LABORATORIO 4: CONFIGURACIÓN DE LA POLÍTICA DE SEGURIDAD LOCAL DE WINDOWS

Realizado por: Jesús Padilla Crespo

Laboratorio 4: Configuración de la política de seguridad local de Windows

Introducción

En esta práctica de laboratorio, configurará la política de seguridad local de Windows. La política 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 política de seguridad local es un poco diferente, según la versión de Windows. Pero una vez abierto, las configuraciones son las mismas para los pasos restantes de esta práctica de laboratorio.

Instrucciones

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 políticas se deben configurar manualmente en cada computadora.

La política 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 Política 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.
- Al iniciar sesión, a los usuarios se les presentará el título y el texto que se indica a continuación:
  - Título: **Precaución:**
  - Texto: **Se supervisa su actividad. Esta computadora es solamente para uso comercial.**

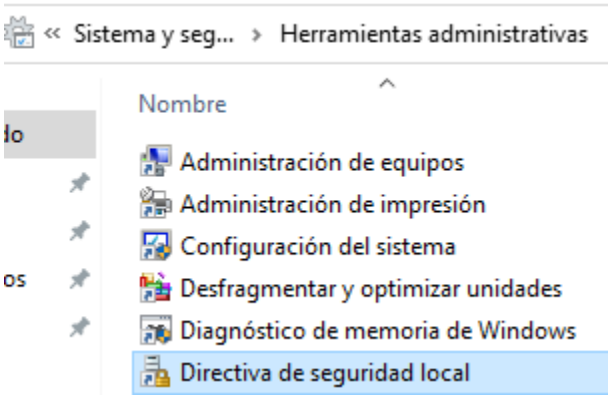
- Los usuarios recibirán un recordatorio para cambiar la contraseña 7 días antes de que expire.

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

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

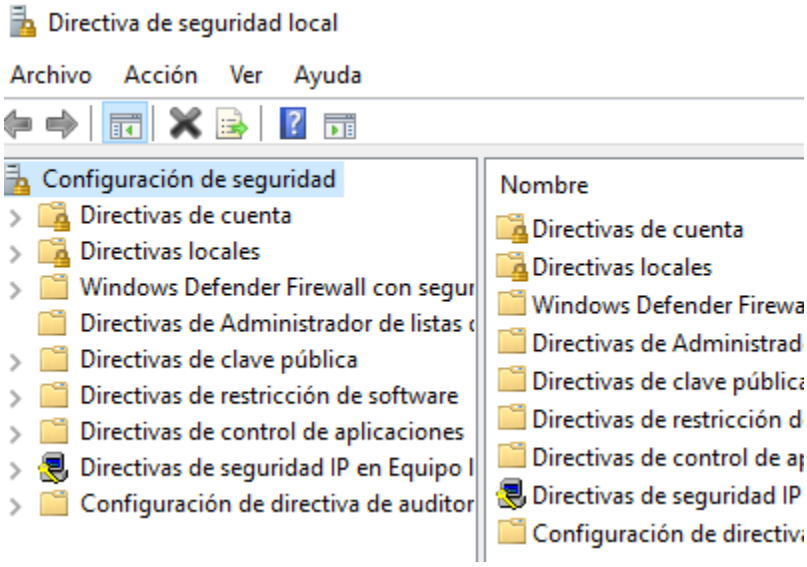
a. Para acceder a Política de seguridad local en Windows 10, puede utilizar las siguientes dos rutas de acceso:

Herramientas administrativas > Política de seguridad local



O **busque > secpol.msc** y luego haga clic en **secpol**.

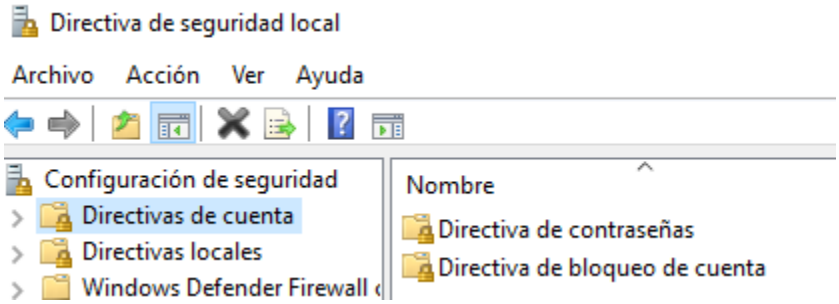
b. Se abre la ventana **Política de seguridad local**. Esta práctica de laboratorio se centra en las **Políticas de cuenta** y las **Políticas locales**, como se destaca en la figura a continuación. El resto de las opciones de **Configuración de seguridad** se encuentran fuera del alcance de este curso.



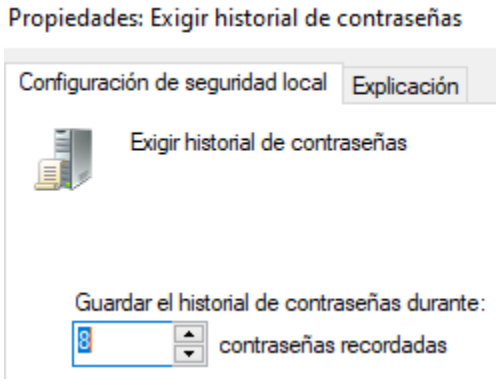
Paso 3: Configure la configuración de seguridad de la política de contraseñas.

Los primeros seis requisitos de la política de seguridad de la empresa se configuran en la sección **Políticas de cuenta** de la herramienta **Políticas de seguridad local**.

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



b. La primera política, **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 política 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**.



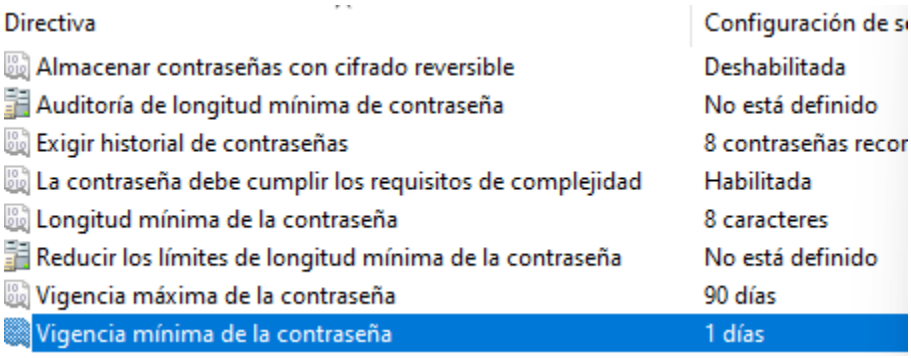
c. Mediante los requisitos de la política de seguridad del Paso 1, llene los valores que debe establecer en **Política de seguridad local** para las configuraciones de seguridad de **Política de contraseñas** restantes.

Política	Configuración de seguridad
Exigir el historial de contraseñas	8
Duración máxima de contraseña	*90*
Antigüedad mínima de contraseña	*1*
Longitud mínima de la contraseña	*8*
La contraseña debe cumplir con los requisitos de complejidad	*Habilitada*

Política	Configuración de seguridad
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 política 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 políticas y establezca los valores según las entradas en la tabla anterior.



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

a. De acuerdo con la política de seguridad en el paso 1, ¿cuántas veces se le permite a un usuario intentar iniciar sesión antes de que se le bloquee la cuenta?

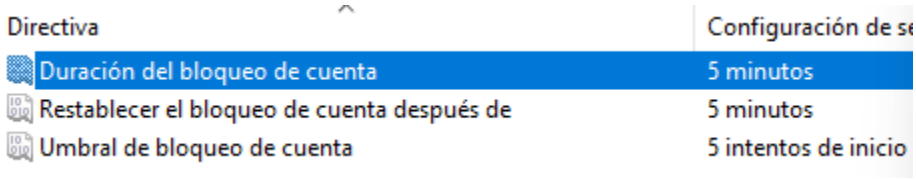
5 intentos.

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

5 minutos.

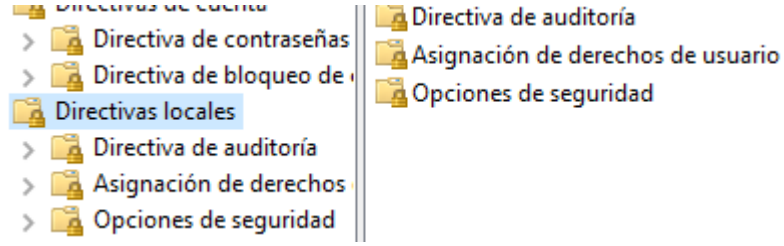
c. Utilice la configuración de seguridad **Política de bloqueo de cuentas** en **Política de seguridad local** para configurar los requisitos de las políticas.

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

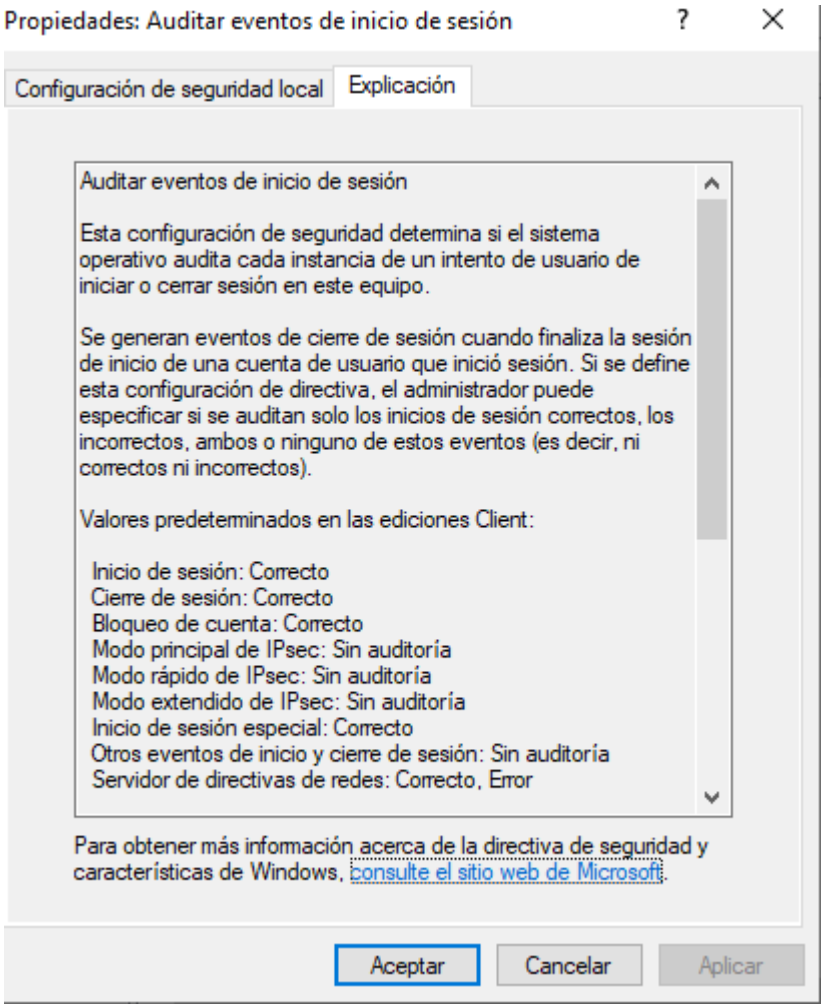


Paso 5: Configure la seguridad de la política de auditoría.

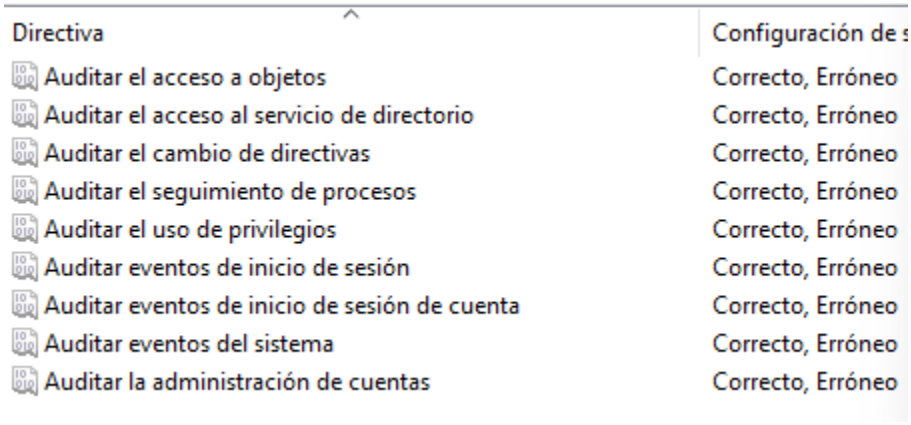
a. En Política de seguridad local, expanda el menú Políticas locales, y luego haga clic en Política de auditoría.



b. Haga doble clic en **Auditar eventos de inicio de sesión de cuenta** para abrir la ventana **Propiedades**. Haga clic en la pestaña **Explicar** para obtener sobre esta configuración de seguridad.



c. Haga clic en la pestaña **Configuración de seguridad local**, y luego en las casillas de verificación para **Correcto** y **Error**. Haga clic en **Aceptar** para cerrar la ventana **Propiedades** y aplicar las configuraciones de seguridad.



Directiva	Configuración de s
Auditar el acceso a objetos	Correcto, Erróneo
Auditar el acceso al servicio de directorio	Correcto, Erróneo
Auditar el cambio de directivas	Correcto, Erróneo
Auditar el seguimiento de procesos	Correcto, Erróneo
Auditar el uso de privilegios	Correcto, Erróneo
Auditar eventos de inicio de sesión	Correcto, Erróneo
Auditar eventos de inicio de sesión de cuenta	Correcto, Erróneo
Auditar eventos del sistema	Correcto, Erróneo
Auditar la administración de cuentas	Correcto, Erróneo

d. Continúe modificando el resto de las configuraciones de seguridad de **Política de auditoría**. Haga clic en la pestaña **Explicar** para cada uno y lea lo que hace. Haga clic en las casillas de verificación **Correcto** y **Error** en cada ventana de **Propiedades**.

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

a. En Política de seguridad local, haga clic en Asignación de derechos de usuario en Políticas locales para ver la configuración de seguridad.

b. Aunque ninguna de las configuraciones de seguridad debe modificarse para cumplir con los requisitos de la política de seguridad, pase cierto tiempo viendo las configuraciones predeterminadas.

Pregunta:

¿Hay alguna que usted recomendara cambiar? ¿Por qué?

Tener acceso a este equipo desde la red, yo pondría "administradores"

Según las condiciones cambiara el permiso de "invitado" en inicio local.

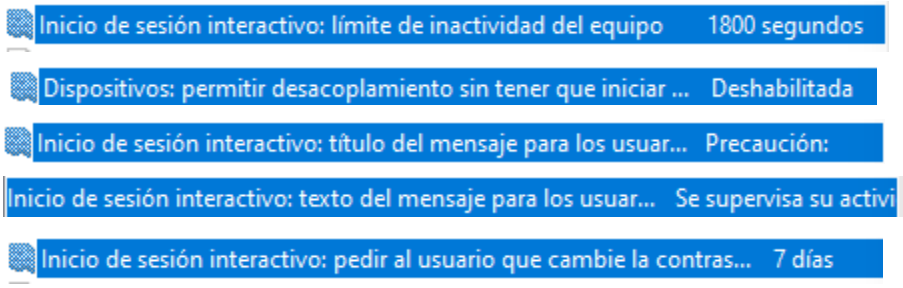
Lo contrario en "denegar inicio de sesión" según las condiciones claro.

c. En Política de seguridad local, haga clic en Opciones de seguridad en Políticas locales para ver la configuración de seguridad.

d. En cuanto a los requisitos restantes de la política de seguridad del paso 1, enumere los valores de las políticas 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 inactividad de la máquina	1800 segundos
Dispositivos: Permitir el desacoplamiento sin tener que iniciar sesión	Deshabilitada
Inicio de sesión interactivo: Título de mensajes para los usuarios que intenten iniciar sesión	Precaución

Política	Configuración de seguridad
Inicio de sesión interactivo: Mensaje de texto para los usuarios que intenten iniciar sesión	Se supervisa su actividad. Esta computadora es solamente para uso comercial.
Inicio de sesión interactivo: Se exige al usuario cambiar la contraseña antes del vencimiento	7 días



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

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

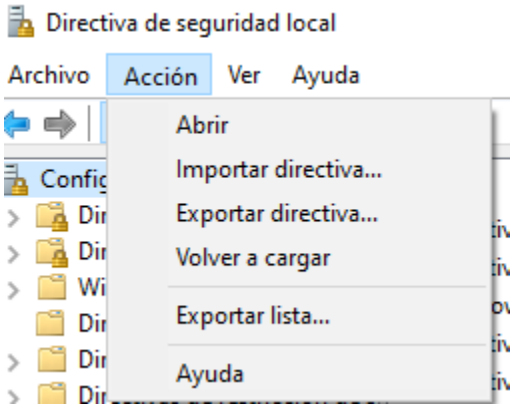
Panel de control > Cuentas de usuario > Realizar cambios en mi cuenta en Configuración de PC > Opciones de inicio de sesión, y luego, en **Contraseña**, haga clic en **Cambiar**.

Se le debe indicar con un mensaje que su nueva contraseña no cumple con los requisitos de políticas de contraseña.

Paso 8: Exportar e importar la configuración de las políticas de seguridad.

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

a. En la barra de menú en Políticas de seguridad local, haga clic en Acción > Exportar política…



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

c. Copie el archivo de política 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 **Política de seguridad local**, y haga clic en **Acción > Importar política…** Busque el archivo **.inf** en la unidad de memoria flash y ábralo para aplicar la política de seguridad a la nueva computadora.

