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

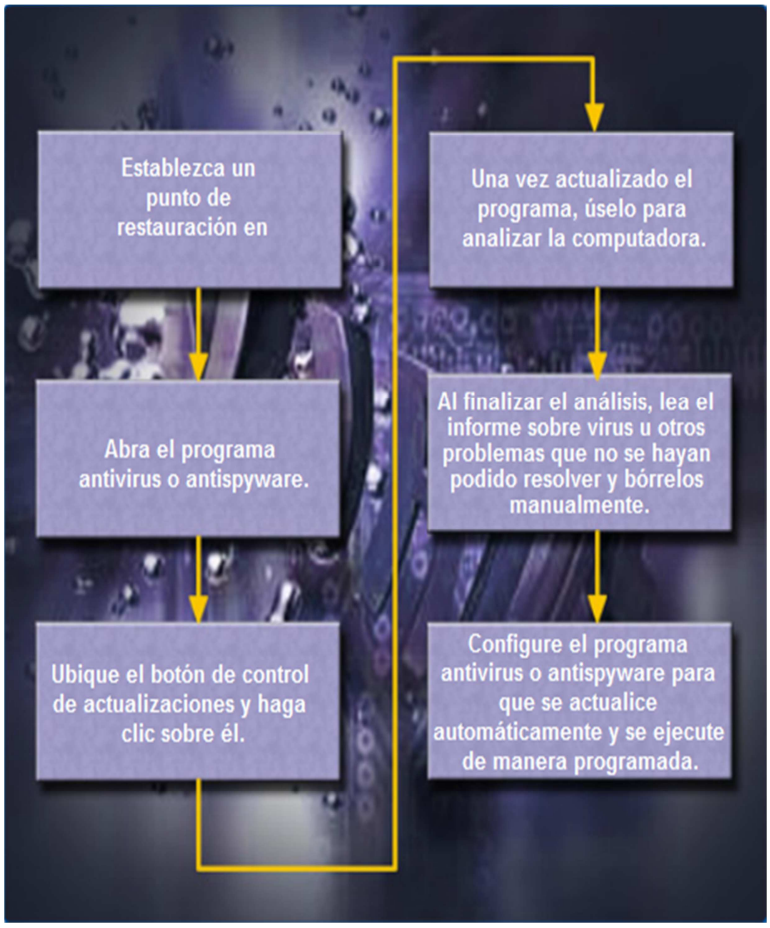
La seguridad es tanto un proceso como una tecnología en constante cambio. Todos los días se descubren nuevas vulnerabilidades. Los atacantes están continuamente buscando nuevos métodos de ataque. Los fabricantes de software deben crear y lanzar periódicamente nuevos parches para corregir errores y vulnerabilidades 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.

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.

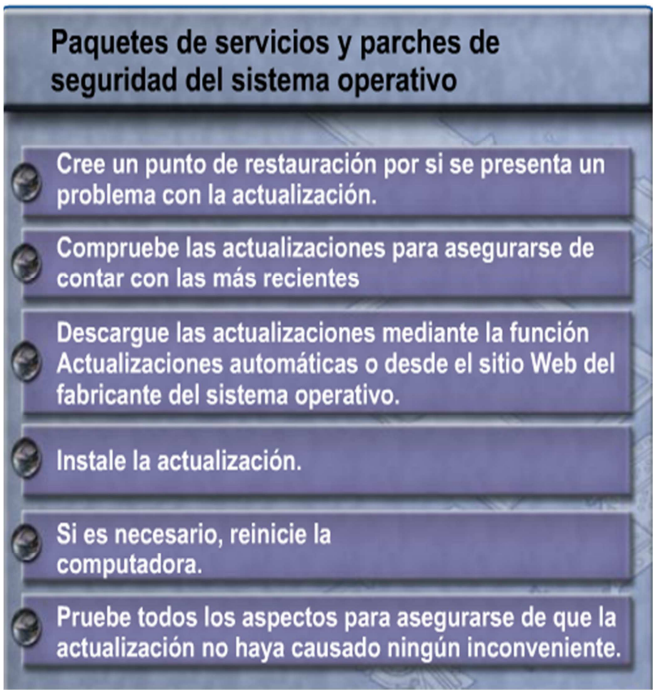
9.4.1 Explicación de la instalación de paquetes de servicios de sistemas operativos y parches de seguridad

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.