Soporte Técnico de Hardware y Software

FUNDAMENTO DE SEGURIDAD

Semana 8B

OBJETIVO DEL LABORATORIO

Describe los procedimientos de seguridad para una red lan, reconociendo la importancia y beneficios de la seguridad.

MARCO TEÓRICO

* Amenazas de seguridad
* Procedimientos de seguridad.
* Técnicas de mantenimiento preventivo comunes para propósitos de seguridad.
* Proceso básico de resolución de problemas de seguridad.

RECURSOS

1. Hardware

* Una computadora con una unidad de disco duro en blanco
* DVD o unidad de memoria flash USB de instalación de Windows 8.1 y 8.0

1. Software

* Sistema Operativo de Windows 8.1 y 8.0

PROCEDIMIENTO

Práctica de laboratorio 16:

12.2.1.8 Lab Configuración de la directiva de seguridad local de Windows

Introducción

En esta práctica de laboratorio, configurará la directiva de seguridad local de Windows. La directiva de seguridad local de Windows se utiliza para configurar una variedad de requisitos de seguridad para las computadoras independientes que no forman parte de un dominio de Active Directory. 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.

1. Equipo recomendado

* Una computadora con Windows instalado.

Nota: El acceso de las herramientas de la directiva de seguridad local es un poco diferente, según la versión de Windows. Pero después de que esté abierto, las configuraciones son las mismas para los pasos restantes en esta práctica de laboratorio.

* + 1. Revise los requisitos de seguridad.

El cliente debe tener seis computadoras independientes con Windows en una sucursal configurada según la política de seguridad de la organización. Estas computadoras no forman parte de un dominio de Active Directory. Las directivas se deben configurar manualmente en cada computadora.

La directiva de seguridad es la siguiente:

* Las contraseñas deben tener al menos 8 caracteres.
* Las contraseñas deben cambiar cada 90 días.
* Un usuario puede modificar la contraseña una vez al día.
* Un usuario debe utilizar una contraseña única al menos en 8 cambios de contraseña.
* Una contraseña debe constar de tres de los siguientes cuatro elementos:
* Al menos un carácter alfabético en minúsculas.
* Al menos un carácter alfabético en mayúsculas.
* Al menos un carácter numérico.
* Al menos un carácter de símbolo.
* Los usuarios son bloqueados de la computadora después de 5 intentos de ingresar la contraseña correcta. Un usuario debe esperar 5 minutos para que el contador se restablezca.
* Cada configuración de seguridad para la Directiva de Auditoría debe estar habilitada.
* Después de 30 minutos de inactividad, la cuenta del usuario se cerrará automáticamente (solamente para Windows 8.1 y 8.0).
* Los usuarios deben iniciar sesión antes de eliminar una computadora portátil de la estación de acoplamiento
* En iniciar sesión, a los usuarios se les presentarán los siguientes títulos y textos:
* Título: Precaución:
* Texto: Se controla su actividad. Esta computadora es solamente para uso comercial.
* Los usuarios recibirán un recordatorio para cambiar la contraseña 7 días antes de que expire.

La herramienta de directivas de seguridad local de Windows proporciona muchas más configuraciones que están fuera del alcance de este curso.

* + 1. Abra la herramienta de directivas de seguridad local de Windows.
       1. Para acceder a la directiva de seguridad local de Windows 7 y Vista, utilice la siguiente ruta de acceso:

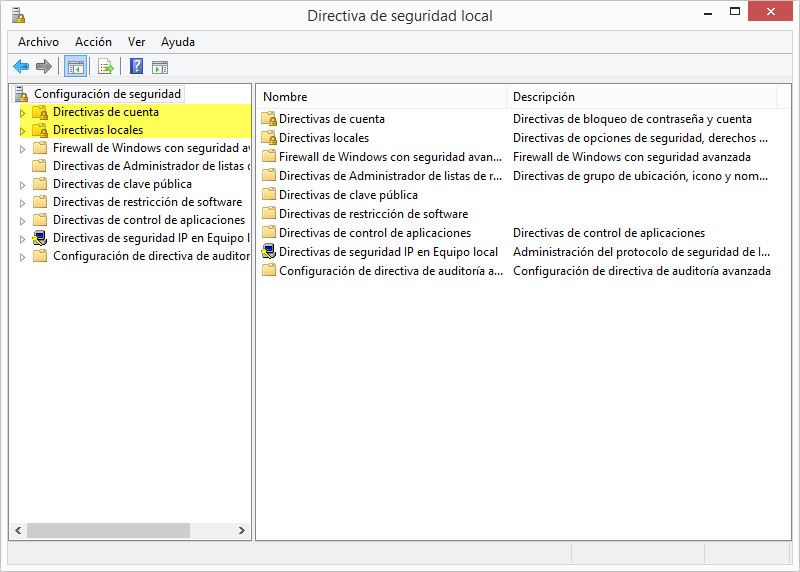
Inicio > Herramientas administrativas > Directiva de seguridad local

* + - 1. Para acceder a la directiva de seguridad local de Windows 8 y 8.1, utilice la siguiente ruta de acceso:

Buscar > secpol.msc y luego haga clic en secpol.

* + - 1. Se abre la ventana Directiva de seguridad local. Esta práctica de laboratorio se centra en las Directivas de cuenta y las Directivas locales, como se destaca en la figura a continuación. El resto de las opciones de Configuración de seguridad se encuentran fuera del alcance de este curso.

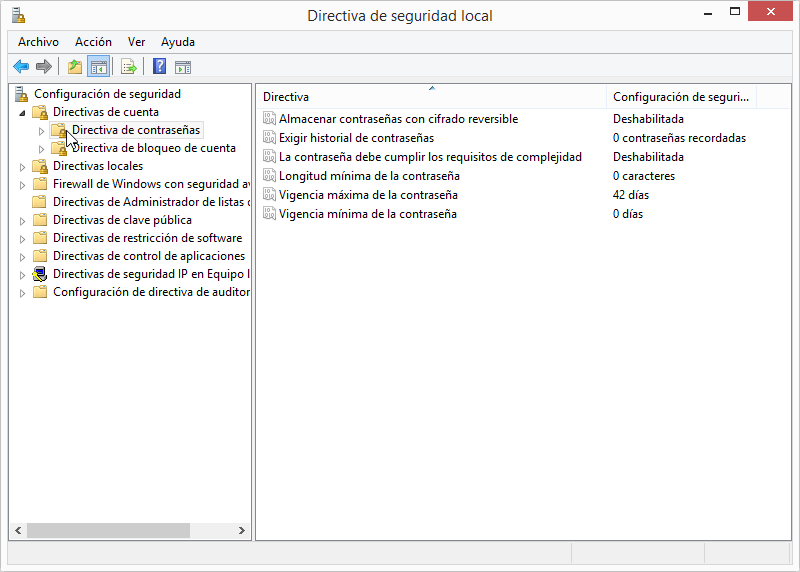
Nota: Las capturas de pantalla de Windows 8.1 se usan en este laboratorio.



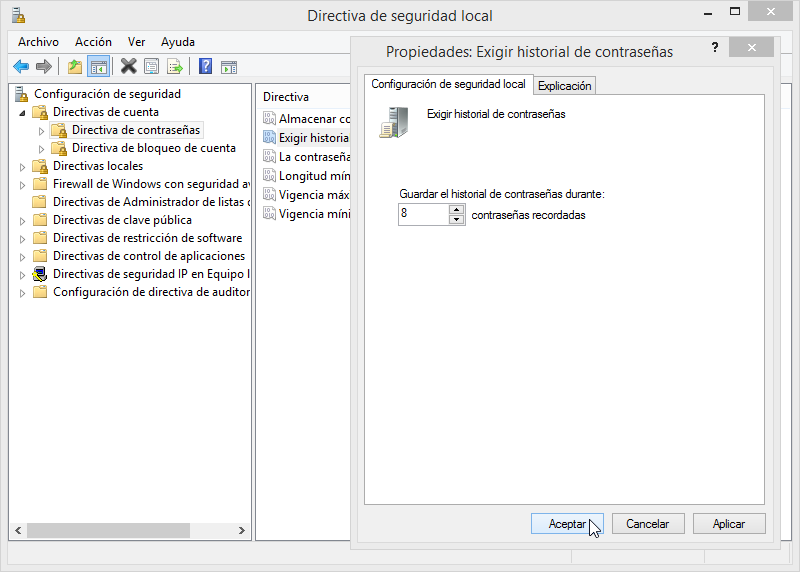
* + 1. Configure la configuración de seguridad de la directiva de contraseñas.

Los primeros seis requisitos de la directiva de seguridad de la empresa se configuran en la sección Directivas de cuenta de la herramienta Directivas de seguridad local.

* + - 1. Haga clic en la flecha junto a Directivas de seguridad para expandirla, y luego haga clic en Directiva de contraseñas. Se muestran seis políticas en el panel derecho con sus configuraciones de seguridad predeterminadas asociadas.



* + - 1. La primera directiva, Exigir historial de contraseñas, se utiliza para establecer la cantidad de contraseñas únicas que el usuario debe introducir antes de permitirle reutilizar una contraseña. Según la directiva de seguridad de la organización en el paso 1, la configuración de seguridad para esta política debe ser 8. Haga doble clic en Exigir historial de contraseñas para abrir la ventana Exigir propiedades del historial de contraseñas. Defina el valor en 8.

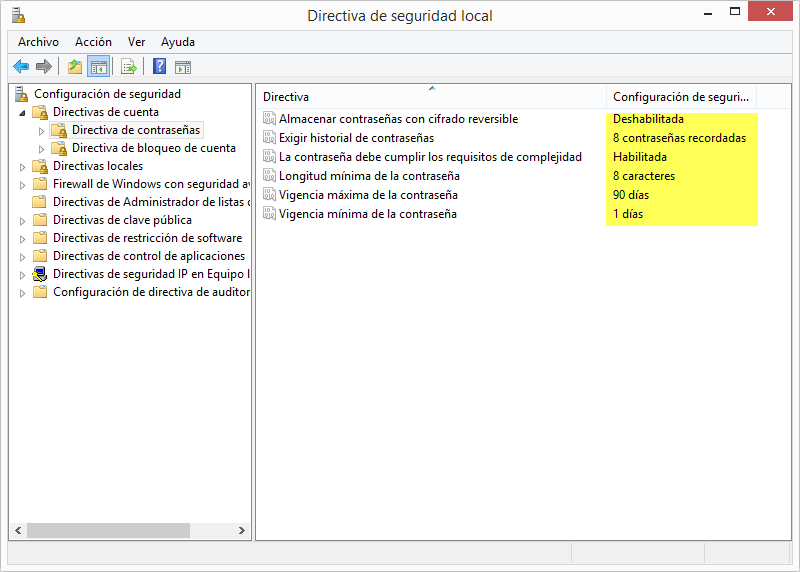


* + - 1. Mediante los requisitos de la política de seguridad del Paso 1, llene los valores que debe establecer en Directiva de seguridad local para las configuraciones de seguridad de Directiva de contraseñas restantes.

|  |  |
| --- | --- |
| Política | Configuración de seguridad |
| Exigir el historial de contraseñas | 8 |
| Duración máxima de contraseña |  |
| Antigüedad mínima de contraseña |  |
| Longitud mínima de la contraseña |  |
| La contraseña debe cumplir con los requisitos de complejidad |  |
| Guarde las contraseñas mediante cifrado reversible | Disabled |

Nota: La configuración de seguridad Almacenar contraseñas con cifrado reversible debe estar desactivada en todo momento. Almacenar contraseñas mediante cifrado reversible es esencialmente lo mismo que almacenar las versiones de texto no cifrado de las contraseñas. Por este motivo, esta directiva nunca debe activarse a menos que los requisitos de aplicaciones sobrepasen la necesidad de proteger la contraseña.

* + - 1. Haga doble clic en cada una de las directivas y establezca los valores según las entradas en la tabla anterior. Al hacerlo, la configuración se debe parecer a lo siguiente:



* + 1. Configure las configuraciones seguridad de la directiva de bloqueo de cuentas.
       1. De acuerdo con la directiva de seguridad en el paso 1, ¿cuántas veces se le permite a un usuario intentar iniciar sesión antes de que su cuenta sea bloqueada?

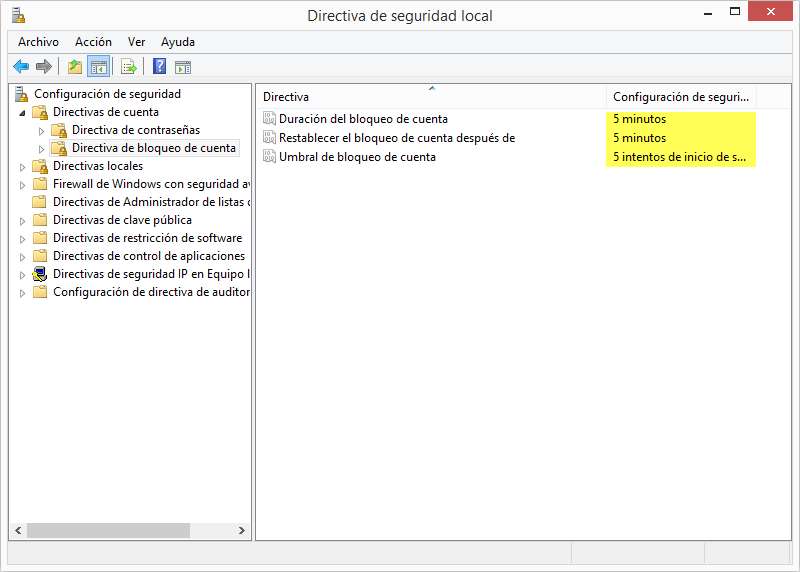
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. ¿Cuánto tiempo debe esperar el usuario antes de intentar volver a iniciar sesión?

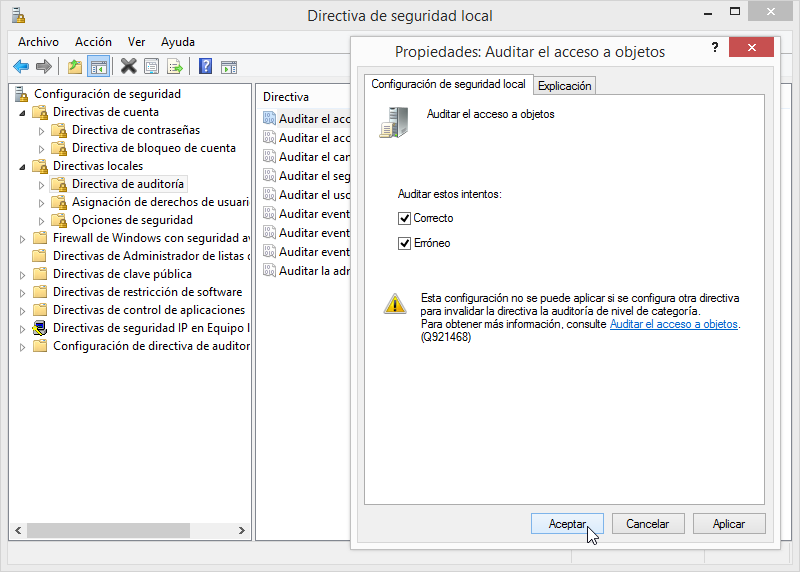
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. Utilice la configuración de seguridad Directiva de bloqueo de cuentas en Directiva de seguridad local para configurar los requisitos de las directivas. Cuando se instala, la configuración debe parecerse a lo siguiente.

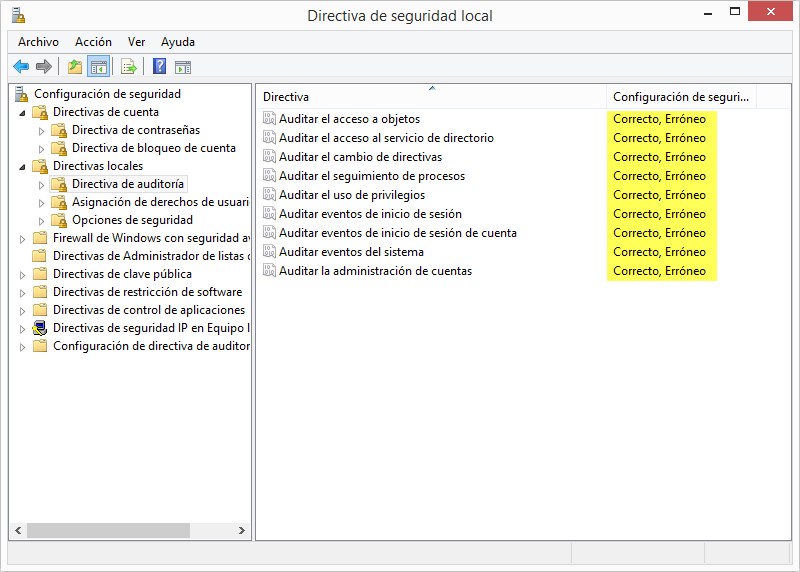
Sugerencia: Primero deberá configurar el Umbral de bloqueo de cuenta.



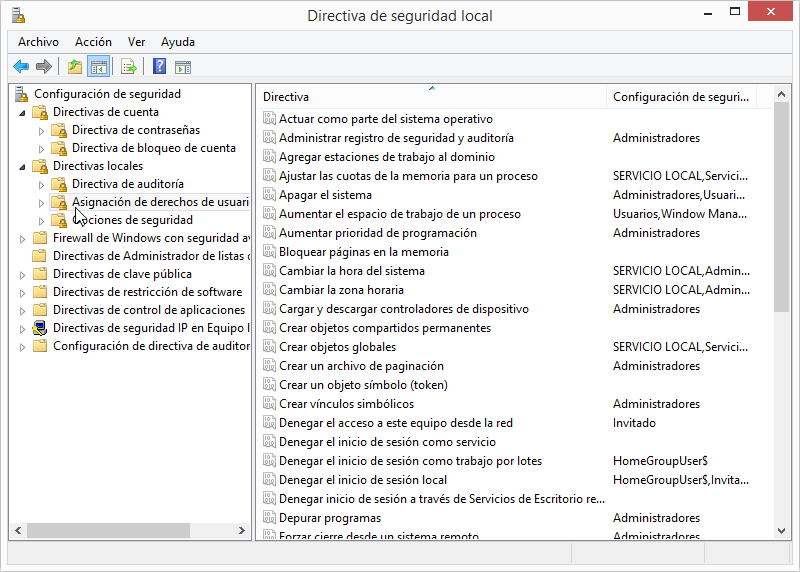
* + 1. Configure la seguridad de la directiva de auditoría.
       1. En Directiva de seguridad local, expanda el menú Directivas locales, y luego haga clic en Directiva de auditoría.
       2. Haga doble clic en Auditar eventos de inicio de sesión de cuenta para abrir la ventana Propiedades. Haga clic en la ficha Explicar para obtener sobre esta configuración de seguridad.
       3. Haga clic en la ficha Configuración de seguridad, y luego haga clic en las casillas de verificación para Correcto y Error. Haga clic en Aceptar para cerrar la ventana Propiedades y aplicar las configuraciones de seguridad.



* + - 1. Continúe modificando el resto de las configuraciones de seguridad de Directiva de auditoría. Haga clic en la ficha Explicar para cada uno y lea lo que hace. Haga clic en las casillas de verificación Correcto y Error en cada ventana de Propiedades. Después de que termine, su configuración de Directiva de auditoría debe parecerse a lo siguiente:



* + 1. Configure las configuraciones de seguridad de directivas locales adicionales
       1. En Directiva de seguridad local, haga clic en Asignación de derechos de usuario en Directivas locales para ver la configuración de seguridad.

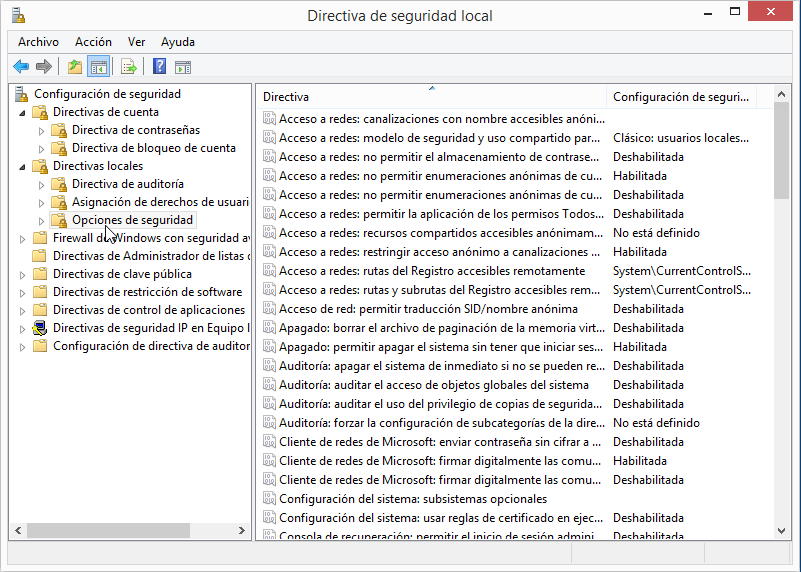


* + - 1. Aunque ninguna de las configuraciones de seguridad debe modificarse para cumplir con los requisitos de la directiva de seguridad, pase cierto tiempo viendo las configuraciones predeterminadas. ¿Hay alguna que usted recomendara cambiar? ¿Por qué?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. En Directiva de seguridad local, haga clic en Opciones de seguridad en Directivas locales para ver la configuración de seguridad.



* + - 1. Mediante los requisitos restantes de la política de seguridad del Paso 1, enumere los valores de las directivas y la configuración de seguridad que necesita cambiar en Opciones de seguridad en la siguiente tabla. La primera ya se completó.

|  |  |
| --- | --- |
| Política | Configuración de seguridad |
| Inicio de sesión interactivo: Límite de la inactividad de la máquina (Windows 8.1 y 8.0 solamente) | 1800 segundos |
|  |  |
|  |  |
|  |  |
|  |  |

* + 1. Pruebe las configuraciones de seguridad de directivas de contraseña.
       1. Pruebe las configuraciones de seguridad de directivas de contraseña intentando cambiar la contraseña. Intente con una nueva contraseña que no cumpla con la longitud o los requisitos de complejidad.

En 7 y Windows Vista, utilice la siguiente ruta:

Panel de control > Cuentas de usuario > Cambiar su contraseña

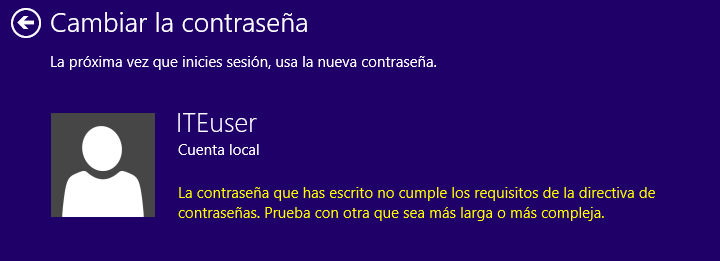
En Windows 8,1, utilice la siguiente ruta:

Panel de control > Cuentas de usuario > Realizar cambios en mi cuenta en Configuración > Opciones de inicio de sesión, y luego haga clic en Cambiar bajo Contraseña.

En Windows 8,0, utilice la siguiente ruta:

Panel de control > Cuentas de usuario > Realizar cambios en mi cuenta en Configuración, y luego en Cambie su contraseña.

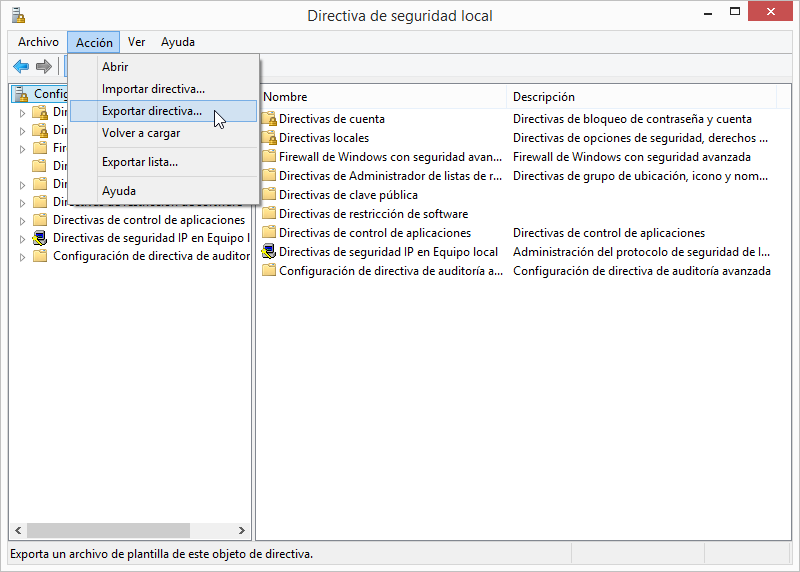
* + - 1. Debe presentarse con un mensaje que su nueva contraseña no cumple con los requisitos de directivas de contraseña, como este mensaje en Windows 8.1:



* + 1. Configuración de la directiva de seguridad de exportación y de importación.

El cliente tiene otras 5 computadoras independientes que deben cumplir los mismos requisitos de la directiva de seguridad. En lugar de configurar manualmente las configuraciones cada equipo, exporta las configuraciones de la computadora.

* + - 1. En la barra de menú en Directivas de seguridad local, haga clic en Acción > Directiva de exportación…



* + - 1. Elija un nombre para el archivo .inf y guárdelo en una ubicación de su elección.
      2. Copie el archivo de directiva de seguridad .inf a una unidad de memoria flash. Lleve la unidad de memoria flash a otra computadora. Inserte la unidad de memoria flash, abra Directiva de seguridad local, y haga clic en Acción > Importar directiva… Ubique el archivo .inf en la unidad de memoria flash y ábralo para aplicar la directiva de seguridad a la nueva computadora.

CONCLUSIONES Y RECOMENDACIONES DE LA EXPERIENCIA

* Asegúrese de que los estudiantes pueden describir la variedad de amenazas de seguridad comunes incluido el malware, suplantación, correo electrónico no deseado, ataques de día cero, e ingeniería social.
* Los estudiantes deben poder explicar la importancia de una política de seguridad
* Asegúrese de que los estudiantes puedan describir las técnicas para proteger los hosts, los datos, y las redes.
* Los estudiantes deben poder implementar la seguridad en Windows y un router inalámbrico.
* Los estudiantes deben poder explicar cómo mantener seguros los hosts, los datos, y las redes.
* Los estudiantes deben poder resolver los problemas de seguridad básicas.

ACTIVIDAD VIRTUAL

Revisa y analiza los siguientes enlaces, luego responde las preguntas propuestas:

* <https://support.microsoft.com/es-pe/help/17127/windows-back-up-restore>
* <https://www.monografias.com/trabajos-pdf/manejar-reparar-computadora/manejar-reparar-computadora2.shtml>

1. ¿Qué nivel de permiso de seguridad de Windows se requiere para un usuario local para realizar copias de seguridad de los archivos de otro usuario?
2. ¿Cuándo una persona que repara computadoras querría implementar la función del tiempo de espera de inactividad?
3. ¿Cuáles son las tres reglas que aumentan el nivel de seguridad de una contraseña?
4. ¿Qué amenaza de seguridad se instala en una computadora sin el conocimiento del usuario y luego supervisa la actividad de la computadora?
5. Cuando un técnico de soporte trabaja en la resolución de un problema de seguridad en un sistema, ¿qué medida debe tomar inmediatamente antes de registrar los hallazgos y cerrar la solicitud?