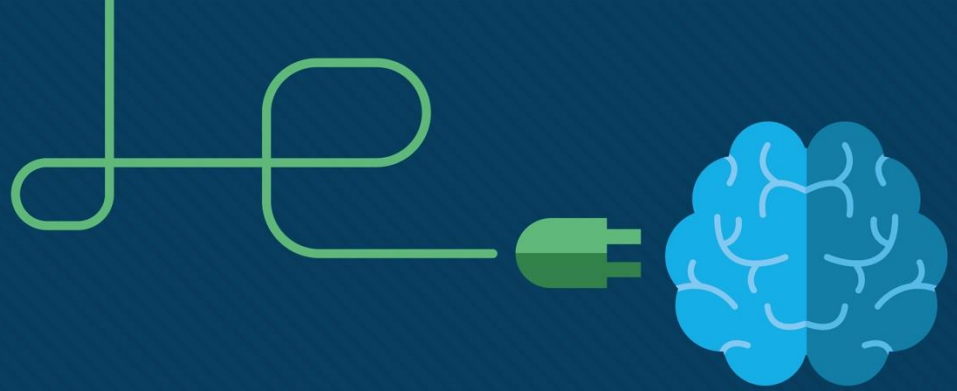


Capítulo 13: Seguridad

IT Essentials v7.0

Capítulo 13: Secciones y objetivos

- 13.1 Amenazas para la seguridad
  - Explicar las amenazas de seguridad.
    - Describa los diferentes tipos de malware.
    - Describa las medidas que protegen contra el software malicioso.
    - Describa los diferentes tipos de ataques a la red.
    - Describa los diferentes ataques de ingeniería social.

- 13.2 Procedimientos de seguridad
  - Explique los procedimientos de seguridad.
    - Explique qué es una política de seguridad.
    - Explique las medidas de seguridad física.
    - Describa las medidas que protegen los datos.
    - Describa cómo destruir datos.

Capítulo 13: Secciones y objetivos (continuación)

- 13.3 Protección de las estaciones de trabajo con Windows
  - Configurar las políticas y las opciones básicas de seguridad de los dispositivos finales.
    - Explique cómo proteger una estación de trabajo.
    - Configuración de la seguridad mediante la herramienta de política de seguridad local en Windows.
    - Administre usuarios y grupos de Windows
    - Configure la seguridad mediante la herramienta de firewall de Windows.
    - Configure un navegador para el acceso seguro.
    - Configure el mantenimiento de la seguridad en Windows.
- 13.4 Seguridad inalámbrica
  - Configure la seguridad inalámbrica.
    - Configure los dispositivos inalámbricos para una comunicación segura.

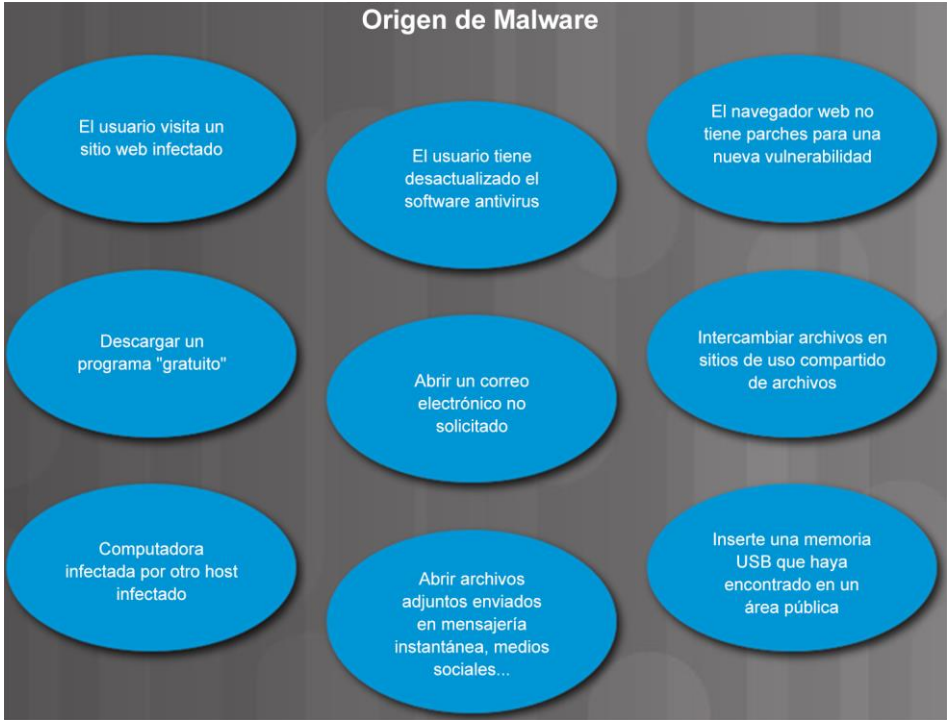
Capítulo 13: Secciones y objetivos (continuación)

- 13.5: Proceso básico de solución de problemas de seguridad
  - Explique cómo resolver problemas de seguridad básicos.
    - Explicar los seis pasos del proceso de resolución de problemas de seguridad.
    - Describa problemas y soluciones avanzados de seguridad.

13.1 Amenazas para la seguridad

Malware

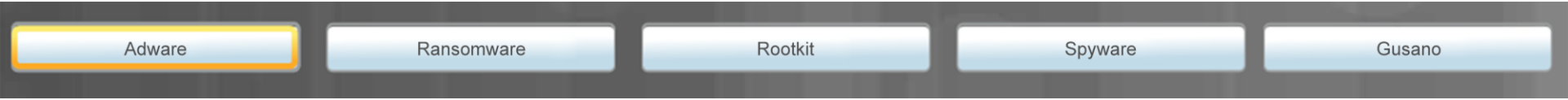
- Existen muchos tipos de amenazas creadas para interrumpir las computadoras y las redes.
  - La mayor amenaza y la más común para las computadoras y los datos que contienen es el malware.
- El malware se suele instalar en una computadora sin el conocimiento del usuario. Una vez que un host está infectado, el malware puede:
  - Cambiar la configuración de la computadora
  - Eliminar archivos o dañar discos duros.
  - Recopilar la información almacenada en la computadora sin el consentimiento del usuario.
  - Abrir ventanas adicionales en la computadora o redirigir el navegador.



Virus y Caballos de Troya

- El primer y el tipo más común de malware informático es un **virus**.
  - Los virus requieren una acción humana para propagarse e infectar otras computadoras.
  - El virus se oculta mediante su unión a un código informático, al software o a los documentos de la computadora. Cuando se abre, el virus se ejecuta e infecta la computadora.
- Los delincuentes cibernéticos también utilizan **Caballos de Troya** para poner en riesgo a los hosts.
  - Un caballo de Troya es un programa que parece útil pero también transporta código malicioso.
  - Los caballos de Troya a menudo se proporcionan con programas gratuitos en línea, como los juegos de computadora.

Tipos de malware



- **El adware** puede mostrar anuncios no solicitados mediante ventanas emergentes del navegador web, nuevas barras de herramientas o redireccionamientos inesperados a un sitio web diferente
- **Por lo general,** el ransomware deniega a un usuario el acceso a sus archivos mediante el cifrado de los archivos y la visualización de un mensaje que exige un rescate por la clave de descifrado.
- **Los rootkits** son difíciles de detectar y son utilizados por los ciberdelincuentes para obtener acceso de nivel de administrador a una computadora.
- El spyware es similar al adware, pero se utiliza para recopilar información sobre el usuario y volver a enviarla a ciberdelincuentes.
- **Los gusanos** son programas de replicación automática que se propagan automáticamente sin la intervención del usuario mediante el aprovechamiento de vulnerabilidades en el software.

Programas contra malware

- Es importante que proteja las computadoras y los dispositivos móviles mediante un software antivirus reconocido.
- En la actualidad, los programas antivirus se conocen comúnmente como programas antimalware.
  - Los programas antimalware pueden detectar y bloquear troyanos, rootkits, ransomware, spyware, registradores de teclado y programas de adware.
  - Los programas antimalware buscan continuamente patrones conocidos contra una base de datos de firmas de malware conocidas.
  - También pueden utilizar técnicas heurísticas de identificación de malware, que pueden detectar comportamientos específicos asociados con algunos tipos de malware.

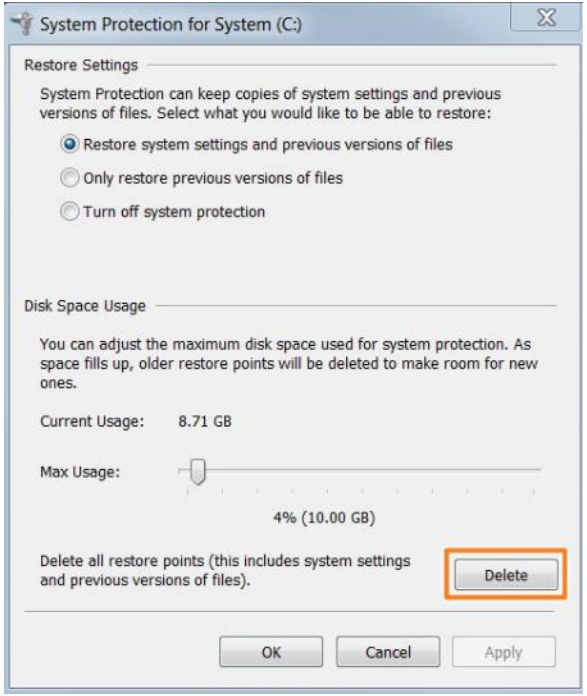
Actualización de archivos de firma

- El nuevo malware siempre está en desarrollo; por lo tanto, el software antimalware se debe actualizar periódicamente. Este proceso a menudo se activa como opción predeterminada.
- Siempre descargue los archivos de firma del sitio web del fabricante, para asegurarse de que la actualización sea auténtica y no esté dañada por virus.
  - Para evitar el exceso de tráfico en un único sitio web, algunos fabricantes distribuyen los archivos de firma para que puedan descargarse de varios sitios de descarga. Estos sitios de descarga se denominan “reflejos”.
- **PRECAUCIÓN**: Al descargar archivos de firma de un reflejo, asegúrese de que el sitio reflejado sea un sitio legítimo. Siempre acceda al enlace del sitio reflejado desde el sitio web del fabricante.

Explicación de video: Programas antimalware

Reparación de sistemas infectados

- Cuando un programa de protección contra malware detecta que una PC está infectada, elimina la amenaza o la pone en cuarentena. No obstante, lo más probable es que la computadora siga en riesgo.
- Muchos programas antimalware se pueden configurar para que se ejecuten cuando se inicia el sistema, antes de que se cargue Windows.
- La eliminación del malware puede requerir que la computadora se reinicie en modo seguro.
- Es posible que deba comunicarse con un especialista para asegurarse de que la PC esté completamente limpia. De lo contrario, es posible que sea necesario formatear nuevamente la computadora, volver a instalar el sistema operativo y recuperar los datos a partir de las copias de respaldo más recientes.
- El servicio de restauración del SO puede incluir archivos infectados en un punto de restauración. Por lo tanto, una vez que se eliminó el malware de una computadora, deben eliminarse los archivos de restauración del sistema.



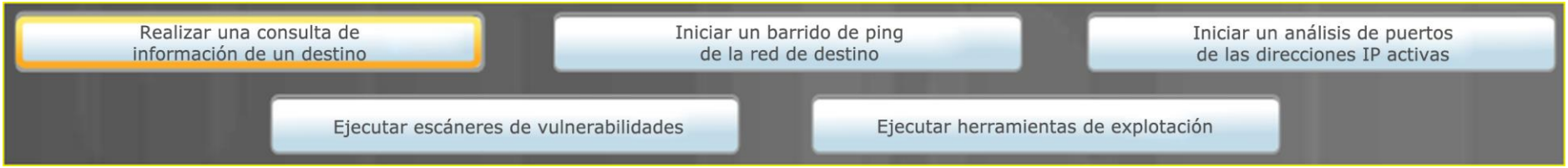
Explicación de video: corrección de un sistema infectado

Demostración en video: reparación de un sistema infectado

En esta demostración en video, aprenderá cómo corregir un sistema infectado:

- Utilizar seguridad de Windows
  - Utilizar la protección contra virus y amenazas para localizar amenazas
  - Ejecutar un análisis completo
  - Comprobar que no haya archivos sospechosos en el Administrador de tareas en Inicio
- Cambiar el proceso de arranque para controlar cómo arranca el sistema

Las redes son objetivos



- El atacante busca información de la red sobre un objetivo mediante la búsqueda de Google, Whois y otras herramientas.
- El atacante inicia un barrido de ping de la dirección de red pública del objetivo detectado para determinar cuáles son las direcciones IP que están activas.
- El atacante determina qué servicios están disponibles en el puerto activo mediante Nmap, SuperScan y otras herramientas.
- El atacante ejecuta un escáner de vulnerabilidades para descubrir el tipo de aplicaciones y SO que se ejecutan en el host de destino mediante Nipper, Secuna PSI y otras herramientas.
- El atacante intenta descubrir los servicios vulnerables para atacar utilizando Metasploit, Core Impact y otras herramientas.

Tipos de ataques de TCP/IP

Denegación de servicio (DoS) | DoS distribuida | Envenenamiento de DNS | Ataque man-in-the-middle

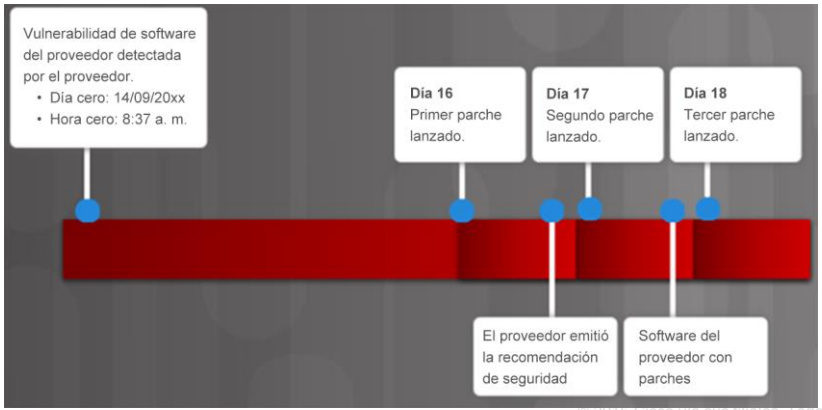
- **Negación de servicio (DoS)** es un ataque en el que el atacante inunda un dispositivo objetivo con solicitudes falsas para crear una negación de servicio para usuarios legítimos.
- **DoS distribuido** es un ataque de DoS amplificado que utiliza muchos hosts infectados denominados zombis para saturar un objetivo.
- **El envenenamiento de DNS** es un ataque en el que el atacante ha logrado infectar un host para aceptar registros DNS falsos que apuntan a servidores maliciosos.
- **El Hombre-en-medio** es un ataque en el que un atacante intercepta la comunicación entre dos hosts.

Tipos de ataques de TCP/IP (Cont.)

- **La repetición** es un tipo de ataque de suplantación de identidad en el que el atacante captura un paquete autenticado, lo modifica y lo envía al destino original.
- **La suplantación de identidad** es un ataque en el que el atacante falsifica una dirección IP para obtener acceso a los recursos.
- **El ataque de saturación de SYN** es un tipo de ataque que se aprovecha de la comunicación tridireccional de TCP.

Día cero

- Los dos términos siguientes se utilizan comúnmente para describir cuándo se detecta una amenaza:
  - **Día cero**: a veces, también se los conoce como ataques de día cero, amenazas de día cero o explotaciones de día cero. Este es el día en que el proveedor descubrió una vulnerabilidad desconocida. El término es una referencia a la cantidad de tiempo que un proveedor ha tenido para abordar la vulnerabilidad.
  - **Hora cero**: describe el momento en que se detecta la vulnerabilidad.
- El software puede continuar siendo atacado hasta que se encuentre disponible un parche que aborde la vulnerabilidad.

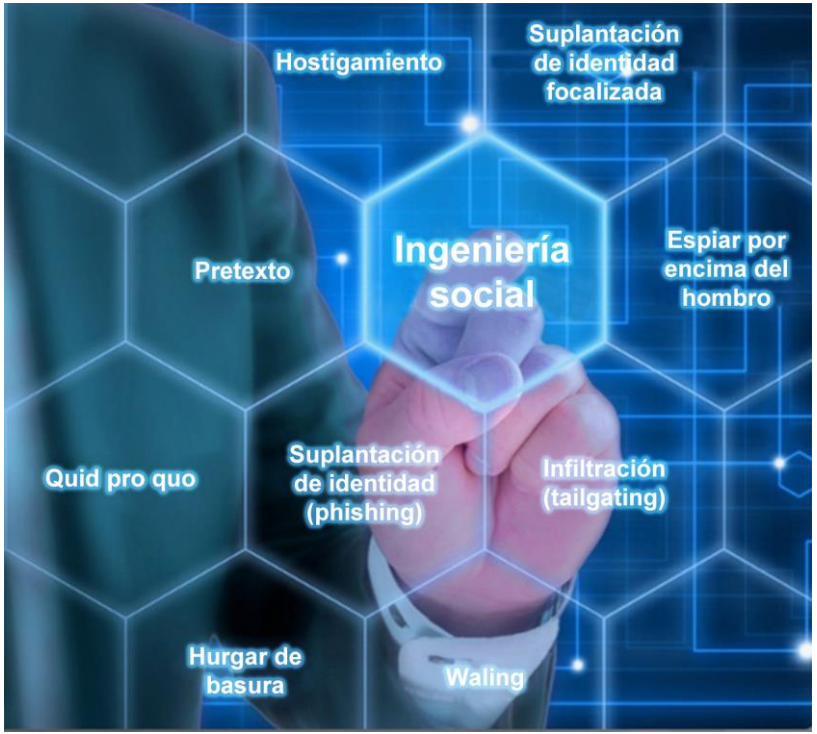


Protección contra ataques a la red

- No existe una única solución para proteger contra todos los ataques de TCP/IP o de día cero.
- Una solución es utilizar un enfoque de defensa en profundidad, también conocido como enfoque en capas, para la seguridad.
  - Esto requiere una combinación de dispositivos y servicios de red que trabajen juntos en conjunto.
- Todos los dispositivos de red, incluidos el router y los switches, deben estar protegidos para evitar que los atacantes manipulen los dispositivos.

Ingeniería social

- Los ciberdelincuentes utilizan técnicas de ingeniería social para engañar a objetivos desprevenidos para que revelen información confidencial.
- La ingeniería social es un ataque de acceso que intenta manipular a las personas para que realicen acciones o divulguen información confidencial.
- Los ingenieros sociales, a menudo, confían en la naturaleza humana y la predisposición a ayudar que tienen las personas.
- **Nota**: la ingeniería social se utiliza con frecuencia junto con otros ataques a la red.



Técnicas de ingeniería social

- **Pretexto** Un atacante finge necesitar datos personales para confirmar la identidad del destinatario.
- **Suplantación de identidad** Un atacante envía un correo electrónico fraudulento disfrazado como proveniente de una fuente confiable.
- **Suplantación de identidad focalizada** Un atacante crea un ataque de suplantación de identidad orientado para una organización o persona específica
- **Correo no deseado**: correo electrónico no solicitado que suele contener enlaces nocivos, malware o contenido engañoso.
- **Algo por algo**: Cuando un atacante solicita información personal a cambio de algo.
- **Señuelo**: un atacante deja una unidad de memoria Flash infectada por malware en una ubicación pública.
- **Suplantación de identidad**: Un atacante finge ser una persona que no es.
- **Seguimiento**: Cuando un atacante sigue a una persona autorizada a un lugar seguro.
- **Espiar por encima del hombro**: un atacante mira por encima del hombro de una persona para robar información.
- **Hurgar en la basura**: un atacante busca información confidencial en la basura.

Protección contra la ingeniería social

13.2 Procedimientos de seguridad

Qué es una política de seguridad

- Una política de seguridad es:
  - un conjunto de objetivos de seguridad que garantizan la seguridad de una red, datos y computadoras en una organización.
  - un documento en constante evolución, según los cambios tecnológicos, el negocio y los requisitos de los empleados.
  - generalmente creado por un comité con miembros compuestos por la administración y el personal de TI.
- Es responsabilidad del personal de TI implementar las especificaciones de la política de seguridad en la red.

La política de seguridad identifica

- ¿Qué activos requieren protección?
- ¿Cuáles son las posibles amenazas?
- ¿Cómo se debe proceder en caso de una infracción a la seguridad?
- ¿Qué tipo de capacitación se ofrecerá para instruir a los usuarios finales?

Política de seguridad

- Políticas de identificación y autenticación
- Políticas de contraseña
- Políticas de usos aceptables
- Políticas de acceso remoto
- Políticas de mantenimiento de la red
- Políticas de manejo de incidentes

Categoría de política de seguridad

- **Políticas de autenticación e identificación**: describen los procedimientos de verificación y determinan cuáles son las personas autorizadas que pueden acceder a los recursos de red.
- **Políticas de contraseña**: garantizan que las contraseñas cumplan con requisitos mínimos y se cambien periódicamente.
- **Políticas de uso aceptable**: identifican los recursos y el uso de red que son aceptables para la organización y pueden incluir ramificaciones de violación de políticas.
- **Políticas de acceso remoto**: identifican cómo los usuarios remotos pueden obtener acceso a la red y qué es accesible de manera remota.
- **Políticas de mantenimiento de red**: especifican los sistemas operativos de los dispositivos de la red y los procedimientos de actualización de las aplicaciones de los usuarios finales.
- **Políticas de manejo de incidentes**: describen cómo se manejan los incidentes de seguridad.

Protección de dispositivos y datos

- El objetivo de la política de seguridad es garantizar un entorno de red seguro y proteger los activos.
- Entre los activos de una organización, se incluye los datos, los empleados y los dispositivos físicos, como las computadoras y los equipos de red.
- La política de seguridad debe identificar el hardware y los equipos que se pueden utilizar para evitar el robo, el vandalismo y la pérdida de datos.

Seguridad física

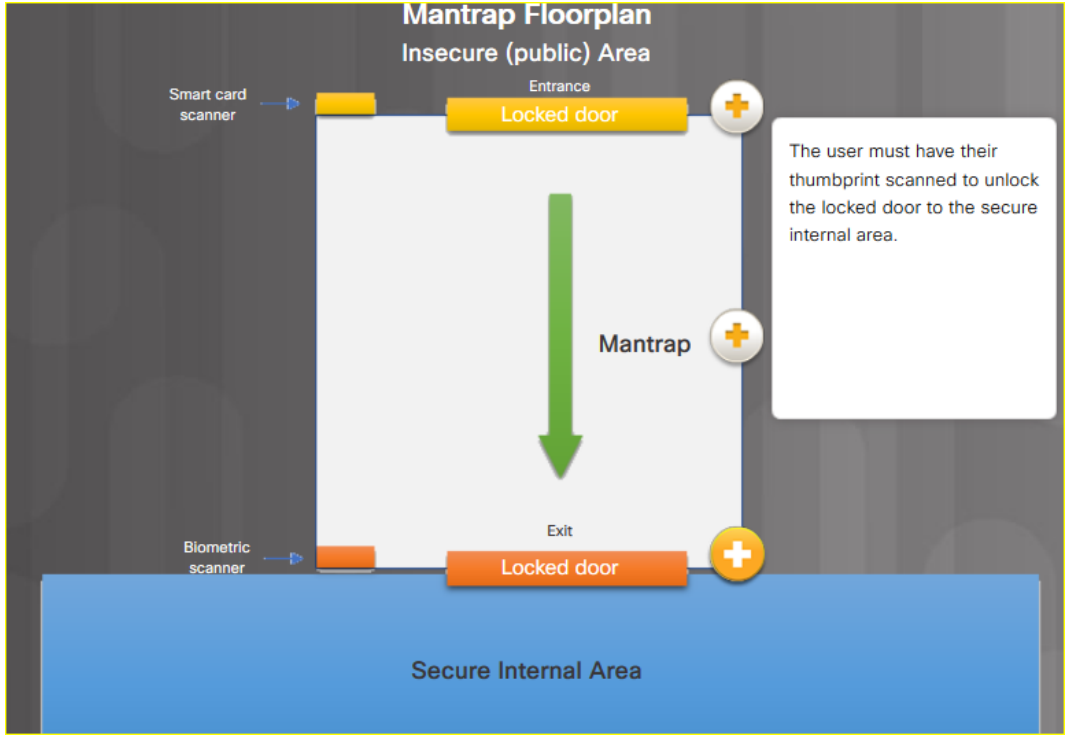
- La seguridad física es tan importante como la seguridad de los datos.
  - Por ejemplo, si una computadora se toma de una organización, los datos también se roban, o lo que es peor, se pierden.
- La seguridad física implica protección:
  - Acceso a la propiedad de una organización
  - Acceso a áreas restringidas
  - Infraestructura de redes y computación

Categoría de política de seguridad

- **Bloqueo convencional**: se desbloquea al ingresar la clave requerida en el mecanismo de manejo de la puerta.
- **Bloqueo con cerrojo**: se desbloquea al ingresar la clave requerida en un cerrojo separado del mecanismo de manejo de la puerta.
- **Bloqueo electrónico**: se desbloquea al ingresar un código de combinación secreto o un PIN en el teclado.
- **Bloqueo basado en tokens**: se desbloquea pasando una tarjeta segura o mediante un lector de proximidad cercana para detectar una tarjeta inteligente o un llavero transmisor inalámbrico.
- **Bloqueo biométrico**: se desbloquea mediante un escáner biométrico, como un lector de huellas digitales.
- **Bloqueo de varios factores**: un bloqueo que utiliza una combinación de los mecanismos anteriores.

Trampas

- En entornos de alta seguridad, las trampas se suelen utilizar para limitar el acceso a áreas restringidas y evitar el seguimiento.
  - Una trampa es una sala pequeña con dos puertas, una de las cuales debe cerrarse antes de que la otra pueda abrirse.
  - Por lo general, una persona ingresa a la trampa mediante el desbloqueo de una puerta. Una vez dentro de la trampa la primera puerta se cierra y, luego, el usuario debe desbloquear la segunda puerta para ingresar al área restringida.



Protección de las computadoras y el hardware de red

- Las organizaciones deben proteger sus infraestructuras informáticas y de red.
  - Esto incluye cableado, equipos de telecomunicaciones y dispositivos de red.
- Existen varios métodos para proteger físicamente los equipos informáticos y de red.
- Los equipos de red deben instalarse en áreas protegidas. Asimismo, todo el cableado debe colocarse en conductos o tenderse dentro de las paredes, a fin de evitar su alteración o el acceso no autorizado.

Protección de las computadoras y el hardware de red (Cont.)

- Entre algunos de los factores que determinan cuáles son los equipos más eficaces para la protección de equipos y datos se incluyen los siguientes:
  - La forma en que se utiliza el equipo.
  - El lugar donde se encuentran los equipos de computación.
  - El tipo de acceso de usuario a los datos que se necesita.
- Por ejemplo:
  - Una computadora de un lugar público concurrido exige protección adicional contra robo y vandalismo.
  - Un servidor muy ocupado de un centro de atención telefónica debe protegerse en una sala de equipos cerrada con llave.
  - Al usar una computadora portátil en un lugar público, las llaves de seguridad, aseguran el bloqueo de la computadora en caso de que el usuario se aleje de la computadora portátil.

Datos: su mayor activo

- Es probable que los datos sean los activos más valiosos de una organización. Como datos de la organización, se pueden incluir datos de investigación y desarrollo, ventas, finanzas, recursos humanos, empleados y clientes.
- Los datos pueden perderse o dañarse en circunstancias tales como robos, fallas de equipos o un desastre.
- La pérdida o la exfiltración de datos son términos utilizados para describir cuando los datos se pierden, se roban o se filtran al público.
- Los datos se pueden proteger de la pérdida de datos mediante copias de seguridad de datos, cifrado de archivos/carpetas y permisos.

Copias de respaldo de datos

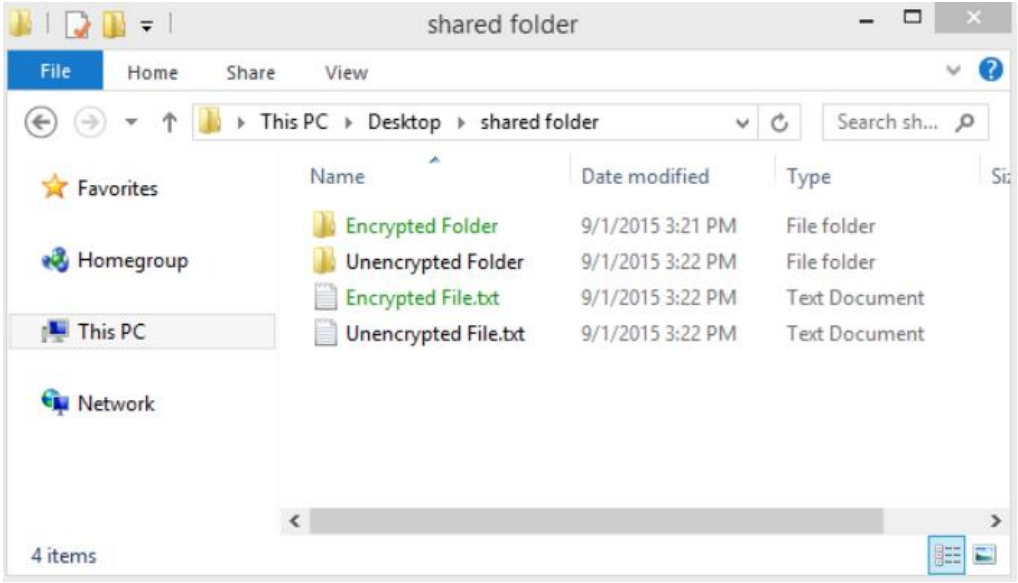
- La realización de copias de respaldo de datos es uno de los métodos más eficaces para evitar la pérdida de estos.
  - Las copias de respaldo de datos almacenan una copia de la información de una computadora en medios de copia de respaldo extraíbles.
  - Las copias de respaldo de datos deben realizarse con regularidad e identificarse en la política de seguridad.
  - Las copias de respaldo de datos suelen almacenarse externamente para proteger los medios de copia de respaldo en caso de que ocurra algo en la instalación principal.
- Los hosts de Windows tienen una utilidad de copia de respaldo y restauración.
- Los hosts de macOS cuentan con una utilidad denominada **Time Machine** para realizar las funciones de copia de respaldo y restauración.

Permisos de archivo y de carpeta

- Los permisos son las reglas que configura para limitar la carpeta o el acceso a los archivos para una persona o para un grupo de usuarios.
- Debe limitarse el acceso de los usuarios solo a los recursos que necesitan de una computadora o red.
  - Esto se conoce como “principio de privilegios mínimos”.

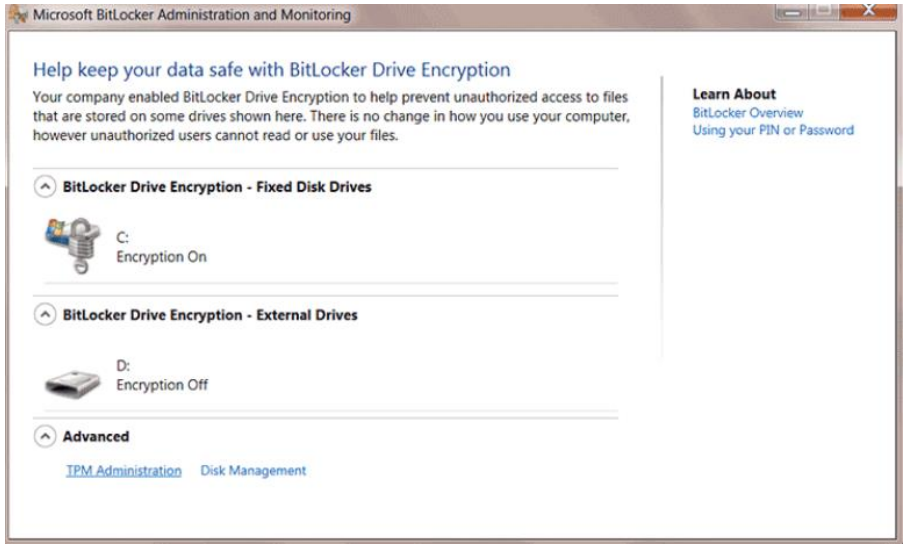
Cifrado de archivo y de carpeta

- El cifrado suele utilizarse para proteger datos.
  - El cifrado es el proceso que consiste en transformar datos mediante un algoritmo complicado para hacerlos ilegibles.
  - Se debe utilizar una clave especial para volver a convertir la información ilegible en datos legibles.
- El sistema de encriptación de archivos (EFS, Encrypting File System) es una característica de Windows que permite encriptar datos.
  - El EFS está directamente vinculado a una cuenta de usuario determinada.
    - Solo el usuario que cifró los datos puede acceder a estos una vez encriptados.

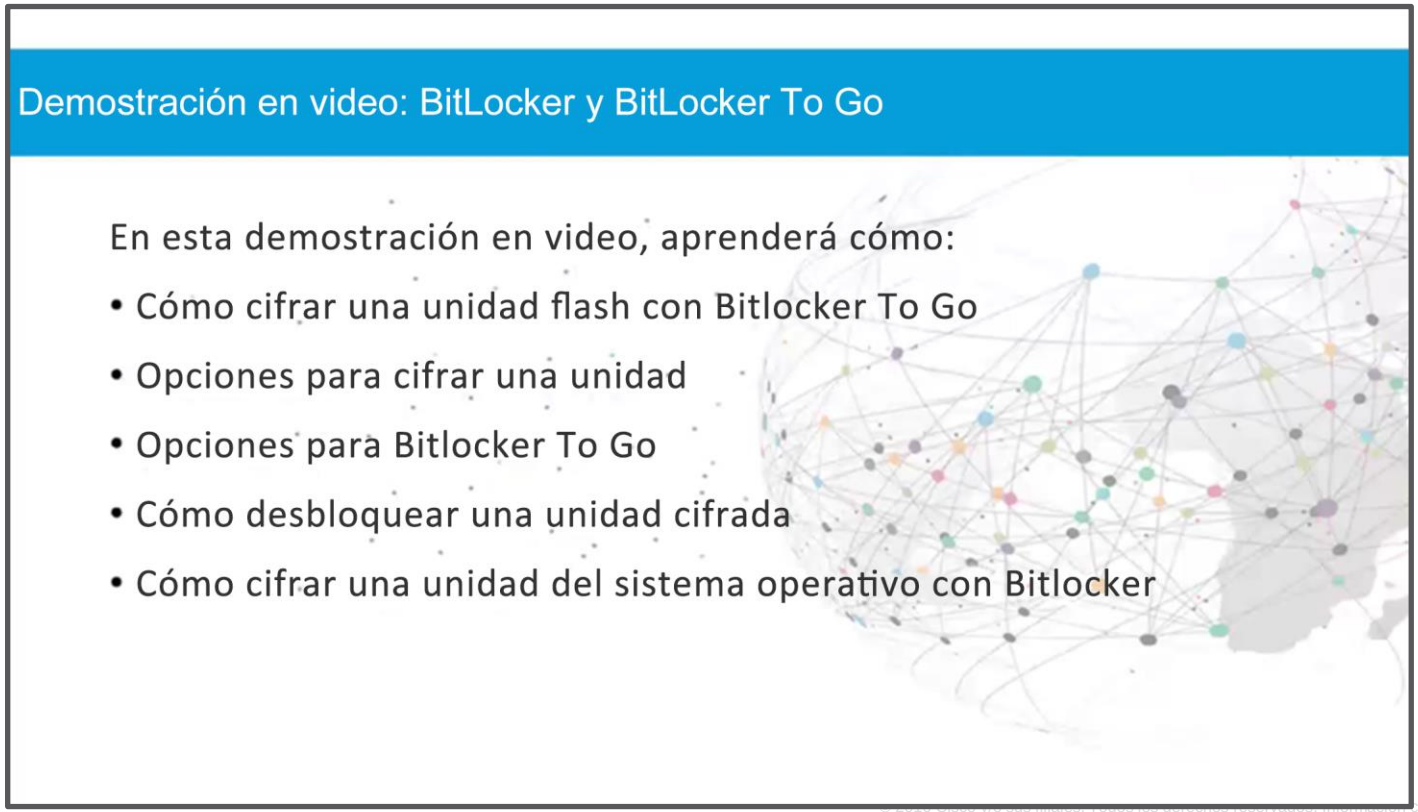


Windows BitLocker y BitLocker To Go

- Puede cifrar una unidad de disco duro completa con una función denominada BitLocker.
- Para utilizar BitLocker:
  - Se debe contar con dos volúmenes como mínimo en un disco duro.
  - El Módulo de plataforma segura (TPM) se debe habilitar en el BIOS.
    - TPM es un chip especializado instalado en la placa base que almacena claves de cifrado, certificados digitales y contraseñas.
- El cifrado de BitLocker también se puede usar con unidades extraíbles mediante BitLocker To Go.
  - BitLocker To Go no utiliza un chip del TPM, pero aún así, proporciona cifrado y requiere una contraseña.



Demostración en video: BitLocker y BitLocker To Go

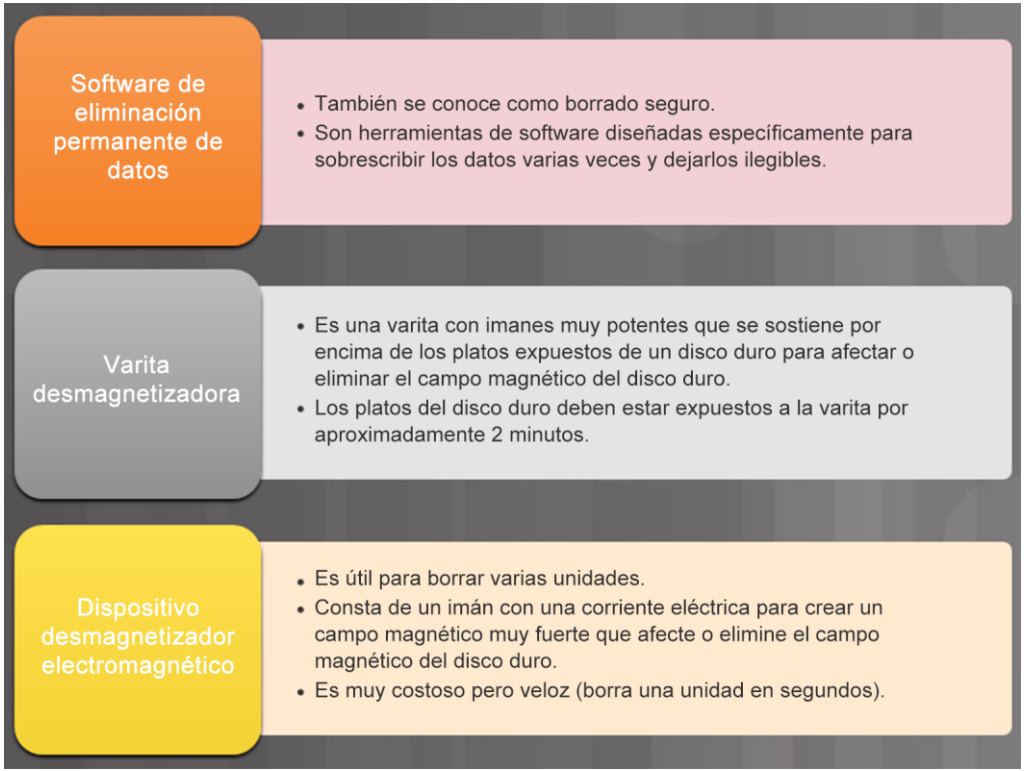


Práctica de laboratorio: BitLocker y BitLocker To Go

En esta práctica de laboratorio, debe activar el cifrado de BitLocker en una unidad de datos extraíble y en la unidad del sistema informático.

Medios magnéticos de eliminación de datos

- Los datos de protección también incluyen la eliminación de los archivos de dispositivos de almacenamiento cuando ya no se necesitan.
- La simple eliminación de archivos o formatear la unidad no es suficiente para proteger su privacidad.
- Las herramientas de software pueden utilizarse para recuperar carpetas, archivos e incluso particiones enteras.
  - Por este motivo, los medios de almacenamiento se deben borrar completamente mediante uno o más de los métodos presentes en la figura:

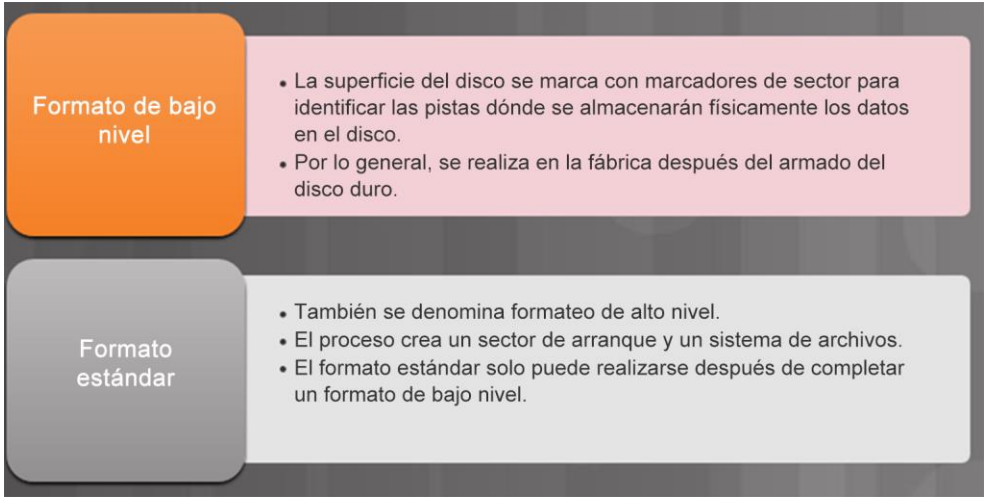


Otros medios de eliminación de datos

- Las unidades de estado sólido (SSD, solid state drives) están compuestas por memoria flash en lugar de platos magnéticos.
  - Las técnicas frecuentes para borrar datos, como la desmagnetización, no son eficaces con memoria flash.
  - Para asegurar completamente que no se puedan recuperar los datos de una SSD y una SSD híbrida, realice una eliminación segura.
- Otros medios de almacenamiento y documentos (p. ej., discos ópticos, eMMC, barras USB) también se deben destruir.
  - Utilice una trituradora o un incinerador diseñado para destruir documentos y cada tipo de medios.
- Al considerar sobre los dispositivos que deban ser eliminados o destruidos, recuerde que los dispositivos además de las computadoras y los dispositivos móviles almacenan datos.
  - Las impresoras y los dispositivos multifunción también pueden contener un disco duro que tiene mantiene en caché los documentos que se imprimieron o analizaron. Esta función en caché se puede desactivar a veces, o el dispositivo necesita ser limpiado regularmente.

Reciclado y destrucción del disco duro

- Cuando un medio de almacenamiento ya no es necesario, el medio pueden ser:
  - **Destruido**: La destrucción del disco duro asegura completamente que los datos no se pueden recuperar de un disco duro.
  - **Reciclado**: Las unidades de disco duro que se han limpiado se pueden reutilizar en otras computadoras. Se puede volver a formatear la unidad e instalar un nuevo sistema operativo.



13.3 Protección de las estaciones de trabajo con Windows

Protección de una computadora

- Las computadoras y las estaciones de trabajo deben protegerse del robo.
  - Bloquee su estación de trabajo cuando esté ausente para evitar que usuarios no autorizados roben o accedan a recursos de red y computadoras locales.
  - Si debe dejar una computadora en un área pública abierta, deben usarse los bloqueos de cable para disuadir el robo.
  - Utilice una pantalla de privacidad para proteger la información que se muestra en la pantalla de los curiosos
- El acceso a su computadora también debe estar protegido.
  - Hay tres niveles de protección de contraseña que se pueden utilizar en una computadora.

Protección del BIOS

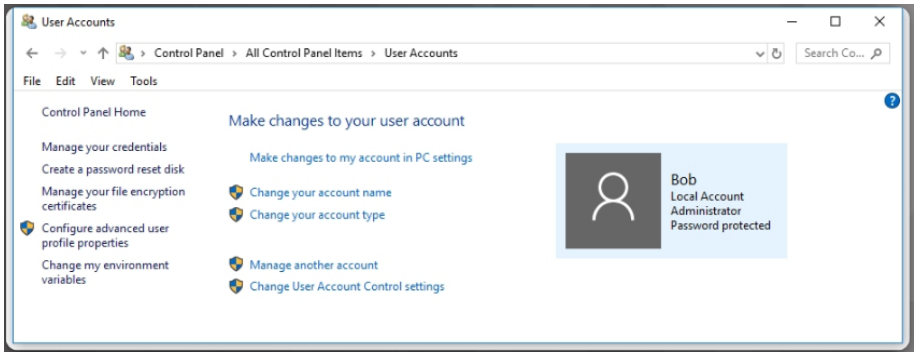
- Se puede eludir una contraseña de inicio de sesión de Windows, Linux o Mac.
- La configuración de una contraseña del BIOS o de UEFI impide que alguien modifique los ajustes de configuración y también puede evitar que alguien arranque la computadora.
- Todos los usuarios, independientemente de la cuenta de usuario, comparten contraseñas de BIOS.
- Las contraseñas de UEFI se pueden establecer en función de cada usuario; no obstante, se requiere un servidor de autenticación.

Protección del inicio de sesión de Windows

- El tipo más común de protección de contraseña es el inicio de sesión de la computadora.
- Según su sistema de computación, Windows 10 también puede admitir otras opciones de inicio de sesión. Específicamente, Windows 10 admite las siguientes opciones de inicio de sesión:
  - **Windows Hello**: característica que permite que Windows use el reconocimiento facial o use su huella digital para acceder a Windows.
  - **PIN**: Ingrese un número de PIN previamente configurado para acceder a Windows.
  - **Contraseña de imagen**: usted elige una imagen y gestos para usar con la imagen y crear una contraseña única.
  - **Bloqueo dinámico**: la función hace que el bloqueo de Windows se produzca cuando un dispositivo preemparejado, como un teléfono celular, sale del alcance de la computadora.

Administración local de contraseñas

- La administración de contraseñas para las computadoras Windows independientes se realiza en forma local por medio de la herramienta **Cuentas de usuario** de Windows.
  - Para crear, eliminar o modificar una contraseña en Windows, utilice **Panel de control > Cuentas de usuario**
- También es importante asegurar que las computadoras estén protegidas cuando los usuarios no las utilizan.
  - Las políticas de seguridad deben incluir una regla que exija que la PC se bloquee al activarse el protector de pantalla.
  - En todas las versiones de Windows, use **Panel de control > Personalización > Protector de pantalla**
    - Elija un protector de pantalla y un tiempo de espera y, a continuación, seleccione la opción **Mostrar la pantalla de inicio de sesión al reanudar**.



Nombres de usuario y contraseñas

- Los nombres de usuario, al igual que las contraseñas, son datos importantes que no se deben revelar.
- Las pautas para crear contraseñas son un componente importante de las políticas de seguridad.
- Todo usuario que deba iniciar sesión en una PC o conectarse a un recurso de red debe tener una contraseña.
- Las contraseñas ayudan a impedir el robo de datos y las acciones malintencionadas.
- Las contraseñas ayudan a asegurar que el registro de eventos se lleve a cabo correctamente al asegurar que el usuario es la persona correcta.

Política de seguridad local de Windows

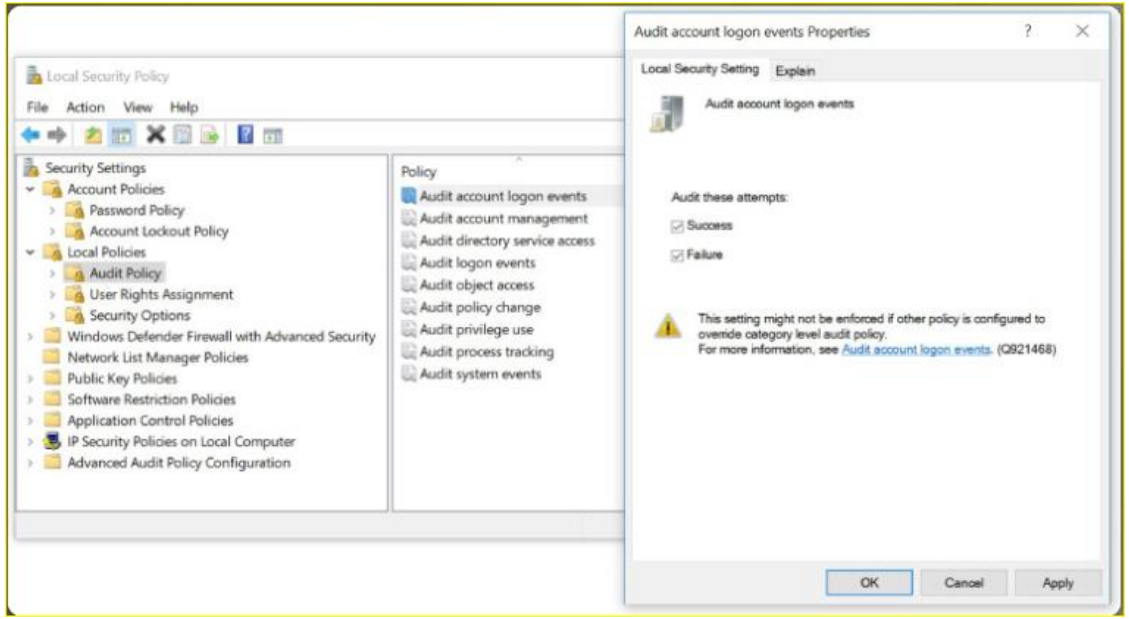
- En la mayoría de las redes que usan computadoras Windows, Active Directory se configura con los dominios en un servidor Windows.
  - Las computadoras con Windows son miembros de un dominio.
  - El administrador configura una política de seguridad de dominio que se aplica a todas las computadoras que se unan.
  - Las políticas de cuenta se configuran automáticamente cuando un usuario inicia sesión en Windows.
- La Política de seguridad local de Windows se puede utilizar para aplicar la configuración de seguridad en computadoras independientes que no forman parte de un dominio de Active Directory.
  - Para acceder a la Política de seguridad local en Windows 7 y Vista, utilice **Inicio > Panel de control > Herramientas administrativas > Política de seguridad local**.
  - En Windows 8, 8.1 y Windows 10, use **Buscar > secpol.msc** y, a continuación, haga clic en **secpol**.
- **Nota**: En todas las versiones de Windows, puede usar el comando de **Ejecutar secpol.msc** para abrir la herramienta de la Política de seguridad local.

Configuración de seguridad de políticas de la cuenta

- La política de seguridad identificará las políticas de contraseñas requeridas.
- La política de seguridad local de Windows se puede utilizar para implementar las políticas de contraseña.
  - Use **Políticas de la cuenta > Política de contraseña** para aplicar los requisitos de contraseña
  - Use **Políticas de la cuenta > Política de bloqueo de cuenta** para evitar ataques de fuerza bruta
    - Esta Política de bloqueo de cuenta también protege contra un ataque de diccionario. Este es un tipo de ataque de fuerza bruta que prueba cada palabra de un diccionario con la esperanza de obtener acceso.

Configuración de seguridad de políticas locales

- La política local de la Política de seguridad local se utiliza para configurar las políticas de auditoría, políticas de derechos de usuario y políticas de seguridad.
  - También se puede utilizar para registrar los intentos de inicio de sesión correctos e incorrectos.
- Utilice **Políticas locales > Políticas de auditoría** para habilitar la auditoría.



Exportación de la política de seguridad local

- Es posible que un administrador deba implementar una política local amplia para los derechos de usuario y las opciones de seguridad. Es probable que esta política deba replicarse en cada sistema.
- Para ayudar a simplificar este proceso, la **Política de seguridad local** se puede exportar y copiar a otros hosts de Windows.
- Los pasos para replicar una Política de seguridad local en otras computadoras son los siguientes:
    1. Utilice la función **Acción > Exportar lista…** para exportar la política de un host seguro.
    2. Guarde la política con un nombre, como **workstation.inf** en un medio externo.
    3. Luego, importe el archivo de la política de seguridad local a otras computadoras independientes.

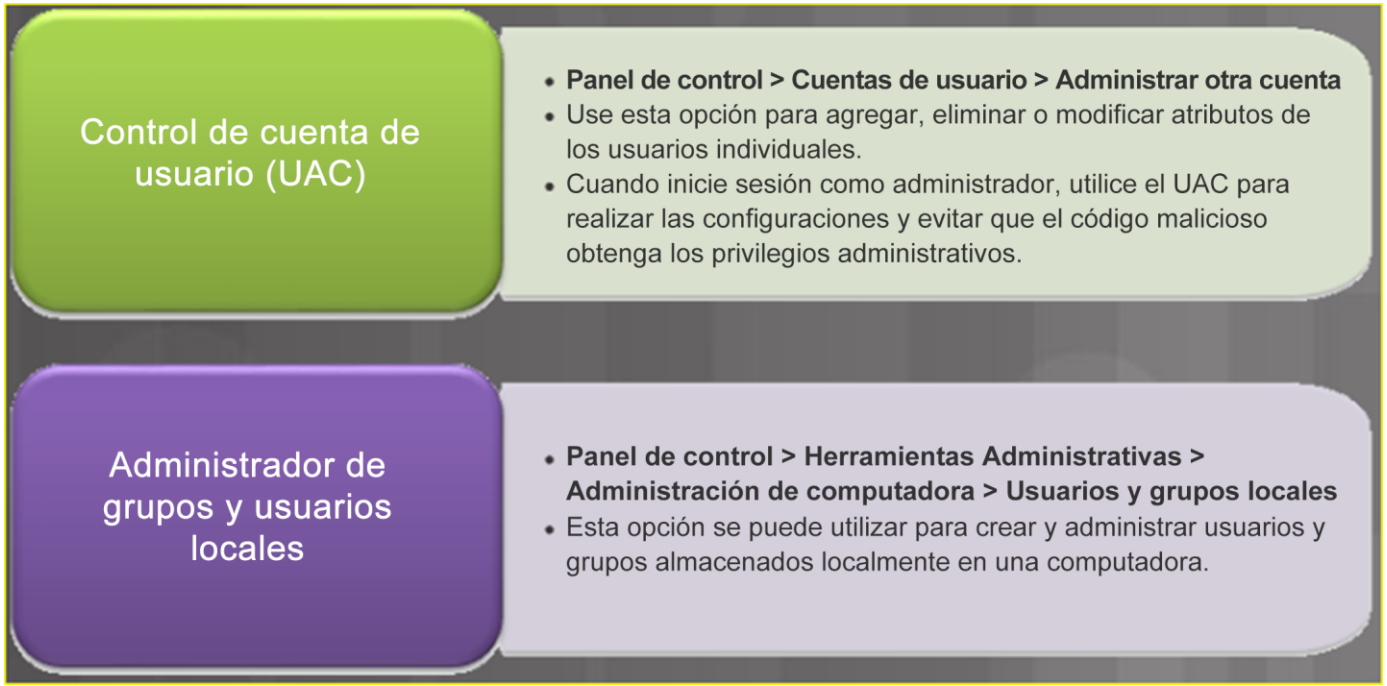
Práctica de laboratorio: Configuración de la política de seguridad local de Windows

En esta práctica de laboratorio, configurará la política de seguridad local de Windows. Modificará las solicitudes de contraseña, permitirá la auditoría, configurará algunos derechos de usuario, y establecerá algunas opciones de seguridad. Luego, utilizará el Administrador de eventos para ver la información registrada.

Mantenimiento de cuentas

- **Finalizar el acceso del empleado:** cuando un empleado abandona una organización, deshabilite inmediatamente la cuenta o cambie las credenciales de inicio de sesión.
- **Acceso de invitado:** se puede crear una Cuenta de invitado especial para usuarios temporales e invitados con privilegios adicionales y se la puede deshabilitar según sea necesario.
- **Seguimiento de los tiempos de inicio de sesión:** Permita el inicio de sesión del empleado solo durante horas especificadas del día y bloquee los inicios de sesión del resto del día.
- **Registre los intentos fallidos de inicio de sesión:** Configure una cantidad específica de veces que un usuario puede intentar iniciar sesión.
- **Tiempo de espera de inactividad y bloqueo de pantalla:** Configure un temporizador de inactividad para cerrar automáticamente la sesión del usuario. El usuario debe volver a iniciar sesión para desbloquear la pantalla.

Administración de las herramientas y tareas de cuentas de usuarios



Administrador de usuarios y grupos locales

- La herramienta Usuarios y grupos locales puede limitar la capacidad de los usuarios y grupos de realizar ciertas acciones asignándoles permisos y derechos.
- Para configurar todos los usuarios y grupos de una computadora mediante las herramientas del **Administrador de usuarios y grupos locales**, escriba **lusrmgr.msc** en la casilla Buscar o en la utilidad Ejecutar.
  - En la ventana **Usuarios y grupos locales > Usuarios** se muestran las cuentas de usuario actuales en la computadora.
- Al hacer doble clic a un usuario o hacer clic con el botón secundario y seleccionar **Propiedades**, se abre la ventana Propiedades del usuario:
  - cambiar las opciones del usuario definidas cuando se creó al usuario.
  - bloquear una cuenta
  - asignar un usuario a un grupo
  - controlar a qué carpetas tiene acceso el usuario.
  - Para agregar un usuario, haga clic en el menú **Acción** y seleccione **Usuario nuevo**.
  - En esta página, puede asignar un nombre de usuario, nombre completo, descripción y opciones de cuenta.

Administración de usuarios

- Los usuarios pueden ser asignados a los grupos para facilitar la administración.
- La herramienta Administrador de usuarios y grupos locales se utiliza para administrar grupos locales en una computadora con Windows.
  - Use **Panel de control > Herramientas Administrativas > Usuarios y grupos locales** para abrir el Administrador de usuarios y grupos locales.
  - En la ventana Usuarios y grupos locales, haga doble clic en **Grupos** para enumerar todos los grupos locales en la computadora.
- Haga doble clic en un grupo para ver sus propiedades.
- Para crear un nuevo grupo, haga clic en **Acción > Nuevo grupo** para abrir la ventana **Nuevo grupo**.
  - Aquí puede crear nuevos grupos y asignarles usuarios.

Usuarios y computadoras de Active Directory

- Mientras que las cuentas locales se almacenan en la base de datos de Cuentas de seguridad locales de una máquina local, las cuentas de dominio se almacenan en Active Directory en un Controlador de dominio (DC) de Windows Server.
- Solo los administradores de dominio pueden crear cuentas de dominio en el controlador de dominio.
  - Se puede acceder a las cuentas de dominio desde cualquier computadora que esté conectada al dominio.
- Active Directory es una base de datos de todas las computadoras, los usuarios y los servicios de un dominio de Active Directory.
  - La consola de usuarios y computadoras de Active Directory en Windows Server se utiliza para administrar usuarios, grupos y unidades organizativas (OU) de Active Directory.
    - Las unidades organizativas proporcionan una manera de subdividir un dominio en unidades administrativas más pequeñas.
- La creación de una nueva cuenta de grupo en Active Directory es similar a la creación de un nuevo usuario.
  - Abra Usuarios y computadoras de Active Directory y seleccione el contenedor que alojará al grupo, haga clic en **Acción**, haga clic en **Nuevo** y, luego, haga clic en **Grupo** ; posteriormente, complete los detalles del grupo y haga clic en **Aceptar**.

Práctica de laboratorio: Configuración de usuarios y grupos en Windows

En esta práctica de laboratorio, creará usuarios y grupos y eliminará a usuarios que utilizan el Administrador de usuarios y grupos locales. También asignará permisos de grupo y de usuario a las carpetas.

Firewalls

- Un firewall protege las computadoras y las redes evitando que el tráfico no deseado ingrese a las redes internas.
- Un firewall puede permitir que los usuarios externos tengan acceso controlado a servicios específicos.
- Los servicios de Firewall se pueden suministrar de la siguiente manera:
  - **Firewall basado en host**: uso de software como Firewall de Windows Defender.
  - **Oficina pequeña en el hogar (SOHO)**: solución basada en la red que utiliza un router inalámbrico doméstico o de oficina pequeña.
  - **Solución de pequeña o mediana empresa**: solución basada en la red mediante un dispositivo exclusivo, como un Cisco Adaptive Security Appliance (ASA) o habilitada en un router de servicios integrados (ISR) de Cisco.
  - Esta sección se centra en la solución de firewall basada en hosts mediante el Firewall de Windows.

Firewalls en software

- Un firewall de software es un programa que proporciona servicios de firewall en una computadora para permitir o denegar el tráfico a la computadora.
  - Un firewall de software aplica un conjunto de reglas a las transmisiones de datos mediante la inspección y el filtrado de paquetes de datos.
- El Firewall de Windows es un ejemplo de firewall de software que ayuda a evitar que los ciberdelincuentes y el malware obtengan acceso a su computadora.
  - Se instala de manera predeterminada durante la instalación del SO de Windows.
    - **Nota**: En Windows 10, se cambió el nombre de Firewall de Windows a Firewall de Windows Defender. En esta sección, el Firewall de Windows incluye Firewall de Windows Defender.
- La configuración de Firewall de Windows se determina en la ventana Firewall de Windows.
  - Para cambiar la configuración de Firewall de Windows, debe tener privilegios de administrador para abrir la ventana Firewall de Windows.
  - Para abrir la ventana Firewall de Windows, use **Panel de control > Firewall de Windows**.

Firewalls de Windows

- El Firewall de Windows tiene un conjunto estándar de reglas de entrada y salida que se habilitan según la ubicación de la red conectada.
  - Las reglas de Firewall se pueden habilitar para una red privada, una red pública o de invitado, o una red de dominio corporativo.
- Desde la ventana de Firewall de Windows, puede habilitar o deshabilitar el Firewall de Windows, cambiar la configuración de notificaciones, permitir que ingresen aplicaciones al firewall, configurar opciones avanzadas o restaurar valores predeterminados del firewall.
- Si desea utilizar otro firewall de software, deberá deshabilitar el Firewall de Windows.

Configuración de excepciones en Firewall de Windows

- Puede permitir o denegar el acceso a determinados programas o puertos desde la ventana de Firewall de Windows.
- Para configurar excepciones y permitir o bloquear aplicaciones o puertos, haga clic en **Permitir una aplicación o una función a través del Firewall de Windows** para abrir la ventana de aplicaciones permitidas y poder:
  - Agregar un programa o puerto permitido
  - Cambiar un programa o puerto permitido
  - Eliminar un programa o puerto permitido

Firewalls de Windows con seguridad avanzada

- Otra herramienta de Windows que está disponible para proporcionar un mayor control de acceso con las políticas de Firewall de Windows es el Firewall de Windows con seguridad avanzada.
  - Se llama Firewall de Windows Defender con seguridad avanzada en Windows 10.
- Para abrirla, desde la ventana de Firewall de Windows, haga clic en **Configuración avanzada** para abrirla.
  - **Nota**: de manera alternativa, introduzca **wf.msc** en el cuadro de búsqueda y presione Enter.
- Firewall de Windows Defender con seguridad avanzada proporciona estas características:
  - **Reglas de entrada y de salida**: configure reglas de entrada que se aplican al tráfico de Internet entrante y a las reglas salientes que se aplican al tráfico que sale de la computadora.
  - **Reglas de seguridad de conexión**: protege el tráfico entre dos computadoras y requiere que ambas computadoras tengan definidas y habilitadas las mismas reglas.
  - **Monitoreo**: muestra las reglas de entrada o de salida del firewall, o las reglas de seguridad de conexión activas.

Práctica de laboratorio: Configuración del Firewall de Windows

En esta práctica de laboratorio, se explora el Firewall de Windows y se configuran algunos parámetros avanzados.

Seguridad Web

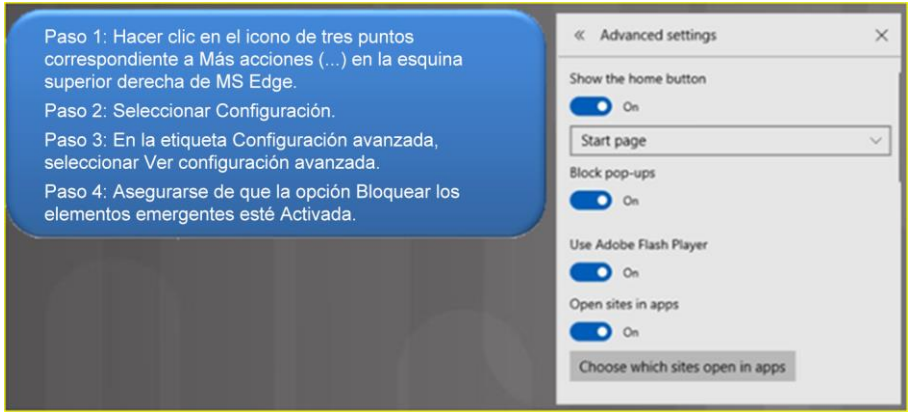
- Los navegadores web no solo se utilizan para la navegación web, sino que ahora también se utilizan para ejecutar otras aplicaciones, incluidas Microsoft 365, Google Docs, la interfaz para usuarios de SSL de acceso remoto y mucho más.
- Para admitir estas funciones adicionales, los navegadores utilizan complementos para admitir otros tipos de contenido.
  - Sin embargo, algunos de estos complementos también pueden presentar problemas de seguridad.
- Los navegadores son objetivos de ataque y deben protegerse.

Navegación InPrivate

- Los navegadores web retienen la información acerca de las páginas web que visita, las búsquedas que realiza, y otra información identificable, incluyendo los nombres de usuario, contraseñas y más.
- La información que conservan los navegadores web se puede recuperar y aprovechar para robar su identidad o su dinero, o cambiar sus contraseñas en cuentas importantes.
- Para mejorar la seguridad al utilizar una computadora pública, siempre:
  - **Borre el historial de navegación**: todos los navegadores web tienen una forma de borrar el historial de navegación, las cookies, los archivos y más.
  - **Use el modo InPrivate**: el navegador InPrivate almacena los archivos y las cookies temporalmente y los elimina cuando se termina la sesión InPrivate.
- Para Internet Explorer 11, utilice **Herramientas > Navegación InPrivate**
  - **Nota:** Como alternativa, presione **Ctrl+Mayús+P** para abrir una ventana InPrivate.

Bloqueador de elementos emergentes

- Los elementos emergentes se inician durante la exploración, por ejemplo, un enlace en una página que abre un elemento emergente para mostrar información adicional o una imagen ampliada.
- Algunos elementos emergentes son iniciados por un sitio web o un anunciante y, a menudo, son no deseados o molestos.
- La mayoría de los navegadores web ofrecen la capacidad de bloquear ventanas emergentes.
  - Esto permite al usuario a limitar o bloquear la mayoría de los elementos emergentes que aparecen al navegar en la Web.
  - Para habilitar la función de bloqueador de elementos emergentes de Internet Explorer 11, use **Herramientas > Bloqueador de elementos emergentes > Activar bloqueador de elementos emergentes**.



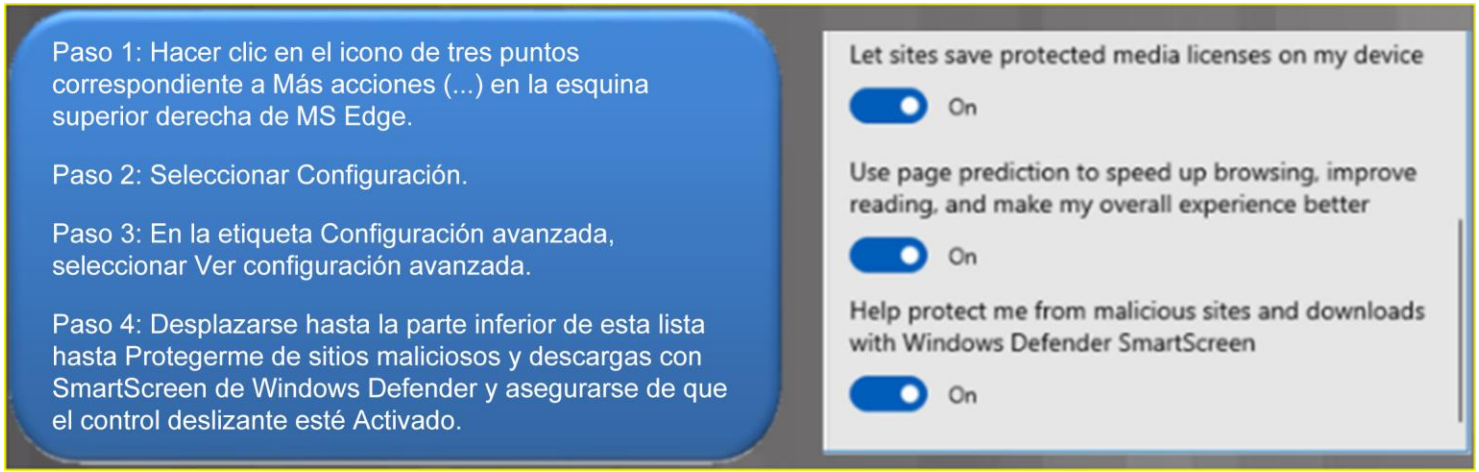
Filtro SmartScreen

Paso 1: Hacer clic en el icono de tres puntos correspondiente a Más acciones (...) en la esquina superior derecha de MS Edge.

Paso 2: Seleccionar Configuración.

Paso 3: En la etiqueta Configuración avanzada, seleccionar Ver configuración avanzada.

Paso 4: Desplazarse hasta la parte inferior de esta lista hasta Protegerme de sitios maliciosos y descargas con SmartScreen de Windows Defender y asegurarse de que el control deslizante esté Activado.



Filtrado de ActiveX

- Es posible que algunos navegadores web requieran que instale un control de ActiveX.
  - Los controles de ActiveX se pueden utilizar por motivos maliciosos.
- Cuando se habilita el filtrado ActiveX, puede elegir a qué sitios web se les permite ejecutar controles ActiveX.
  - Los sitios que no estén aprobados no pueden ejecutar estos controles, y el navegador no muestra notificaciones para que los instale o los habilite.
- Para habilitar el filtrado Active X en Internet Explorer 11, utilice **Herramientas > Filtrado de ActiveX**.
- Para ver el contenido ActiveX en un sitio web con el filtrado de ActiveX habilitado, haga clic en el ícono azul de **Filtrado de ActiveX** en la barra de direcciones y, luego, haga clic en **Desactivar el filtrado de ActiveX**.
  - Después de ver el contenido, puede volver a activar el filtrado ActiveX para el sitio web siguiendo los mismos pasos.

Configuración restrictiva

- Los dispositivos a menudo incluyen funciones de seguridad que no están habilitadas o las funciones de seguridad utilizan la configuración predeterminada.
  - Una configuración permisiva predeterminada puede dejar los dispositivos expuestos a atacantes.
- Muchos dispositivos ahora se envían con configuración restrictiva y deben configurarse para habilitar el acceso.
- Es su responsabilidad proteger los dispositivos y configurar los parámetros restrictivos siempre que sea posible.

Deshabilitar la reproducción automática

- Los hosts más antiguos de Windows usaban la ejecución automática para simplificar la experiencia del usuario.
  - Cuando se insertan nuevos medios (por ej., unidad de memoria Flash, CD o DVD) en la computadora, la ejecución automática busca automáticamente un archivo llamado **autorun.inf** y lo ejecuta.
  - Los usuarios maliciosos utilizaban esta función para infectar los hosts.
- Los hosts Windows más modernos ahora utilizan la reproducción automática.
- La reproducción automática proporciona controles adicionales y puede pedir al usuario que elija una acción según el contenido de los nuevos medios.
  - Use la ventana **Panel de control > Reproducción automática** para abrir la ventana de reproducción automática y configurar las acciones asociadas a los medios específicos.
- La solución más segura es desactivar la reproducción automática.

Paquetes de servicios y parches de seguridad del sistema operativo

- Los parches son actualizaciones de códigos que proporcionan los fabricantes para evitar que un virus o gusano recientemente descubierto logre atacar con éxito.
  - Los fabricantes pueden combinar parches y actualizaciones en una aplicación de actualización integral denominada “paquete de servicios”.
- Es fundamental aplicar parches de seguridad y actualizaciones del SO siempre que sea posible.
- Windows verifica sistemáticamente el sitio web de Windows Update en busca de actualizaciones de alta prioridad que ayuden a proteger una computadora de las amenazas de seguridad más recientes.
  - Según la configuración seleccionada, Windows descarga e instala automáticamente todas las actualizaciones de alta prioridad que la PC necesita, o notifica al usuario que dichas actualizaciones están disponibles.

13.4 Configuración de la seguridad inalámbrica.

Tipos comunes de cifrado de comunicaciones

- La comunicación entre dos computadoras puede requerir una comunicación segura.
- Existen dos requisitos principales:
  - El primer requisito es que la información recibida no haya sido alterada por alguien que haya interceptado el mensaje.
  - La segunda es que cualquier persona que pueda interceptar el mensaje no pueda leerlo.
- Las siguientes tecnologías cumplen estos requisitos:
  - Codificación hash
  - Cifrado simétrico
  - Cifrado asimétrico

Tipos comunes de cifrado de comunicaciones (Cont.)

- La codificación hash, o hashing, asegura la integridad del mensaje.
  - Esto significa que el mensaje no se ha dañado ni fue manipulado durante la transmisión.
  - La codificación hash utiliza una función matemática para crear un valor numérico, denominado síntesis del mensaje que es exclusivo para los datos.
  - El algoritmo de hash más popular es el algoritmo de hash seguro (SHA) que reemplaza el algoritmo de síntesis del mensaje 5 (MD5) más antiguo.

Tipos comunes de cifrado de comunicaciones (Cont.)

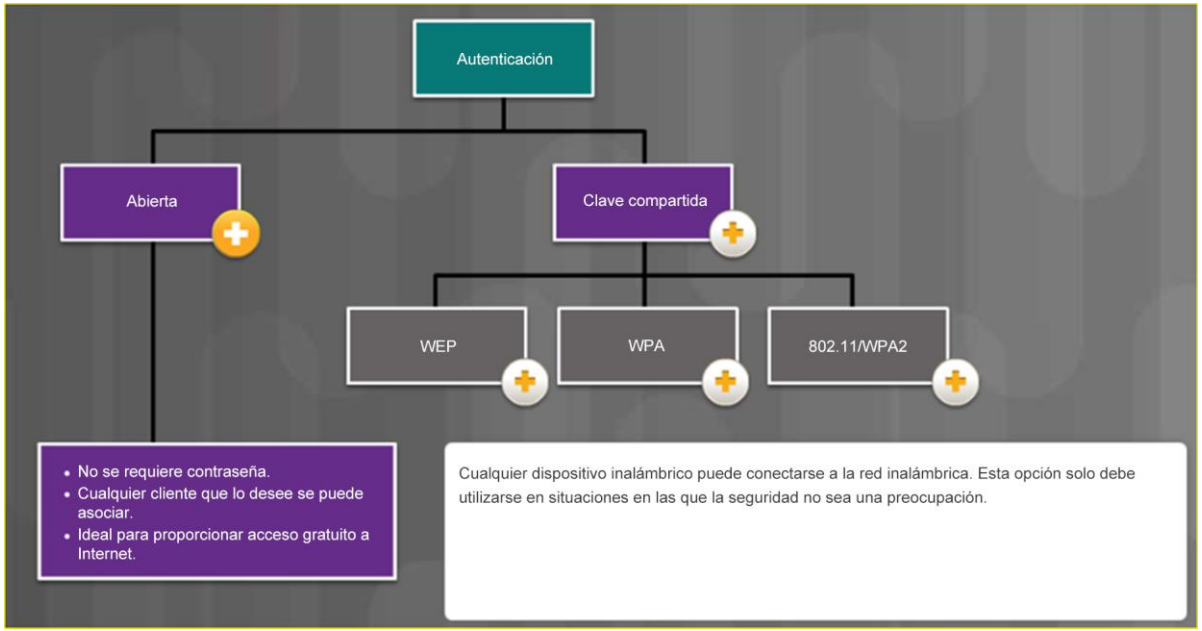
- El cifrado simétrico garantiza la confidencialidad del mensaje.
  - Si se intercepta un mensaje cifrado, no puede ser comprendido. Puede descifrarse únicamente (es decir, leer) con la contraseña (es decir, clave) que se cifró.
  - El cifrado simétrico exige que ambas partes de una conversación cifrada utilicen una clave de cifrado idéntica para codificar y decodificar los datos.
  - El estándar de cifrado avanzado (AES) y el antiguo algoritmo de cifrado triple de datos (3DES) son ejemplos del cifrado simétrico.
- El cifrado asimétrico también garantiza la confidencialidad del mensaje.
  - El cifrado asimétrico exige dos claves: una clave privada y una clave pública.
  - La clave pública puede distribuirse ampliamente, incluso enviarse por correo electrónico en forma de texto simple o publicarse en la Web.
  - En cambio, una persona conserva la clave privada, y esta no debe revelarse a nadie.
  - RSA es el ejemplo más común de cifrado asimétrico.

Identificadores del conjunto de servicios

- Identificador de conjunto de servicios (SSID, Service Set Identifier) es el nombre de la red inalámbrica.
  - Un punto de acceso o router inalámbrico realiza el broadcast del SSID de manera predeterminada, de modo que los dispositivos puedan detectar la red inalámbrica.
- Si se deshabilitó la configuración de difusón del SSID en un router o punto de acceso, los usuarios deben ingresar manualmente la SSID en clientes inalámbricos para conectarse a la red inalámbrica.
  - Deshabilitar la difusión del SSID brinda muy poca seguridad:
    - Alguien que conozca el SSID de la red inalámbrica puede introducirlo manualmente.
    - Una red inalámbrica también transmitirá el SSID durante un escaneo de la computadora.
    - También se puede interceptar un SSID en tránsito.

Métodos de autenticación

- Una clave compartida proporciona mecanismos para autenticar y descifrar datos entre el cliente inalámbrico y un AP de router inalámbrico.
- WEP representa las siglas en inglés de Privacidad alámbrica equivalente.
- WPA significa Acceso protegido Wi-Fi.
- IEEE 802.11i/WPA2 es un estándar del sector para proteger las WLAN. Ambos usan el Estándar de encriptación avanzada (AES)



Modos de seguridad inalámbrica

Modos de seguridad inalámbrica

Instrucciones

Haga clic en cada botón para obtener más información sobre los modos de seguridad inalámbrica.

WPA2

Utilice un sistema de cifrado inalámbrico para codificar la información que desea enviar, a fin de evitar la captura y el uso no deseados de los datos. La mayoría de los puntos de acceso inalámbrico admiten varios modos de seguridad diferentes. Como se analizó en el capítulo anterior, implemente siempre el modo de seguridad más seguro (WPA2) posible.

WPA2 | WPS

Modos de seguridad inalámbrica (Cont.)

Modos de seguridad inalámbrica

Instrucciones

Haga clic en cada botón para obtener más información sobre los modos de seguridad inalámbrica.

WPS

Muchos routers ofrecen Configuración protegida para Wi-Fi (WPS). Con WPS, el router y el dispositivo inalámbrico tienen cada uno un botón que, al presionarse en ambos dispositivos, configura automáticamente la seguridad de Wi-Fi entre los dispositivos. También es común utilizar una solución de software mediante un PIN. Es importante saber que WPS no es un estándar totalmente seguro. Es vulnerable a los ataques de fuerza bruta. WPS debe desactivarse como práctica de seguridad recomendada.

WPA2

WPS

Actualizaciones de firmware

- La mayoría de los routers inalámbricos ofrecen firmware actualizable.
  - Las versiones de firmware pueden contener correcciones de problemas comunes informados por los clientes así como las vulnerabilidades de seguridad.
- Es importante revisar periódicamente el sitio web del fabricante para ver el firmware actualizado.
- Es común utilizar una GUI para cargar el firmware en el router inalámbrico.

Firewalls

- Un firewall de hardware inspecciona los paquetes de datos de la red antes de que lleguen a los dispositivos de la red interna.
  - Es posible configurar el firewall para que bloquee puertos individuales, un rango de puertos o tráfico específico de una aplicación.
- La mayoría de los routers inalámbricos también incluyen un firewall de hardware integrado.
- Pueden configurarse para permitir dos tipos diferentes de tráfico en su red:
  - Las respuestas al tráfico que se origina desde el interior de la red.
  - El tráfico destinado a un puerto que se dejó intencionalmente abierto.

Reenvío y activación de puertos

- Los firewalls de hardware se pueden utilizar para bloquear puertos, a fin de impedir el acceso no autorizado entrante y saliente de una LAN.
- No obstante, existen situaciones en las que deben abrirse puertos específicos para que determinados programas y aplicaciones puedan comunicarse con dispositivos de otras redes.
- La redirección de puertos es un método basado en reglas que permite dirigir el tráfico entre dispositivos de redes independientes.

Universal Plug and Play

- Plug and play universal (UPnP) es un protocolo que permite que los dispositivos dinámicamente se agreguen a una red sin necesidad de intervención del usuario o de la configuración.
- El reenvío a puerto se suele utilizar para:
  - Transmisión de medios
  - Organización de juegos
  - Proporcionar servicios de computadoras domésticas y de pequeñas empresas a Internet.

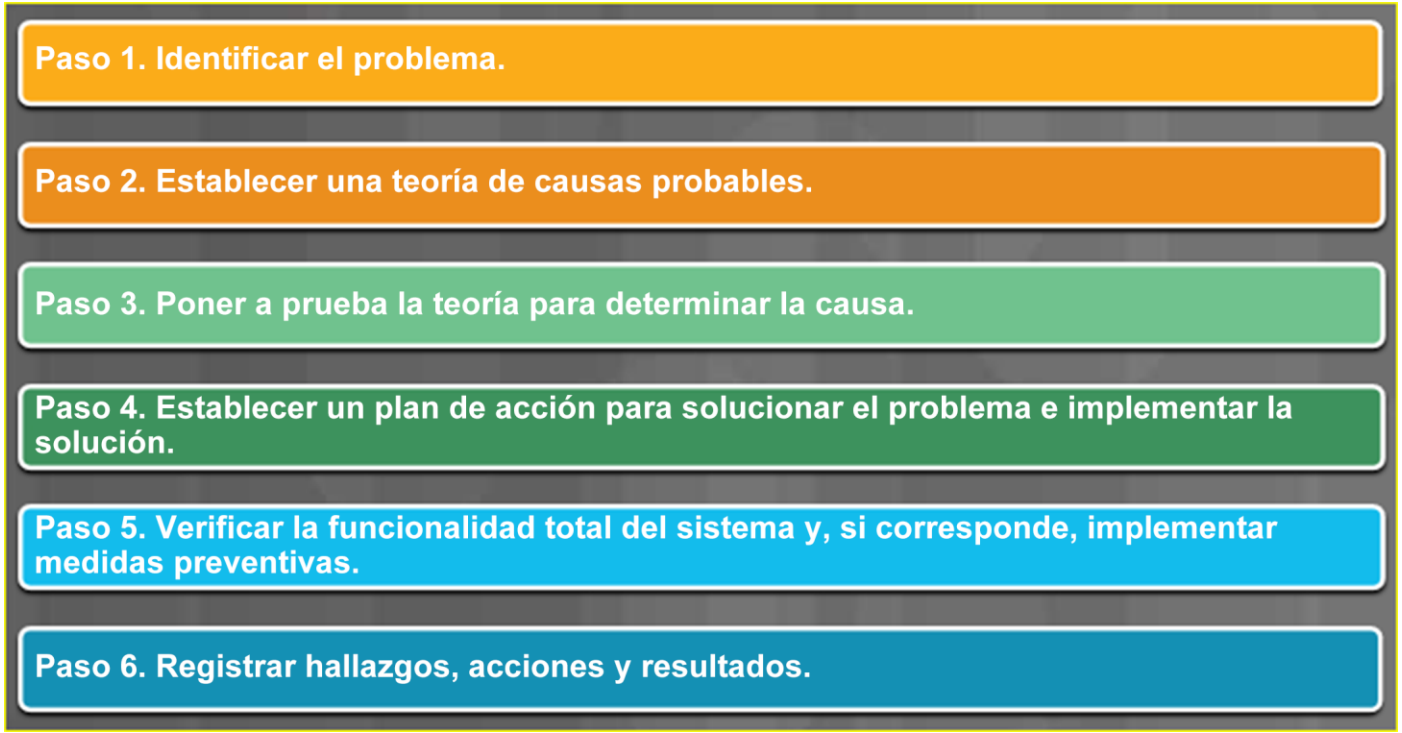
Packet Tracer: Configuración de la seguridad inalámbrica

En esta actividad, configurará el router inalámbrico para:

- Utilizar el modo WPA2 Personal como método de seguridad
- Confiar en el filtrado MAC para mejorar la seguridad
- Admitir el reenvío a puerto asignado único

13.5: Proceso básico de solución de problemas de seguridad

Proceso de resolución de problemas



Identificación del problema

Paso 1: Identificar el problema.	
Preguntas abiertas	• ¿Cuándo comenzó el problema? • ¿Qué problemas tiene? • ¿Qué sitios web visitó recientemente? • ¿Qué software de seguridad tiene instalado en la computadora? • ¿Quién más utilizó la computadora recientemente?
Preguntas cerradas	• ¿Está actualizado el software de seguridad? • ¿Realizó un proceso de detección de virus en la computadora recientemente? • ¿Abrió archivos adjuntos a algún correo electrónico sospechoso? • ¿Cambió la contraseña recientemente? • ¿Compartió la contraseña?

Establecimiento de una teoría de causa probable

Paso 2: Establecer una teoría de causas probables	
Causas comunes de los problemas de seguridad	• Virus • Troyano • Gusano • Spyware • Adware • Grayware o malware • Ardid de suplantación de identidad (phishing) • Contraseña comprometida • Salas de equipos sin protección • Entorno laboral sin seguridad

Prueba la teoría para determinar la causa

Paso 3: Poner a prueba la teoría para determinar la causa	
Pasos comunes para determinar la causa	• Desconectarse de la red. • Actualizar las firmas de antivirus y spyware. • Examinar la computadora con un software de protección. • Revisar que la computadora tenga los últimos parches y actualizaciones del sistema operativo. • Reiniciar la computadora o el dispositivo de red. • Iniciar sesión como usuario administrador para cambiar la contraseña de un usuario. • Implementar medidas de seguridad en salas de equipos. • Implementar medidas de seguridad en el entorno laboral. • Hacer cumplir la política de seguridad.

Establecimiento de un plan de acción para resolver el problema e implementar la solución

Paso 4: Establecer un plan de acción para resolver el problema e implementar la solución	
Si no logró solucionar el problema en el paso anterior, debe realizarse una investigación más exhaustiva para implementar la solución.	• Registros de reparaciones de soporte técnico • Otros técnicos • Sitios web de preguntas frecuentes de fabricantes • Sitios web técnicos • Grupos de noticias • Manuales de PC • Manuales de dispositivos • Foros en línea • Buscando en Internet

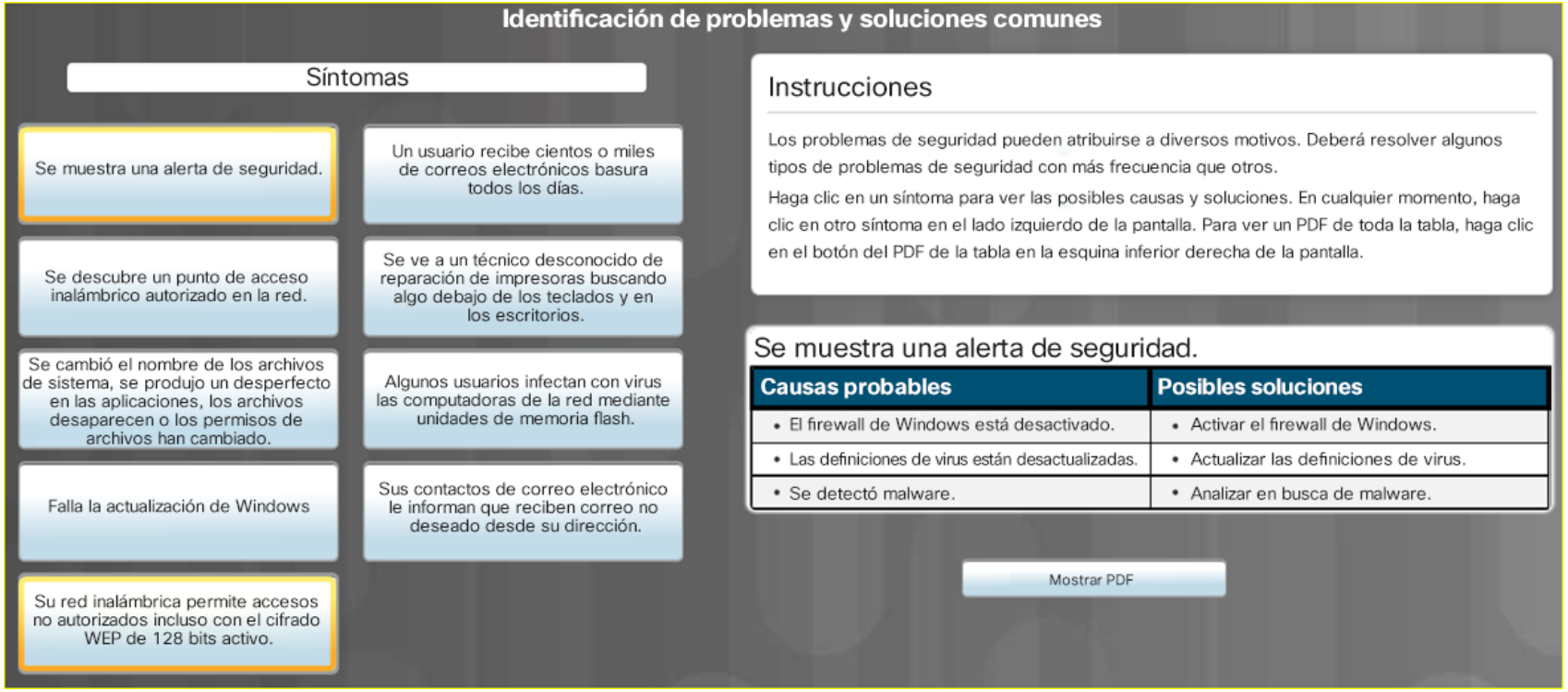
Verificación de la funcionalidad completa del sistema y, si corresponde, implementación de medidas preventivas

Paso 5: Verificar la funcionalidad total del sistema y, si corresponde, implementar medidas preventivas	
Verificar la solución y la funcionalidad total del sistema para las computadoras portátiles	• Volver a examinar la computadora para asegurarse de que no haya quedado ningún virus. • Volver a examinar la computadora para asegurarse de que no haya quedado ningún spyware. • Revisar los registros del software de seguridad para asegurarse de que no haya quedado ningún problema. • Revisar que la computadora tenga los últimos parches y actualizaciones del sistema operativo. • Probar la conectividad de la red y de Internet. • Asegurarse de que todas las aplicaciones funcionen. • Verificar el acceso a recursos autorizados, como impresoras y bases de datos compartidas. • Asegurarse de que las entradas estén protegidas. • Asegurarse de que se haga cumplir la política de seguridad.

Registro de hallazgos, acciones y resultados

Paso 6: Registrar hallazgos, acciones y resultados	
Registrar hallazgos, acciones y resultados	• Analizar la solución implementada con el cliente. • Solicitarle al cliente que verifique que se haya solucionado el problema. • Proporcionarle todos los documentos pertinentes al cliente. • Registrar los pasos que siguió para resolver el problema en la solicitud de trabajo y en el registro diario del técnico. • Registrar todos los componentes utilizados en la reparación. • Registrar el tiempo que le llevó resolver el problema.

Identificación de problemas y soluciones comunes



Práctica de laboratorio: documentación de la información del cliente en una solicitud de trabajo

En esta práctica de laboratorio, documentará información del cliente en una solicitud de trabajo.

13.6 Resumen del capítulo

Capítulo 13: Seguridad

- Explique las amenazas de seguridad comunes y cómo evitar y recuperarse de las amenazas.
- Identifique el propósito y el uso de los procedimientos de seguridad en la protección de equipos físicos y datos.
- Proteja las estaciones de trabajo de Windows dentro del BIOS, el sistema operativo y el firewall.
- Configure las opciones de seguridad inalámbrica en un router doméstico o de oficina pequeña.
- Resolución de problemas comunes de seguridad


CISCO