|  |  |  |
| --- | --- | --- |
| Sistemas Operativos en Red | | |
| UT 3 \_ej04 | Gestión de usuarios, grupos y equipos | |
| Nombre y Apellido |  | Políticas de grupo |

Aplica las siguientes políticas de grupo, no se te olvide actualizar la política antes de comprobar si se aplica al usuario o el equipo. Crea la unidad organizativa profes y alumnos y añades en cada una sus correspondientes usuarios. Crea todas las políticas en un único archivo, que se aplicarán solamente a la UO alumnos y comprobamos que a profes no se aplica y después también se aplicará a la UO profes, comprobando que ahora a los usuarios de ambas UO se aplican dichas políticas.

Una vez creadas las políticas captura la pantalla que muestra los ámbitos a los que se aplican

1. **La vigencia máxima de la contraseña para todos los usuarios de la máquina será de 15 días**

Clic en directiva equipo local-configuración del equipo-configuración de Windows-configuración de seguridad-directiva de cuenta-directiva de contraseña-vigencia máxima de la contraseña.-doble clic.



1. **Las contraseñas deben cumplir con los requisitos de complejidad por defecto de Windows server ¿Cuáles son estos requerimientos?**

Clic en directiva equipo local-configuración del equipo-configuración de Windows-configuración de seguridad-directiva de cuenta-directiva de seguridad-propiedades de la contraseña debe cumplir los requisitos de complejidad.



1. **Los usuarios que requieran cambiar su contraseña no podrán usar un password que se haya usado antes por lo menos desde los 2 últimos cambios.**

Clic en directiva equipo local-configuración del equipo-configuración de Windows-configuración de seguridad-directivas de cuenta-directivas de contraseña-exigir historial de contraseñas-escribimos 2-aceptar.



1. **Los usuarios del grupo smr1 pueden apagar la máquina una vez hayan iniciado sesión, pero los usuarios del grupo smr2 no podrán apagar el equipo** (Desde el sistema operativo).

Clic en directiva equipo local-configuración del equipo-configuración de Windows-configuración de seguridad-directivas locales-asignación de derechos de usuario-apagar el sistema.

(Es importante seleccionar los grupos que van a usar esa directiva: Clic en tipos de objetos para seleccionar la casilla grupos, para que busque también los grupos existentes-aceptar-seleccionamos el grupo smr1)



1. **Los usuarios del grupo smr1 podrán cambiar la hora de la máquina local**.

Directiva equipo local-configuración del equipo-configuración de Windows-configuración de seguridad-directivas locales-asignación de derechos de usuario-cambiar la hora del sistema-agregar usuario o grupo.



1. **Desactivar la ventana emergente de reproducción automática**

Directiva equipo local-configuración del equipo-plantillas administrativas-componentes de Windows-directivas de reproducción automática-desactivar reproducción automática.



1. **No permitir el apagado remoto de la máquina**

Directiva equipo local-configuración del equipo-plantillas administrativas-componentes de Windows-opciones de apagado-desactivar interfaz de apagado remoto heredada.



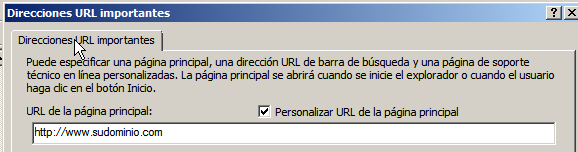
1. **Aplicar cuotas de 50MB para todos los usuarios locales y remotos** (Esta es un cuota muy baja y es usada solo para fines académicos).

Directiva equipo local-configuración del equipo-plantillas administrativas-sistema-cuotas de disco-limite de cuota y nivel de aviso predeterminados.

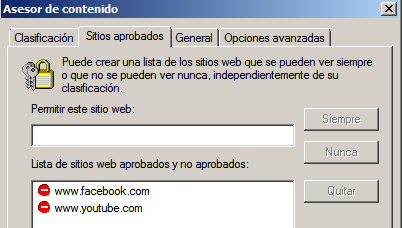


1. **La página principal que se cargará para cada usuario cuando abra su navegador será: http://www.sudominio.com** (Página institucional de su empresa).

Directiva equipo local-configuración de usuario-configuración de Windows-mantenimiento de internet Explorer-direcciones URL-direcciones URL importantes.



1. **Restringir desde el navegador el acceso a los siguientes sitios: www.facebook.com y www.youtube.com por URL, para todos los usuarios.** El administrador será el único con la contraseña de supervisor para el Asesor de Contenidos.



Directiva equipo local-configuración de usuario-configuración de Windows-mantenimiento de internet Explorer-seguridad-zonas de seguridad y clasificación de contenido.

1. **Ocultar la unidad C:\** (NOTA: Esto no restringirá el acceso a dicha unidad).

Directiva equipo local-configuración de usuario-plantillas administrativas-componentes de Windows-explorador de Windows-ocultar estas unidades especificadas en mi pc.



1. **Ocultar el menú opciones de carpeta del menú de herramientas.** Esto con el fin de que los usuarios no puedan ver archivos ocultos o cambiar algunas configuraciones de las carpetas.

Directiva equipo local-configuración de usuario-plantillas administrativas-componentes de Windows-explorador de Windows-quitar el menú opciones de carpeta del menú herramientas.



1. **Restringir el acceso a la unidad E:\ desde mi PC**

Directiva equipo local-configuración de usuario-plantillas administrativas-componentes de Windows-explorador de Windows-ocultar estas unidades especificadas en mi PC.

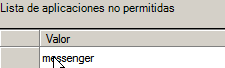
1. **Limitar el tamaño de la papelera de reciclaje a 100MB**

Directiva equipo local-configuración de usuario-plantillas administrativas-componentes de Windows-explorador de Windows-tamaño máximo permitido de la papelera de reciclaje



1. **No permitir que se ejecute Messenger.**

Directiva equipo local-configuración de usuario-plantillas administrativas-sistema-no ejecutar aplicaciones de Windows especificadas.



1. **Ocultar todos los elementos del escritorio para todos los usuarios.**

Directiva equipo local-configuración de usuario-plantillas administrativas-escritorio-ocultar y deshabilitar todos los elementos del escritorio.



1. **Bloquear la barra de tareas**

Directiva equipo local-configuración de usuario-plantillas administrativas-menu inicio y barra de tareas-bloquear la barra de tareas



1. **Prohibir el acceso del Lecto-escritura a cualquier medio de almacenamiento extraíble.**

Directiva equipo local-configuración de usuario-plantillas administrativas-sistema-acceso de almacenamiento extraíble-discos extraíbles: denegar acceso de lectura

