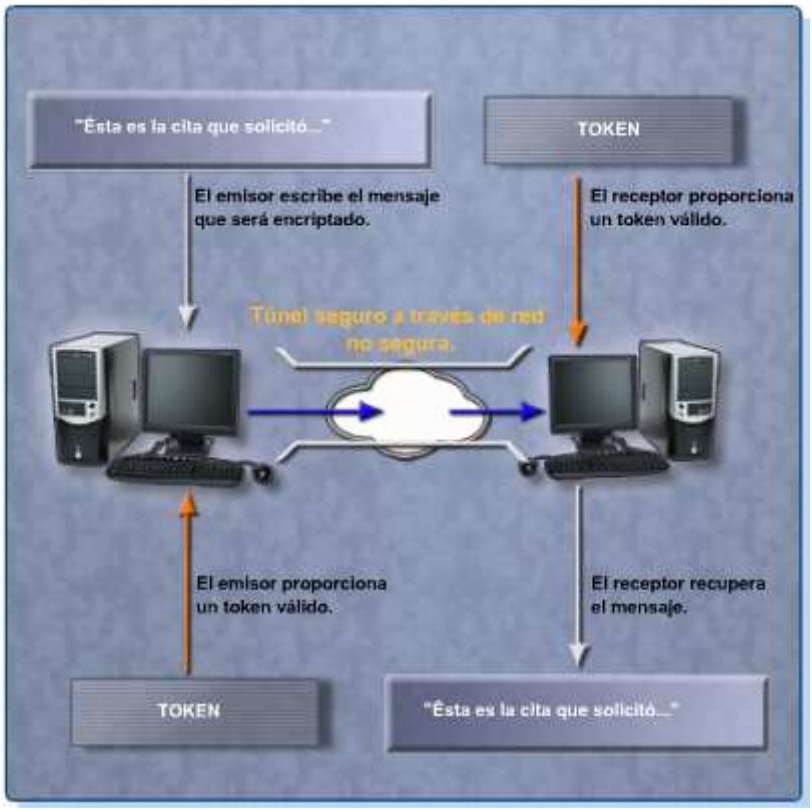
Encriptación simétrica



Encriptación asimétrica



Red privada virtual



16.2 Selección de los componentes de seguridad según las necesidades del cliente

16.2.2 Descripción y comparación de dispositivos de control de acceso

La computadora y los datos pueden protegerse con técnicas de protección superpuesta para prevenir el acceso no autorizado a los datos confidenciales. Un ejemplo de protección superpuesta es usar dos técnicas diferentes para proteger un mismo recurso. Esto se conoce como seguridad de doble factor, como muestra la Figura 1. Al elegir un programa de seguridad, se debe considerar el costo de la implementación con el valor de los datos o equipos que se protegerán.

Seguridad física

Use un hardware de seguridad para ayudar a prevenir las brechas en la seguridad y la pérdida de datos o equipos. Las medidas de control de acceso para la seguridad física incluyen:

- Traba: es el dispositivo más común para proteger áreas físicas. Si se pierde una clave, todas las trabas de claves idénticas deben cambiarse.
- Conducto: armazón que protege los medios de la infraestructura contra los daños y el acceso no autorizado.
- Tarjeta magnética: herramienta usada para proteger áreas físicas. Si se pierde una tarjeta magnética o si la roban, sólo debe desactivarse la tarjeta perdida. El sistema de tarjetas magnéticas es más costoso que las trabas de seguridad.
- Equipo de vídeo: graba imágenes y audio para la actividad de monitoreo. Se deben controlar los datos grabados para detectar posibles problemas.
- Personal de seguridad: controla la entrada a las instalaciones y supervisa las actividades realizadas dentro de éstas.

Deben instalarse equipos de red en áreas protegidas. Todo el cableado debe estar contenido en conductos o debe pasar por dentro de las paredes para prevenir el acceso no autorizado o la adulteración. Deben deshabilitarse las tomas de red en desuso. Si hay equipos de red dañados o que hayan sido robados, es posible que algunos usuarios de red tengan denegado el servicio.

La política de seguridad debe especificar el nivel de seguridad requerido para la organización. Los dispositivos biométricos, que miden la información física de un usuario, son ideales para el uso en áreas altamente seguras. Sin embargo, para la mayoría de las organizaciones pequeñas, este tipo de solución no es viable.

Datos de seguridad

Puede proteger los datos con dispositivos de seguridad que autentican el acceso de los empleados. La identificación de doble factor es un método que se emplea para incrementar la seguridad. Para acceder a los datos, los empleados deben usar una contraseña y un dispositivo de seguridad de datos similar a los que se mencionan aquí:

- Tarjeta inteligente: dispositivo que tiene la capacidad de almacenar datos de manera segura. La memoria interna es un chip de circuito integrado (ICC) incorporado que se conecta a un lector, ya sea directamente o a través de una conexión inalámbrica. Las tarjetas inteligentes se utilizan en muchas aplicaciones universales, como credenciales de identificación de seguridad, dispositivos de autenticación en línea y pagos seguros con tarjetas de crédito.
- Llavero transmisor de seguridad: dispositivo pequeño similar a un llavero. Tiene un sistema de radio pequeño y de corto alcance que se comunica con la

computadora. El dispositivo es muy pequeño, de modo que se pueda sujetar a un llavero. La computadora debe detectar la señal del llavero transmisor antes de aceptar un nombre de usuario y una contraseña.

- Dispositivo biométrico: identifica una característica física del usuario, como huellas digitales o patrones del iris. Al usuario se le otorga acceso si estas características coinciden con las registradas en la base de datos y si suministra la información correcta de inicio de sesión.

El nivel de seguridad que el cliente necesita determina los dispositivos que se deben seleccionar para proteger los datos y los equipos.

16.2 Selección de los componentes de seguridad según las necesidades del cliente

16.2.3 Descripción y comparación de los distintos tipos de firewall

Los firewalls de hardware y software protegen los datos y equipos de una red contra el acceso no autorizado. Además de un software de seguridad, debe usarse un firewall.

Los firewalls de hardware y software tienen varios modos de filtrar el tráfico de datos de la red:

- Filtro de paquete: conjunto de reglas que autorizan o deniegan el tráfico en función de criterios como direcciones IP, protocolos y puertos utilizados.
- Firewall del proxy: firewall que inspecciona todo el tráfico y autoriza o deniega paquetes en función de las reglas configuradas. Un proxy puede actuar como una gateway que protege las computadoras dentro de la red.
- Inspección de paquetes de estado: firewall que mantiene un registro del estado de las conexiones de red que se transmiten a través del firewall. No se autoriza a atravesar el firewall a los paquetes que no forman parte de una conexión conocida.

Firewall de hardware
Un firewall de hardware es un componente de filtrado físico que inspecciona los paquetes de datos de la red antes de que lleguen a las computadoras y otros dispositivos

de la red. A menudo, los firewalls de hardware se instalan en los routers. Un firewall de hardware es una unidad independiente que no usa los recursos de las computadoras que protege, de modo que no afecta el rendimiento del procesamiento.

Firewall de software
Un firewall de software es una aplicación instalada en una computadora que inspecciona y filtra los paquetes de datos. El firewall de Windows es un ejemplo de un firewall de software que se incluye en el sistema operativo Windows. Un firewall de software utiliza los recursos de la computadora, lo que da como resultado un rendimiento inferior para el usuario.

Tenga en cuenta los elementos enumerados en la Figura 1 al seleccionar un firewall.

NOTA: En una red segura, si el rendimiento de la computadora no es un problema, se debe habilitar el firewall del sistema operativo para obtener una protección adicional. Es posible que algunas aplicaciones no funcionen de manera adecuada, a menos que el firewall esté correctamente configurado para dichas aplicaciones.

Firewall de software y de hardware

Firewall de hardware	Firewall de software
Autónomo, utiliza hardware específico.	Disponible como software de terceros a precios variados.
El costo inicial de las actualizaciones de hardware y software puede ser alto.	El sistema operativo Windows XP incluye un firewall de software.
Pueden protegerse varias computadoras.	Por lo general, protege sólo la computadora en la que está instalado.
Pequeño impacto en el rendimiento de la computadora.	Utiliza la CPU y puede reducir la velocidad de la computadora.

.

16.3Implementación de una política de seguridad del cliente

. Agregar capas de seguridad en una red puede hacer más segura la red, pero las capas adicionales de protección son costosas. Debe considerar el valor de los datos y equipos que desea proteger con el costo de protección al implementar la política de seguridad del cliente.

Al completar esta sección, alcanzará los siguientes objetivos:

- Configurar los parámetros de seguridad.
- Describir la configuración de los distintos tipos de firewall.
- Describir la protección contra software malicioso.

Costos de seguridad

16.3 Implementación de una política de seguridad del cliente

16.3.1 Configuración de los parámetros de seguridad

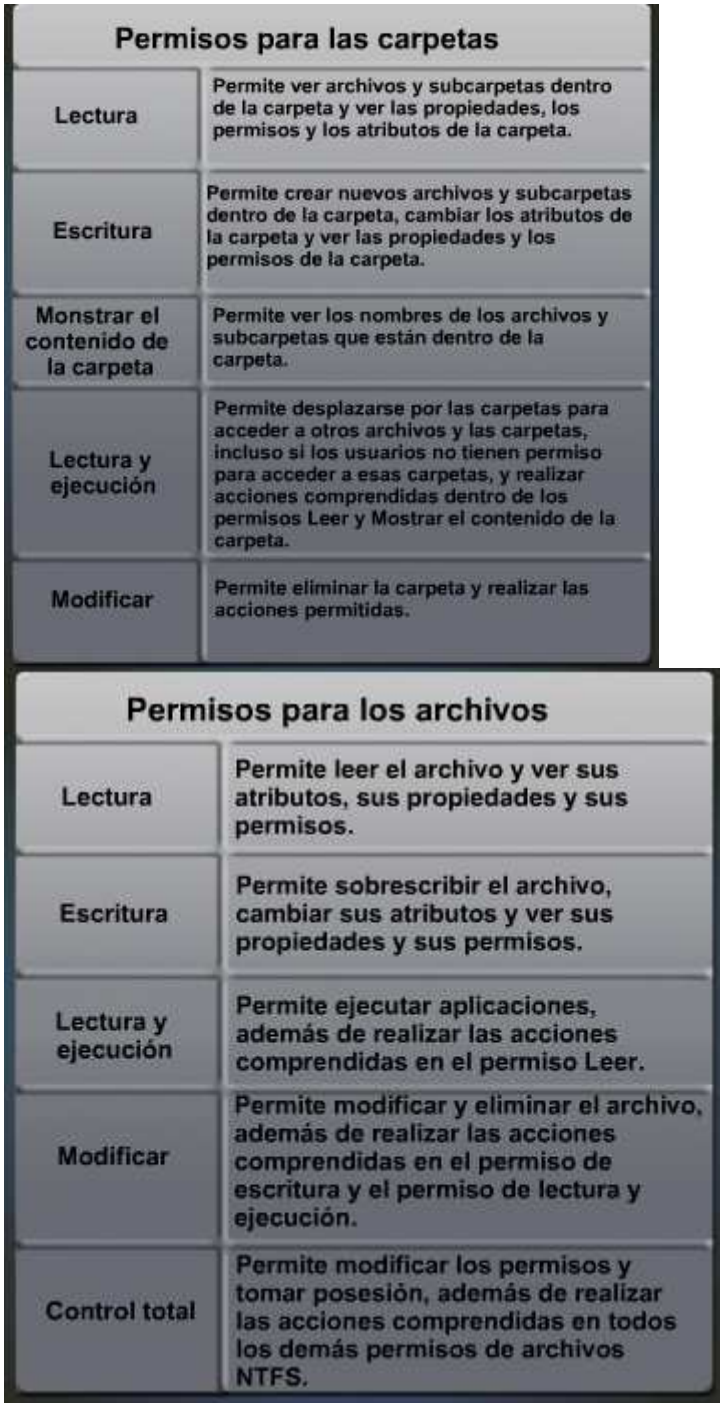
Dos aspectos en los que comúnmente se cometen errores de seguridad son los permisos de acceso a carpetas y archivos y la configuración de la seguridad inalámbrica.

Niveles de permiso de carpetas y archivos
Los niveles de permiso se configuran para restringir el acceso de usuarios individuales o grupales a datos específicos. Las FAT y el NTFS permiten a los usuarios que cuentan con acceso a la red compartir carpetas y obtener permisos de acceso a carpetas. En la Figura 1, se muestran los permisos de carpetas. El NTFS proporciona la seguridad adicional de permisos de archivos. En la Figura 2, se muestran los permisos de archivos.

Configuración de seguridad inalámbrica
Las siguientes herramientas, que se muestran en la Figura 3, se usan para configurar la seguridad inalámbrica:

- Privacidad equivalente por cable (WEP): encripta los datos de broadcast entre el punto de acceso inalámbrico y el cliente con una clave de encriptación de 64 bits o 128 bits. La Figura 4 muestra la configuración de WEP.
- Acceso Wi-Fi protegido (WPA): ofrece una mejor encriptación y autenticación que la WEP.
- Filtrado de direcciones MAC: restringe el acceso de la computadora a un punto de acceso inalámbrico para prevenir que un usuario casual acceda a la red. El filtrado de direcciones MAC, como muestra la Figura 5, es vulnerable cuando se usa solo y debe combinarse con otro filtrado de seguridad.
- Broadcasting del identificador de conjunto de servicios (SSID): el SSID inalámbrico transmite por broadcast la identidad de la red. Desactivar el SSID hace que parezca que la red desaparece, pero ésta es una medida poco confiable de seguridad de red inalámbrica.

- Antenas inalámbricas: el patrón de ganancia y señal de la antena conectada a un punto de acceso inalámbrico puede incidir en el lugar donde se recibe la señal. Para evitar transmitir señales fuera del área de red, instale una antena con un patrón que ofrezca cobertura a los usuarios de su red.



Permisos para las carpetas	
Lectura	Permite ver archivos y subcarpetas dentro de la carpeta y ver las propiedades, los permisos y los atributos de la carpeta.
Escritura	Permite crear nuevos archivos y subcarpetas dentro de la carpeta, cambiar los atributos de la carpeta y ver las propiedades y los permisos de la carpeta.
Monstrar el contenido de la carpeta	Permite ver los nombres de los archivos y subcarpetas que están dentro de la carpeta.
Lectura y ejecución	Permite desplazarse por las carpetas para acceder a otros archivos y las carpetas, incluso si los usuarios no tienen permiso para acceder a esas carpetas, y realizar acciones comprendidas dentro de los permisos Leer y Mostrar el contenido de la carpeta.
Modificar	Permite eliminar la carpeta y realizar las acciones permitidas.

Permisos para los archivos	
Lectura	Permite leer el archivo y ver sus atributos, sus propiedades y sus permisos.
Escritura	Permite sobrescribir el archivo, cambiar sus atributos y ver sus propiedades y sus permisos.
Lectura y ejecución	Permite ejecutar aplicaciones, además de realizar las acciones comprendidas en el permiso Leer.
Modificar	Permite modificar y eliminar el archivo, además de realizar las acciones comprendidas en el permiso de escritura y el permiso de lectura y ejecución.
Control total	Permite modificar los permisos y tomar posesión, además de realizar las acciones comprendidas en todos los demás permisos de archivos NTFS.

16.3 Implementación de una política de seguridad del cliente

16.3.2 Descripción de la configuración de los distintos tipos de firewall

Un firewall impide selectivamente que los usuarios externos establezcan conexiones con una computadora o con un segmento de red. Los firewalls generalmente trabajan abriendo y cerrando los puertos que utilizan las diferentes aplicaciones. Al abrir sólo los puertos requeridos en un firewall, se implementa una política de seguridad restrictiva. Se deniega todo paquete que no esté explícitamente permitido. En cambio, una política de seguridad permisiva permite el acceso a través de todos los puertos, excepto aquellos explícitamente denegados. En una ocasión, se envió software y hardware con todos los parámetros configurados como permisivos. Dado que muchos usuarios no configuraron los equipos, los parámetros permisivos por defecto dejaron muchos dispositivos expuestos a atacantes. La mayoría de los dispositivos ahora se envían con parámetros lo más restrictivos posibles, sin dejar de permitir una fácil instalación.

Firewall de software

Por lo general, los firewalls de software corresponden a una aplicación de software que se ejecuta en la computadora que protegen, o bien, forman parte del sistema operativo. Existen varios firewalls de software de otros fabricantes. Además, como muestra la Figura 1, Windows XP cuenta con un firewall de software incorporado.

La configuración del firewall de Windows XP puede completarse de dos maneras:

- Automáticamente: Aparece un mensaje en el cual el usuario debe seleccionar entre las opciones "Mantener el bloqueo", "Desbloquear" o "Preguntarme más tarde" para todos los pedidos no solicitados. Estas solicitudes pueden provenir de aplicaciones legítimas que no fueron configuradas previamente, o bien, de un virus o gusano que ha infectado el sistema.

- Administrar los parámetros de seguridad: El usuario agrega manualmente el programa o los puertos que se requieren para las aplicaciones en uso en la red.

Para agregar un programa, seleccione:
Inicio > Panel de control > Centro de seguridad > Firewall de Windows > Excepciones > Agregar programa.

Para desactivar el firewall, seleccione:
Inicio > Panel de control > Centro de seguridad > Firewall de Windows.

16.3 Implementación de una política de seguridad del cliente

16.3.3 Descripción de la protección contra software malicioso

El malware es un software malicioso que se instala en una computadora sin el conocimiento ni el permiso del usuario. Ciertos tipos de malware, tales como el spyware y los ataques de suplantación de identidad, recogen datos sobre el usuario que un atacante puede usar para obtener información confidencial.

Debe ejecutar programas de análisis de virus y spyware para detectar y limpiar el software no deseado. Muchos navegadores ahora vienen equipados con herramientas y configuraciones especiales que impiden el funcionamiento de varios tipos de software malicioso. Es posible que se requieran varios programas diferentes y análisis múltiples para eliminar completamente todo el software malicioso:

- **Protección contra virus**: los programas antivirus normalmente se ejecutan de manera automática en un segundo plano y controlan posibles problemas. Cuando se detecta un virus, se advierte al usuario, y el programa intenta poner en cuarentena o eliminar el virus.
- **Protección contra spyware**: los programas antispyware buscan registradores de digitación y otros tipos de malware a fin de eliminarlos de la computadora.
- **Protección contra adware**: los programas antiadware buscan programas que exhiben avisos publicitarios en la computadora.
- **Protección contra suplantación de identidad**: los programas que protegen contra la suplantación de identidad bloquean las direcciones IP de sitios Web de suplantación de identidad conocidos y advierten al usuario sobre sitios Web sospechosos.

Una forma peligrosa de software malicioso que incorpora elementos de ingeniería social es el ataque de suplantación de identidad.

NOTA: El software malicioso puede incorporarse en el sistema operativo. Existen herramientas de eliminación especiales que ofrecen los fabricantes de sistemas operativos para limpiar el sistema operativo.

16.4Realización del mantenimiento preventivo de la seguridad

Se requieren varias tareas de mantenimiento para garantizar que la protección sea efectiva. Esta sección describe la manera de maximizar la protección realizando actualizaciones, copias de seguridad y reconfiguraciones de los sistemas operativos, las cuentas de usuario y los datos.

Al completar esta sección, alcanzará los siguientes objetivos:

- Describir la configuración de las actualizaciones del sistema operativo.
- Realizar mantenimiento de cuentas.
- Explicar los procedimientos de creación de copias de seguridad de datos, el acceso a ellas y los medios de copia de seguridad físicos seguros

16.4 Realización del mantenimiento preventivo de la seguridad

16.4.1 Descripción de la configuración de actualizaciones del sistema operativo

Un sistema operativo es un objetivo probable de ataque, ya que al obtener el control de dicho sistema, es posible controlar la computadora. Entonces, la computadora afectada puede ser capturada y manejada por criminales. Una práctica común consiste en convertir las computadoras infectadas en generadores de correo electrónico no deseado que envíen correos electrónicos nocivos sin que el usuario pueda detenerlos. Una computadora infectada de esta manera se denomina computadora "zombi".

Windows XP descarga e instala actualizaciones automáticas del sistema operativo por defecto. Sin embargo, quizás ésta no sea la mejor manera de actualizar los sistemas. Las actualizaciones pueden entrar en conflicto con la política de seguridad de una organización o con otros parámetros de configuración de una computadora. Además, es posible que un administrador desee evaluar las actualizaciones antes de que se distribuyan a todas las computadoras de la red. Las siguientes opciones disponibles en Windows XP le proporcionan al usuario la capacidad de controlar cuándo se actualiza el software:

- Actualización automática: descarga e instala las actualizaciones automáticamente sin la intervención del usuario.
- Sólo descargar las actualizaciones: descarga las actualizaciones automáticamente, pero se requiere que el usuario las instale.
- Notificarme: notifica al usuario que hay actualizaciones disponibles y brinda la opción de descarga e instalación.
- Desactivar actualizaciones automáticas: impide cualquier tipo de búsqueda de actualizaciones.

Si el usuario cuenta con una red de acceso telefónico, la instalación de Windows Update debe configurarse para notificar al usuario sobre las actualizaciones disponibles, o bien, debe desactivarse. Es posible que el usuario con conexión de acceso telefónico desee controlar la actualización y seleccione el horario en que ésta no interrumpa otra actividad de red ni utilice los recursos limitados disponibles.

16.4 Descripción de los procedimientos de mantenimiento preventivo para las computadoras portátiles

16.4.2 Mantenimiento de cuentas.

Es posible que los empleados de una organización requieran distintos niveles de acceso a los datos. Por ejemplo, quizás, un administrador y un contador sean los únicos empleados de una organización que tengan acceso a los archivos de la nómina de sueldos.

Es posible agrupar a los empleados según los requisitos laborales y concederles acceso a archivos de acuerdo con los permisos del grupo. Este proceso ayuda a administrar el acceso a la red por parte de los empleados. Pueden configurarse cuentas temporales para los empleados que necesitan acceso por poco tiempo. Una administración adecuada del acceso a la red puede ayudar a reducir las áreas de vulnerabilidad que permiten que un virus o un software malicioso se introduzca en la red.

Suspensión del acceso de un empleado
Cuando un empleado abandona una organización, debe concluirse de inmediato el acceso a los datos y al hardware de la red. Si el empleado anterior almacenó archivos en un espacio personal del servidor, desactive la cuenta para eliminar el acceso. Si después de un tiempo el reemplazante del empleado requiere acceso a las aplicaciones y al espacio de almacenamiento, vuelva a habilitar la cuenta y cambie el nombre por el del nuevo empleado.

Cuentas de invitados
Es posible que los empleados interinos y los invitados necesiten tener acceso a la red. Por ejemplo, quizás muchos visitantes necesiten tener acceso al correo electrónico, a Internet y a una impresora de red. Todos estos recursos pueden estar disponibles para una cuenta especial llamada Invitado. Cuando los visitantes están presentes, se les puede asignar una cuenta de invitado. Cuado no hay visitantes presentes, se puede suspender la cuenta hasta que el llegue un nuevo visitante.

Es posible que algunas cuentas de visitante requieran un acceso extensivo a los recursos, como en el caso de un consultor o un auditor financiero. Este tipo de acceso debe otorgarse sólo para el período requerido para completar el trabajo.

16.4 Realización del mantenimiento preventivo de la seguridad

16.4.3 Explicación de los procedimientos de creación de copias de seguridad de datos, acceso a ellas y medios de copia de seguridad físicos seguros

Una copia de seguridad de datos almacena una copia de la información de una computadora en un medio de copia de seguridad extraíble que puede guardarse en un lugar seguro. Si el hardware de la computadora falla, se puede restaurar la copia de seguridad de datos para que el proceso pueda continuar.

Las copias de seguridad de datos deben realizarse a diario. La copia de seguridad de datos más reciente generalmente se almacena fuera del sitio de trabajo para proteger el medio de copia de seguridad por si algo sucede con la instalación principal. Los medios de copia de seguridad a menudo se reutilizan para ahorrar dinero. Siempre siga las pautas de rotación de medios de cada organización.

Las operaciones de creación de copias de seguridad pueden realizarse en la línea de comandos o desde un archivo de lote mediante el comando NTBACKUP. Los parámetros por defecto para un NTBACKUP serán los establecidos en la utilidad de seguridad de Windows. Todas las opciones que desee sobrescribir deben incluirse en la línea de comando. El comando NTBACKUP no se puede utilizar para restaurar archivos.

Una combinación de tipos de copias de seguridad, como muestra la Figura 1, permite que se realicen eficazmente copias de seguridad de los datos. Una copia de seguridad completa es una copia de todos los archivos de la unidad. Una copia de seguridad incremental realiza copias de los archivos creados y modificados desde la última copia de seguridad normal o incremental. Indica los archivos que se han realizado copias de seguridad. Una copia de seguridad diferencial copia los archivos creados o cambiados desde la última copia de seguridad normal o incremental, pero no indica qué archivos se han realizado copias de seguridad. Hacer copias de seguridad de los datos puede tomar tiempo; por lo tanto, es preferible realizar las copias de seguridad cuando el tráfico de la red es bajo. Otros tipos de copias de seguridad incluyen la copia de seguridad diaria y la copia de seguridad simple, las cuales no indican los archivos que se han realizado copias de seguridad.

El medio de copia de seguridad de datos es tan importante como los datos en la computadora. Debe almacenar el medio de copia de seguridad en una instalación de almacenamiento fuera del sitio de trabajo, con temperatura controlada y con la seguridad física adecuada. Las copias de seguridad deben estar disponibles de inmediato para el acceso en caso de una emergencia.

Tipos de copias de seguridad

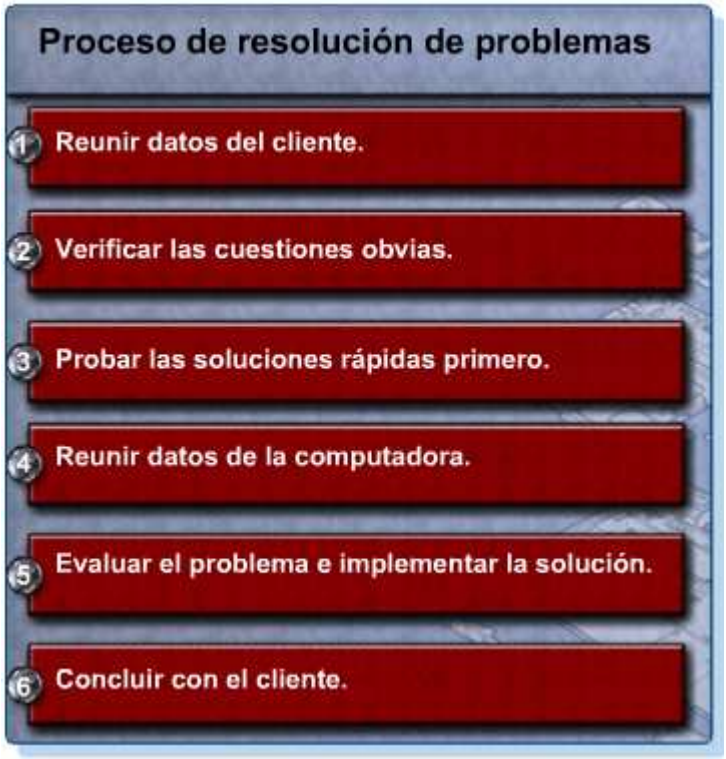
Tipo de copia de seguridad	Descripción
Copia de seguridad normal o completa	Archiva todos los elementos seleccionados.
Copia de seguridad incremental	Archiva todos los elementos seleccionados que se modificaron desde la última copia de seguridad completa o incremental.
Copia de seguridad diferencial	Archiva todos los elementos seleccionados que se modificaron desde la última copia de seguridad completa o incremental.
Copia de seguridad diaria	Archiva todos los elementos seleccionados que se modificaron el día en que se realizó la copia de seguridad.
Copia de seguridad de copia	Archiva todos los elementos seleccionados.

16.5Resolución de problemas de seguridad

El proceso de resolución de problemas se usa para resolver problemas de seguridad. Estos problemas van desde los simples, como crear una copia de seguridad, hasta los más complejos, como la configuración del firewall. Siga los pasos para la resolución de problemas a modo de guía para poder diagnosticar y reparar problemas.

Al completar esta sección, alcanzará los siguientes objetivos:

- Revisar el proceso de resolución de problemas.
- Identificar problemas y soluciones comunes.
- Aplicar las habilidades de resolución de problemas.



16.5 Resolución de problemas de seguridad

16.5.1 Revisión del proceso de resolución de problemas

Los técnicos en computación deben ser capaces de analizar las amenazas contra la seguridad y determinar qué método corresponde utilizar para proteger los activos y reparar los daños. Este proceso se denomina resolución de problemas.

El primer paso en el proceso de resolución de problemas es reunir los datos del cliente. Las figuras 1 y 2 enumeran las preguntas abiertas y cerradas para formular al cliente.

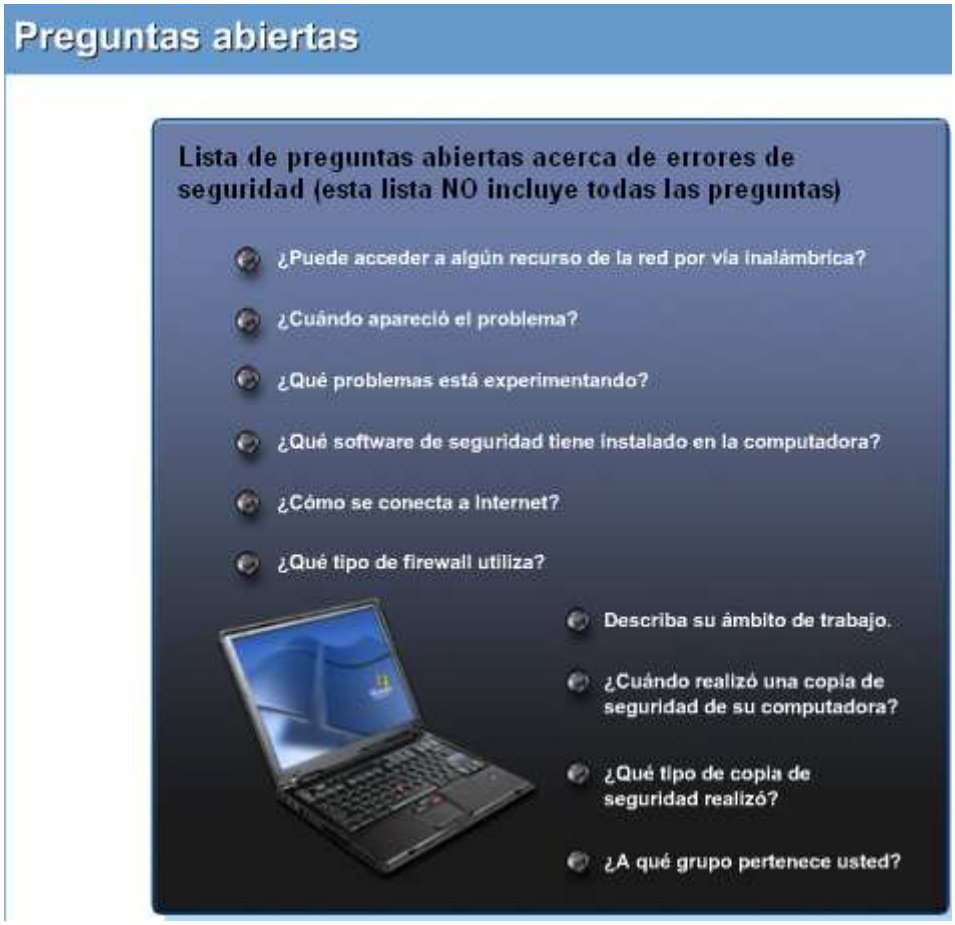
Una vez que haya hablado con el cliente, deberá verificar las cuestiones obvias. La Figura 3 enumera los problemas relacionados con las computadoras portátiles.

Una vez que las cuestiones obvias se hayan verificado, pruebe con algunas soluciones rápidas. En la Figura 4, se mencionan algunas soluciones rápidas para problemas relacionados con computadoras portátiles.

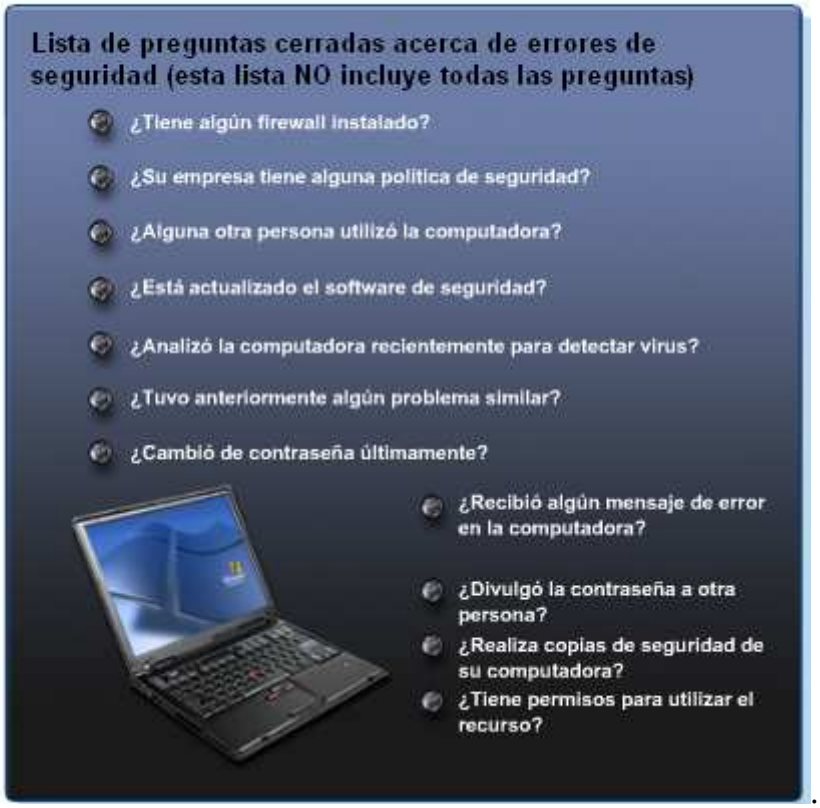
Si las soluciones rápidas no permiten resolver el problema, deberá reunir datos de la computadora. En la Figura 5, se muestran diversos modos de reunir información sobre el problema de la computadora portátil.

En este momento, tendrá la información necesaria para evaluar el problema, buscar e implementar las soluciones posibles. En la Figura 6, se muestran recursos para soluciones posibles.

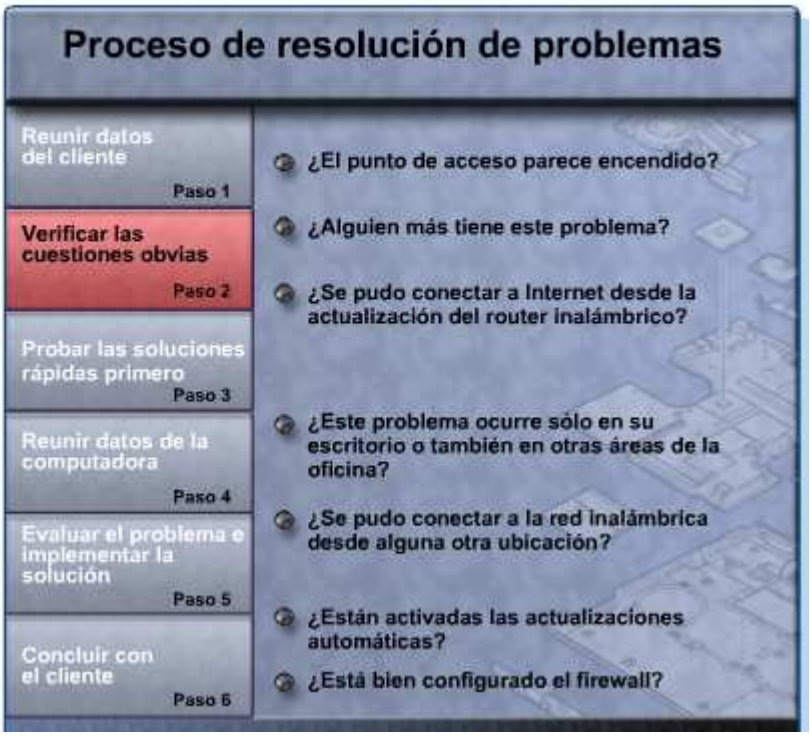
Una vez solucionado el problema, concluirá con el cliente. En la Figura 7, se muestra una lista de tareas necesarias para completar este paso.



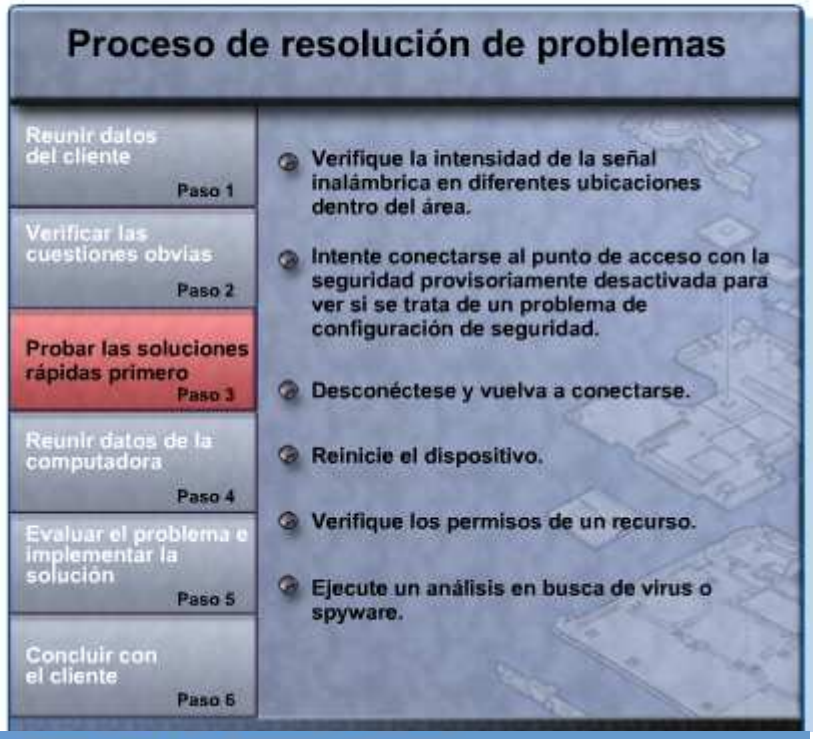
Preguntas cerradas



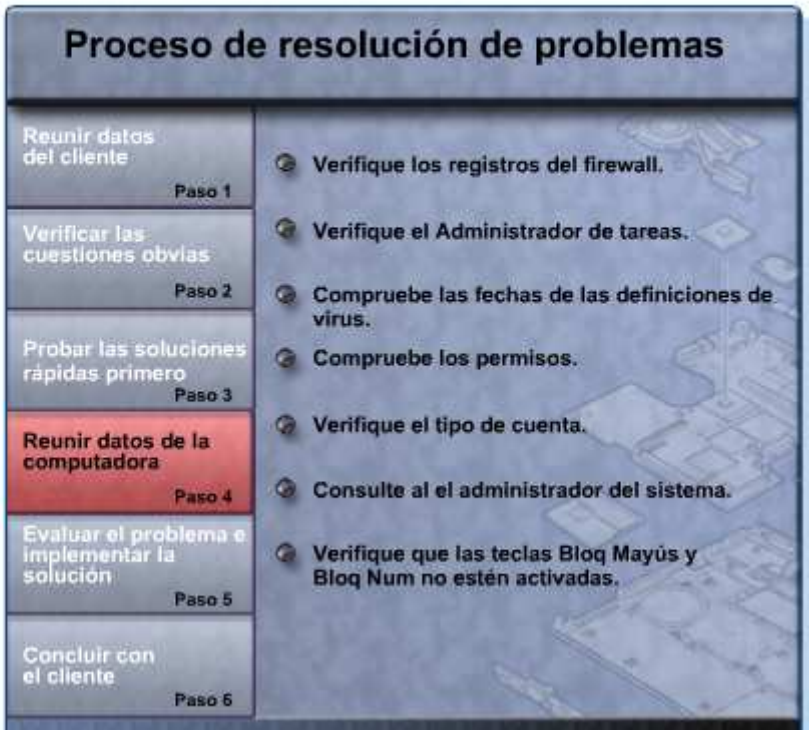
Verificar las cuestiones obvias



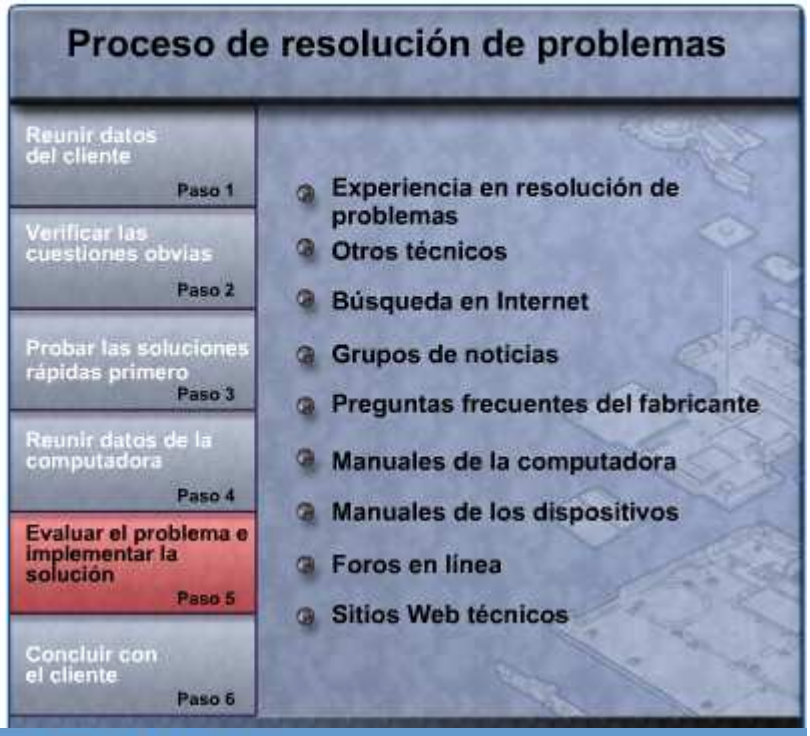
Probar las soluciones rápidas primero



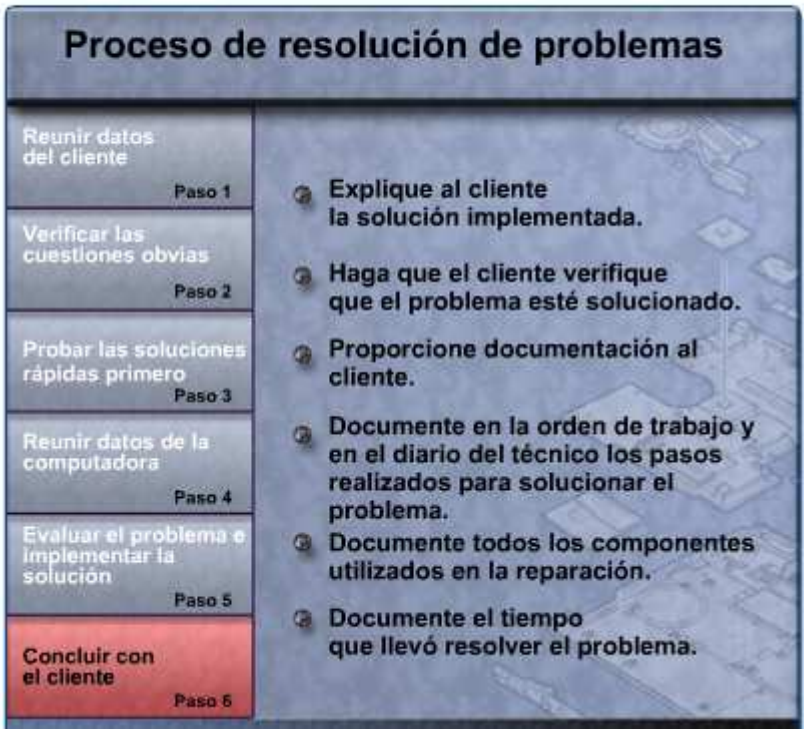
Reunir datos de la computadora



Evaluar el problema e implementar la solución



Concluir con el cliente



16.5 Resolución de problemas de seguridad

16.5.2 Identificación de problemas y soluciones comunes.

Los problemas de seguridad en la computadora pueden atribuirse a problemas de hardware, software o redes, o bien a una combinación de los tres. Usted resolverá

algunos tipos de problemas de seguridad con más frecuencia que otros. La Figura 1 presenta una tabla de los problemas de seguridad comunes y las soluciones.

Problemas y soluciones comunes

Síntoma del problema	Solución posible
Un cliente informa que una copia de seguridad que comenzó a realizarse la noche anterior aún no finalizó.	Recomiende al cliente implementar otro método de copias de seguridad que le permita ahorrar tiempo.
Un consultor visita la empresa y no puede acceder mediante la cuenta de invitado a los archivos que necesita.	Otorgue acceso a los archivos durante la visita. Cuando el consultor se marche, deshabilite la cuenta.
Un usuario se niega a enviarle por correo electrónico el ID y la clave del estudiante que usted le solicitó.	Informe al usuario que no se le solicitaron esos datos. Obtenga información y advierta a otras personas acerca de este ataque por suplantación de identidad.
Un usuario puede ubicar un archivo en el servidor, pero no puede descargarlo.	Cambie los permisos de los usuarios de este archivo de lectura a lectura y ejecución.
Un usuario no se puede conectar a la red con un router inalámbrico, incluso después de haber configurado la correspondiente clave de seguridad.	Verifique que la dirección MAC del usuario esté en la lista de la tabla de filtros de dirección MAC.

16.5 Resolución de problemas de seguridad

16.5.3 Aplicación de las habilidades de resolución de problemas

Ahora que conoce el proceso de resolución de problemas, es momento de aplicar su habilidad para escuchar y diagnosticar.

La primera práctica de laboratorio está diseñada para reforzar sus habilidades con los problemas de seguridad. Deberá indicarle al cliente la manera de corregir un problema de seguridad que impide la conexión a la red inalámbrica.

La segunda práctica de laboratorio está diseñada para reforzar sus habilidades de comunicación y resolución de problemas. En esta práctica de laboratorio, realizará los siguientes pasos:

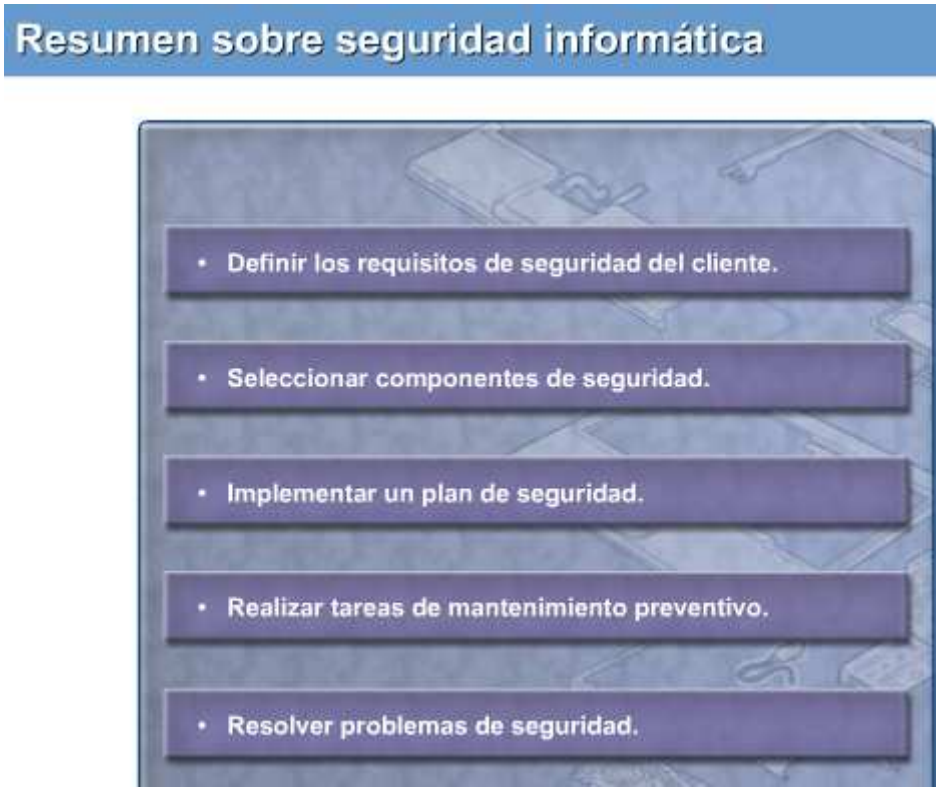
Recibir la orden de trabajo.

Acompañar al cliente en los diferentes pasos para evaluar y resolver el problema.
Documentar el problema y la solución.

16.6 Resumen

En este capítulo, se abordó el tema de la seguridad informática y la importancia de proteger computadoras, redes y datos. Se describieron las amenazas, los procedimientos y las tareas de mantenimiento preventivo relacionadas con la seguridad física y de los datos para ayudarlo a mantener protegidos las computadoras y los datos. La seguridad protege las computadoras, los equipos de red y los datos frente a cualquier pérdida o peligro físico. Algunos de los conceptos importantes de este capítulo que cabe recordar son:

- Las amenazas contra la seguridad pueden provenir desde un origen interno o externo de la organización.
- Los virus y gusanos constituyen amenazas comunes que atacan los datos.
- El desarrollo y el mantenimiento de un plan de seguridad son indispensables para proteger tanto los datos como los equipos frente a pérdidas.
- Es esencial mantener los sistemas operativos y las aplicaciones actualizados y protegidos con parches y paquetes de servicios.



¿Qué aspecto de la seguridad incluye tecnología biométrica y el bloqueo de puertas?

- Protección del acceso a archivos de datos
- Protección del acceso a inicios de sesión
- Protección del acceso inalámbrico
- ✓ Protección del acceso a las instalaciones

¿Qué práctica es un requisito mínimo para la protección de una red?

- Implementar un firewall.
- ✓ Crear información de inicio de sesión segura para todos los usuarios.
- Encriptar todos los datos.
- Registrar todas las actividades de la red.

¿Qué elemento protege físicamente los medios de red contra los daños y el acceso no autorizado?

- ✓ Conducto
- Candado
- Personal de seguridad
- Equipo de vídeo

¿Qué tipo de ataque es ejecutado por un pirata informático que simula ser una organización de confianza y envía mensajes de correo electrónico para engañar al usuario y lograr que proporcione información confidencial?

- Denegación de servicio
- Grayware
- ✓ Suplantación de identidad
- Troyano

¿Desde qué punto debe comenzar a recopilar información el técnico para resolver problemas informáticos?

- Base de conocimiento del sistema operativo
- Registros del sistema operativo
- ✓ Usuario
- Proveedor del equipo

Un consultor de seguridad está buscando un dispositivo de hardware que permita sólo a los usuarios autorizados obtener acceso a los datos confidenciales. ¿Qué dispositivo le garantiza que sólo podrán acceder a los datos los empleados autorizados?

- Candado de cable
- Candado de estación de acoplamiento
- Gabinete con candado
- ✓ Dispositivo de seguridad

En una red con Windows XP, ¿qué tarea es necesaria para garantizar que se elimine cualquier vulnerabilidad del sistema operativo y se reparen los errores identificados?

- Realizar una auditoría de los archivos del sistema y del usuario ubicados en el sistema periódicamente.
- Utilizar un firewall basado en software periódicamente.
- Instalar un programa contra spyware de terceros para supervisar el tráfico periódicamente.
- ✓ Descargar e instalar actualizaciones del sistema operativo periódicamente.

Un técnico nota que la política de seguridad corporativa es considerada una política de seguridad restrictiva. ¿Qué definición corresponde a una política de seguridad restrictiva?

- Se permite todo el tráfico que no esté denegado específicamente.
- Sólo se permite el tráfico que ingresa a la red a través de puertos específicos.
- ✓ Se deniega todo el tráfico que no esté permitido específicamente.
- Se permite el tráfico si aprueba correctamente todas las medidas de seguridad configuradas.