Directivas de seguridad y auditorías.

Caso práctico

La empresa que gestiona Carlos es absorbida por la empresa Coluro, y Carlos es nombrado Administrador de sistemas de toda la corporación. Es todo un reto, ya que la nueva empresa cuenta con sedes repartidas por todo el país.

Los cambios de empleados y la redistribución de subredes es lo que más le preocupa a Carlos, por lo que va a**auditar el sistema** para comprobar los **posibles fallos**. Se reunirá con su equipo, para proponer la implantación de un protocolo de seguridad ajustado a la nueva situación que garantice la **estabilidad y la integridad** de la información.

El establecimiento de unas **reglas** adecuadas en un sistema, es primordial para garantizar su buen funcionamiento. A través de las **directivas de seguridad**, no sólo se organizan los usuarios, grupos y recursos de un sistema, sino que también se proporciona **estabilidad** para que éstos puedan realizar sus cometidos sin preocuparse de aspectos inherentes a la seguridad.

Por otro lado, es necesario verificar que las reglas de juego aplicadas son válidas, y también que todos los participantes las cumplen. Mediante la **auditoría**se registran las actividades especificadas para supervisarlas posteriormente e identificar las cuestiones que merecen una investigación más profunda.

Directivas de seguridad.

Caso práctico

Bartolomé es el antiguo administrador de sistemas de Coluro. Carlos decide reunirse con él para investigar sobre la política de seguridad que estaba implantada en la empresa antes de la absorción.
Bartolomé le explica la distribución de usuarios y equipos en el dominio, así como las restricciones de seguridad que se esperaba para con cada uno de ellos.

Haciendo uso de esta información, Carlos se reúne de nuevo con su equipo y estudian las directivas de seguridad que habrá que actualizar y las que habrá que modificar e implantar para el sistema de la nueva empresa.

La **directiva de seguridad** rige el comportamiento del equipo en aspectos relacionados con la seguridad.

Puede ser de diversos tipos:

- **Directiva de seguridad local**: tiene como ámbito de aplicación el propio equipo, en modo local, influyendo a todos los usuarios que se identifiquen en él de este modo.
- **Directiva de seguridad de dominio**: tiene como ámbito de aplicación el dominio al que pertenece el equipo, influyendo a todos los usuarios que se conecten a él de este modo.

- **Directiva de seguridad del controlador de dominio**: tiene como ámbito de aplicación todos los equipos que actúen como controladores de dominio.

Aparte existen más directivas en función, como hemos visto, del ámbito en el que se aplican. Por ejemplo, directivas de sitios, de unidades organizativas, etc.

Cualquier directiva de seguridad deberá está vinculada a un objeto directiva de grupo.

Las directivas de grupo se tratan en el siguiente apartado.

Autoevaluación

¿Qué directivas se aplican en el caso de que un usuario X acceda en local a un equipo que pertenece a un dominio?

- Directivas de seguridad local.
- Directivas de seguridad de dominio.
- Directivas de seguridad del DC.
- Se aplicarían las directivas locales y las del dominio.

Directivas de grupo.

Caso práctico

Una vez que se ha establecido la **organización de usuarios y equipos** dentro del sistema, el equipo de administración procede a recopilar toda la información necesaria de los usuarios de la empresa así como de los equipos que manejan.

Toda esta información se estudia detalladamente y, de acuerdo con las directivas de seguridad establecidas, se diseña un **esquema de grupos** que permita la correcta aplicación del protocolo de seguridad.

Con los grupos ya creados, sólo falta definir qué directivas se aplicarán a cada uno de ellos y cómo afectará la**organización del sistema** a la **herencia** y al **bloqueo** de éstas.

Tras definir las directivas de grupo necesarias, se aplican y se comprueba si el efecto producido es el esperado.

Los (GPO) establecen el comportamiento del equipo y del usuario. Cada GPO afecta a la cuenta de usuario, de grupo y de equipo. Una vez que son creados se vinculan a sitios, dominios o UOs, de forma que los usuarios y los equipos que se encuentran en estos contenedores reciben los parámetros de configuración establecidos por cada una de los GPO.

Dentro del GPO **las directivas se organizan jerárquicamente**. El árbol del GPO se vertebra en dos ramas:

- **Configuración del equipo**: Contiene todos los parámetros que se aplican al iniciar el equipo, sin importar qué usuario lo hace.
- **Configuración de usuario**: Contiene todos los parámetros que se aplican al usuario que inicia sesión, sin importar en qué equipo lo hace.

Además de la aplicación inicial del GPO, sus directivas se pueden evaluar de forma periódica o bajo demanda, cuando el administrador lo estime oportuno.

El administrador tiene la **potestad de habilitar o deshabilitar** de forma selectiva partes de una GPO, ya se trate de la configuración de equipo o de usuario. Esto es muy útil cuando se quiere personalizar el acceso a un usuario o a un equipo dentro del sistema sin afectar al resto de miembros.

Las directivas se aplican siguiendo el siguiente orden:

1. Directivas de equipo local.
2. Directivas de usuario local.
3. Directivas de grupo del sitio.
4. Directivas de grupo del dominio.
5. Directivas de grupo de la unidad organizativa.
6. Directivas de grupo del controlador de dominio.

Las directivas de grupo se gestionan a través de la herramienta **Administración de directivas de grupo**, disponible en la opción **Herramientas administrativas** de Windows o a través de la orden **gpedit.msc**.

Por defecto, Windows Server 2008 proporciona dos directivas:

- **Default Domain Policy** (Política de dominio por defecto): se aplica a todos los equipos del dominio y afecta a ambas configuraciones (de equipo y de usuario).
- **Default Controller Domain Policy** (Política de controlador de dominio por defecto): se aplica a todos los equipos que sean DC, afectando también a ambas configuraciones.

Directivas en Windows Server 2008.

Cuando se ha creado un GPO con la configuración deseada, se puede aplicar directamente a los contenedores que se desee, o bien se puede reconfigurar desde la propia **herramienta de Administración de directivas de grupo.**

Principalmente se pueden llevar a cabo las siguientes operaciones:

- **Cambiar el orden de aplicación de las directivas** (respecto del orden de aplicación por defecto).
- **Forzar la aplicación de una directiva**, en el caso de que existan otras que la anulen por el orden jerárquico.
- **Bloquear la herencia de directivas**, impidiendo que un contenedor reciba por defecto la configuración del contenedor padre.
- **Modificar los permisos de una directiva** o sus propiedades.

Para saber más

En el siguiente documento tienes más información sobre las directivas de Windows Server 2008.

Planificación e implementación de directivas de grupo.

Autoevaluación

¿Cuál de las siguientes operaciones sobre directivas no se puede realizar en Windows Server 2008?

- Cambiar la configuración de un GPO por otra totalmente distinta.
- Establecer un orden de aplicación de los GPO diferente al ordinario.
- Aplicar un GPO a equipos que se encuentran fuera de su alcance.
- Evitar que un contenedor herede el GPO de quien lo contiene.

Vincular un GPO.

Aunque puede crearse un GPO sin vínculo a ningún nodo, la realidad es que un GPO se crea con la finalidad de ser aplicado a otros objetos.

Vincular un GPO consiste en aplicar las directivas que contiene a todos los objetos del contenedor al que se asocia.

El vínculo de un GPO con un contenedor:

- **No es único**: puede vincularse un GPO a diferentes contenedores.
- **No es permanente**: en cualquier momento puede eliminarse el vínculo con el contenedor.

Los vínculos de un GPO pueden establecerse de las siguientes formas:

- **De forma automática**, seleccionando la opción **Crear un GPO en este contenedor y vincularlo aquí,**disponible en la herramienta de Administración de directivas de grupo. En esa opción, el contenedor será sustituido por el contenedor que hayamos seleccionado previamente (dominio, UO, etc.).
- **De forma manual**, creando por un lado el GPO y por otro el contenedor al que se va a vincular. Se hará uso de la opción **Vincular un GPO existente,** que aparece al seleccionar el contenedor deseado en la herramienta de Administración de directivas de grupo.

Debes conocer

Para conocer con más detalle el proceso de creación, eliminación y vinculación de un GPO:

Crear y vincular GPOs.

Autoevaluación

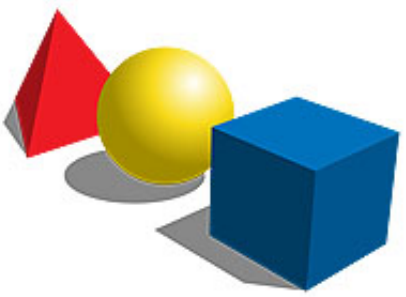
¿Cuáles de las siguientes afirmaciones sobre vínculos de GPO son correctas?

- [ ] El vínculo de un GPO con un contenedor es único y permanente.
- [ ] Se puede crear un GPO por un lado, un contenedor por otro y posteriormente vincularlos.
- [ ] Se puede crear un GPO sólo cuando el contenedor al que se prevé a vincular ya exista.
- [ ] Se puede crear un vínculo de un GPO al contenedor en el mismo momento que se crea el GPO.

Mostrar Información

Configuraciones interesantes de un GPO.

Dentro de todas las configuraciones posibles sobre un GPO destacamos, por su interés, las siguientes:



- **Scripts**: el script es un conjunto de órdenes que se ejecuta de forma automática cuando el usuario accede a un equipo o cuando el equipo se inicia o se apaga. Los scripts se pueden almacenar en archivos de lotes (BAT) o en archivos de comandos (VBS y JS principalmente). La asignación del script al GPO se hace a través de la opción **Configuración de Windows** del equipo o usuario del GPO.
- **Redireccionamiento de carpetas**: se pueden redirigir carpetas especiales de los usuarios (ubicadas en Usuarios), a una ubicación de red en el servidor, de forma que los usuarios puedan trabajar con su contenido independientemente del equipo desde el que inicien sesión. Esta operación se hace a través de la opción**Configuración de Windows** del equipo o usuario del GPO.
- **Plantillas administrativas**: Se utilizan para administrar la configuración de parte del Registro del sistema. A través de las diferentes opciones de Plantillas administrativas se pueden gestionar:
  - **Directivas de Windows**, que controlan diferentes características de Windows, mediante la opción**Componentes de Windows**.
  - **Directivas del Panel de control**, mediante la opción **Panel de control**.
  - **Directivas del sistema**, mediante la opción **Sistema**
  - **Directivas de contraseñas**, mediante la opción **Directiva de contraseñas**, integrada en **Directiva de cuentas**.
  - **Directivas de bloqueo de cuentas**, mediante la opción **Directiva de bloqueo de cuentas**, integrada en **Directiva de cuentas**.
  - **Directivas del GPO**, mediante la opción **Directiva de grupo**, integrada en **Sistema**.

Debes conocer

Para conocer el procedimiento detallado de algunas de las configuraciones propuestas, puedes consultar estos documentos:

Creación de scripts.

Redireccionamiento de carpetas.

Aplicar o modificar la directiva de bloqueo de cuentas.

Autoevaluación

Se pueden redirigir carpetas a ubicaciones diferentes, según el usuario pertenezca a un grupo u otro.

- Verdadero.
- Falso.

Trabajar con directivas.

Ya sabemos cómo vincular y modificar GPOs. La estructura de directivas se basa, por defecto, en dos

principios:

- Los GPOs vinculados a un contenedor se propagan por todos los contenedores que éste tenga. Esto se conoce como**herencia**.
- La aplicación de GPOs sigue el orden de prioridades **local** → **sitio** → **dominio** → **UO** → **DC**.

Tal y como adelantamos anteriormente, existen mecanismos para flexibilizar la aplicación de estos principios a través de la herramienta de **Administración de directivas de grupo**:

- **Variar el orden de aplicación de directivas.**
  Para cambiar el orden de los vínculos simplemente hay que desplazarlos hacia arriba o abajo en la lista, teniendo en cuenta que el vínculo con mayor prioridad es el que está en la parte más alta.

- **Bloquear la herencia de directivas de grupo.**
  El bloqueo de herencia impide que los GPOs vinculados a contenedores principales se propaguen a los secundarios.

Debes conocer

Para conocer el procedimiento detallado de bloqueo de herencia, consulta esta información:

Bloquear la herencia de GPO.

- **Forzar un vínculo de GPO.**
  Al forzar un vínculo de GPO, este siempre tiene prioridad sobre el resto de los vínculos de GPO de los objetos secundarios. Un GPO nunca se fuerza de forma predeterminada.

Debes conocer

Para conocer el procedimiento detallado de forzado de vínculo, consulta esta información:

Forzar un vínculo de GPO.

- **Deshabilitar un vínculo de GPO**.
  Se puede impedir la ejecución de un vínculo de GPO para un sitio, un dominio o una UO determinados deshabilitándolo. Esta operación no deshabilita el GPO, sino el vínculo.

Debes conocer

Para conocer el procedimiento detallado de cómo deshabilitar un vínculo de GPO, consulta esta información:

Deshabilitar un vínculo de GPO.

GPO de inicio.

Un **GPO de inicio** es una colección de valores de la **directiva Plantilla administrativa**, (de usuario y de equipo), en un único objeto que se utiliza como base para posteriores GPOs.

Todas las GPO de inicio están almacenadas en la carpeta **StarterGPOs**, ubicada en la carpeta compartida **sysvol**. Si no hay ninguna GPO de inicio, esta carpeta no existirá y se pedirá que se cree cuando se genere la primera GPO de inicio.

Debes conocer

Para conocer detalladamente cómo crear, modificar y eliminar un GPO de inicio consulta esta documentación:

Crear y editar un GPO de inicio.

Eliminar un GPO de inicio.

Una de las opciones más interesantes de los GPO de inicio es la posibilidad de **importarlos y exportarlos**, ya que se facilita enormemente su distribución y uso compartido con otros entornos.

Debes conocer

Aquí tienes información sobre el proceso de importación y exportación de un GPO de inicio:

Importar y exportar un GPO de inicio.

La versatilidad del GPO de inicio permite al administrador **generar nuevos GPOs a partir de un GPO de inicio**, los cuales personalizará y vinculará a un contenedor.

La creación de un nuevo GPO a partir de un GPO de inicio se puede llevar a cabo de dos formas:

- **Generando el GPO en el nodo del GPO de inicio**, en cuyo caso el proceso lo realizaríamos desde el propio GPO de inicio.
- **Generando el GPO en su nodo**, de forma que al crearlo seleccionaríamos el GPO de inicio de origen.

Debes conocer

En este documento se explican los dos mecanismos de creación de un GPO a partir de un GPO de inicio:

Crear un GPO a partir de un GPO de inicio.

Autoevaluación

Señala las operaciones que pueden realizarse sobre GPOs de inicio.

- [ ] Crear un GPO de inicio.
- [ ] Eliminar un GPO de inicio.
- [ ] Exportar un GPO de inicio.
- [ ] Generar un GPO a partir de un GPO de inicio.

Mostrar Información

Filtro WMI.

Se pueden dar casos en los que las directivas no sean efectivas si se aplican a todo el contenedor. Por ejemplo, si unos equipos tienen una versión de sistema operativo distinta de otros. En estos casos es conveniente hacer uso de los filtros WMIdentro del GPO.

WMI permite interactuar con el equipo al que se aplica el GPO y, dependiendo del filtro, decidirá si se aplica la directiva o no. Es decir, el filtro permite especificar los criterios que deben cumplirse para que se aplique el GPO sin necesidad de redistribuir los contenedores. Esos criterios reciben el nombre de **consultas**.

Todos los filtros WMI quedan almacenados y disponibles para poder ser utilizados desde los GPOs. Se guardan a nivel de dominio, de forma que el GPO y el filtro WMI vinculado deben pertenecer al mismo dominio.

Cada GPO sólo puede tener un filtro WMI asociado, pero el filtro puede tener varias consultas. Asimismo, un mismo filtro puede ser utilizado por diferentes GPOs.

Los filtros WMI se crean desde la propia herramienta de **Administración de directivas de grupo**, bajo la opción de **Filtros WMI**. También se pueden eliminar, vincular, copiar, pegar, importar, etc.

El filtrado WMI sólo es efectivo a partir de Windows XP, es decir, los equipos con versiones de Windows anteriores a XP no interpretan los filtros por lo que no producirán el efecto esperado.

Para saber más

La creación de filtros WMI es una labor un tanto tediosa por la complejidad de las consultas. En el siguiente enlace puedes encontrar algunos ejemplos de consultas a aplicar:

Filtros WMI.

Autoevaluación

¿Cuál de las siguientes afirmaciones acerca de filtros WMI es correcta?

- Un GPO puede tener uno o más filtros WMI vinculados.
- Un filtro WMI puede vincularse a uno o más GPO.
- Un filtro WMI se compone de una única consulta.
- Es posible vincular un filtro WMI del dominio A con un GPO del dominio B.

Directiva de bucle invertido.

La **configuración de usuario**, por defecto, se rige por los GPO vinculados al objeto usuario. Así, un usuario puede iniciar sesión en cualquier equipo de la misma manera.

En ocasiones este comportamiento puede no ser deseable; es decir, se busca que un usuario se configure de forma diferente dependiendo del equipo que utilice. Aquí es donde entra a jugar el procesamiento de bucle invertido.

La directiva de bucle invertido altera el orden de ejecución de los GPO, haciendo que la configuración de usuario no esté determinada por las directivas de los GPO vinculados al usuario sino por las de los GPO vinculados al equipo.

Esta directiva se encuentra en la ruta **Configuración del equipo → Directivas → Plantillas administrativas → Sistema → Directiva de grupo** de la herramienta de **Administración de directivas de grupo**. Cuando el bucle está habilitado puede adoptar dos modos:

- **Sustitución**: la lista de GPO para el usuario se reemplaza por completo por la lista de GPO que se obtuvo para el equipo cuando se encendió.
  Este modo es el ideal cuando se persigue que los usuarios reciban una configuración estándar en vez de la configuración habitual para ellos. Por ejemplo, un alumno en un aula temática (se fuerza a que tenga unas determinadas opciones).

- **Combinación**: La lista de los GPO que se obtiene para el equipo al encenderse se adjunta a la lista de los GPO obtenidos para el usuario cuando inicia sesión. En caso de conflicto prevalecen las directivas de equipo.
  Este modo es el ideal cuando se persigue que los usuarios conserven su configuración típica a la par que reciben ciertos parámetros de configuración “obligatorios”. Por ejemplo, un usuario que accede a una sala de conferencias a dar una charla, mantiene su configuración pero se reemplaza, por ejemplo, el fondo de escritorio o se le deshabilitan ciertas aplicaciones.

Autoevaluación

Todos los usuarios del grupo Comercial no tienen acceso a Internet. ¿Qué medida adoptaré si quiero que estos usuarios puedan acceder a Internet en los ordenadores de la cafetería manteniendo el resto de sus funcionalidades?

- Habrá que crear un grupo Cafetería y meter ahí a todos los usuarios.
- Aplicaré un bucle invertido de sustitución.

- Aplicaré un bucle invertido de combinación.
- No se puede hacer nada porque siempre prevalece la directiva más restrictiva.

Modelado y resultados de GPO.

Hemos estudiado la vinculación de GPO y la aplicación de filtros WMI como herramientas para administrar la seguridad de los diferentes elementos del sistema. La implantación de directivas siempre se hace a partir de una planificación, en la que se tiene en cuenta el impacto teórico de toda la política de grupos adoptada.

Sin embargo, en ocasiones los efectos generados no son los deseados y es posible que pueda incluso inutilizar usuarios y/o equipos del sistema. Para evitarlo existe la posibilidad de simular la implementación de directivas antes de su implantación a través de un proceso conocido como **modelado de GPO**

El modelado de GPO se lleva a cabo a través del Asistente para modelado de directivas de grupo, disponible a través de la herramienta de **Administración de directivas de grupo**.

Sólo es posible ejecutar un modelado de GPO sobre un equipo Windows Server que sea controlador de dominio.

El asistente necesita saber, al menos, el controlador de dominio sobre el que ejecutará el modelado y con qué usuario y equipo se va a simular. Se pueden proporcionar más datos como el grupo al que pertenece el usuario o incluso los filtros WMI que se le van a aplicar.

Como resultado de la simulación, se obtiene un **resumen** que muestra qué directivas se han aplicado y cuál era su configuración.

La simulación generada queda registrada en el nodo de Modelado de GPO y puede eliminarse, modificarse (creando otro modelado a partir de este) o volver a ejecutarse en otro momento.

Cuando las directivas son vigentes y se quiere obtener información sobre ellas, especialmente cuando no se consigue un efecto deseado, se puede hacer uso de **Resultados de GPO**, disponible a través de la herramienta de **Administración de directivas de grupo**.

El Asistente para resultados de GPO es muy similar al utilizado en el caso del modelado y proporciona prácticamente los mismos resultados que el modelado.

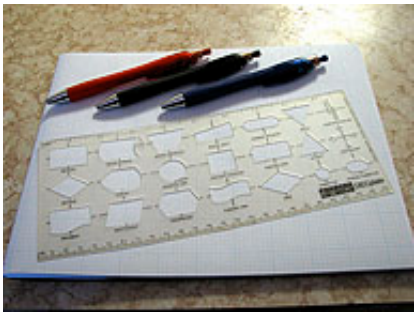
La opción Modelado de GPO se utiliza para observar el efecto de las directivas antes de su implantación.
La opción Resultados de GPO se utiliza para observar el efecto de las directivas ya implantadas.

Autoevaluación

Si quiero comprobar cómo afectaría un GPO a un usuario del dominio que trabaja en un equipo bajo Windows 7 utilizaría…

- Usaré Modelado de GPO y estudiaré el resumen obtenido.
- Usaré Resultado de GPO y estudiaré el resumen obtenido.
- Puedo utilizar Modelado de GPO o Resultados de GPO indistintamente ya que los resúmenes son similares.
- No es posible utilizar ninguna de las herramientas mencionadas por que el equipo no es Windows Server.

El complemento Plantillas de seguridad.



El **complemento Plantillas de seguridad** permite definir y modificar plantillas de seguridad personalizadas, tomando como punto de partida una plantilla vacía o una plantilla predefinida por el sistema (Windows Server).

Este complemento pertenece a la **Consola de Administración de Microsoft (MMC)** y hay que agregarlo a ésta para poder trabajar con él. Recuerda que para acceder a esta consola se ejecuta la orden **mmc**.

Una plantilla de seguridad es un archivo de texto que representa una configuración de seguridad. Puede aplicarse a un equipo local o incluso integrarse en un GPO.

La plantilla de seguridad se puede:

- **Crear desde cero.**
- **Crear a partir de una plantilla predefinida** incluida en Windows Server.
- **Crear a partir de modificaciones en otra plantilla** de seguridad.

A través de la plantilla de seguridad pueden definirse los siguientes componentes:

- **Directivas de cuenta.**
  - Directiva de contraseñas.
  - Directiva de bloqueo de cuenta.
  - Directiva Kerberos.
- **Directivas locales.**
  - Directiva de auditoría.
  - Asignación de derechos de usuario.
  - Opciones de seguridad.
- **Registro de sucesos:** configuración de registro de sucesos de aplicación, sistema y seguridad.
- **Grupos restringidos:** pertenencia a grupos de seguridad.
- **Servicios del sistema:** modos de inicio y permisos para servicios del sistema.
- **Del registro:** permisos de claves de registro.
- **Sistema de archivos:** permisos de archivos y carpetas.

Debes conocer

A continuación tienes información detallada sobre el proceso de creación de plantillas de seguridad:

Plantillas de seguridad.

El complemento Configuración y análisis de seguridad.

El **complemento Configuración y análisis de seguridad** también pertenece a la Consola de Administración de Microsoft, y se utiliza para configurar el equipo y analizar su seguridad de forma local.

Para ejecutar este complemento **es necesario** disponer de:

- **Una base de datos.**
- **Una plantilla de seguridad.**

El proceso de configuración y análisis de seguridad es muy sencillo:

- Se analiza el sistema contra una plantilla de seguridad determinada. El resultado de este análisis se almacena en una base de datos de configuración de seguridad.
- Posteriormente se analiza el sistema.

- Al final se contrastan los resultados obtenidos con los proporcionados con la base de datos. En definitiva, se obtiene el contraste entre las dos situaciones.

El análisis de seguridad puede identificar agujeros de seguridad en la configuración actual y también qué cambios produciría una determinada plantilla si se aplicara al equipo.

Como se ha dicho, **el análisis se realiza a nivel local**, pero es posible contrastar la configuración de seguridad local con la configuración de GPO, si se descarga la base de datos del dominio. En concreto, la base de datos se ubica en la ruta **Windows\Security\Database** bajo el nombre de **Secedit.sdb**.

Los resultados del contraste se observan para cada objeto, detallando las configuraciones de la base de datos y la del sistema:

- Un indicador **rojo** señala que existe diferencia en ese elemento entre base de datos y sistema.
- Un indicador **verde** señala que hay coherencia en ese elemento entre base de datos y sistema.
- Si **no hay indicador** significa que esa configuración no estaba especificada en la base de datos.

Para saber más

En el siguiente enlace puedes encontrar información sobre cómo utilizar Secedit.sdb para un análisis de seguridad:

Análisis de seguridad con Secedit.sdb.

Autoevaluación

¿En cuál de las siguientes situaciones podría utilizar el complemento de Configuración y análisis de seguridad?

- Para analizar el impacto de una plantilla de seguridad en el dominio.
- Para analizar si una determinada plantilla es efectiva en un equipo a nivel local.
- Para identificar agujeros de seguridad en todos los equipos del sitio.
- Para comprobar si la base de datos Secedit.sdb está actualizada.

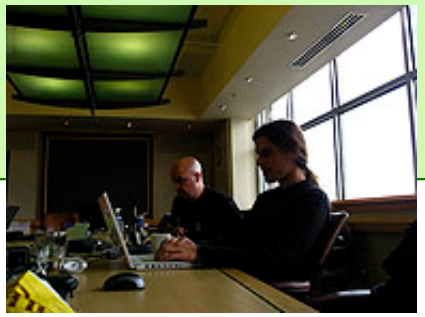
Auditorías.

Caso práctico

Ya ha pasado un tiempo y parece que el **sistema de Coluro se ha estabilizado**. Durante el periodo de adaptación el equipo de administración del sistema ha estado adaptando el estado de los equipos y de los usuarios a las nuevas condiciones.

En una de las reuniones semanales que Carlos, como jefe del equipo de administración, mantiene con el resto de directivos de la empresa, se le plantean algunos problemas que los usuarios de diferentes departamentos están teniendo en su desempeño diario.

Carlos toma nota y se reúne con su equipo. Es posible que haya algún que otro desajuste en la



configuración que se ha establecido, pero también es posible que se estén produciendo **accesos indebidos**, o incluso**ataques a la red**. Para analizar la situación y tomar medidas se propone la realización de una **auditoría del sistema**.

La auditoría es un componente importante en la seguridad del sistema.

La auditoría supervisa eventos relacionados con la seguridad del sistema.

Puede registrar sucesos correctos para proporcionar documentación de modificaciones y también, y esto es lo más importante, puede registrar accesos potencialmente peligrosos a los recursos del entorno, ya sean intencionados o no.

La auditoría implica el uso de hasta tres herramientas de administración:

- La **directiva** de auditoría.
- La **configuración** de auditoría de los objetos.
- El **registro** de seguridad.

El procedimiento típico en una auditoría es:

1. **Establecer la configuración específica de la auditoría.**
   A. Seleccionar los sucesos que se auditarán. Los sucesos más comunes son:
      - El acceso a objetos, como pueden ser archivos y carpetas.
      - La administración de cuentas de usuarios y de grupos.
      - El inicio y fin de sesión de los usuarios.
   B. Definir el tamaño y la configuración del registro de seguridad.
   C. Determinar a qué objetos se desea controlar el acceso.
2. **Permitir la directiva de auditoria.**
3. **Evaluar los eventos en el registro de seguridad.**

Directiva de auditoría.

La directiva de auditoría prepara el sistema para ser inspeccionado en las categorías de suceso que se determinen. **Si una directiva de auditoría no está permitida, se omitirá.**

Tras la instalación de Windows Server se activan de forma predeterminada varias categorías de auditoría:

- De acceso a objetos (archivos, impresoras, etc.).
- De acceso al servicio de directorio (objetos del AD que tienen SACL definidas).
- De cambio de directivas.
- De cambio de contraseña.
- De seguimiento de procesos (accesos a programas y procesos).
- De uso de privilegios (cambios de permisos).
- De administración de cuentas (modificación de cuentas).
- De sucesos al inicio de sesión (de los servicios).
- De sucesos al inicio de sesión de cuenta (de los usuarios).
- De los sucesos del sistema (apagado, reiniciado,…).

Los valores posibles a la hora de configurar una directiva de auditoría son:

- **Correcto**: se registrarán todos los sucesos correctos correspondientes a la directiva.
- **Error**: se registrarán todos los sucesos erróneos correspondientes a la directiva.
- **Sin auditoría**: la directiva no está activada.

Para saber más

En el siguiente enlace tienes información más detallada sobre cada uno de los procesos de auditoría mencionados anteriormente:

Directiva de auditoría.

Autoevaluación

¿Qué debería hacer para averiguar si hay usuarios que están intentando cambiar la hora del equipo sin tener permisos?

- Lanzar una auditoría de cambio de directivas con valor "Error".
- Lanzar una auditoría de acceso a objetos con valor "Error".
- Lanzar una auditoría de uso de privilegios con valor "Error".
- Lanzar una auditoría de acceso a objetos con valor "Correcto".

Auditoría del acceso a objetos.

Cada objeto tiene asociado un bloque de información de seguridad llamado **descriptor de seguridad**. Este descriptor se divide esencialmente en dos partes:

- **Lista de control de acceso discrecional (DACL),** que contiene información sobre qué usuarios y grupos tienen acceso a un objeto junto con los permisos sobre éste.
- **Lista de control de acceso al sistema (SACL),** que contiene información de los sucesos que se van a auditar:
  - Los usuarios o grupos que se auditan al acceder al objeto.
  - Los sucesos que se auditan en el acceso.
  - La bandera que indica si se auditan aciertos, errores o ambas cosas.

La auditoría de acceso a objetos se establece desde la directiva de grupo correspondiente.

Las auditorías de acceso a objetos deben programarse con cautela, ya que existen muchas acciones ordinarias que provocan un número considerable de accesos a objetos, (como archivos con permisos, antivirus, etc.). El elevado número de eventos a grabar puede afectar notablemente al rendimiento del servidor o del recurso y, en definitiva, puede crearnos problemas de inestabilidad en el sistema.

Debes conocer

En el siguiente artículo se explica de forma detallada cómo auditar el acceso a objetos:

Auditar el acceso a objetos.

Autoevaluación

Señala las afirmaciones correctas:

- [ ] La SACL contiene información sobre qué usuarios se van a auditar.
- [ ] La DACL contiene información sobre los usuarios que tienen acceso a un objeto.
- [ ] Se pueden auditar aciertos o errores, pero no ambas cosas simultáneamente.
- [ ] La auditoría de acceso a un objeto se establece desde su propia GPO.

Mostrar Información

Auditoría del acceso a archivos y carpetas.

La auditoría del acceso a archivos y carpetas ofrece información sobre el uso que se está haciendo de los recursos y los problemas de seguridad potenciales.

Se puede auditar el acceso a archivos y carpetas en volúmenes NTFS.

Siguiendo el procedimiento ordinario de auditoría, habrá que especificar qué archivos y carpetas se van a auditar, los sucesos y los usuarios/grupos para los que estará dirigida. Además, habrá que habilitar la directiva Auditar el acceso a objetos, (y Auditar el acceso del servicio de directorio, en el caso de un controlador de dominio).

La configuración de auditoría de acceso a un archivo o carpeta, se hace directamente sobre él, agregando los sucesos a auditar y los usuarios/grupos objetivo en la pestaña **Auditoría**, a la que se llega tras la secuencia: **menú contextual → Propiedades → Seguridad → Opciones avanzadas → Auditoría.**

Tras seleccionar los usuarios/grupos objetivo se pide especificar:

- **A qué se aplica**: en el caso de un archivo ese campo está bloqueado, porque es un elemento único. En el caso de una carpeta, se puede elegir si auditar todo su contenido o parte de él.
- **Qué sucesos se auditan**: aparece un listado de acciones posibles sobre el archivo o carpeta, dando la posibilidad de establecer sobre cada una si se auditan los aciertos, los fallos o ambas opciones. La selección de sucesos va ligada a los permisos, de forma que la auditoría de un acceso implica la auditoría sobre los accesos dependientes de él. Por ejemplo, la auditoría del Control total implica la auditoría de todos los posibles accesos.
- **Si se hereda (sólo para carpetas):** en caso afirmativo se marcaría la casilla Aplicar estos valores de auditoría sólo a objetos y/o contenedores dentro de este contenedor.

La auditoría de acceso a archivos y carpetas también puede hacer uso de las herramientas de herencia estudiadas en la unidad. Así, se puede:

- **Forzar la herencia**: Activando en la pestaña **Auditoría,** la casilla **Reemplazar todas las entradas de auditoría existentes y heredables en todos los descendientes con entradas de auditoría heredables de este objeto**.
- **Bloquear la herencia**: Desactivando en la pestaña **Auditoría,** la **casilla Incluir todas las entradas de auditoría heredables del objeto principal de este objeto**.

La configuración de entradas de auditoría no habilita, por si misma, la directiva de auditoría.

Para saber más

En el siguiente artículo se explica de forma más detallada cómo auditar el acceso a archivos y carpetas:

Auditar el acceso a archivos y carpetas.

Registros de seguridad.

Tras habilitar la directiva de auditoría, previa configuración, el sistema comenzará a registrar los sucesos que se hayan especificado en las entradas de auditoría.

Los resultados pueden consultarse en cualquier momento a través del **Visor de eventos**, en la rama **Registros de Windows → Seguridad**.

Autoevaluación

¿En qué ubicación del Visor de eventos podemos consultar los registros generados por una auditoría que controla el acceso de un grupo de usuarios a Internet Explorer?

- En Registros de Windows → Seguridad.
- En Registros de aplicaciones y servicios → Internet Explorer.
- En Registros de Windows → Aplicación.
- En el Visor de eventos no se pueden consultar los registros de seguridad.