# IT Essentials: PC Hardware and Software Version 4.0 Spanish
# Capítulo 9

## 9.0 Introducción

Los técnicos deben tener conocimiento acerca de la seguridad de las computadoras y las redes. La falta de implementación de los procedimientos de seguridad adecuados puede tener consecuencias negativas para los usuarios, las computadoras y el público en general. Si no se siguen tales procedimientos de seguridad, se pueden poner en peligro la información privada, los secretos de la empresa, la información financiera, las computadoras y los datos relacionados con la seguridad nacional.

Al completar este capítulo, alcanzará los siguientes objetivos:

- Explicar la importancia de la seguridad.
- Describir las amenazas contra la seguridad.
- Identificar procedimientos de seguridad.
- Identificar técnicas comunes de mantenimiento preventivo para mayor lograr seguridad.
- Solucionar problemas de seguridad.

## Seguridad informática

9.1
Explicación de la importancia de la seguridad

La seguridad de las computadoras y las redes ayuda a conservar el funcionamiento de los equipos y los datos, además de proporcionar acceso sólo a determinados usuarios. Todo miembro de una organización debe considerar la seguridad como una cuestión de alta prioridad, ya que una falla puede perjudicar a todos.

Algunos de los peligros a los que están expuestas las computadoras y las redes son: robo, pérdida, intrusión en la red y daño físico. El daño o la pérdida de equipos pueden conllevar una pérdida de productividad. La reparación y la sustitución de equipos pueden costar tiempo y dinero a la empresa. El uso no autorizado de una red puede exponer la información confidencial y reducir los recursos de red.

Los ataques que disminuyen intencionalmente el rendimiento de una computadora o una red también pueden perjudicar la producción de una organización. La implementación deficiente de medidas de seguridad en dispositivos de redes inalámbricas demuestra que para el acceso no autorizado de intrusos, no se necesita ineludiblemente una conectividad física.

Las principal responsabilidad del técnico es mantener un nivel eficaz de seguridad, tanto de los datos como de la red. Un cliente o una organización puede depender del técnico para asegurar la integridad de sus datos y computadoras. El técnico debe ejecutar tareas más delicadas que las de un empleado común y corriente. Puede tener que efectuar reparaciones, ajustes e instalación de equipos. Necesita saber cómo configurar determinadas opciones para mantener la red protegida, pero disponible para aquellas personas que necesitan utilizarla. Debe cerciorarse de que se apliquen todos los parches y actualizaciones de software y de que haya instalado software antivirus y de protección contra spyware. Además, se le solicitará que explique a los usuarios cómo mantener buenas prácticas de seguridad en las computadoras.

9.2 Descripción de las amenazas contra la seguridad

Para proteger las computadoras y las redes correctamente, es preciso que el técnico comprenda ambos tipos de amenazas contra la seguridad informática:

- Física: eventos o ataques que consisten en el robo, el daño o la destrucción de equipos, como servidores, switches y cables.
- De datos: eventos o ataques que consisten en la eliminación, el daño o el robo de información, o bien en la denegación o la autorización de acceso a ella.

Las amenazas contra la seguridad pueden originarse dentro o fuera de la organización, y el nivel de daño potencial puede variar en gran medida:

- Amenazas internas: empleados que tienen acceso a la información, los equipos y la red.
  - Las amenazas malintencionadas ocurren cuando el empleado tiene la intención de causar un daño.
  - Las amenazas accidentales tienen lugar cuando el usuario daña la información o el equipo de manera involuntaria.
- Amenazas externas: usuarios fuera de la organización que no tienen acceso

autorizado a la red o los recursos.
- Amenazas no estructuradas: el atacante utiliza los recursos disponibles, como contraseñas o comandos, para obtener acceso a la red y ejecutar programas diseñados para producir daños.
- Amenazas estructuradas: el atacante utiliza un código para acceder al sistema operativo y al software.

Las pérdidas o daños físicos de los equipos pueden resultar costosos, y la pérdida de información puede ser perjudicial para la empresa u organización. Las amenazas que atentan contra la información cambian constantemente a medida que los atacantes descubren nuevas formas de obtener acceso y cometer delitos.

Al completar esta sección, alcanzará los siguientes objetivos:

- Definir virus, gusano y troyano.
- Brindar una explicación sobre la seguridad en la Web.
- Definir adware, spyware y grayware.
- Explicar el concepto de denegación de servicio.
- Describir el correo no deseado y las ventanas emergentes.
- Brindar una explicación de la ingeniería social.
- Brindar una explicación de los ataques de TCP/IP.
- Explicar los conceptos de deconstrucción y reciclado de hardware.

## 9.2 Descripción de las amenazas contra la seguridad

### 9.2.1 Definición de virus, gusano y troyano

Los virus de computadora son creados y enviados deliberadamente por atacantes. Los virus se adjuntan a pequeñas porciones de código informático, software o documentos, y se ejecutan al iniciar el software en cuestión en una computadora. Si se propagan hacia otras computadoras, es probable que éstas continúen propagándolos.

Los virus pueden definirse como programas creados malintencionadamente y enviados por atacantes. Se transmiten a otras computadoras por correo electrónico, transferencias de archivos y mensajería instantánea. Para esconderse, los virus se adjuntan a un archivo almacenado en la computadora. Cuando se accede al archivo, el virus se ejecuta e infecta la computadora. Los virus son capaces de dañar, e incluso eliminar, archivos de la computadora, utilizar el servicio de correo electrónico para propagarse hacia otras computadoras o, incluso, borrar todos los archivos del disco duro.

Algunos virus pueden resultar excepcionalmente peligrosos. El tipo más perjudicial de virus se utiliza para registrar las pulsaciones de teclas. Los atacantes pueden utilizar estos virus para obtener información confidencial, como contraseñas y números de tarjetas de crédito. Los virus también pueden alterar o destruir la información almacenada en la computadora. Los virus ocultos pueden infectar la computadora y permanecer inactivos hasta que el atacante los ejecute.

Un gusano es un programa capaz de replicarse y dañar redes. Utiliza la red para duplicar su código de acceso en los hosts de una red. Por lo general, lo hace sin la intervención del usuario. A diferencia del virus, el gusano no necesita adjuntarse a un programa para infectar un host. Incluso si no daña los datos o las aplicaciones de los hosts infectados,

resulta problemático para las redes ya que consume ancho de banda.

El troyano es técnicamente un gusano. No necesita adjuntarse a otro software. En cambio, la amenaza del troyano se oculta en software que parece realizar determinada tarea pero que, entre bambalinas, realiza otra. Por lo general, el troyano se presenta disfrazado de software útil. Puede reproducirse como un virus y propagarse a otras computadoras. Los daños ocasionados en la información y la producción pueden ser significativos. Es probable que se requieran los servicios de reparación de un técnico y que los empleados pierdan o deban reemplazar información. Una computadora infectada puede estar enviando información esencial a la competencia y, al mismo tiempo, infectando otras computadoras de la red.

El software de protección contra virus, conocido como software antivirus, está diseñado especialmente para detectar, desactivar y eliminar virus, gusanos y troyanos antes de que infecten la computadora. Sin embargo, el software antivirus se desactualiza rápidamente, y es responsabilidad del técnico aplicar las actualizaciones, los parches y las definiciones de virus más recientes como parte de un programa de mantenimiento periódico. Muchas organizaciones cuentan con políticas escritas de seguridad que prohíben a los empleados instalar software que no haya sido proporcionado por la empresa. Algunas organizaciones también ponen al tanto a los empleados acerca de los peligros relacionados con la apertura de archivos adjuntos de correo electrónico que pueden contener virus o gusanos.

**Ataque informático**


## 9.2 DescripciÃ³n de las amenazas contra la seguridad

### 9.2.2Explicación de la seguridad en la Web

La seguridad en la Web es importante debido a la cantidad de usuarios que utilizan la World Wide Web a diario. Algunas de las funciones que hacen que la Web sea útil y

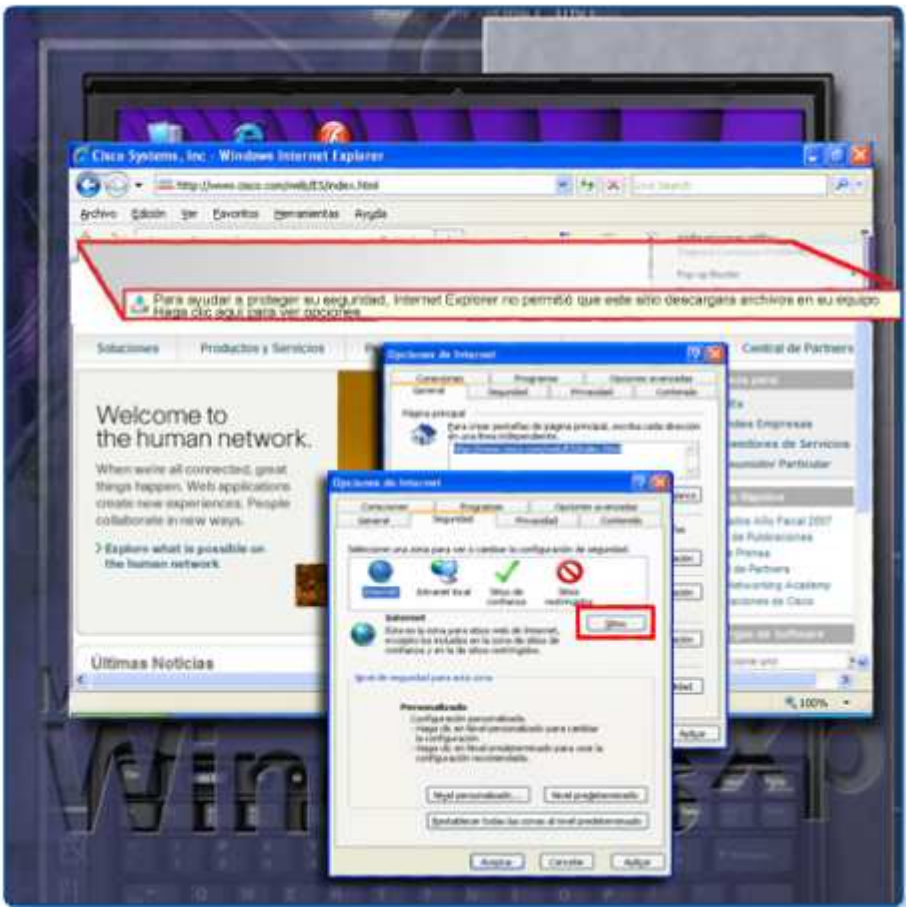
entretenida pueden también resultar perjudiciales para la computadora.

Las herramientas empleadas para aumentar la capacidad y versatilidad de las páginas Web, como se ilustra en la Figura 1, pueden asimismo tornar la computadora más vulnerable a los ataques. Éstos son algunos ejemplos de herramientas Web:

- **ActiveX**: tecnología creada por Microsoft para controlar la interactividad en las páginas Web. Si una página tiene ActiveX, es necesario descargar un applet, un pequeño programa, para poder utilizar todas las funciones.
- **Java**: lenguaje de programación que permite ejecutar applets dentro del explorador Web. Como ejemplos de applets, podemos mencionar una calculadora o un contador.
- **JavaScript**: lenguaje de programación desarrollado para interactuar con el código fuente HTML y permitir la navegación en sitios Web interactivos. Por ejemplo: un aviso publicitario rotativo o una ventana emergente.

Los atacantes pueden utilizar cualquiera de estas herramientas para instalar un programa en una determinada computadora. Para evitar estos ataques, la mayoría de los exploradores tienen opciones que obligan al usuario a autorizar la descarga o el uso de ActiveX, Java o JavaScript, como se muestra en la Figura 2.

# Seguridad del explorador




## 9.2 DescripciÃ³n de las amenazas contra la seguridad

### 9.2.3 Definición de adware, spyware y grayware

Por lo general, las aplicaciones de adware, spyware y grayware se instalan en la computadora sin que el usuario se entere. Estos programas reúnen información almacenada en la computadora, cambian la configuración de ésta o abren ventanas adicionales sin la autorización del usuario.

El adware es un programa de software que muestra publicidad en la pantalla. Suele distribuirse con el software descargado. Por lo general, el adware aparece en una ventana emergente. A veces, estas ventanas emergentes son difíciles de controlar, y tienden a abrirse nuevas ventanas cada vez más rápido y antes de que el usuario pueda cerrarlas.

El grayware o malware es un archivo o programa potencialmente perjudicial que no entra en la categoría de virus. Muchos ataques de grayware incluyen la suplantación de identidad con el fin de persuadir al lector para que inadvertidamente otorgue a los atacantes acceso a información personal. Al completar un formulario en línea, la información se envía al atacante. El grayware puede eliminarse mediante herramientas de eliminación de spyware y adware.

El spyware, un tipo de grayware, es similar al adware. Se distribuye sin la intervención ni

el conocimiento del usuario. Una vez instalado, el spyware controla la actividad de la computadora. Luego, envía esta información a la organización que creó el spyware.

La suplantación de identidad es una forma de ingeniería social en la cual el atacante simula representar a una organización externa auténtica, como un banco. Se envía un correo electrónico a la posible víctima, donde es probable que el atacante solicite verificar determinada información, como una contraseña o un nombre de usuario, supuestamente para prevenir efectos no deseados.

NOTA: Es muy raro que se deba divulgar en línea información confidencial personal o financiera. No confíe. Use el servicio postal para compartir información confidencial.


9.2 DescripciÃ³n de las amenazas contra la seguridad

9.2.4Explicación de denegación de servicio

La denegación de servicio (DoS) es una forma de ataque que impide al usuario acceder a los servicios normales, como correo electrónico y servidor Web, ya que el sistema está ocupado respondiendo a una inmensa cantidad de solicitudes poco frecuentes. El ataque de DoS actúa mediante el envío de cierta cantidad de solicitudes para un recurso del sistema, de modo que el servicio requerido se sobrecarga y deja de funcionar.

Los ataques de DoS más comunes son:

- Ping de la muerte: una serie de pings reiterados, de mayor tamaño de lo normal, que hacen que colapse la computadora receptora.

- Bomba de correo electrónico: una gran cantidad de correo electrónico masivo que satura el servidor de correo electrónico e impide el acceso del usuario.

Los ataques DoS distribuidos (DDoS) son un tipo de DoS que utilizan muchas computadoras infectadas, denominadas computadoras "zombi", para ejecutar un ataque. El objetivo de los ataques de DDoS es obstruir o saturar el acceso a un determinado servidor. Dado que las computadoras zombi están situadas en distintos puntos geográficos, resulta difícil rastrear el origen del ataque.

## 9.2 DescripciÃ³n de las amenazas contra la seguridad

### 9.2.5Descripción del correo no deseado y las ventanas emergentes

El correo no deseado, conocido también como correo basura, es correo no solicitado, como se muestra en la Figura 1. En la mayoría de los casos, el correo no deseado se usa como medio de publicidad. Sin embargo, este tipo de correo puede utilizarse para enviar enlaces perjudiciales o contenido engañoso, como se muestra en la Figura 2.

Si se usa como método de ataque, el correo no deseado puede incluir enlaces con sitios Web infectados o archivos adjuntos capaces de infectar la computadora. Estos enlaces o archivos adjuntos pueden hacer que se abran muchas ventanas para llamar la atención del usuario y llevarlo a sitios publicitarios. Estas ventanas se denominan ventanas emergentes. Como se ilustra en la Figura 2, las ventanas emergentes sin control pueden cubrir rápidamente la pantalla del usuario e impedir que éste realice su trabajo.

Muchos programas antivirus y de correo electrónico automáticamente detectan y eliminan el correo no deseado del buzón de entrada. Sin embargo, es posible que se siga filtrando algún mensaje de correo no deseado, por lo que debe prestarse atención a las siguientes indicaciones:

- Campo de asunto vacío
- Direcciones de remitente incompletas
- Mensajes de correo electrónico generados por computadora
- Respuestas a mensajes no enviados por el usuario

## 9.2 DescripciÃ³n de las amenazas contra la seguridad

### 9.2.6 Explicación de la ingeniería social

Se denomina ingeniero social a toda persona capaz de obtener acceso a un equipo o una red engañando a otros usuarios para que le suministren los datos de acceso necesarios. Por lo general, el ingeniero social se gana la confianza de un empleado y lo convence para que divulgue información sobre nombres de usuario y contraseñas.

El ingeniero social puede presentarse como un técnico para lograr ingresar a las instalaciones, como se muestra en la Figura 1. Una vez adentro, el ingeniero social puede vigilar las tareas que se realizan y reunir información, buscar papeles que contengan contraseñas o extensiones de teléfonos en los escritorios u obtener un directorio de la empresa con direcciones de correo electrónico. La Figura 2 enumera algunos de los trucos típicos que puede usar un ingeniero social.

A continuación, encontrará una serie de precauciones que lo ayudarán a protegerse de la

ingeniería social:

- Nunca revele su contraseña.
- Siempre solicite la identificación de las personas desconocidas.
- Restrinja el acceso de visitas inesperadas.
- Acompañe a todas las visitas.
- Nunca publique su contraseña en el área de trabajo.
- Bloquee la computadora al apartarse del escritorio.
- No permita que nadie pase con usted por una puerta que requiera el uso de una tarjeta de acceso.

## 9.2 DescripciÃ³n de las amenazas contra la seguridad

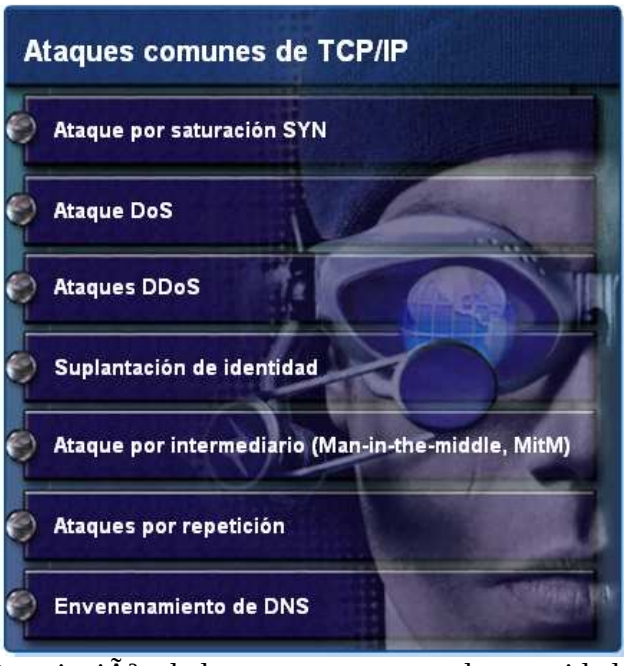
### 9.2.7 Explicación de los ataques de TCP/IP

TCP/IP es un suite de protocolos utilizado para controlar todas las comunicaciones en Internet. Lamentablemente, TCP/IP también puede hacer que la red sea vulnerable a los atacantes.

Algunos de los ataques más comunes son:

- Saturación SYN: abre aleatoriamente puertos TCP y envía al equipo de red o a la computadora una gran cantidad de solicitudes falsas, lo que impide a otros establecer una conexión.
- DoS: envía cantidades inusualmente grandes de solicitudes a un sistema, lo que impide el acceso a los servicios.
- DDoS: utiliza computadoras "zombi" para dificultar el rastreo del origen del ataque DoS.
- Suplantación de identidad o "spoofing": obtiene acceso a los recursos de los dispositivos simulando ser una computadora de confianza.
- Intermediario: intercepta o introduce información falsa en el tráfico entre dos hosts.
- Repetición: utiliza husmeadores de red para extraer nombres de usuarios y contraseñas, y emplearlos posteriormente para obtener acceso.
- Envenenamiento de DNS: modifica los registros de DNS de un sistema para redireccionarlo a servidores falsos donde se almacena la información.

## Ataques comunes de TCP/IP




9.2 DescripciÃ³n de las amenazas contra la seguridad

9.2.8 Explicación de la deconstrucción y el reciclado de hardware

La deconstrucción de hardware es el proceso de eliminar información confidencial del hardware y el software antes del reciclado o descarte. Los datos de las unidades de disco duro deben borrarse por completo a fin de impedir la recuperación mediante aplicaciones de software especiales. Borrar los archivos o incluso formatear la unidad no es suficiente. Se recomienda utilizar alguna herramienta de otros fabricantes para sobrescribir la información varias veces hasta dejarla inutilizable. La única forma de asegurarse de que la información de una unidad de disco duro no pueda recuperarse es destrozar cuidadosamente los platos con un martillo y desechar las piezas de manera segura.

Ciertos medios, como los CD y los disquetes, también deben destruirse. Utilice una máquina trituradora diseñada para tal fin.

9.3Identificación de procedimientos de seguridad

Los planes de seguridad sirven para determinar qué se debe hacer en 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.

Al completar esta sección, alcanzará los siguientes objetivos:

- Explicar los requisitos de una política de seguridad local básica.
- Explicar las tareas necesarias para proteger los equipos físicos.
- Describir formas de proteger los datos.
- Describir técnicas de seguridad inalámbrica.

## Pirámide de seguridad


## 9.3 Identificación de procedimientos de seguridad

### 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 Identificación de procedimientos de seguridad

### 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).

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 Identificación de procedimientos de seguridad

### 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 archivos
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.

## Comparación entre FAT32 y NTFS

| | 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. |

## 9.3 Identificación de procedimientos de seguridad

### 9.3.4 Descripción de técnicas de seguridad inalámbrica

Debido a que, en las redes inalámbricas, el tráfico fluye a través de ondas de radio, resulta fácil para los atacantes controlar y atacar los datos sin tener que conectarse físicamente a la red. Para acceder a la red, el atacante debe estar dentro del alcance de una red inalámbrica desprotegida. El técnico debe saber cómo configurar los puntos de acceso y las tarjetas de redes (NIC) inalámbricas para lograr un nivel adecuado de seguridad.

Al instalar servicios inalámbricos, se deben aplicar inmediatamente técnicas de seguridad inalámbrica a fin de impedir el acceso no deseado a la red, como se muestra en la Figura 1. Los puntos de acceso inalámbrico deben configurarse con opciones básicas de seguridad compatibles con la seguridad actual de la red.

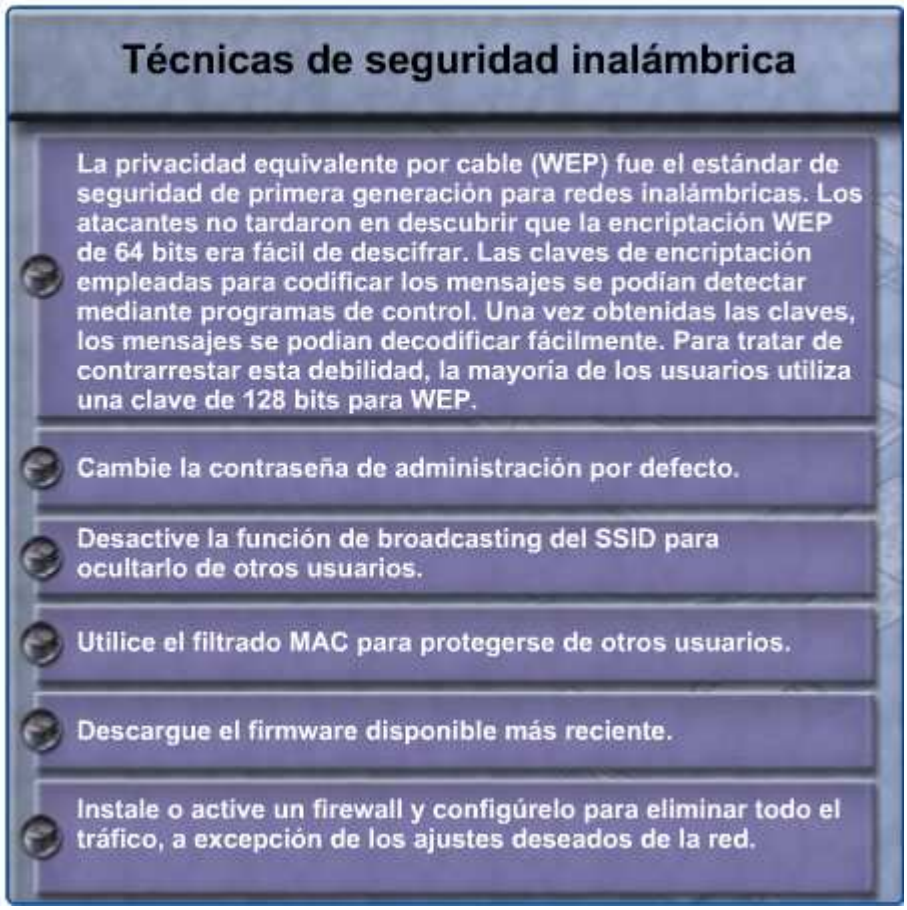
Mientras los datos viajan por la señal de radio, el atacante puede acceder a ellos. Para impedir la captura y el uso no deseados de datos, se puede codificar la información que se envía mediante un sistema de encriptación inalámbrico. Ambos extremos de cada enlace deben utilizar el mismo estándar de encriptación. La Figura 2 muestra los niveles de seguridad aquí descritos:

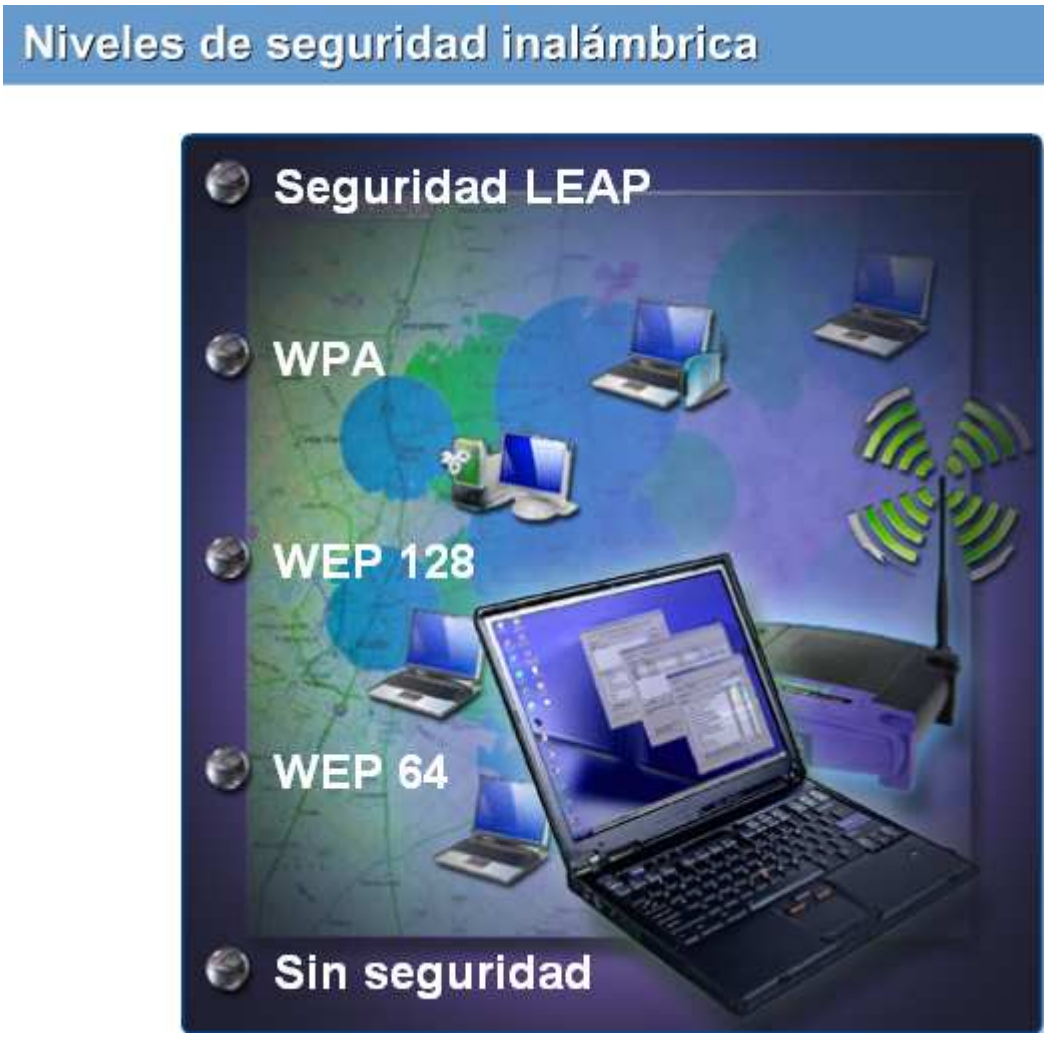
- **Privacidad equivalente por cable (WEP)**: estándar de seguridad de primera

generación para redes inalámbricas. Los atacantes no tardaron en descubrir que la encriptación WEP era fácil de descifrar. Las claves de encriptación empleadas para codificar los mensajes se podían detectar mediante programas de control. Una vez obtenidas las claves, los mensajes se podían decodificar fácilmente.

- **Acceso Wi-Fi protegido (WPA)**: versión mejorada de WEP. Se creó como solución temporal hasta la implementación completa del estándar 802.11i (capa de seguridad para sistemas inalámbricos). Ahora que se ratificó el estándar 802.11i, se lanzó WPA2, que abarca todo el estándar 802.11i.
- **Protocolo liviano de autenticación extensible (LEAP)** o **EAP-Cisco**: protocolo de seguridad inalámbrica creado por Cisco para contrarrestar las debilidades de WEP y WPA. LEAP es un buena opción al utilizar equipos de Cisco con sistemas operativos como Windows y Linux.

La Capa de seguridad de transporte inalámbrico (WTLS) es una capa de seguridad utilizada en dispositivos móviles que emplean el Protocolo de aplicaciones inalámbricas (WAP). Los dispositivos móviles no cuentan con un gran exceso de ancho de banda que pueda asignarse a los protocolos de seguridad. WTLS se creó para proporcionar seguridad a los dispositivos WAP y, a la vez, hacer un uso eficaz del ancho de banda.




9.4 Identificación de técnicas comunes de mantenimiento preventivo para lograr mayor seguridad

La seguridad es tanto un proceso como una tecnología en constante cambio. Todos los días se descubren nuevas vulnerabilidades. Los atacantes están continuamente buscando nuevos métodos de ataque. Los fabricantes de software deben crear y lanzar periódicamente nuevos parches para corregir errores y vulnerabilidades de los productos. Si el técnico deja una computadora desprotegida, el atacante podrá acceder a ésta fácilmente. Las computadoras desprotegidas en Internet se pueden infectar en pocos minutos.

Debido a las cambiantes amenazas contra la seguridad, los técnicos deben saber cómo instalar parches y actualizaciones. También deben poder reconocer cuándo existen nuevas actualizaciones y parches disponibles. Algunos fabricantes publican actualizaciones el mismo día todos los meses, además de ofrecer actualizaciones críticas cuando resultan necesarias. Otros fabricantes proporcionan servicios de actualización automática que aplican parches en el software siempre que se inicia la computadora o envían notificaciones por correo electrónico cuando se publica algún nuevo parche o actualización.

Al completar esta sección, alcanzará los siguientes objetivos:

- Explicar cómo actualizar los archivos de firmas de software antivirus y antispyware.
- Explicar cómo instalar paquetes de servicios de sistemas operativos y parches de

seguridad.

## 9.4 Identificación de técnicas comunes de mantenimiento preventivo para lograr mayor seguridad

### 9.4.1 Explicación de la actualización de los archivos de firmas de software antivirus y antispyware

Las amenazas de virus y gusanos están siempre presentes. Los atacantes están buscando constantemente nuevas formas de infiltrarse en computadoras y redes. Debido a que siempre se desarrollan virus nuevos, es necesario actualizar el software de seguridad de forma continua. Este proceso se puede realizar automáticamente. Sin embargo, el técnico debe saber cómo actualizar manualmente cualquier tipo de software de protección y todas las aplicaciones de los clientes.

Los programas de detección de virus, spyware y adware buscan patrones dentro del código de programación del software instalado en la computadora. Estos patrones se determinan mediante el análisis de los virus interceptados en Internet y en redes LAN. Los patrones de código se denominan firmas. Los creadores de software de protección compilan las firmas en tablas de definiciones de virus. Para actualizar los archivos de firmas del software antivirus y antispyware, primero se debe verificar si los archivos de firmas son los más recientes. Para ello, es necesario consultar la opción "Acerca de" del software de protección o ejecutar la herramienta de actualización correspondiente. Si los archivos de firmas están desactualizados, se deben actualizar manualmente mediante la opción "Actualizar ahora" incluida en la mayoría de las aplicaciones de software de protección.

Se recomienda descargar los archivos de firmas del sitio Web del fabricante para asegurarse de que la actualización sea auténtica y no se encuentre afectada por virus. Esto puede generar una gran demanda en el sitio del fabricante, especialmente al surgir nuevos virus. Para evitar el congestionamiento del tráfico en un solo sitio, algunos fabricantes distribuyen los archivos de firmas para que puedan descargarse de varios sitios. Estos sitios de descarga se denominan "espejos".

PRECAUCIÓN: Al descargar los archivos de firmas de un sitio espejo, asegúrese de que éste sea legítimo. Siempre acceda a los sitios espejo a través de enlaces contenidos en el sitio Web del fabricante.


## 9.4 Identificación de técnicas comunes de mantenimiento preventivo para lograr mayor seguridad

### 9.4.2 Explicación de la instalación de paquetes de servicios de sistemas operativos y parches de seguridad

La eliminación de virus y gusanos de la computadora puede resultar difícil. Para eliminar los virus y reparar el código de la computadora modificado por éstos, se necesitan ciertas herramientas de software. Estas herramientas son suministradas por los fabricantes de sistemas operativos y las empresas de software de seguridad. Asegúrese de descargarlas de un sitio legítimo.

Los fabricantes de sistemas operativos y aplicaciones de software pueden proporcionar actualizaciones de códigos, conocidas como parches, que impiden ataques de virus o gusanos nuevos. Ocasionalmente, los fabricantes combinan parches y actualizaciones en una sola aplicación de actualización integral denominada paquete de servicios. Muchos ataques de virus infames y devastadores podrían haber sido de menor gravedad si más usuarios hubiesen descargado e instalado el paquete de servicios más reciente.

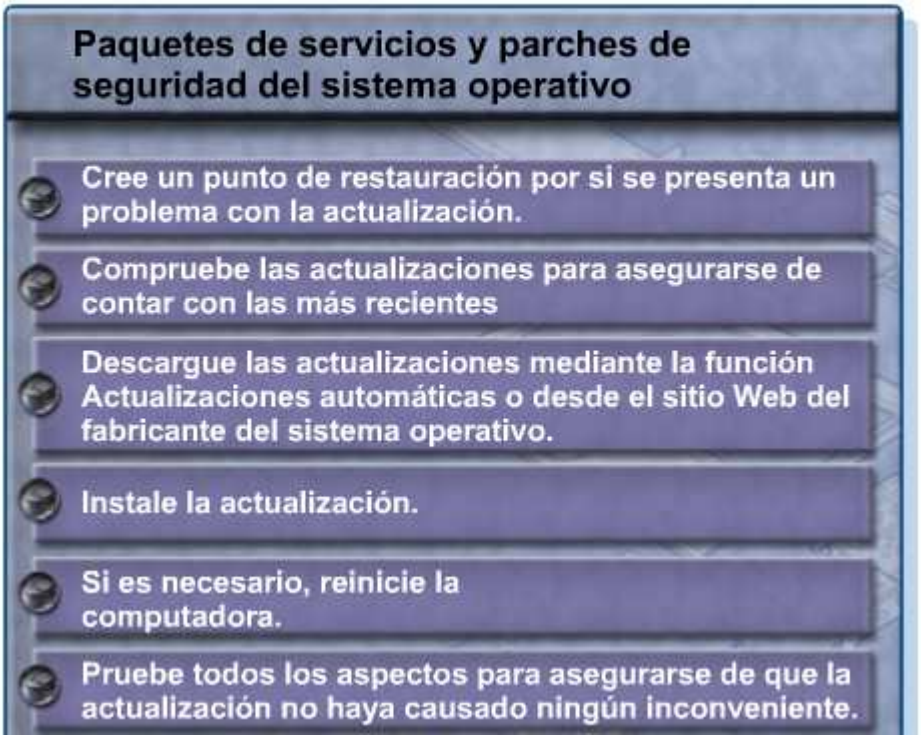
El sistema operativo Windows comprueba periódicamente el sitio Web de Windows Update para determinar si hay actualizaciones de prioridad alta que puedan ayudar a proteger la computadora de las amenazas contra la seguridad más recientes. Estas actualizaciones pueden incluir actualizaciones de seguridad, actualizaciones críticas y paquetes de servicios. Según la configuración elegida, Windows descarga e instala

automáticamente todas las actualizaciones de alta prioridad que necesita la computadora o notifica al usuario acerca de la disponibilidad de estas actualizaciones.

Las actualizaciones, no sólo deben descargarse, sino que también deben instalarse. Si utiliza la configuración automática, puede programar la hora y la fecha de la instalación. De lo contrario, las nuevas actualizaciones se instalarán a las 3 a. m. por defecto. Si la computadora está apagada en el horario de una actualización programada, ésta se instalará la próxima vez que se encienda la computadora. También puede configurar el servicio para que Windows muestre una notificación cuando haya nuevas actualizaciones disponibles e instalarlas usted mismo.

Para actualizar el sistema operativo con un paquete de servicios o parche de seguridad, siga los pasos de la Figura 1.

**Paquetes de servicios y parches de seguridad del SO**

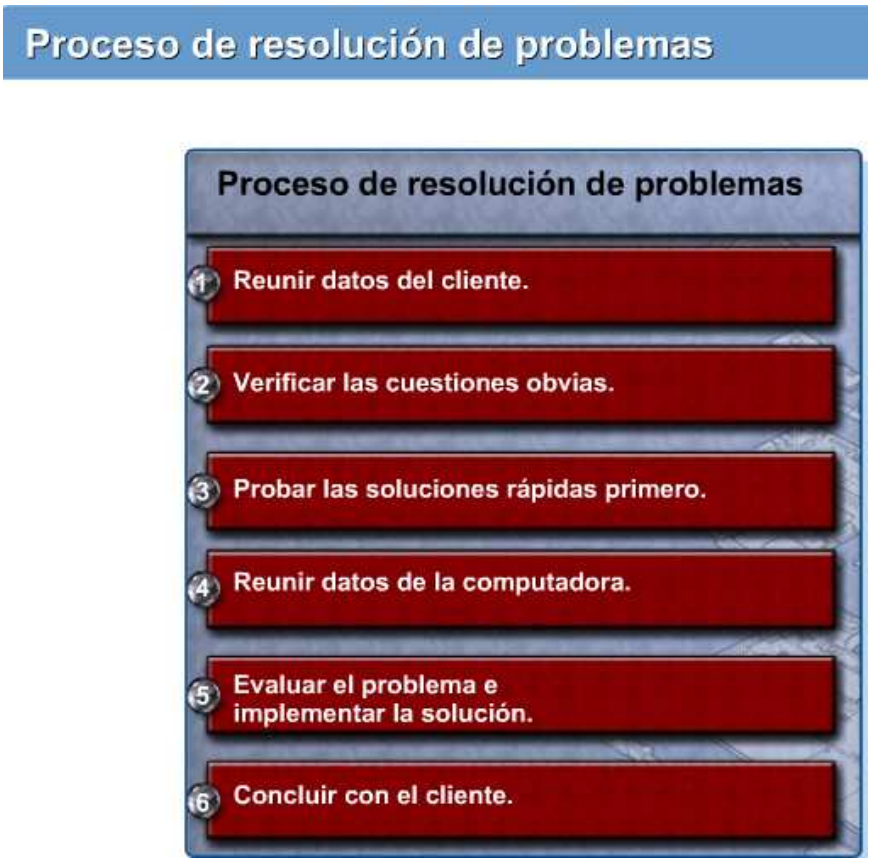



## 9.5 Resolución de problemas de seguridad

El proceso de resolución de problemas se usa para resolver problemas de seguridad. Estos problemas pueden abarcar desde cuestiones simples, como impedir que personas externas vigilen las actividades de los empleados, hasta cuestiones más complejas, como eliminar manualmente archivos infectados. 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.




## 9.5 Resolución de problemas de seguridad

### 9.5.1 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 abiertas

**Lista de preguntas abiertas acerca de errores de seguridad (esta lista NO incluye todas las preguntas)**

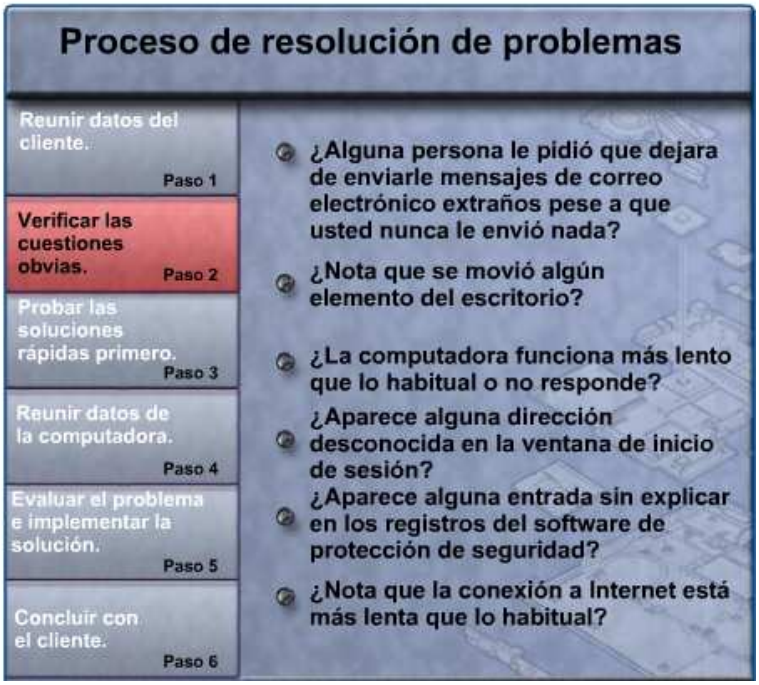
- ¿Cuándo apareció el problema?
- ¿Qué problemas está experimentando?
- ¿Puede suministrar información adicional acerca del problema?
- ¿Qué sitios Web visitó recientemente?
- ¿Qué software de seguridad tiene instalado en la computadora?
- ¿Cómo se conecta a Internet?
- ¿Hubo algún visitante inesperado en su área de trabajo?

## Preguntas cerradas

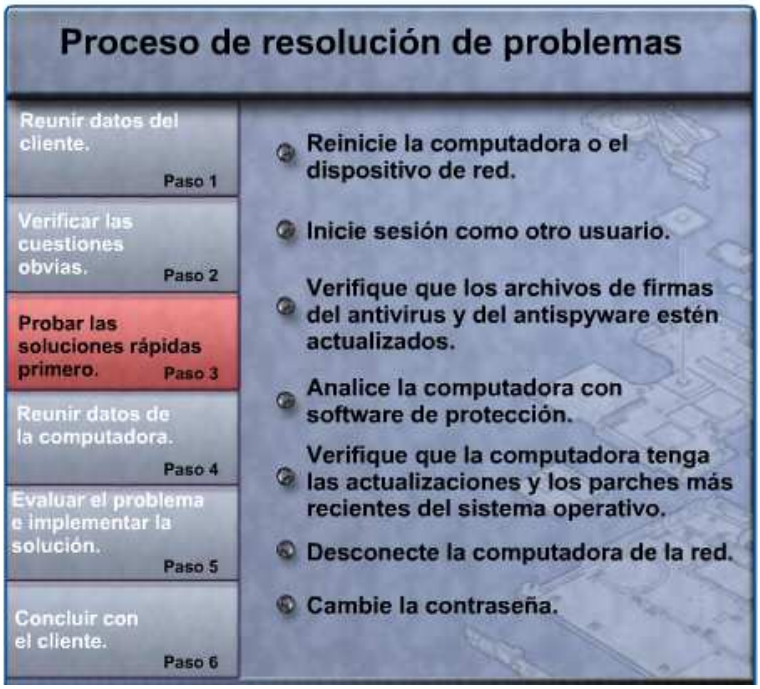
**Lista de preguntas cerradas acerca de errores de seguridad (esta lista NO incluye todas las preguntas)**

- ¿Alguna otra persona utilizó la computadora?
- ¿Está actualizado el software de seguridad?
- ¿Analizó la computadora recientemente para detectar virus?
- ¿Abrió algún archivo adjunto que provenía de un correo electrónico sospechoso?
- ¿Tuvo anteriormente algún problema similar?
- ¿Cambió de contraseña últimamente?
- ¿Recibió algún mensaje de error en la computadora?
- ¿Divulgó la contraseña a otra persona?

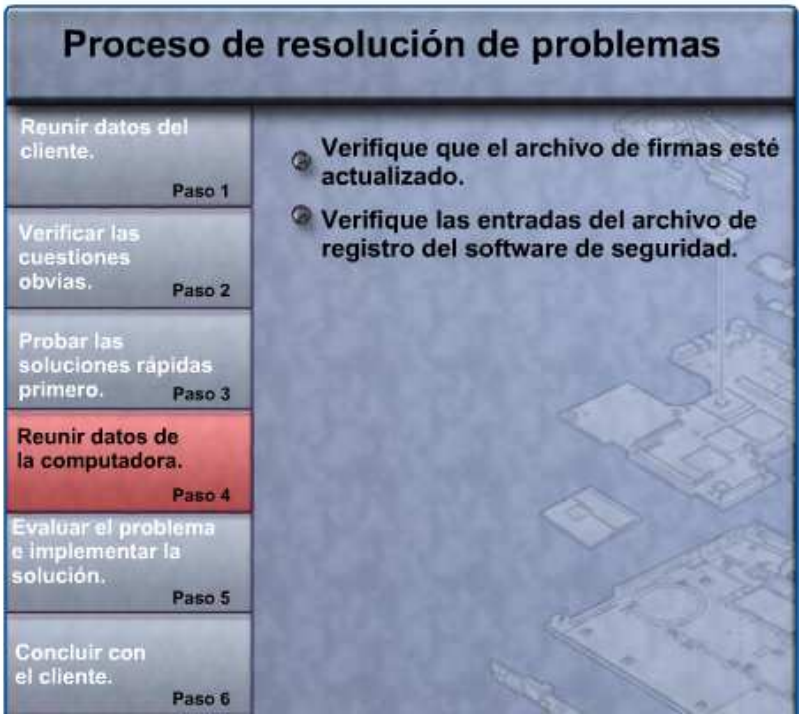
## Verificar las cuestiones obvias




## Probar las soluciones rápidas primero

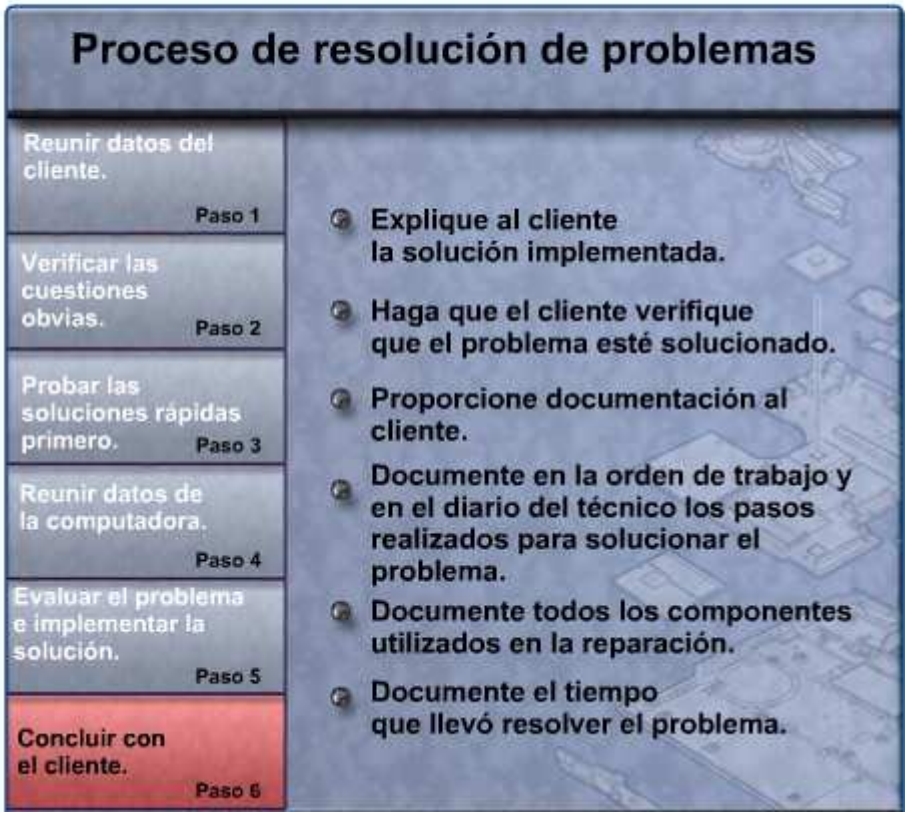


## Reunir datos de la computadora




## Evaluar el problema e implementar la solución

## Concluir con el cliente




9.5 Resolución de problemas de seguridad

9.5.2 Identificación de problemas y soluciones comunes

Los problemas en la computadora pueden atribuirse a problemas de conectividad, software y hardware, o bien, a una combinación de los tres. Usted resolverá algunos tipos de problemas en las computadoras con más frecuencia que otros. La Figura 1 contiene un cuadro con problemas de seguridad y soluciones comunes.

La hoja de trabajo tiene por objeto reforzar las destrezas de comunicación para verificar la información del cliente.

## Problemas y soluciones comunes

| Síntoma del problema | Solución posible |
|---|---|
| La computadora instala las actualizaciones y debe reiniciarse en momentos inoportunos. | Configure la función Actualizaciones automáticas de Windows para que se ejecute diariamente a una hora oportuna, por ejemplo, la hora del almuerzo. |
| La red inalámbrica se encuentra en peligro a pesar de que utiliza encriptación WEP de 64 bits. | Suba el nivel de seguridad a WEP de 128 bits, WAP o seguridad de Cisco EAP. |
| La policía devuelve una computadora portátil. El usuario ya no la necesita. | Una vez que haya recuperado los datos confidenciales, destruya el disco duro y recicle la computadora. |
| Un usuario se queja de recibir muchos mensajes de correo basura a diario. | Es posible que se trate de un ataque de denegación de servicio. En el servidor de correo electrónico, filtre todos los mensajes del emisor. |
| Se advierte que un técnico reparador de impresoras que nadie recuerda haber visto anteriormente está hurgando debajo de los teclados y en los escritorios. | Comuníquese con el personal de seguridad o con la policía. Aconseje a los usuarios que nunca oculten las contraseñas cerca del área de trabajo. |

## 9.6 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 caracteriza a un ataque DDoS?

- [x] Muchos hosts participan en un ataque coordinado.
- [ ] Sólo requiere un breve tiempo establecerlo.
- [ ] Las computadoras hogareñas con conexiones a Internet no son susceptibles.
- [ ] Es fácil determinar la intención de un paquete.

¿Cuáles son las dos opciones que se consideran amenazas físicas? (Elija dos opciones).

- [x] Almacenar las computadoras portátiles en armarios sin llave.
- [ ] El software antivirus tiene definiciones de virus desactualizadas.
- [ ] Todos los usuarios utilizan un nombre de usuario y una contraseña genéricos para conectarse a la red.
- [x] El servidor de red y el equipo de red se encuentran en un rincón de la oficina para su fácil acceso.
- [ ] Las computadoras se encuentran aseguradas a los escritorios de los usuario.

¿Qué tipo de amenaza contra la seguridad se instala en una computadora sin conocimiento del usuario y luego controla todas las actividades de la computadora?

- [ ] Adware
- [ ] Grayware
- [ ] Malware
- [x] Spyware

¿Qué tipo de amenaza contra la seguridad utiliza mensajes de correo electrónico que aparentan ser de un emisor legítimo y solicitan al destinatario del mensaje visitar un sitio Web para ingresar información confidencial?

- [ ] Badware
- [x] Suplantación de identidad
- [ ] Virus "stealth"
- [ ] Gusano

Un técnico intenta asegurar una red inalámbrica. ¿Cuáles son las dos acciones que debe realizar para asegurar el acceso a la red? (Elija dos opciones).

- [x] Cambiar la contraseña por defecto del administrador para todos los puntos de acceso.
- [ ] Instalar una aplicación de seguridad para detener todo el tráfico inalámbrico.
- [ ] Habilitar el broadcast del SSID para un solo punto de acceso.
- [x] Utilizar el filtrado MAC.
- [ ] Utilizar los valores por defecto del SSID para los puntos de acceso.

Un técnico ha configurado una red inalámbrica con encriptación WEP. Varios usuarios que podían utilizar la red inalámbrica ahora no pueden conectarse al punto de acceso. ¿Cuál es la posible causa de este problema de conexión?

- [ ] WEP es una técnica de encriptación segura que requiere un intercambio exitoso para establecer conectividad.
- [ ] El punto de acceso no puede realizar el broadcast del SSID cuando la WEP está habilitada.
- [x] Los usuarios no han configurado sus computadoras para la encriptación WEP.
- [ ] El punto de acceso utiliza una encriptación de 64 bits, lo que resulta obsoleto con las NIC inalámbricas más nuevas.

¿Cuál es el primer paso debe que llevar a cabo un técnico para la resolución de problemas en temas de seguridad?

- [ ] Reunir datos de la computadora.
- [x] Reunir datos del cliente.
- [ ] Evaluar el problema.
- [ ] Verificar las cuestiones obvias.

¿Qué protocolo tiene como objetivo proporcionar seguridad a dispositivos WAP y utiliza de mane eficiente el ancho de banda?

- [ ] SecTLS
- [ ] TCPSec
- [ ] TTL
- [ ] WTCP
- [x] WTLS