




Seguridad y Alta Disponibilidad



UNIDAD 3. **SEGURIDAD LÓGICA**



Contenidos

1. Principios de la Seguridad Lógica
2. Control de acceso lógico
 - 2.1. Política de contraseñas
 - 2.2. Control de acceso a la BIOS y gestor de arranque
 - 2.3. Control de acceso en el sistema operativo
3. Política de Usuarios y Grupos



1

PRINCIPIOS DE LA SEGURIDAD LÓGICA

Principios de la Seguridad Lógica

- **SEGURIDAD LÓGICA** = Aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo permita acceder a ellos a personas autorizadas para hacerlo.
- **Principales amenazas** : Acceso y modificaciones no autorizadas a datos y aplicaciones
- La seguridad lógica se basa en la efectiva administración de los permisos y el control de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos.
- **Principio de seguridad lógica :**

“Todo lo que no está permitido debe estar prohibido”

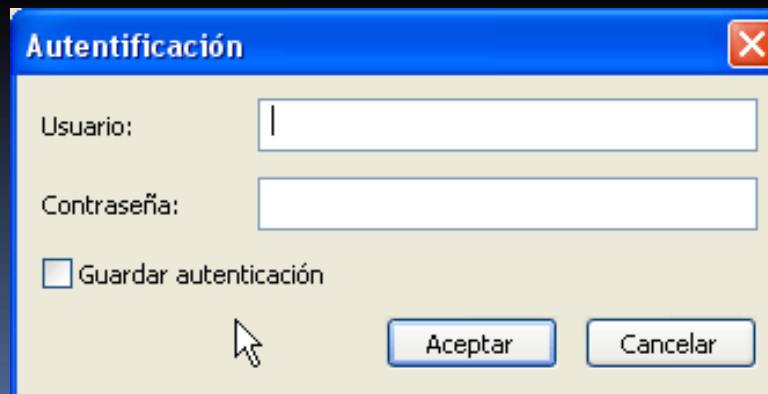


2

CONTROL DE ACCESO LÓGICO

Control de Acceso Lógico

- **Control de acceso lógico al sistema:** prevenir el ingreso de personas no autorizadas a la información del sistema.
- Controlar el acceso conlleva dos procesos:
 - **Identificación:** el usuario se da a conocer en el sistema.
 - **Autenticación:** verificación que realiza el sistema sobre esta identificación.



The image shows a standard Windows-style dialog box titled "Autenticación". It has a blue title bar with a red close button (X) in the top right corner. The main area has a light yellow background. It contains two text input fields: the first is labeled "Usuario:" and the second is labeled "Contraseña:". Below these fields is a checkbox labeled "Guardar autenticación" which is currently unchecked. At the bottom right, there are two buttons: "Aceptar" and "Cancelar". A mouse cursor is visible over the "Aceptar" button.

Control de Acceso Lógico

➤ Ataques más comunes a los sistemas de control de acceso protegidos por contraseñas:

■ Ataque de fuerza bruta:

- Averiguar la clave probando todas las combinaciones posibles
- Cuanto + corta la clave ➡ - combinaciones ➡ + sencillo descifrarla

■ Ataque de diccionario

- Conseguir la clave probando todas las palabras de un diccionario o un conjunto de palabras comunes.
- No se recomienda usar como clave una palabra del propio idioma porque sea fácil de recordar.

➤ Protección:

- Establecer un número máximo de intentos.
Ej: tarjetas SIM se bloquean tras 3 intentos fallidos al introducir el PIN
- Política de contraseñas.

Política de contraseñas

➤ Recomendaciones para que una contraseña sea segura:

- **Establecer una longitud mínima.** Cada carácter aumenta exponencialmente el grado de protección que ofrece la contraseña. *Mínimo recomendado: 8 caracteres. Ideal: 14 o más.*
- **Combinación de caracteres:** letras minúsculas y mayúsculas, números, símbolos especiales...

➤ Métodos:

- ✓ No utilizar secuencias ni caracteres repetidos. Ej: "1234" ó "1111".
- ✓ No utilizar el nombre de inicio de sesión.
- ✓ No utilizar palabras de diccionario de ningún idioma.
- ✓ Utilizar varias contraseñas para distintos entornos.
- ✓ Evitar la opción de contraseña en blanco.
- ✓ Cambiar la contraseña con regularidad.
- ✓ No revelar la contraseña a nadie ni escribirla en equipos que no controlas.

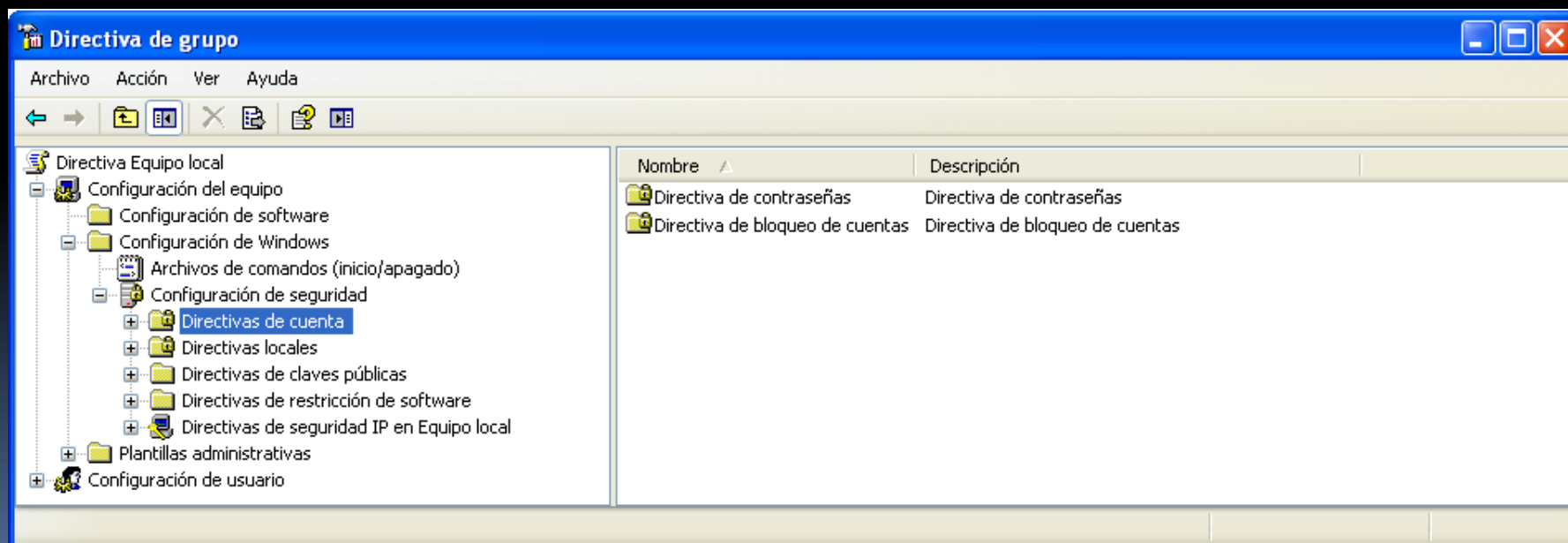


Configuración de contraseñas.

❑ Windows. Directivas de cuentas.

Comando `gpedit.msc`

- ✓ Directiva de contraseñas
- ✓ Directiva de bloqueo de cuentas



Directiva de grupo

Archivo Acción Ver Ayuda

← → ↗ ↖ ? ▶

Directiva Equipo local

- Configuración del equipo
 - Configuración de software
 - Configuración de Windows
 - Archivos de comandos (inicio/apagado)
 - Configuración de seguridad
 - Directivas de cuenta
 - Directiva de contraseñas**
 - Directiva de bloqueo de cuentas
 - Directivas locales
 - Directivas de claves públicas
 - Directivas de restricción de software
 - Directivas de seguridad IP en Equipo local
 - Plantillas administrativas
 - Configuración de usuario

Directiva	Configuración
Almacenar contraseña usando cifrado reversible para todos los usuarios del dominio	Deshabilitada
Forzar el historial de contraseñas	0 contraseñas
Las contraseñas deben cumplir los requerimientos de complejidad	Deshabilitada
Longitud mínima de la contraseña	0 caracteres
Vigencia máxima de la contraseña	42 días
Vigencia mínima de la contraseña	0 días

Directiva de grupo

Archivo Acción Ver Ayuda

← → ↗ ↖ ? ▶

Configuración del equipo

- Configuración de software
- Configuración de Windows
 - Archivos de comandos (inicio/apagado)
 - Configuración de seguridad
 - Directivas de cuenta
 - Directiva de contraseñas
 - Directiva de bloqueo de cuentas**
 - Directivas locales

Directiva	Configuración de seguridad
Duración del bloqueo de cuenta	No aplicable
Restablecer la cuenta de bloqueos después de	No aplicable
Umbral de bloqueos de la cuenta	0 intentos de inicio de sesión incorrectos

Configuración de contraseñas.

❑ **Linux. PAM** (*Pluggable Authentication Module*).

❖ Módulo **pam-cracklib**

- Determina si una contraseña que se va a crear o modificar con el comando ***passwd*** es suficientemente fuerte.
- Instalación: **\$ sudo apt-get install libpam-cracklib**
- Fichero de configuración del comando passwd: ***/etc/pam.d/common-password***

Líneas de configuración convencionales:

```
password required pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 minlen=8
password required pam_unix.so use_authok nullok md5
```

Diagram annotations:

- dcredit=-1**: dígitos
- ucredit=-1**: La contraseña debe contener mayúsculas
- lcredit=-1**: minúsculas
- minlen=8**: longitud mínima
- md5**: Encriptación MD5

❖ Fichero ***/var/log/auth.log***

Control de intentos de login en el sistema. Los intentos fallidos se registran en líneas con información del tipo *invalid password* o *authentication failure*.

Control de acceso mediante contraseñas

- Mecanismos de control de acceso a los sistemas mediante contraseña según distintos niveles:
 - ✓ **1º nivel:** control con contraseña del arranque y de su propia configuración de la BIOS.
 - ✓ **2º nivel:** control mediante contraseña del arranque y de la edición de opciones proporcionadas por los gestores de arranque.
 - ✓ **3º nivel:** control mediante usuario y contraseña por parte del sistema operativo. El SO permite el control de acceso a datos y aplicaciones mediante la configuración de privilegios a los distintos perfiles de usuario o individualmente a éstos.
 - ✓ **4º nivel:** contraseña y cifrado de acceso a datos y a aplicaciones, como archivos ofimáticos, comprimidos, sitios web (mail, banca online...), etc.

Peligros de distribuciones *Live*!

➤ Sistemas operativos en modo *Live*:

Arrancables desde unidades extraíbles (USB, CD o DVD) sin necesidad de formatear e instalarlos en el disco duro. Incluyen gran cantidad de aplicaciones de recuperación de datos y contraseñas de usuario.

➤ Ejemplos de distribuciones arrancables en modo *Live*:

- **Ultimate Boot CD (UBCD).** Contiene utilidades freeware para *Windows* para reparar, restaurar y diagnosticar varios problemas informáticos.
- **Backtrack.** Contiene herramientas de auditorías de seguridad, como *ophcrack* para *Windows* y *John the ripper* para *GNU/Linux*.
- **Ophcrack.** Contiene la aplicación del mismo nombre, para extraer contraseñas de usuarios en *Windows*.

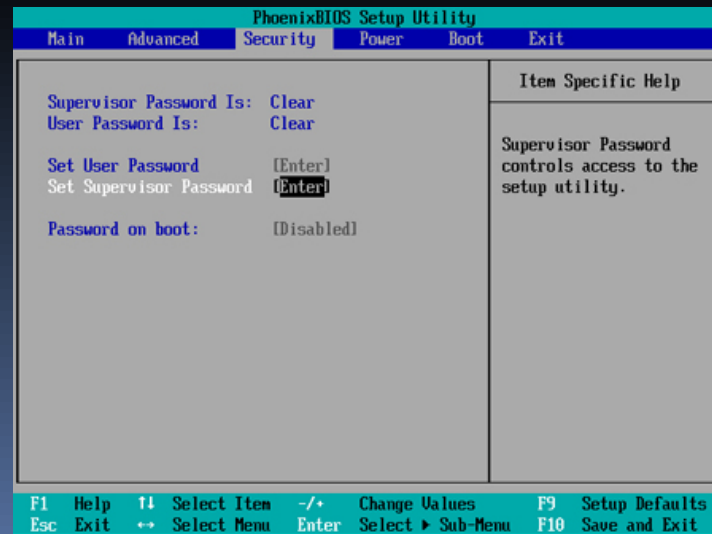
➤ Vulnerabilidades:

Desde estas distribuciones, en la mayoría de las ocasiones, es posible acceder a las particiones y sistemas de ficheros de forma transparente, sin restricciones del S.O., por lo que puede comprometer la seguridad de los datos y ficheros.

Control de acceso en la BIOS

➤ BIOS

- Pequeño programa que se encuentra grabado en una memoria de la placa base. Guarda la configuración de nuestro sistema.
- Reconoce y localiza todos los dispositivos necesarios para cargar el sistema operativo en la memoria RAM.
- Importante proteger la BIOS para que sólo un Administrador o un usuario responsable puedan cambiar los valores de configuración.



Control de acceso en la BIOS

➤ Vulnerabilidades de la BIOS :

1. Se puede resetear y volver a sus valores de fábrica (las contraseñas, por tanto, desaparecerán) quitando la pila o a través de la conexión del jumper *CLR_CMOS*.

Recomendación: **Protección de acceso físico a la placa base** (la forma más sencilla, con un candado que asegure la apertura de la torre y no permita el acceso a la placa base)

2. Se puede acceder y cambiar su configuración si no está protegida por contraseña.

Recomendación: **Solicitar contraseña cada vez que arranque la máquina (*setup*)**. Si no se introduce o se introduce incorrectamente, el sistema no arrancará.

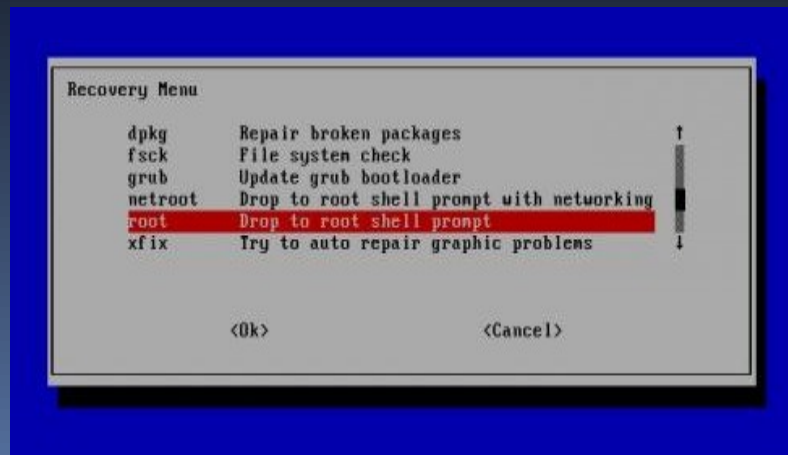
3. Distribuciones *Live*.

Recomendación: Establecer como **primer dispositivo de arranque el disco duro** donde se encuentran los SO (***system***) + contraseña BIOS

Control de acceso al Gestor de Arranque

➤ GRUB

- Gestor de arranque que permite seleccionar con qué sistema operativo arrancar cuando tenemos instalados varios sistemas en el disco duro.
- Opción **recovery mode** para la recuperación en caso de fallo del sistema. Puede modificar contraseñas o acceder a la información del disco duro.
- Recomendación: añadir **contraseña encriptada** al **menú de edición** (es decir, imposibilitar la edición por cualquier usuario no autorizado) y al **modo de recuperación**.



Control de acceso en el Sistema Operativo

➤ Métodos de acceso

- Más seguro: huella digital
- Más usado: login + password

➤ Vulnerabilidades

- Acceso mediante el modo de recuperación (*GNU/Linux*) o modo a prueba de fallos (*Windows*)
- Acceso a la cuenta de Administrador sin contraseña (en la instalación de *Windows XP* no se le asigna ninguna y por defecto suele estar vacía)
- Arrancar con una distribución *Live* para recuperar/borrar/modificar contraseñas.

➤ Recomendaciones

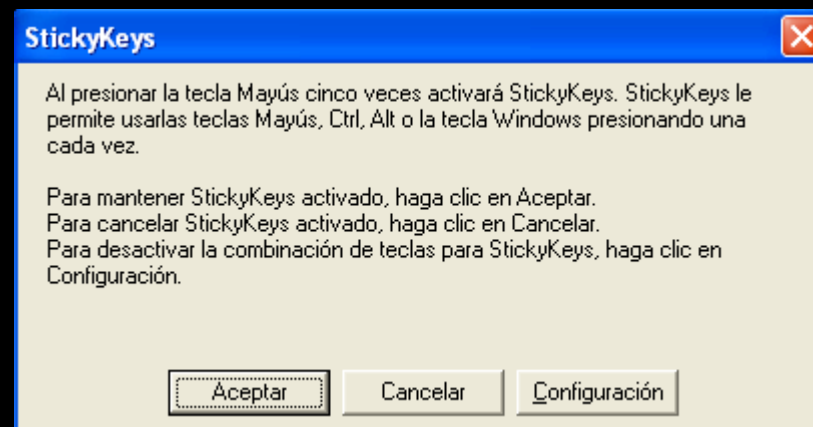
Uso de herramientas de auditoría de sistemas de acceso y nivel de fortaleza de contraseñas.

- **Ophcrack** (*Windows*)
- **John de the Ripper** (*GNU/Linux*)

Práctica. Modificación de contraseñas.

❑ Windows. Explotación del bug *sethc.exe & cmd.exe*

- **sethc.exe**: utilidad *StickyKeys* de ayuda y accesibilidad, que se activa pulsando la *SHIFT* (Mayúsculas) 5 veces seguidas.
- **cmd.exe**: consola de comandos.



Vulnerabilidad: consiste en sustituir el fichero *sethc.exe* por *cmd.exe* y así, cuando pulsemos la tecla SHIFT 5 veces seguidas, se nos abrirá el shell de comandos, desde el cual podemos ejecutar los comandos que queramos sobre el equipo.

La sustitución de los ficheros se puede realizar fácilmente desde una distribución Live con la partición de Windows montada.

```
ubuntu@ubuntu:/media/win/Windows/System32$ cp sethc.exe sethc_old.exe
ubuntu@ubuntu:/media/win/Windows/System32$ cp cmd.exe sethc.exe
```


```
C:\ C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>control userpasswords2
```

Cuentas de usuario


Usuarios

Opciones avanzadas

 Use la siguiente lista para conceder o denegar acceso de usuario a su equipo, así como para cambiar contraseñas y otras configuraciones.

☒ Los usuarios deben escribir su nombre y contraseña para usar el equipo.

Usuarios de este equipo:


Nombre de usuario	Grupo
 Administrador	Administradores

Agregar...

Quitar

Propiedades

Contraseña para Administrador

 Para cambiar la contraseña para Administrador, haga clic en Restablecer contraseña.

Restablecer contraseña...

Aceptar

Cancelar

Aplicar



Administrador

Restablecer contraseña

Contraseña nueva:

Confirmar contraseña nueva:

Aceptar

Cancelar



3

POLÍTICA DE USUARIOS Y GRUPOS

Política de usuarios y grupos

➤ Tareas del administrador

- Definir cuentas de usuario, asignarlas a perfiles determinados, grupos o roles.
- Asignar privilegios sobre los objetos del sistema.
- Determinar el nivel de seguridad de los datos y aplicaciones → clasificar la información, determinar el riesgo ante el acceso de usuarios no autorizados.



Control de acceso a datos y aplicaciones

➤ Permisos de acceso a cada objeto del sistema.

Gestión en red LDAP/ Active Directory.

- **Windows:** Directivas de seguridad local (Directiva de auditoría, asignación de derechos de usuario u Opciones de seguridad)
- **GNU/Linux:** **chmod** (modificar permisos), **chown** (cambiar propietario), **chgrp** (cambiar grupo) sobre archivos.

➤ Listas de control de acceso (ACL)

Permite asignar permisos a un usuario, sin tener en cuenta el grupo al que pertenece.

- **Windows:** **cacls**.
- **GNU/Linux:** **getfacl** (ver) y **setfacl** (modificar-asignar) información de permisos sobre un archivos.

Directiva de grupo

Archivo Acción Ver Ayuda

← → [Iconos]

Directiva Equipo local

- Configuración del equipo
 - Configuración de software
 - Configuración de Windows
 - Archivos de comandos (inicio/apagado)
 - Configuración de seguridad
 - Directivas de cuenta
 - Directivas locales
 - Directiva de auditoría
 - Asignación de derechos de usuario
 - Opciones de seguridad
 - Directivas de claves públicas
 - Directivas de restricción de software
 - Directivas de seguridad IP en Equipo local
 - Plantillas administrativas
- Configuración de usuario
 - Configuración de software
 - Configuración de Windows
 - Plantillas administrativas

Directiva	Configuración de s...
Acceso a redes: no permitir el almacenamiento de credenciales o .NET Passports para la autenticación del dominio	Deshabilitada
Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM	Habilitada
Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM	Deshabilitada
Acceso de red: deja los permisos de Todos para aplicarse a usuarios anónimos	Deshabilitada
Acceso de red: canalizaciones con nombre accesibles anónimamente	COMNAP,COMNOD...
Acceso de red: modelo de seguridad y para compartir para cuentas locales	Sólo invitado: usar...
Acceso de red: permitir traducción SID/nombre anónima	Deshabilitada
Acceso de red: recursos compartidos accesibles anónimamente	COMCFG,DFS\$
Acceso de red: rutas de registro accesibles remotamente	System\CurrentCon...
Apagado: borrar el archivo de páginas de la memoria virtual	Deshabilitada
Apagado: permitir apagar el sistema sin tener que iniciar sesión	Habilitada
Auditoría: apagar el sistema de inmediato si no puede registrar auditorías de seguridad	Deshabilitada
Auditoría: auditar el acceso de objetos globales del sistema	Deshabilitada
Auditoría: auditar el uso del privilegio de copia de seguridad y restauración	Deshabilitada
Cliente de redes de Microsoft: enviar contraseña no cifrada para conectar SMB de otros fabricantes	Deshabilitada
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitada
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Deshabilitada
Codificación de sistema: use algoritmos compatibles FIPS para codificación, algoritmos hash y firma	Deshabilitada
Console de recuperación: permitir el inicio de sesión administrativo automático	Deshabilitada
Console de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Deshabilitada
Controlador de dispositivos: permitir las combinaciones de contraseñas de cuentas de equipo	No está definido

Directiva de grupo

Archivo Acción Ver Ayuda

← → [Iconos]

Directiva Equipo local

- Configuración del equipo
 - Configuración de software
 - Configuración de Windows
 - Archivos de comandos (inicio/apagado)
 - Configuración de seguridad
 - Directivas de cuenta
 - Directivas locales
 - Directiva de auditoría
 - Asignación de derechos de usuario
 - Opciones de seguridad
 - Directivas de claves públicas
 - Directivas de restricción de software
 - Directivas de seguridad IP en Equipo local

Directiva	Configuración de s...
Auditar el acceso a objetos	Sin auditoría
Auditar el acceso del servicio de directorio	Sin auditoría
Auditar el cambio de directivas	Sin auditoría
Auditar el seguimiento de procesos	Sin auditoría
Auditar el uso de privilegios	Sin auditoría
Auditar la administración de cuentas	Sin auditoría
Auditar sucesos de inicio de sesión	Sin auditoría
Auditar sucesos de inicio de sesión de cuenta	Sin auditoría
Auditar sucesos del sistema	Sin auditoría