PRÁCTICA DIRECTIVAS DE SEGURIDAD DE WINDOWS

Se denominan Directivas de grupo al conjunto de valores de configuración utilizados por el administrador para gestionar objetos que actúan durante la inicialización y la finalización de los equipos y durante el inicio de la sesión y el final de la sesión de los usuarios.

Por medio de estas directivas, el administrador controla los entornos de trabajo de los usuarios del dominio y el comportamiento de un objeto determinado. Las Directivas de grupo se pueden utilizar para administrar características tales como instalación de software, plantillas administrativas, redirección de carpetas, configuración de seguridad, secuencias de comandos (inicio o apagado, e inicio de sesión o cierre de sesión) y mantenimiento de Internet Explorer. El administrador de las directivas de grupo puede definir, por ejemplo, los programas que se visualizarán en el escritorio de los usuarios, las opciones del menú Inicio de cada usuario, los archivos que copiarán en la carpeta Mis Documentos, el acceso a los archivos y a las carpetas. También pueden influir en los permisos que se otorgan a las cuentas de usuarios y de grupos.

Las directivas de grupo afectan a usuarios y a equipos. Se activan en el momento que el usuario inicia su sesión, mientras que, por su parte, las directivas de grupo de equipo se activan en el inicio del sistema.

Las Directivas de Seguridad se agrupan en dos categorías:

Según su función.

Directivas de seguridad: ¿Cuántos caracteres tiene una contraseña? ¿Cada cuánto tiempo debe ser cambiada ésta?, etc.

A nivel de dominio. - Son aplicadas en todas las máquinas del dominio.

A nivel de controladores de dominio. - Se aplican tan sólo en los controladores de dominio, pero sin suplantar a las del dominio (en caso de entrar en contradicción una y otra, se aplica la del dominio, no la de los controladores de dominio).

Directivas de Entorno: ¿Quién tiene acceso al panel de control? ¿Cuál es el tamaño máximo del archivo de registro de sistema?

A nivel de equipo local.

A nivel de sitio.

A nivel de dominio.

A nivel de Unidad Organizativa (OU -> Organizational Unit).

Según su objeto de configuración.

Configuración del equipo:

Configuración de software.

Configuración de Windows.

Plantillas administrativas.

Configuración del usuario:

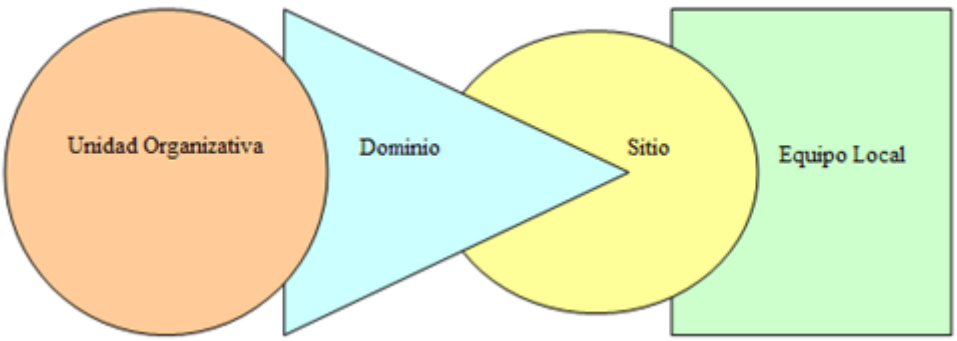
Configuración de software.

Configuración de Windows.

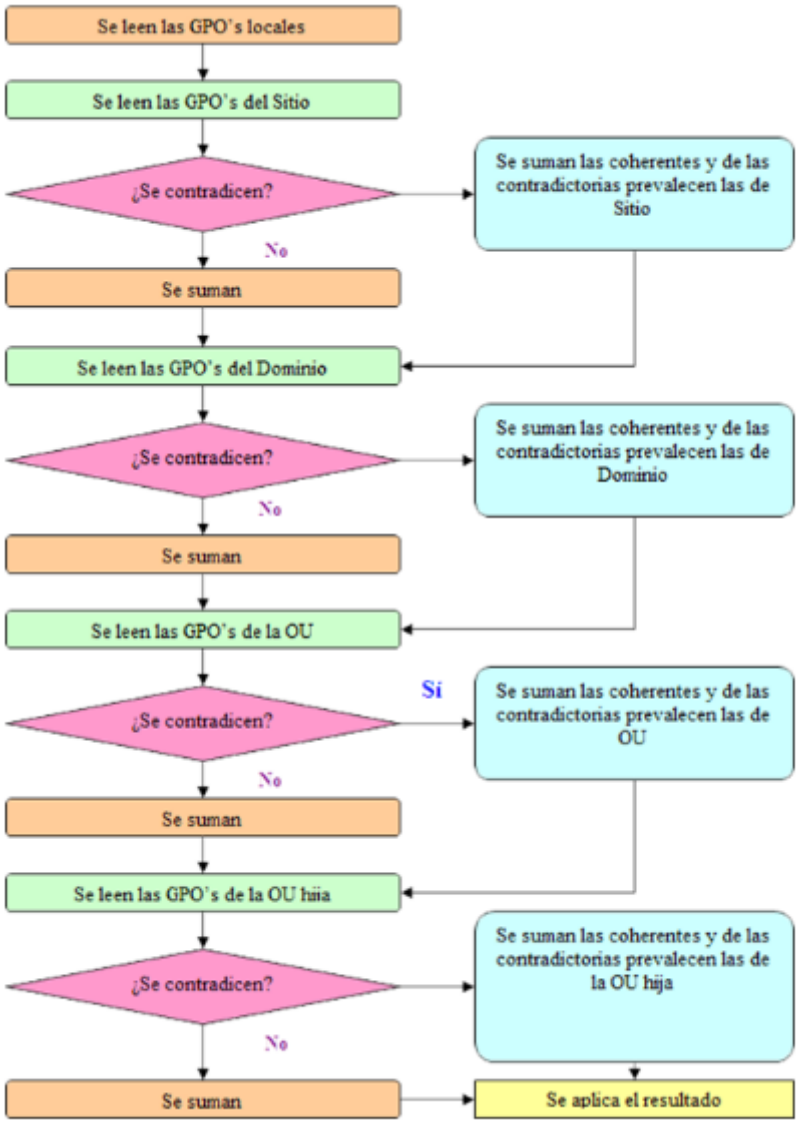
Plantillas administrativas.

Sistema aplicación de las políticas.

Una GPO (Objeto de Directiva de Grupo - Group Policy Object) puede ser contenida por equipos locales, sitios, dominios y unidades organizativas (OU). Un usuario está ubicado en un equipo local que a su vez se ubicará en un sitio, pertenecerá a un dominio y será miembro de una OU se ve claramente que se puede dar el caso de que en el equipo local se aplique una GPO, en el sitio otra, otra para el dominio y otra para la OU. Se podría dar el caso, por tanto, de que las GPO's contuvieran políticas que se contradijeran entre sí. Cuando se dan casos de estos, el sistema de GPO's está implementado para asegurar que siempre se aplicarán las políticas, y para ello establece una forma de prioridad entre éstas por la cual, según dónde estén asignadas, unas prevalecen sobre otras atendiendo a una serie de reglas.



Las GPO’s de una OU prevalecen sobre las del dominio, que a su vez prevalecen sobre las de sitio, las cuales a su vez prevalecen sobre las del equipo local. Por prevalecer no se entiende que unas anulen a otras; las políticas se suman, sólo se anulan en caso de ser contradictorias entre ellas.



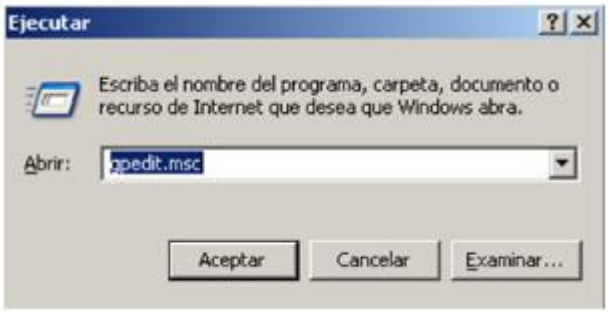
Configurar plantillas de seguridad.

Una plantilla de seguridad es un archivo que representa una configuración de seguridad. Las plantillas de seguridad se pueden aplicar sobre un equipo localmente, importar a un objeto de directiva de grupo o utilizar para analizar la seguridad.

Una plantilla de seguridad contiene cientos de posibles ajustes que se pueden controlar de un ordenador o de múltiples ordenadores. Pueden controlar áreas como derechos de usuario, permisos o políticas de passwords entre otras. Pueden ser personalizadas para incluir casi cualquier ajuste de seguridad sobre un computador destino.

El editor de objetos de directivas de grupo puede abrirse de varias maneras, dependiendo de la acción que desee llevar a cabo y del objeto al que desee aplicar la Directiva de grupo.

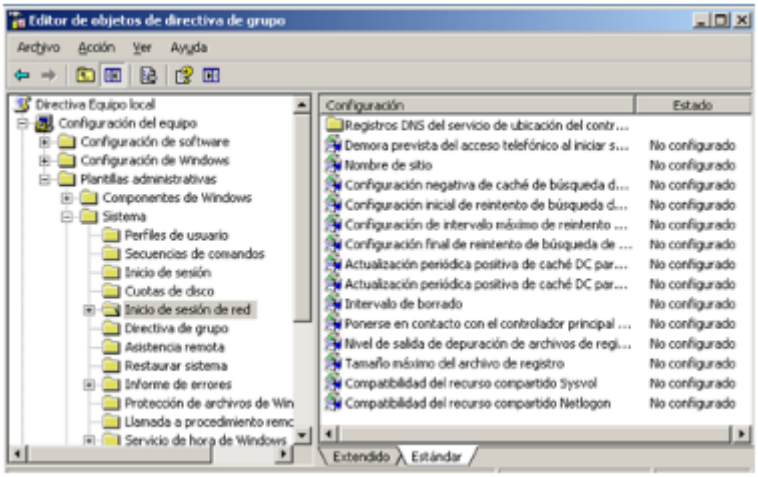
Una de las formas en las que puede abrir el Editor de objetos de directiva de grupo es modificando la directiva de grupo local. Hacer clic en Inicio –> Ejecutar, después escribir “gpedit.msc” y, a continuación, pulsar en “Aceptar”.



Esto hace que se abra el administrador de la directiva de grupo.

Expandir los nodos y buscar la directiva que se quiere modificar.

En el panel de la derecha se observan las directivas definidas.



Para modificar el objeto de dicha directiva hacer clic con el botón derecho del ratón sobre el nombre del objeto y del menú emergente elegir “Propiedades”.

El cuadro de diálogo “Propiedades” de objeto tiene dos fichas: Configuración y Explicación. Dentro de la opción Configuración, se puede marcar cualquiera de las opciones disponibles:

- No configurada.
- Habilitada.
- Deshabilitada.

EJERCICIO A REALIZAR

Este, perfectamente, puede ser un ejemplo de un sistema blindado a prueba de curiosos, que, junto a un perfil móvil obligatorio refuerza el conjunto de directivas de red. Realiza esta configuración y ves indicando paso a paso que sucede con la configuración de cada una de las directivas.

Configuración de Usuario/ Plantillas Administrativas/ Componentes de Windows/ Internet Explorer/

Aplicar el modo de pantalla completa

Deshabilitar la configuración de la página de Opciones avanzadas

Deshabilitar cambio de la configuración de la página de inicio

Desactivar la funcionalidad “Eliminar el historial de exploración”

Impedir la eliminación de archivos temporales de Internet

Deshabilitar el cambio de configuración del idioma

Deshabilitar el Asistente para la conexión a Internet

Deshabilitar el cambio de configuración de conexión

Deshabilitar el cambio de configuración del Proxy

No permitir que usuarios habiliten ni deshabiliten complementos

Configurar Outlook Express

Configuración de Usuario/ Plantillas Administrativas/ Componentes de Windows/ Internet Explorer/ Panel de control de Internet/

Deshabilitar la página General

Deshabilitar la página Seguridad

Deshabilitar la página Contenido

Deshabilitar la página Conexiones

Deshabilitar la página Programas

Deshabilitar la página de Privacidad

Deshabilitar la página Opciones Avanzadas

Configuración de Usuario/ Plantillas Administrativas/ Componentes de Windows/ Internet Explorer/ Menús del explorador/

Menú de archivo: deshabilitar la opción de menú Guardar como…

Menú de archivo: deshabilitar la opción de menú Nuevo

Menú de archivo: deshabilitar la opción de menú Abrir

Menú de archivo: deshabilitar Guardar como página de Web completa

Deshabilitar la opción Guardar este programa en disco

Configuración de Usuario/ Plantillas Administrativas/ Componentes de Windows/ Internet Explorer/ Características de seguridad

Repasar Opciones

Configuración de Usuario/ Plantillas Administrativas/ Componentes de Windows/ Internet Explorer/ Configuración de Internet

Repasar Opciones

Configuración de Usuario/ Plantillas Administrativas/ Componentes de Windows/ Programador de tareas/

Ocultar páginas de propiedades

Evitar que la tarea se ejecute o finalice

Prohibir arrastrar y colocar

Prohibir la creación de nuevas tareas

Prohibir la eliminación de tareas

Ocultar la casilla de verificación de propiedades en el Asistente para agregar tarea programada

Examinar la exploración

Configuración de Usuario/ Plantillas Administrativas/ Sistema/ Opciones de Ctrl.+Alt+Sup/

Quitar la opción Cambiar Contraseña

Configuración de Usuario/ Plantillas Administrativas/ Menú Inicio y barra de tareas/

Quitar vínculos y accesos a Windows Update

Quitar Conexiones de red del menú Inicio

Quitar el menú Buscar del menú Inicio

Quitar el menú Ayuda del menú Inicio

Quitar el menú ejecutar del menú Inicio

Quitar el icono Mis sitios de red del menú Inicio

Agregar cerrar sesión al menú Inicio

Impedir cambios en la configuración de la barra de tareas y del menú Inicio

No guardar historial de documentos abiertos recientemente

Borrar historial de los documentos abiertos recientemente al salir

Desactivar menús personalizados

Desactivar seguimiento del usuario

Bloquear la barra de tareas

Configuración de Usuario/ Plantillas Administrativas/ Escritorio/

Quitar el elemento Propiedades del menú contextual de Mis documentos

Quitar el elemento Propiedades del menú contextual de Mi Pc

Ocultar el icono Mis sitios de red del escritorio

Prohibir al usuario cambiar la ruta de Mis documentos

No guardar la configuración al salir

Quitar el Asistente para limpieza del escritorio

Configuración de Usuario/ Plantillas Administrativas/ Panel de control/

Prohibir el acceso al Panel de Control

Configuración de Usuario/ Plantillas Administrativas/ Panel de control/ Agregar o quitar programas/

Quitar Agregar o quitar programas

Ocultar la página Cambiar o quitar programas

Ocultar la página Agregar nuevos programas

Configuración de Usuario/ Plantillas Administrativas/ Panel de control/ Impresoras/

Impedir la agregación de impresoras

Impedir la eliminación de impresoras

Configuración de Usuario/ Plantillas Administrativas/ Sistema/

Impedir el acceso al símbolo del sistema

Impedir el acceso a herramientas de edición del registro

Configuración de Usuario/ Plantillas Administrativas/ Componentes de Windows/ Explorador de Windows/

Quitar el menú Opciones de carpeta del menú Herramientas

Quitar el menú Archivo del Explorador de Windows

Quitar “Conectar a unidad de red” y “Desconectar de unidad de red”

Ocultar el elemento Administrar del menú contextual del Explorador de Windows

Ocultar estas unidades específicas en Mi Pc

Impedir el acceso a las unidades desde Mi Pc

Ocultar la ficha Hardware

Quitar la ficha DFS

Quitar la ficha Seguridad

Sin “Equipos próximos” en Mis sitios de red

Sin “Toda la red” en Mis sitios de red

Solicitar credenciales para instalaciones de red

Quitar la característica de grabación de CD

Quitar Documentos compartidos de Mi Pc

Configuración de Usuario/ Plantillas Administrativas/ Componentes de Windows/ Windows Installer/

Impedir la instalación de cualquier medio extraíble

Configuración de Usuario/ Plantillas Administrativas/ Componentes de Windows/ Windows Messenger/

No ejecutar automáticamente Windows Messenger al inicio

Configuración de Usuario/ Plantillas Administrativas/ Componentes de Windows/ Windows Update/

Quitar el acceso a todas las características de Windows Update