Práctica de laboratorio: 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.

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.

Paso 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.

Paso 2: Abra la herramienta de directivas de seguridad local de Windows.

a. Para acceder a la directiva de seguridad local de Windows 7 y Vista, utilice la siguiente ruta de acceso:

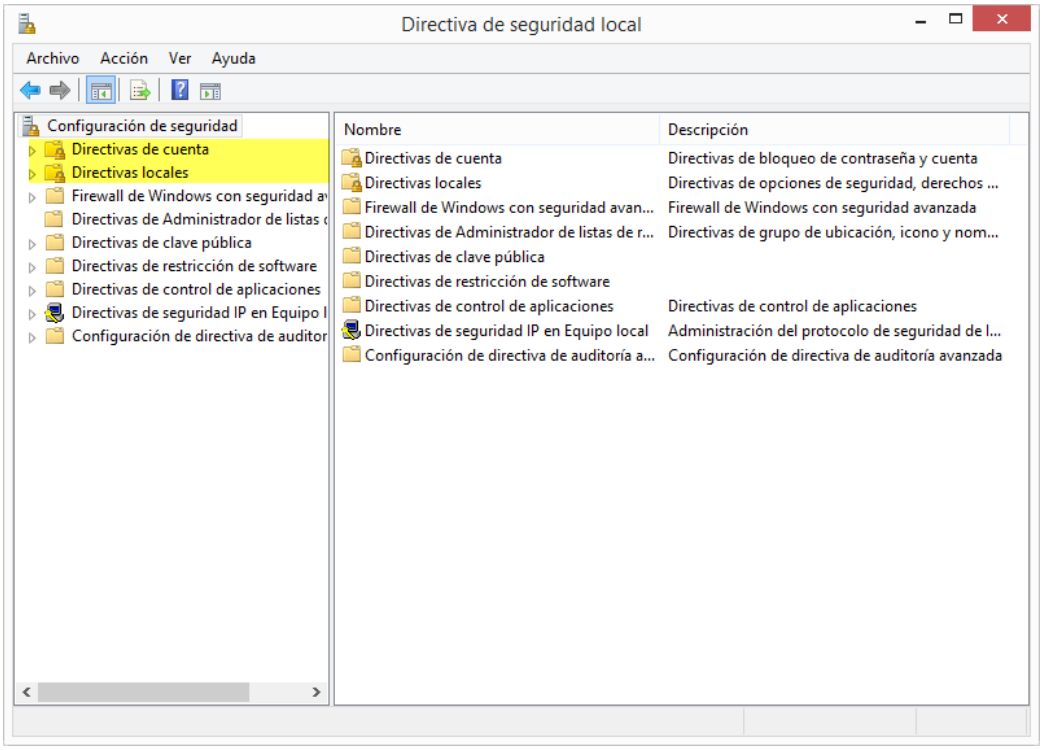
Inicio > Herramientas administrativas > Directiva de seguridad local

b. 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**.

c. 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.

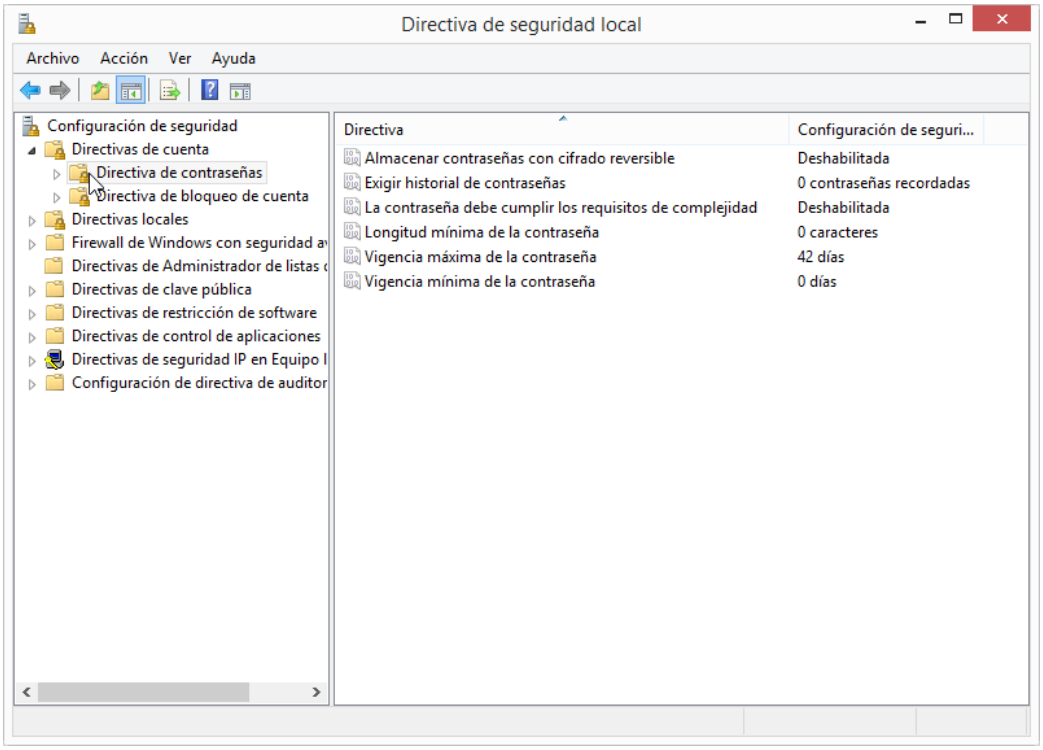
Nota: Las capturas de pantalla de Windows 8.1 se usan en este laboratorio.



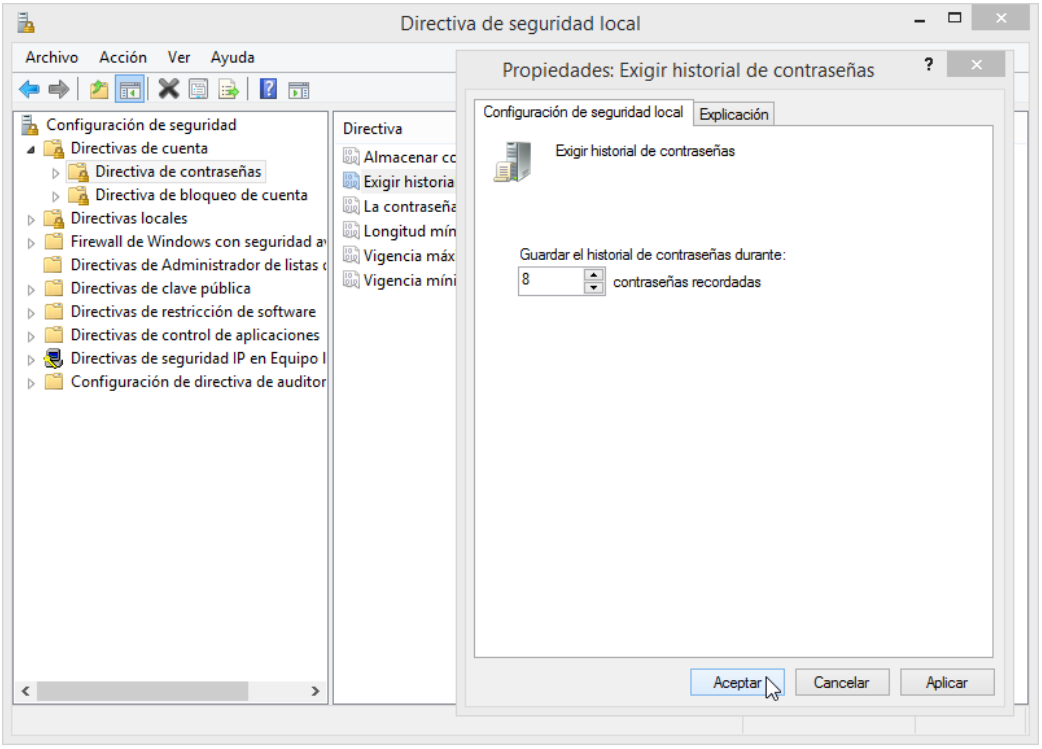
Paso 3: Configure la configuración de seguridad de la directiva de contraseñas.

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**.

a. 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.



b. 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**.

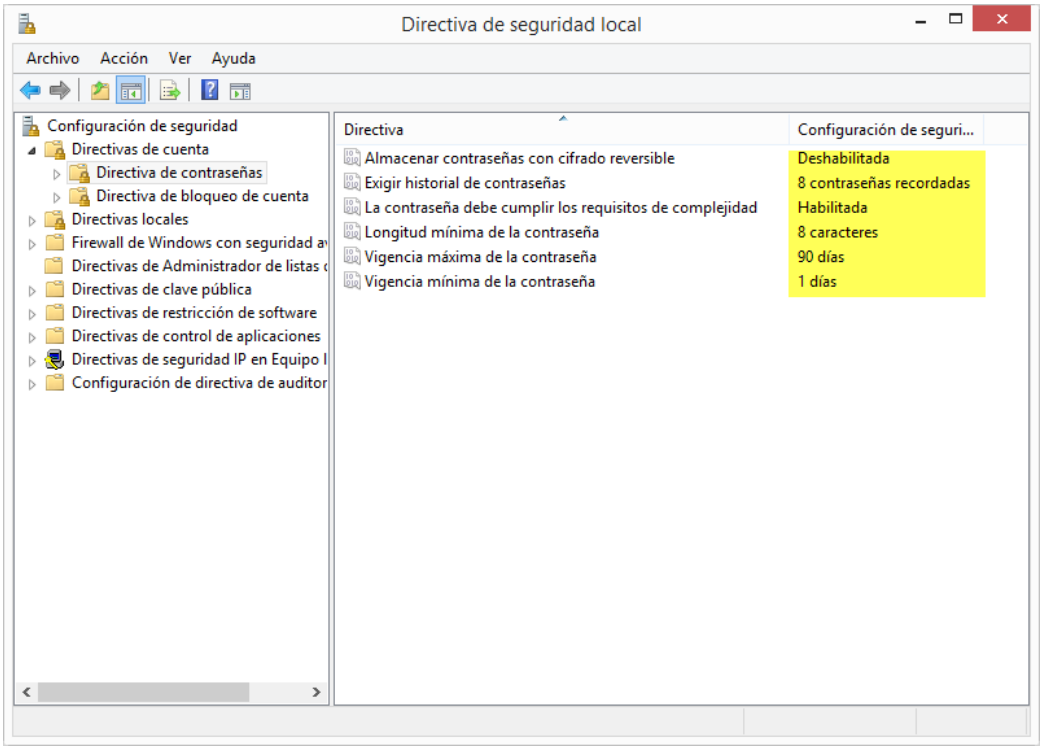


c. Mediante los requisitos de la política de seguridad del Paso 1, llene los valores que debe establecer en **Directiva de seguridad local** para las configuraciones de seguridad de **Directiva de contraseñas** restantes.

Política	Configuración de seguridad
Exigir el historial de contraseñas	8
Duración máxima de contraseña	30 dias
Antigüedad mínima de contraseña	8 dias
Longitud mínima de la contraseña	12 caracteres
La contraseña debe cumplir con los requisitos de complejidad	Mayusculas, numeros, simbolos
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.

d. 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:



Paso 4: Configure las configuraciones seguridad de la directiva de bloqueo de cuentas.

a. 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?

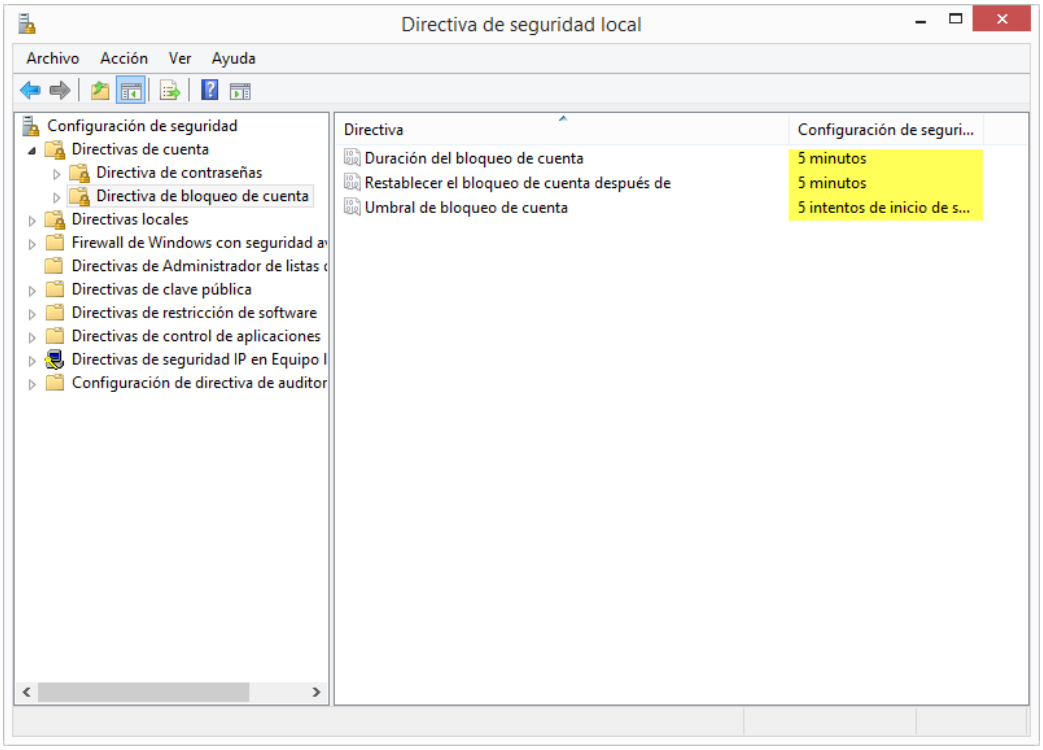
5 veces

b. ¿Cuánto tiempo debe esperar el usuario antes de intentar volver a iniciar sesión?

5 minutos

c. 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**.

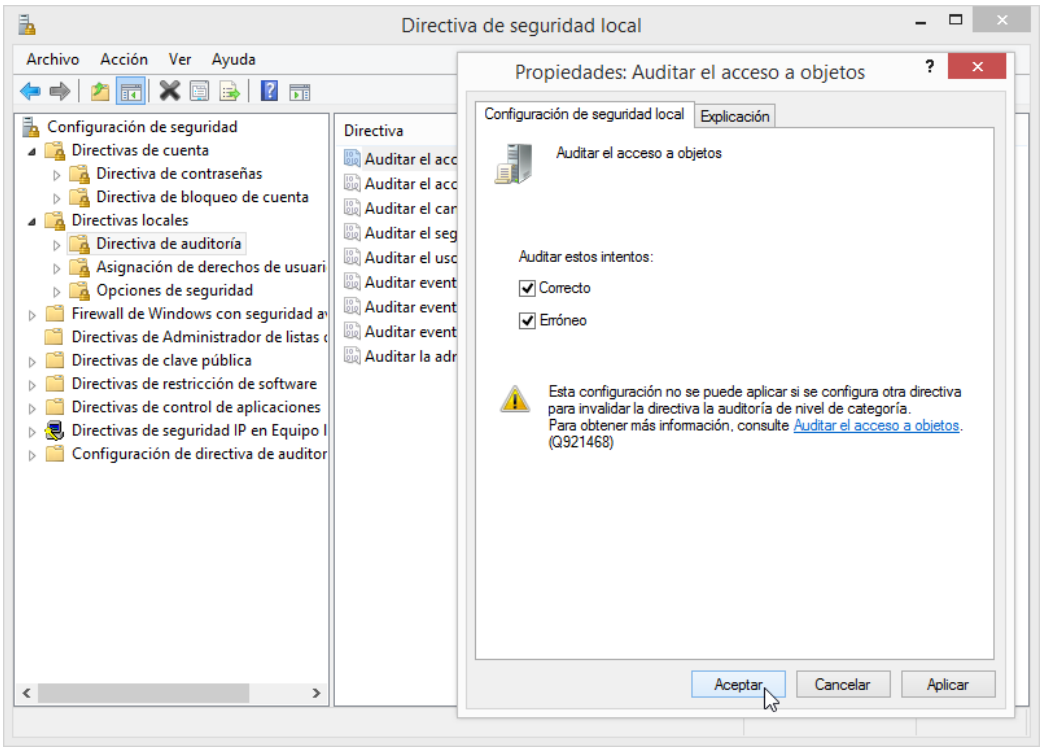


Paso 5: Configure la seguridad de la directiva de auditoría.

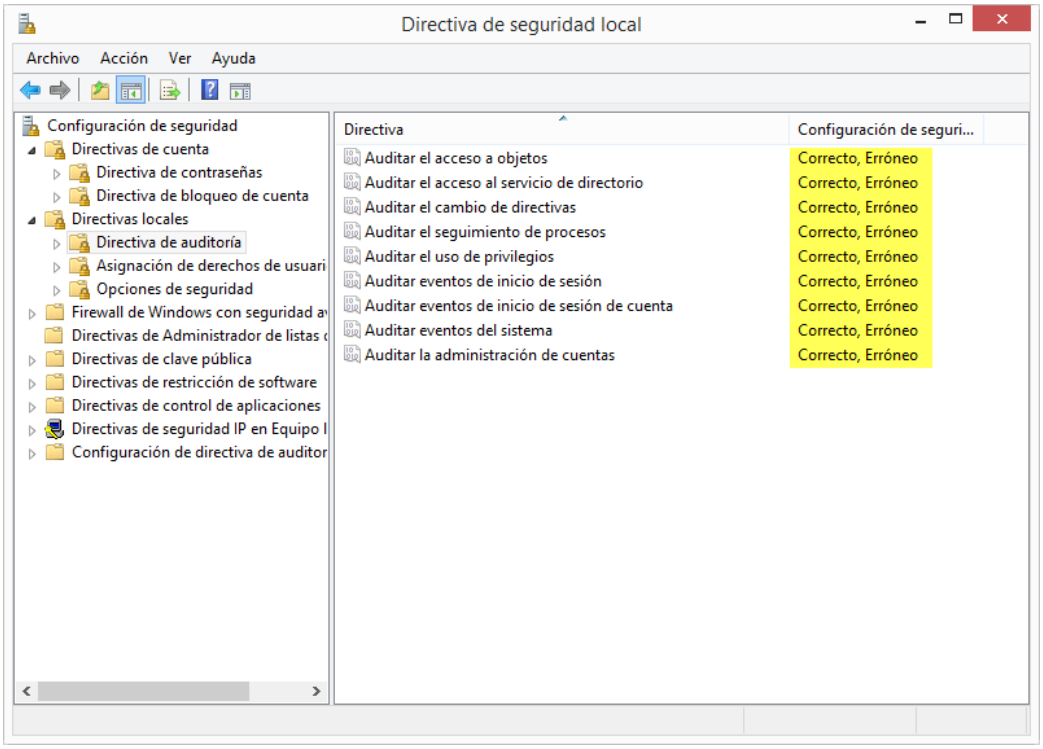
a. En **Directiva de seguridad local**, expanda el menú **Directivas locales**, y luego haga clic en **Directiva de auditoría**.

b. 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.

c. 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.

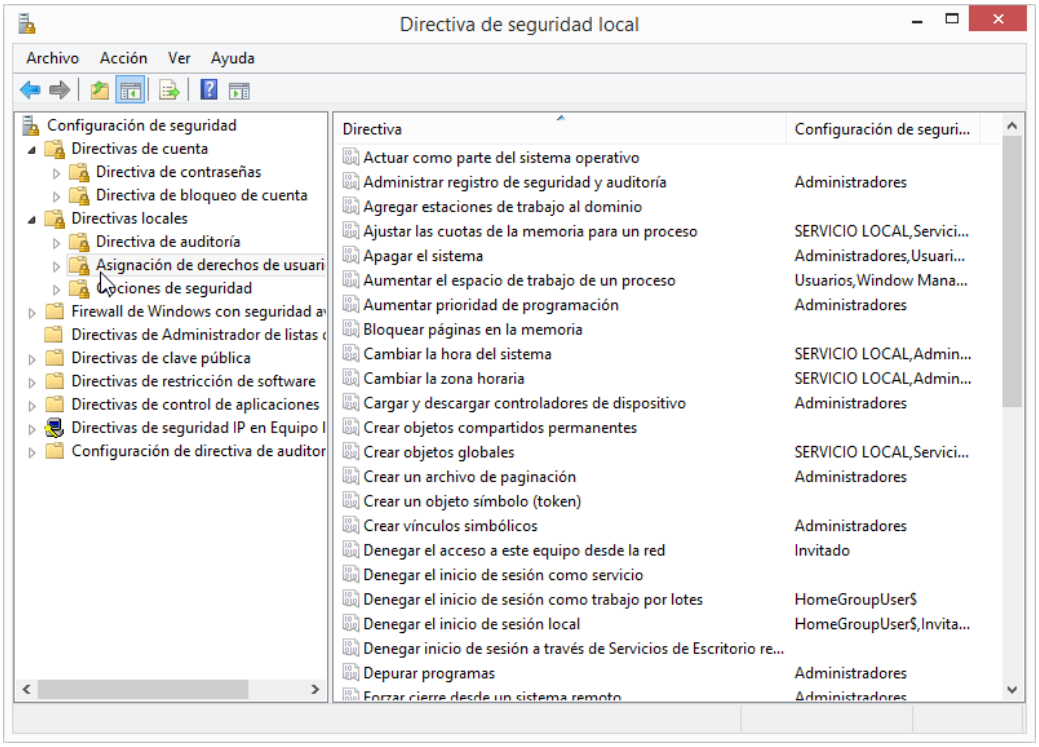


d. Continúe modificando el resto de las configuraciones de seguridad de **Directiva de auditoría**. Haga clic en la ficha **Explicar** para cada uno y lea lo que hace. Haga clic en las casillas de verificación **Correcto** y **Error** en cada ventana de **Propiedades**. Después de que termine, su configuración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



Paso 6: Configure las configuraciones de seguridad de directivas locales adicionales

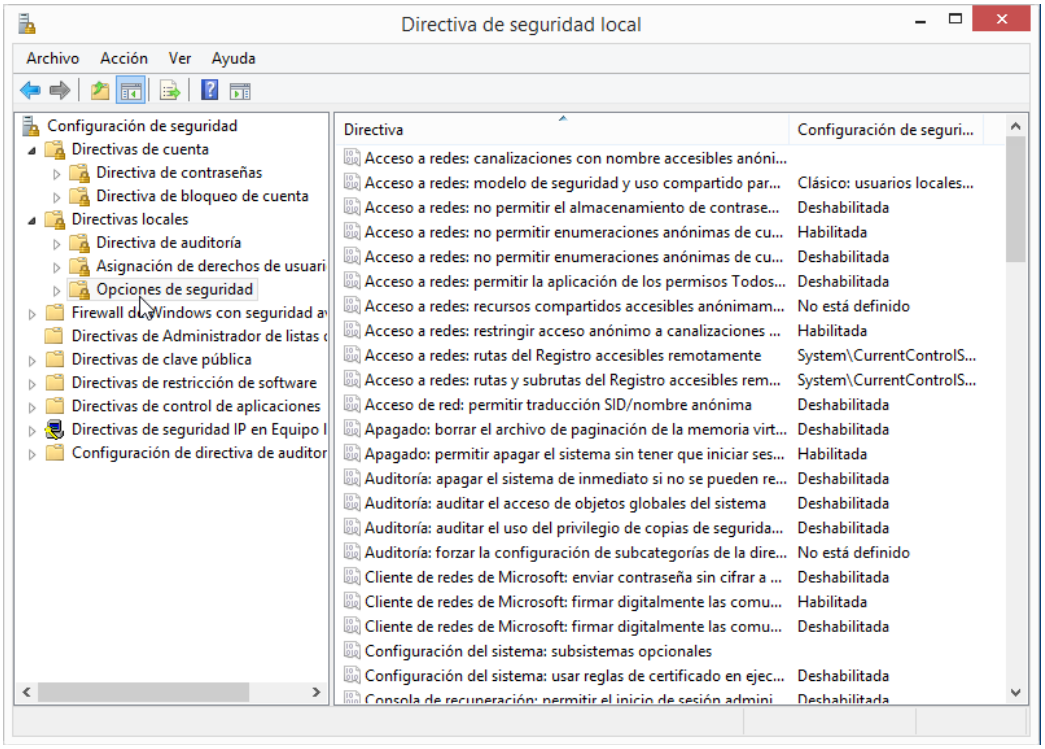
a. En **Directiva de seguridad local**, haga clic en **Asignación de derechos de usuario** en **Directivas locales** para ver la configuración de seguridad.



b. 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?

La de Iniciar Sesión como servicio porque al iniciar seccion en la cuenta de usuario personal la persona debera ser alguien que este autorizado o asignado para el control de ese mismo equipo y para el ingreso a la cuenta de servicio solo una persona con instruccion de ingreso puede utilizar el equipo

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



d. 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
Acceso a Redes	Solo para personal tecnico
Control de cuentas de usuario	vigilancia previa en historial y seguimiento web
Dispositivos	Restringir la conexion a ciertos dispositivos moviles
consola de recuperacion	constante actualizacion de fireware y restriccion de uso para personal no

Paso 7: Pruebe las configuraciones de seguridad de directivas de contraseña.

a. 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

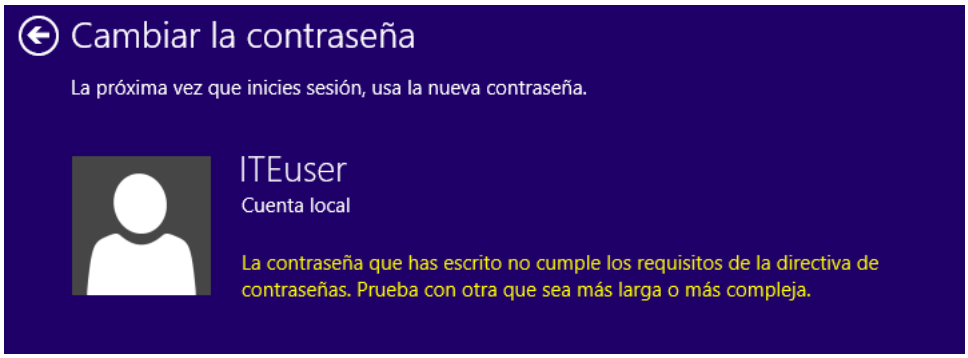
   En Windows 8,1, utilice la siguiente ruta:

   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**.

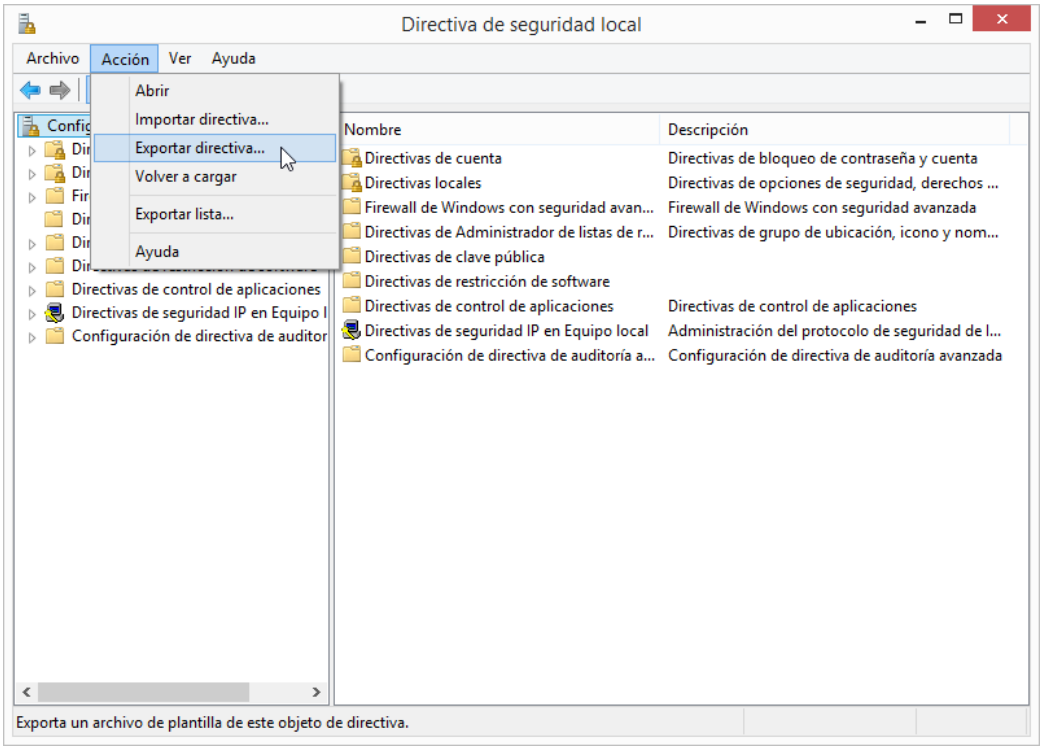
b. Debe presentarse con un mensaje que su nueva contraseña no cumple con los requisitos de directivas de contraseña, como este mensaje en Windows 8.1:



Paso 8: 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.

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



b. Elija un nombre para el archivo **.inf** y guárdelo en una ubicación de su elección.

c. 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.