



**UNIVERSIDAD TECNOLÓGICA DE PANAMÁ
FACULTAD DE INGENIERÍA EN SISTEMAS COMPUTACIONALES
DEPARTAMENTO DE ARQUITECTURA DE COMPUTADORAS Y REDES
LICENCIATURA EN CIBERSEGURIDAD**

LABORATORIO #1

Asignación:

Creación de Usuarios, Grupos y GPO

Curso:

Ciberseguridad I

Estudiantes:

Eduardo Samaniego 8-964-2469

Profesor:

Ricardo Wong

Grupo:

1S3122

2023

Tabla de contenido

Resumen.....	3
Introducción	4
CREACION DE USUARIOS Y GRUPOS	5
Creación de Usuarios	5
Creación de Grupos y Asignaciones de grupos	10
Políticas de grupo.....	19
Directivas de configuración de equipo	20
Referencias.....	52

Resumen

En el presente documento se detallará el proceso integral de creación de usuarios y grupos dentro de un Active Directory, llevado a cabo en un entorno Windows Server 2019. Este procedimiento se ajustará conforme a los lineamientos y requisitos establecidos por el docente facilitador del laboratorio. Durante el desarrollo, se realizarán ajustes a las políticas de seguridad recomendadas, con el propósito de garantizar un funcionamiento óptimo del Directorio Activo.

Es imperativo tener en consideración que se presupone que el estudiante dispone de las máquinas virtuales necesarias y los complementos requeridos para llevar a cabo el proyecto. Dichos elementos incluyen una instancia de Windows Server 2019 y otra de Windows 10. El proceso se llevará a cabo a través de la edición de Windows Server 2019 con experiencia de escritorio (desktop experience).

En una fase inicial, se procederá a la creación de cuatro usuarios, divididos en dos categorías principales: Killers y Timers. Cada una de estas agrupaciones presenta necesidades distintas. Por ejemplo, los usuarios del grupo Killers contarán con el privilegio de apagar el equipo, mientras que los pertenecientes al grupo Timers no dispondrán de esta capacidad. En cambio, los usuarios Timers estarán encargados de gestionar los ajustes horarios del sistema.

La implementación de estas funcionalidades se realizará a través de la configuración de las Políticas de Grupo (GPO) pertinentes. Posteriormente, se llevará a cabo una evaluación exhaustiva para verificar la correcta aplicación de estas políticas en el sistema.

En síntesis, este documento abarca de manera detallada todo el proceso de revisión y detallado de la configuración de usuarios y grupos en un entorno Active Directory, operando en un Windows Server 2019.

Introducción

Con el avance constante de la tecnología y la creciente interconexión de sistemas, la administración eficiente de usuarios y grupos en entornos de red se ha vuelto esencial para garantizar la seguridad y el funcionamiento fluido de las organizaciones. En este contexto, el presente documento se adentra en el detallado proceso de creación y gestión de usuarios y grupos en un entorno de Active Directory, específicamente bajo un entorno Windows Server 2019.

El objetivo principal de este documento es proporcionar una guía completa tomando en consideración el documento proporcionado por el profesor abarcando desde la creación hasta la configuración de estos aspectos clave en la administración de redes. Se presta especial atención a la adhesión a las pautas y exigencias delineadas por el docente facilitador del laboratorio, garantizando así que los procedimientos aquí expuestos se alineen con los requisitos académicos establecidos.

La metodología empleada se basa en la utilización del núcleo (core) del Windows Server 2019 con la experiencia de escritorio (desktop experience), lo que facilita la realización de las operaciones y configuraciones necesarias.

La creación de usuarios se organizará en dos grupos: "Killers" y "Timers", cada uno con funcionalidades específicas y requisitos particulares de seguridad. Se explora cómo las Políticas de Grupo (GPO) pueden ser adaptadas y aplicadas para dar forma a estas funcionalidades según los roles asignados a los usuarios en cada grupo.

Una vez configuradas las políticas, se realizará un minucioso proceso de verificación para confirmar la efectividad de las configuraciones realizadas. Esto permitirá asegurar que las políticas de seguridad y los permisos definidos se apliquen correctamente en el sistema.

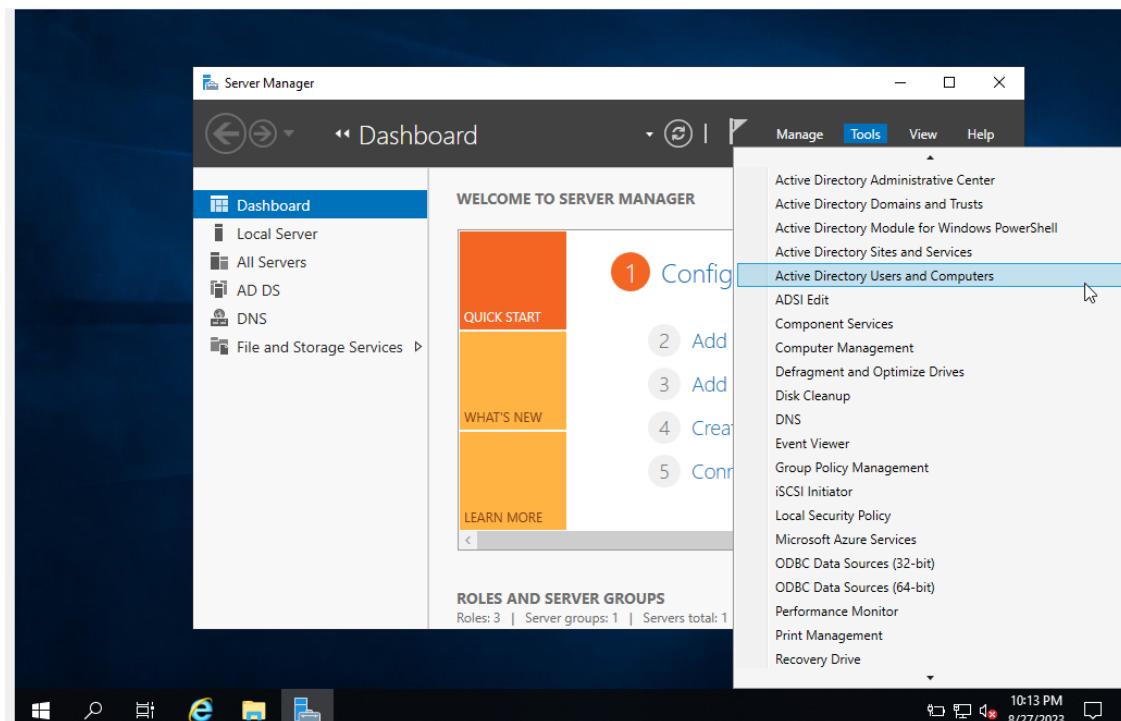
CREACION DE USUARIOS Y GRUPOS

Creación de Usuarios

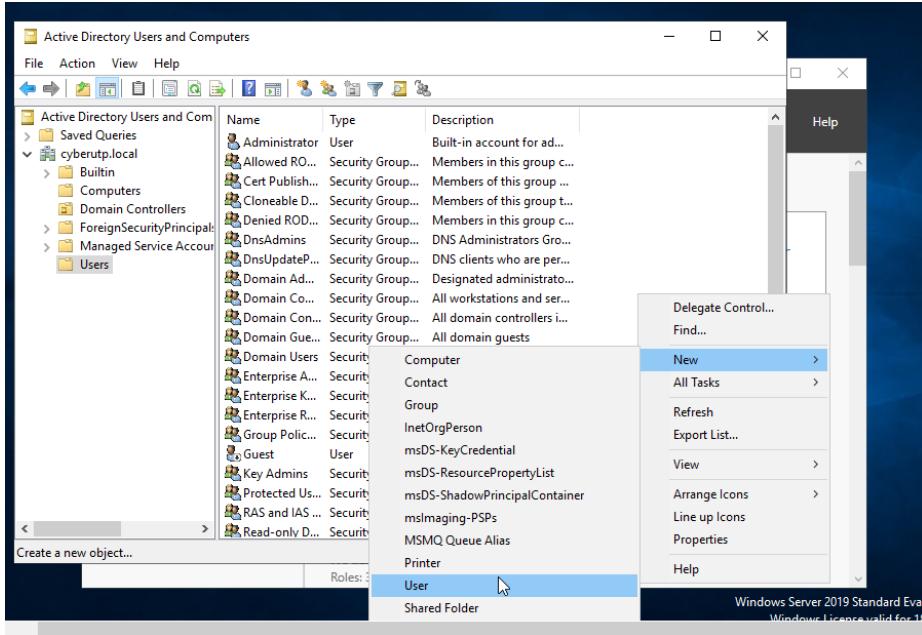
Para el desarrollo de este proyecto crearemos 4 usuarios

Para la creación de usuarios debemos seguir los siguientes pasos

Con un Windows Server con AD seleccionamos tools y posteriormente active directory users and computers

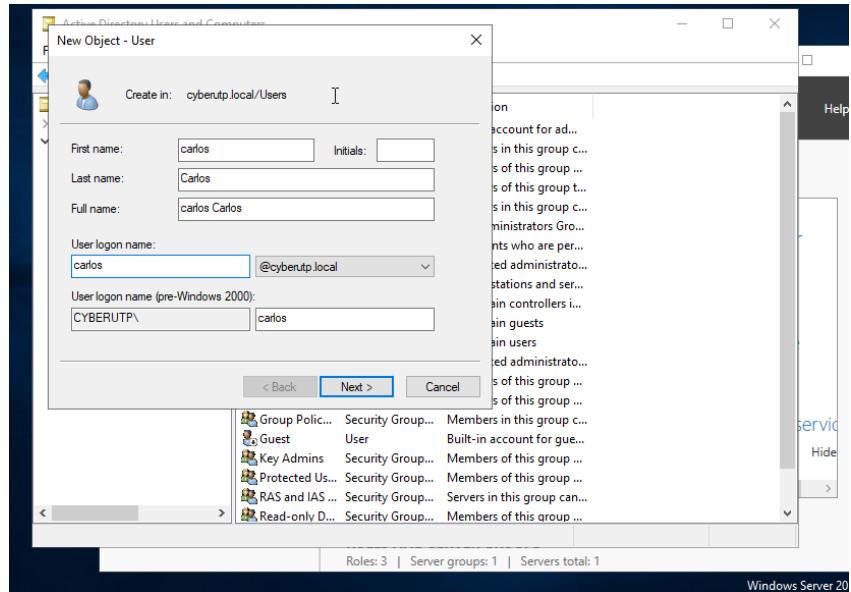


Se abrirá la pestaña vamos a la carpeta users>click derecho>user>new



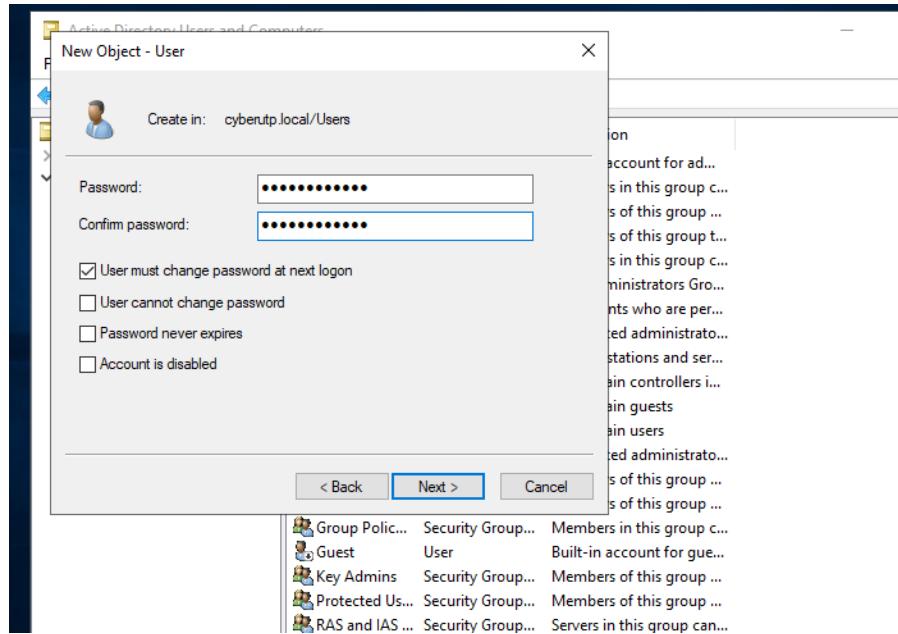
Se nos va a desplegar la ventana de creación de usuarios, asignamos el nombre carlos

Carlos, asignamos también el user logon name, posteriormente le damos click a next

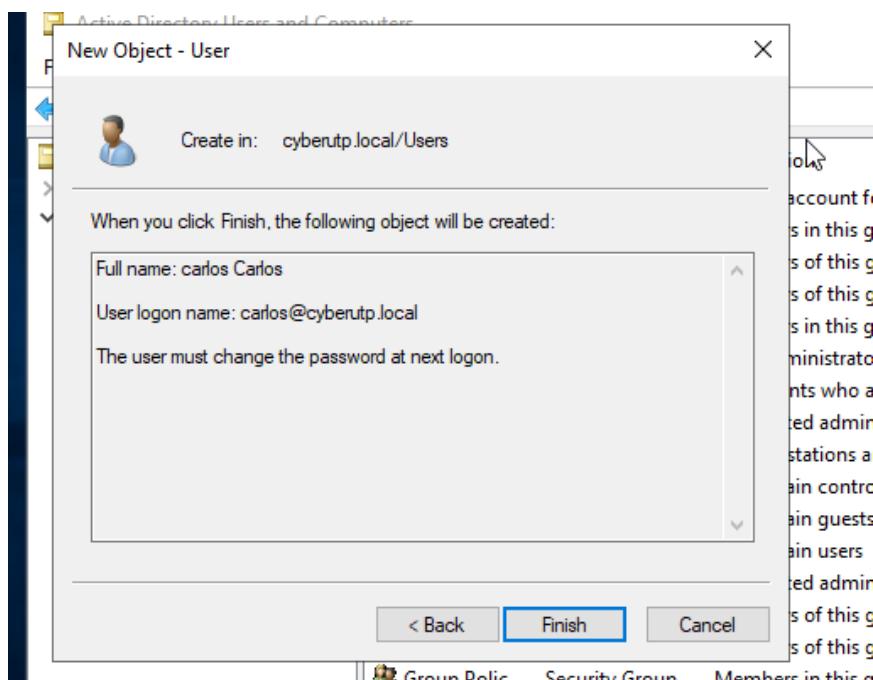


Asignamos la contraseña del usuario y dejamos la palomita de user must change

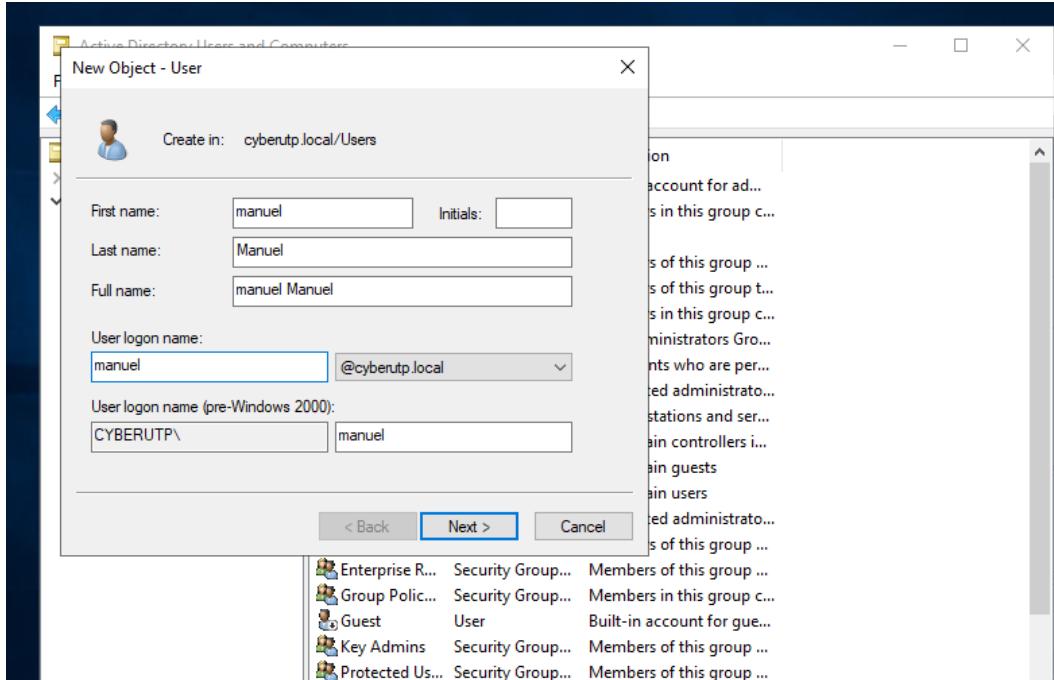
password at next logon



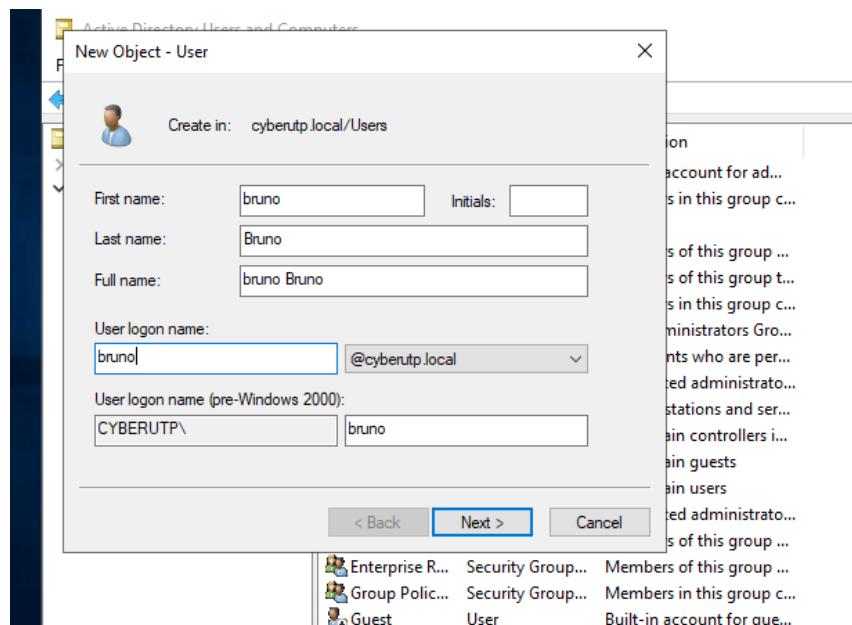
Posteriormente presionamos sobre next y se nos va a mostrar un resumen de todo el usuario



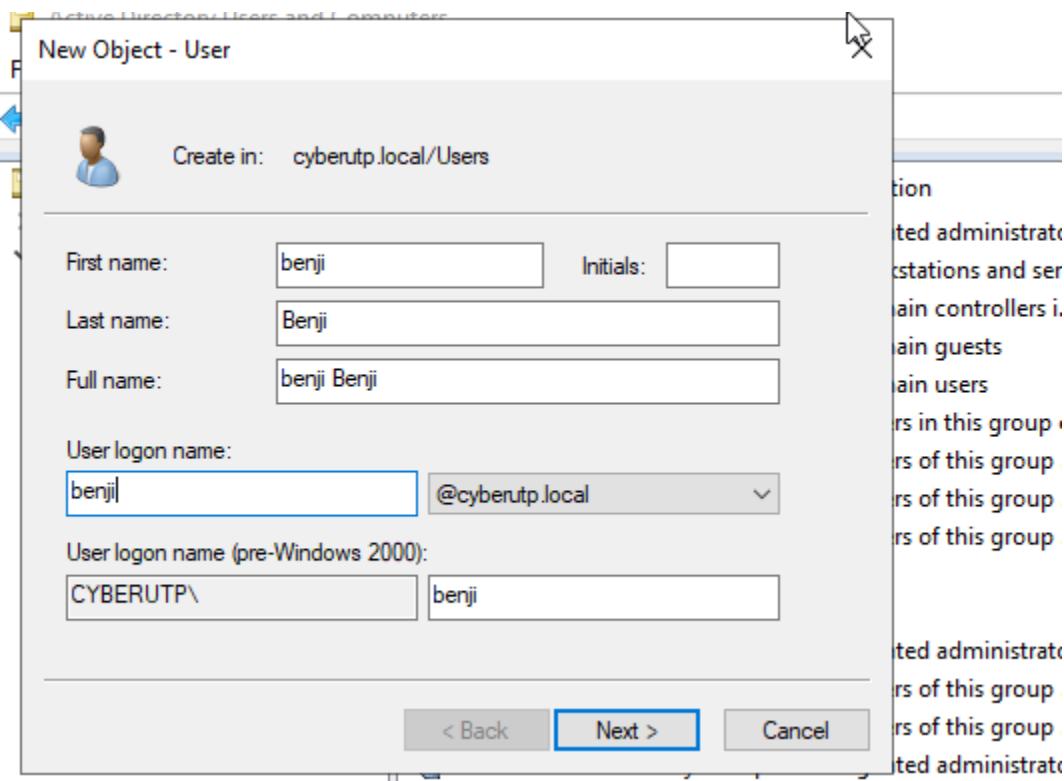
Creamos el usuario Manuel nuevamente con users>click derecho>user>new y asignamos los nombres y user logon name y posteriormente asignamos la contraseña.



Creamos el usuario Bruno nuevamente con users>click derecho>user>new y asignamos los nombres y user logon name y posteriormente asignamos la contraseña



Creamos el usuario Benji nuevamente con users>click derecho>user>new y asignamos los nombres y user logon name y posteriormente asignamos la contraseña



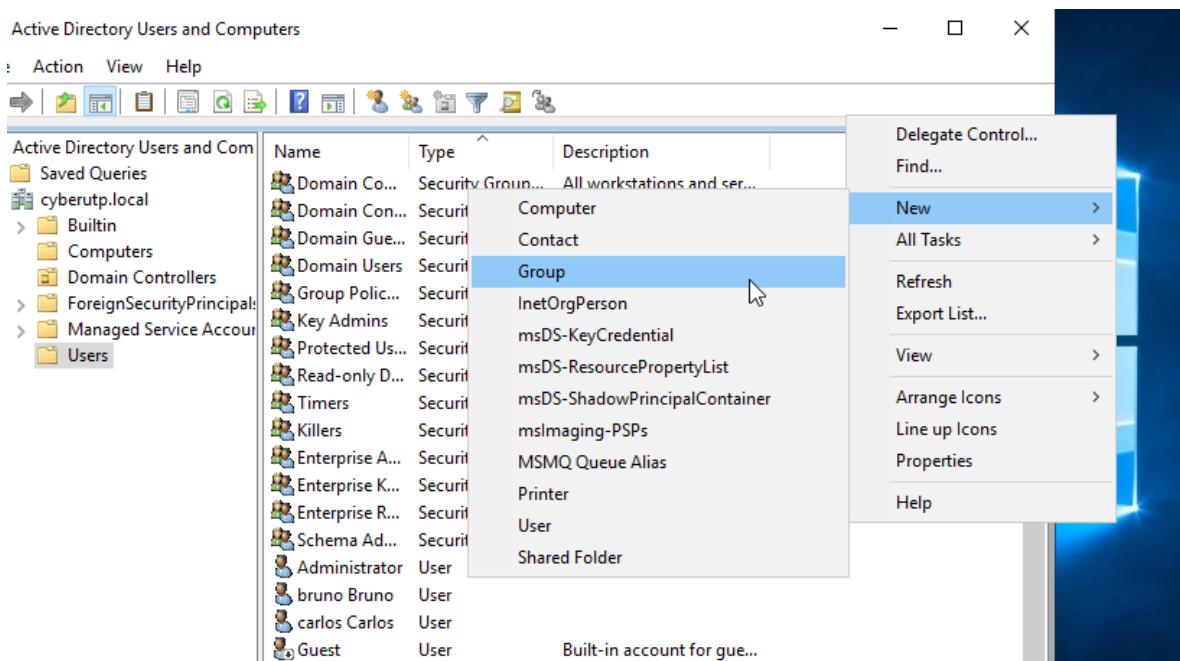
Con eso ya tendríamos los 4 usuarios necesarios para los grupos

Name	Type	Description
Domain Controller	Security Group...	All workstations and servers in this group
Domain Controller	Security Group...	All domain controllers in this group
Domain Guest	Security Group...	All domain guests
Domain User	Security Group...	All domain users
Group Policy	Security Group...	Members in this group
Key Admins	Security Group...	Members of this group
Protected User	Security Group...	Members of this group
Read-only Domain	Security Group...	Members of this group
Timers	Security Group...	
Killers	Security Group...	
Enterprise Admin	Security Group...	Designated administrator
Enterprise Admin	Security Group...	Members of this group
Enterprise Admin	Security Group...	Members of this group
Schema Admin	Security Group...	Designated administrator
Administrator	User	Built-in account for administration
bruno Bruno	User	
carlos Carlos	User	
Guest	User	Built-in account for guest access
manuel Man...	User	
benji Benji	User	

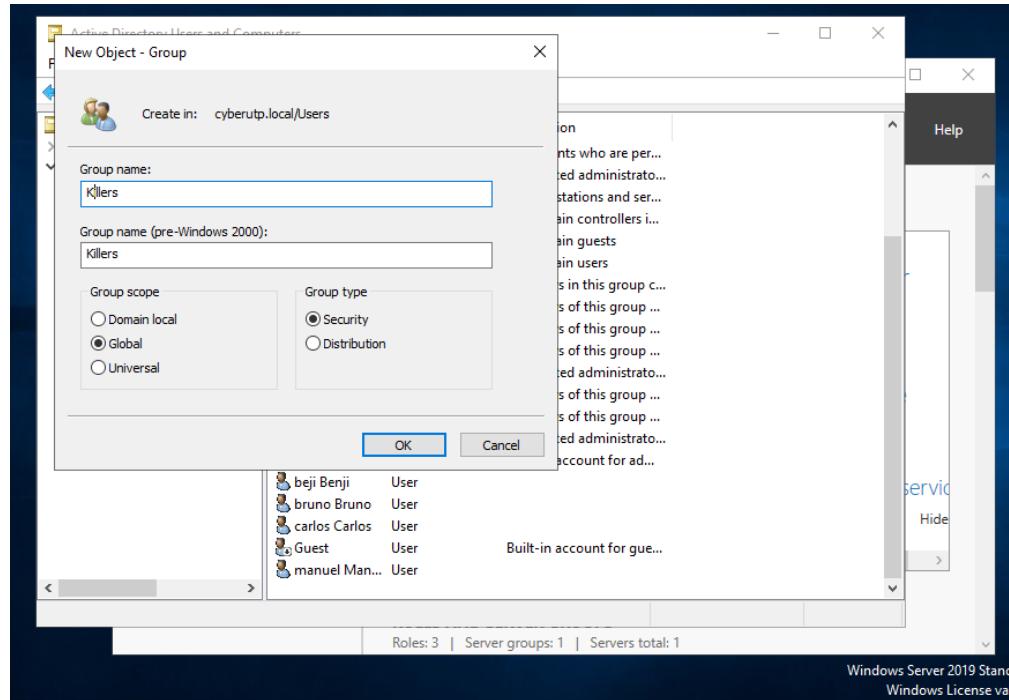
Creación de Grupos y Asignaciones de grupos

Con 4 usuarios crearemos 2 para el grupo killers y 2 para el grupo timers, para ahorrar espacio haremos el proceso completo de capturas para los dos primeros usuarios de cada grupo, el segundo de cada grupo se sobreentiende que es el mismo procedimiento y será más acortado el proceso

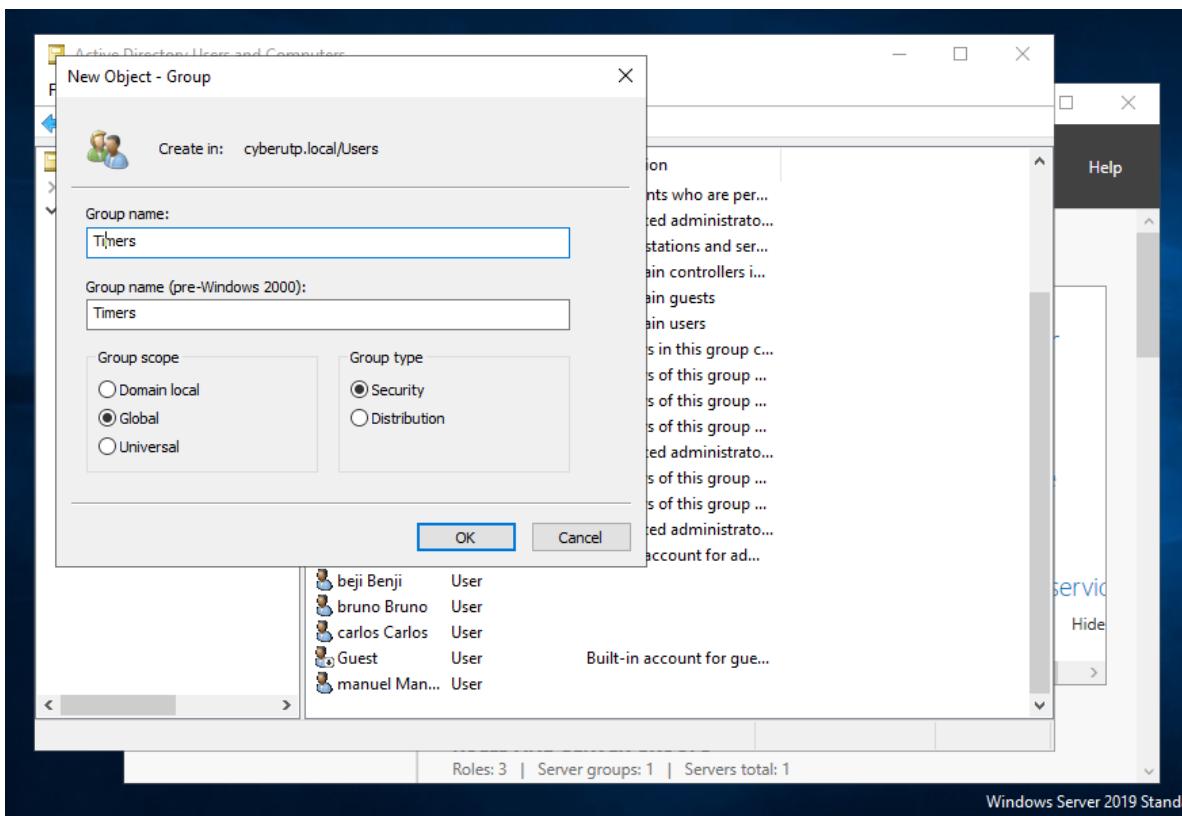
- Crearemos el grupo Killers, en users > click derecho > group > new



- Posteriormente escribiremos el nombre del grupo y presionamos en aceptar



- Haremos el mismo proceso para crear el grupo timers

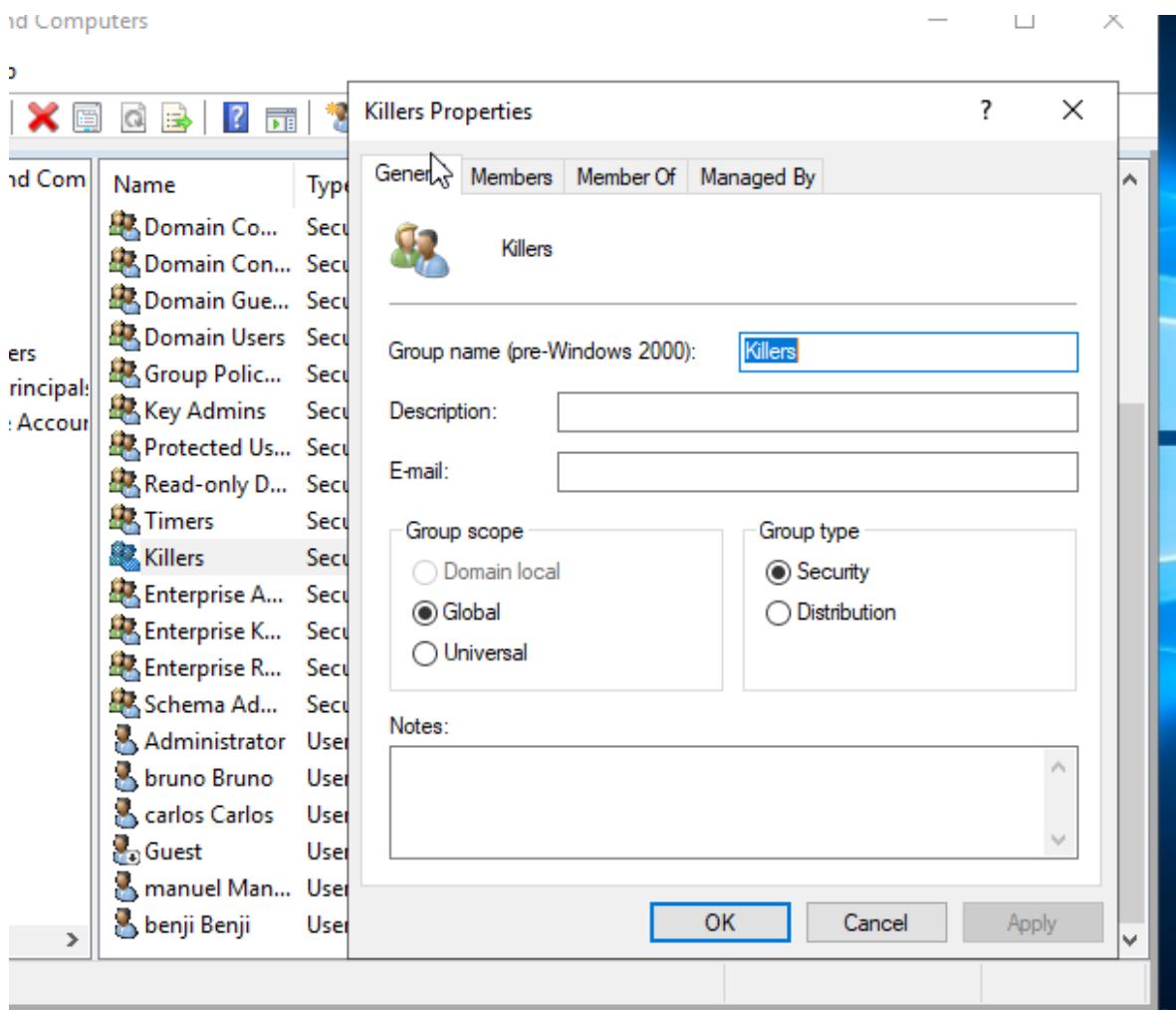


- Con eso ya tendríamos creado los dos grupos detallados en la guía de laboratorio.

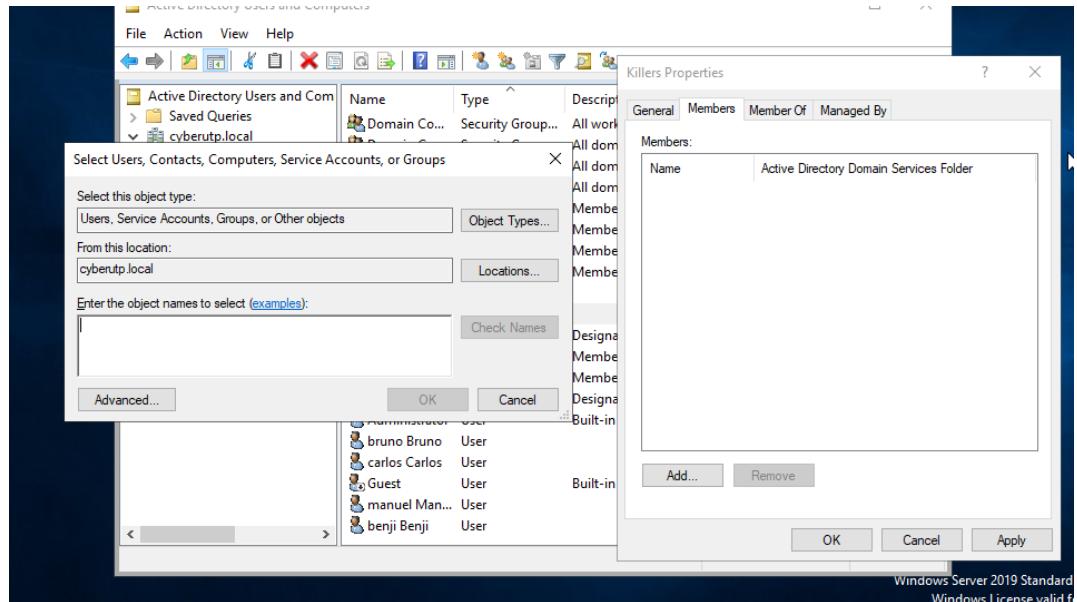


Realizaremos ahora el proceso de agregar usuarios a grupos

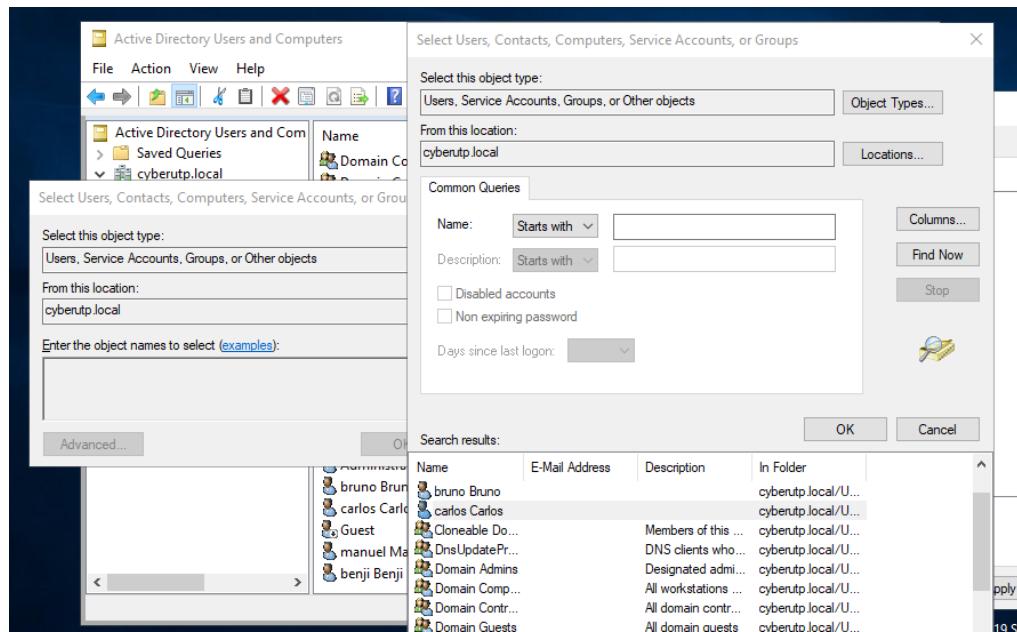
- Daremos click encima del grupo killers para abrirlo



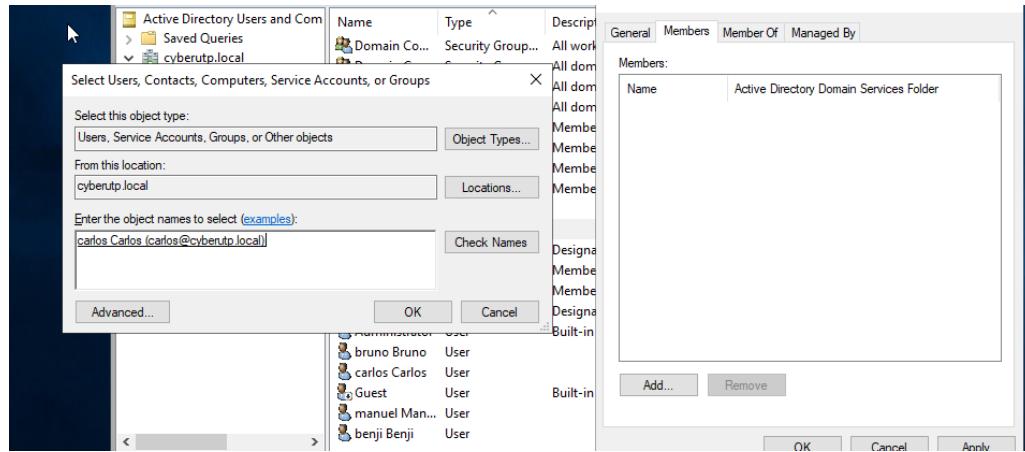
- Luego le damos click a member > add > advanced



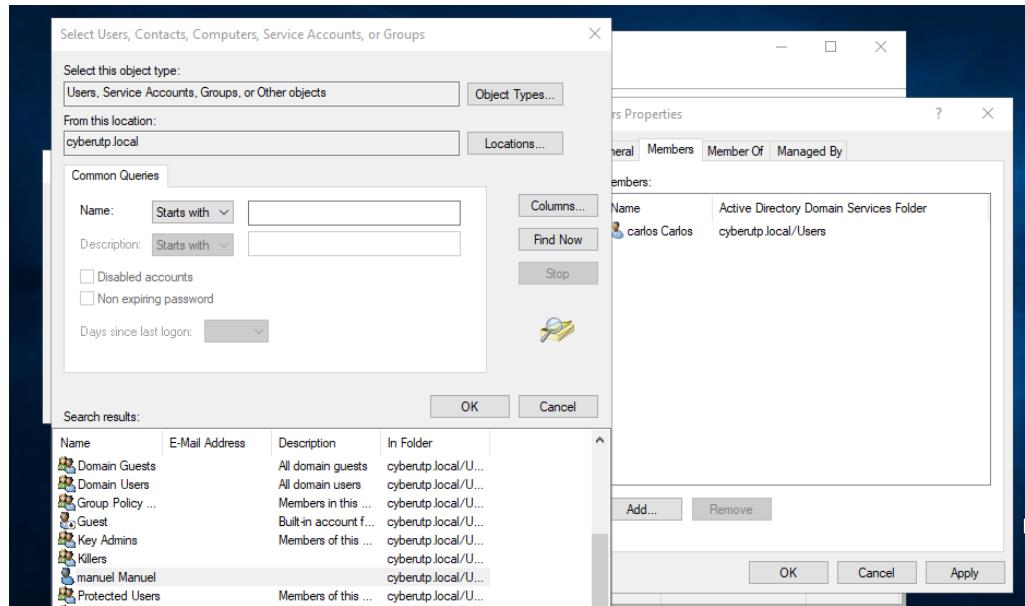
- Damos a Find now y buscamos a Carlos



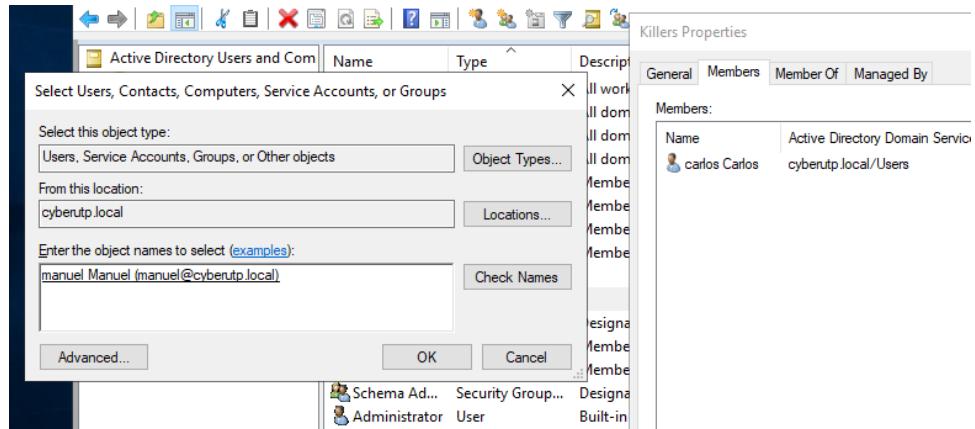
- Luego daremos a ok para tenerlo agregado



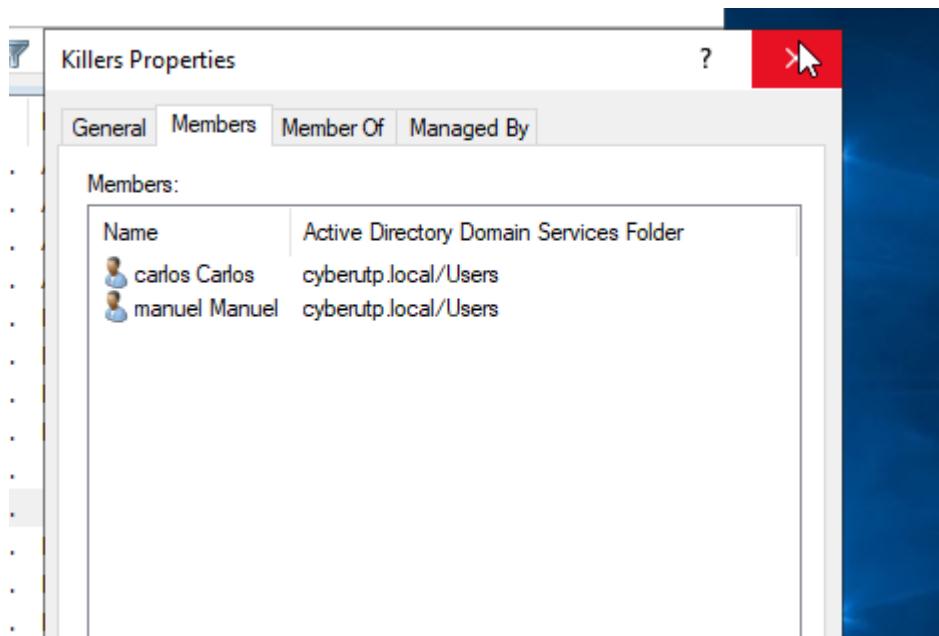
- Agregaremos también al usuario Manuel



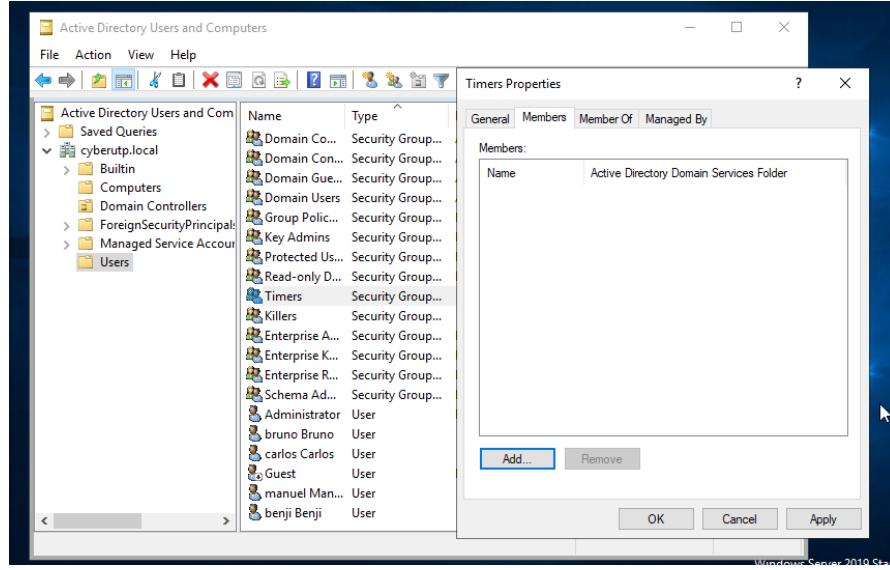
- Damos a ok para que se agregue



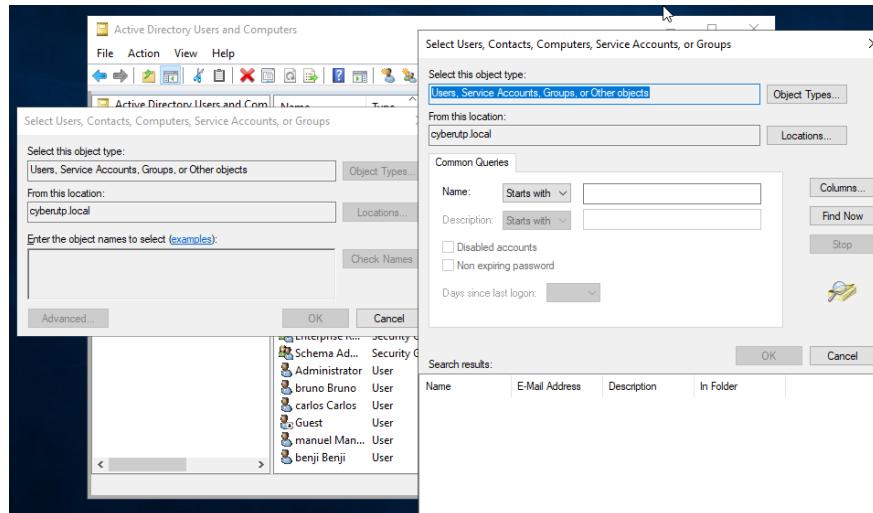
- Con eso ya tendríamos a los dos usuarios killers



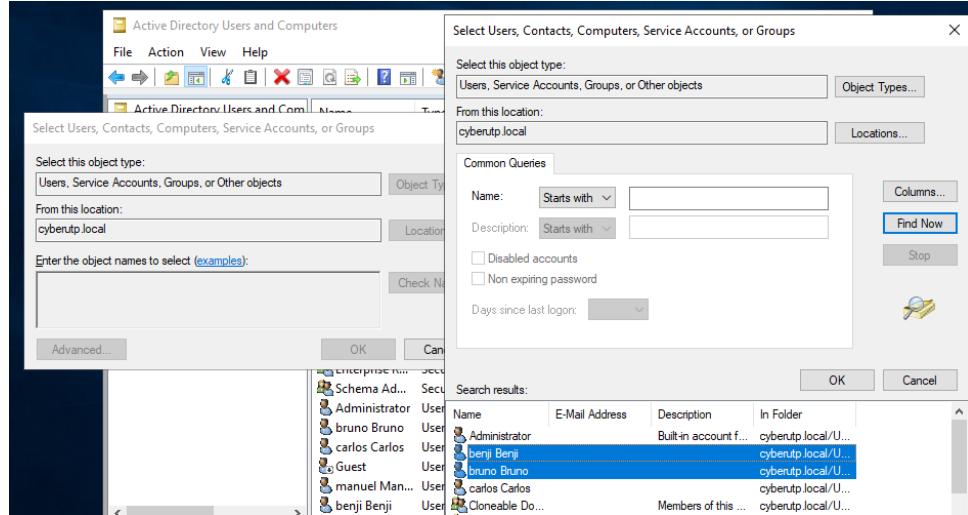
- Ahora vamos a agregar a los timers y presionamos add



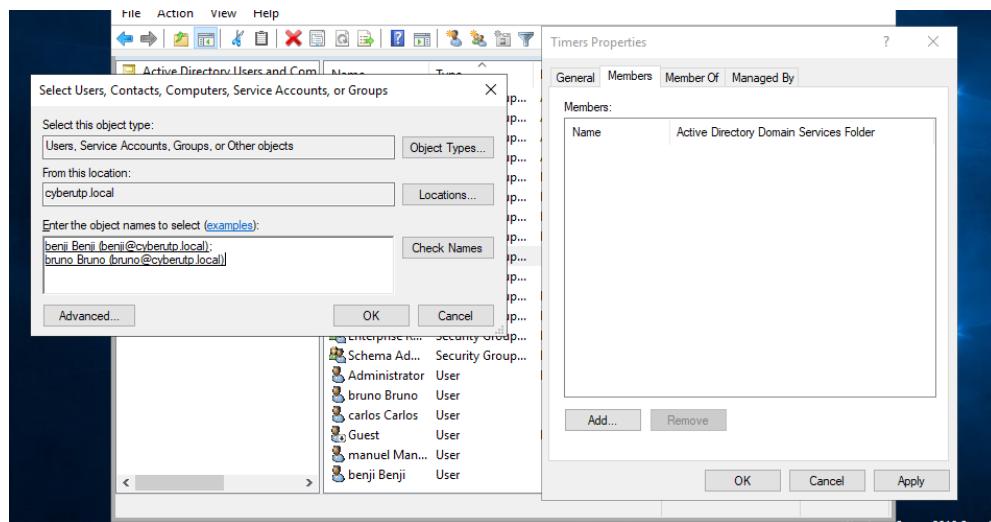
Damos a advanced > Find now



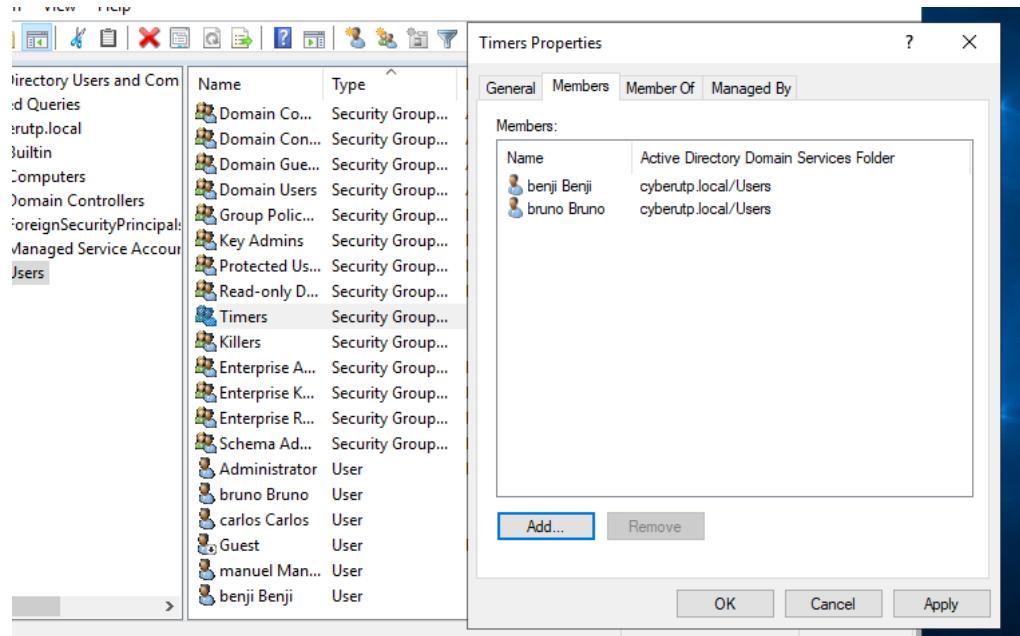
- Seleccionamos los dos usuarios bruno y benji



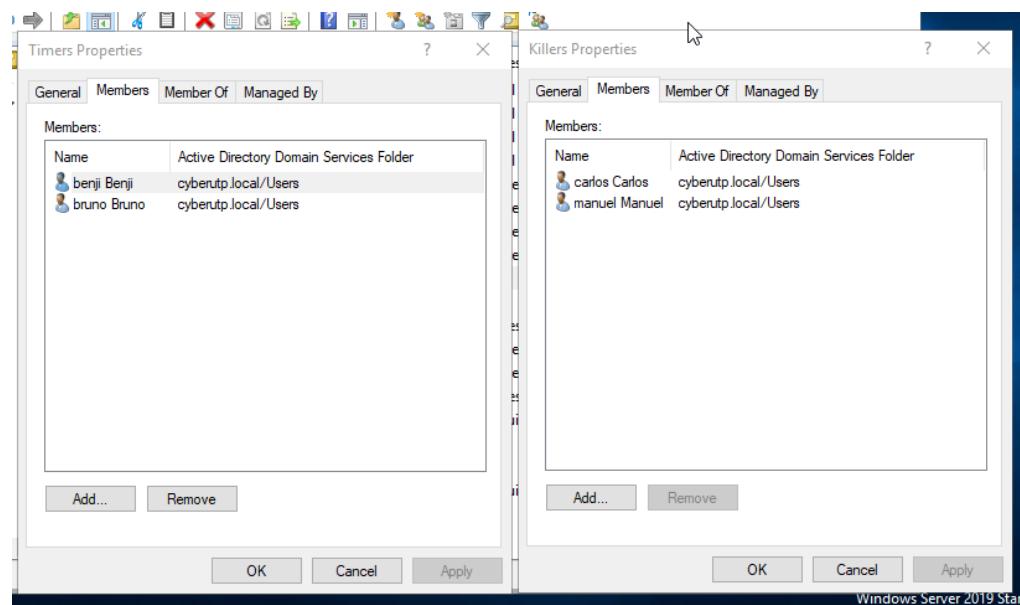
- Se nos van a agregar los dos usuarios al grupo y damos a ok



- Posteriormente le damos a apply

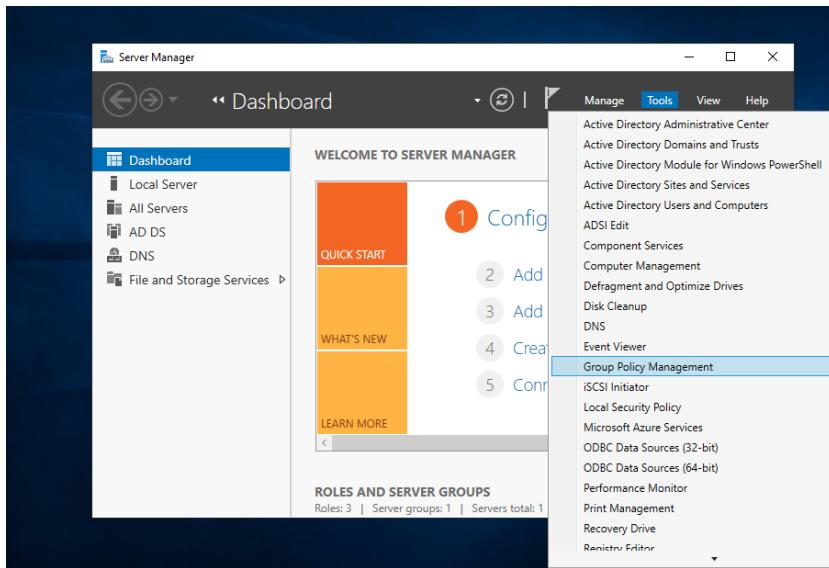


- Su presionamos encima de cada nombre de grupo y nos vamos a members podemos visualizar los integrantes de cada grupo.

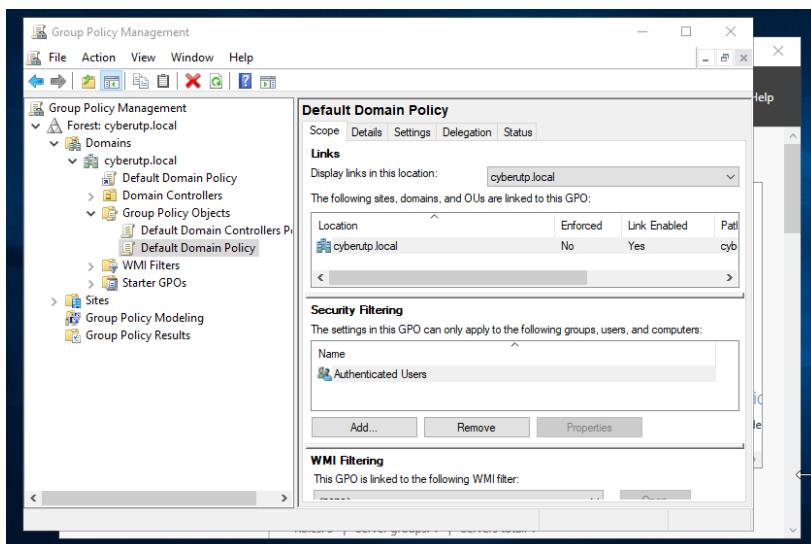


Políticas de grupo

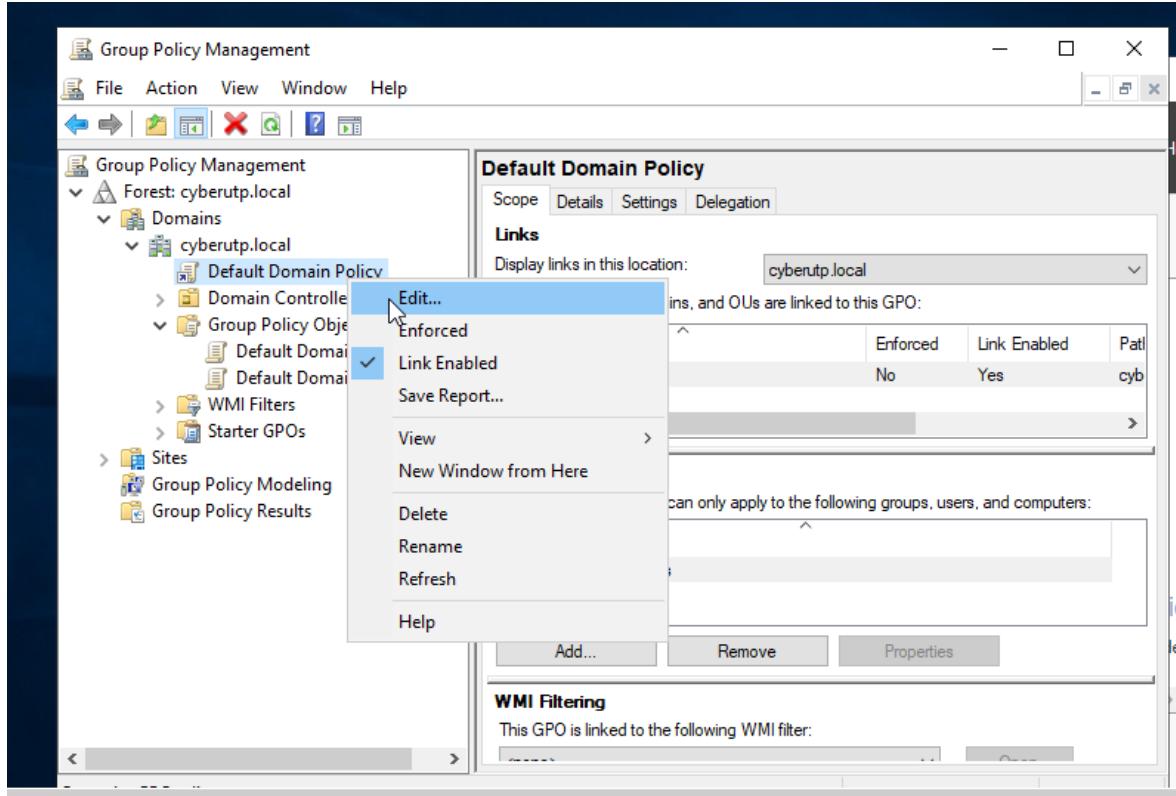
Para realizar el proceso de configuración de las políticas de grupo tenemos en Windows server 2019 el panel de tools, dentro de este tenemos el Group Policy Management.



Una vez abramos este apartado nos aparecerá la ventana como tal, vamos a modificar las políticas por default, esto para nada es recomendable si se quiere una mayor comprensión integridad debería crearse un nuevo documento de políticas en este caso seguiremos con el default



Seguidamente vamos a realizar el proceso de edición para esto damos click derecho y edit

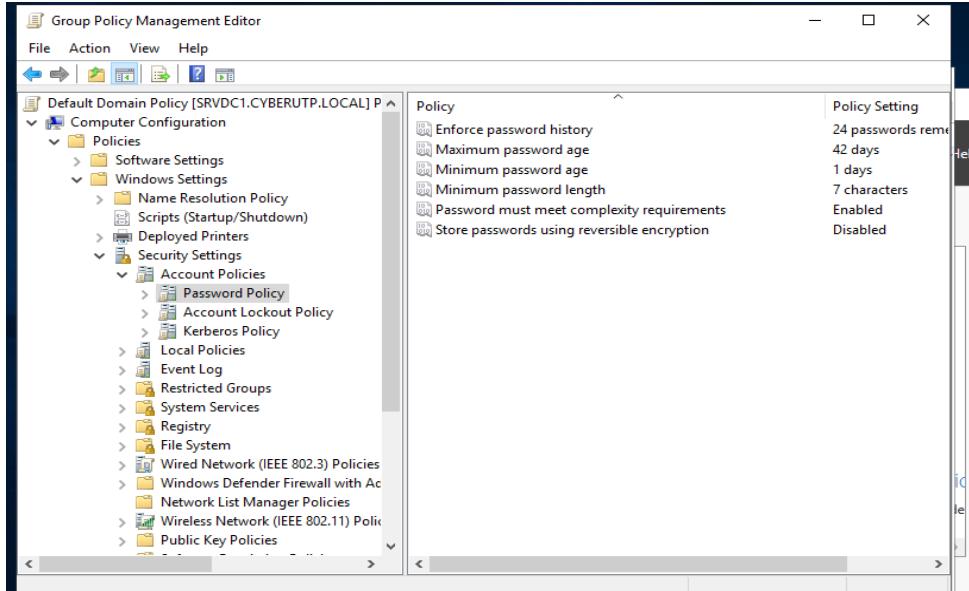


Se nos va a abrir la ventana de group policy management para la edición de las diferentes políticas

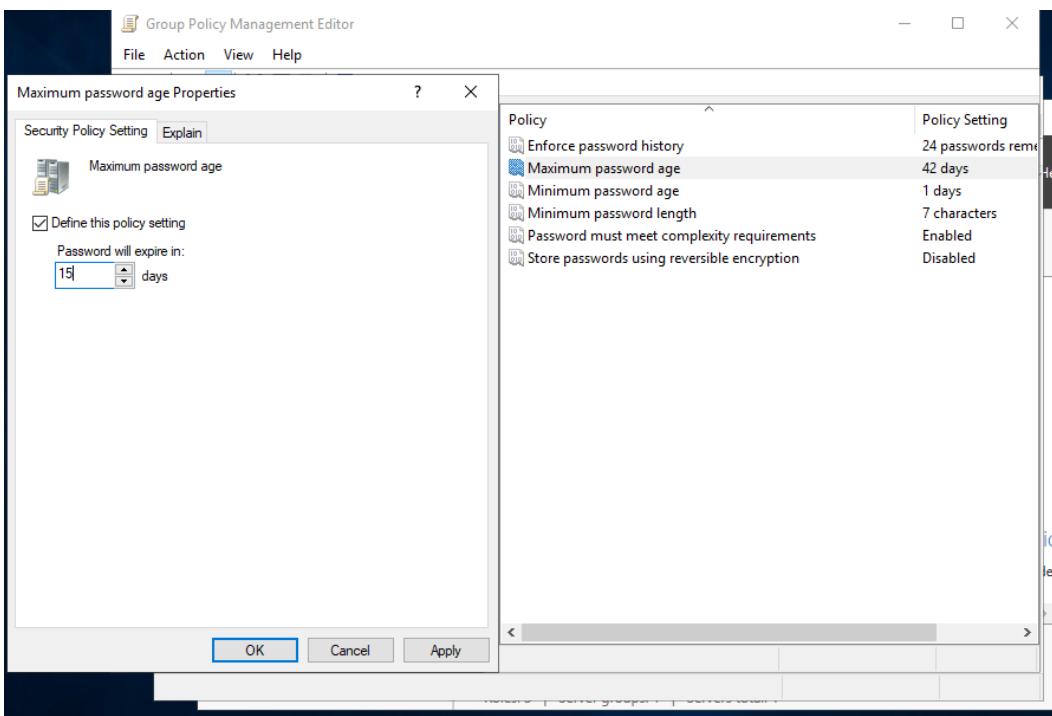
Directivas de configuración de equipo

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

Para realizar esta política tenemos que entrar a policies > Windows settings > security settings > account policies > password policy



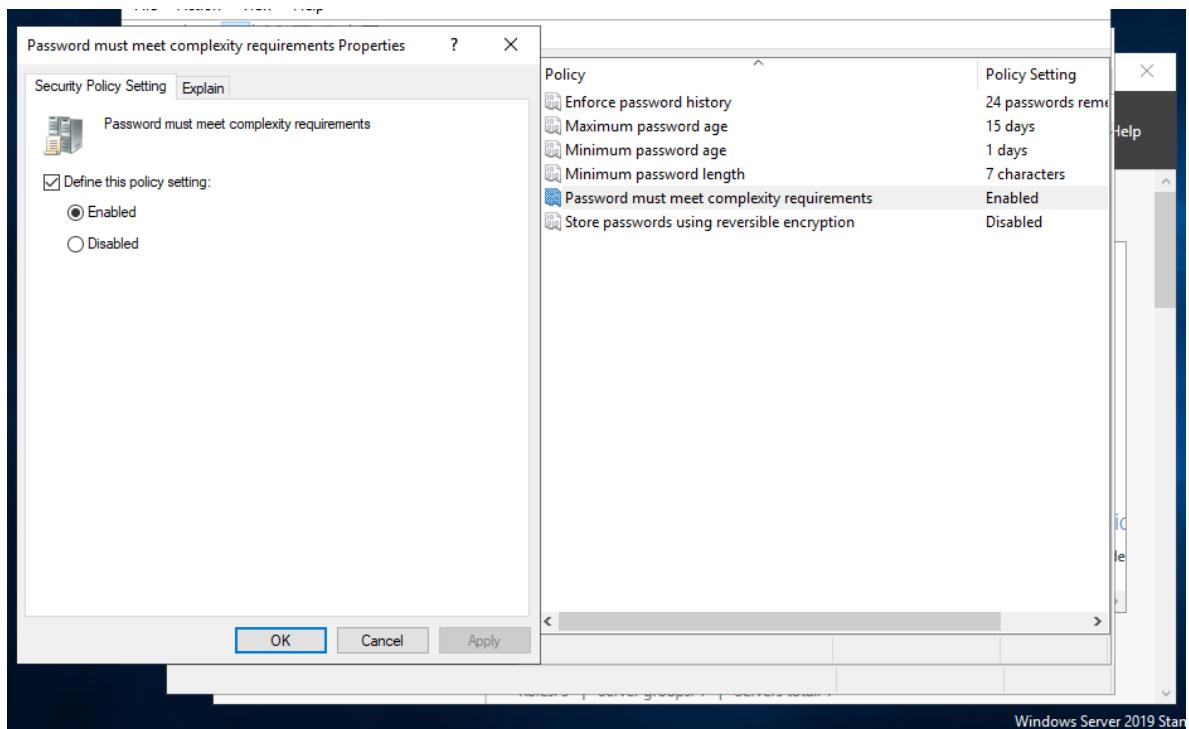
Dentro modificaremos la sección de maximum password age de 42 días a 15 días y posteriormente daremos a ok y apply con esto tendríamos la política activada.



Las contraseñas deben cumplir con los requisitos de complejidad por defecto de Windows server

Para realizar esta política tenemos que entrar a policies >Windows settings > security settings > account policies > password policy.

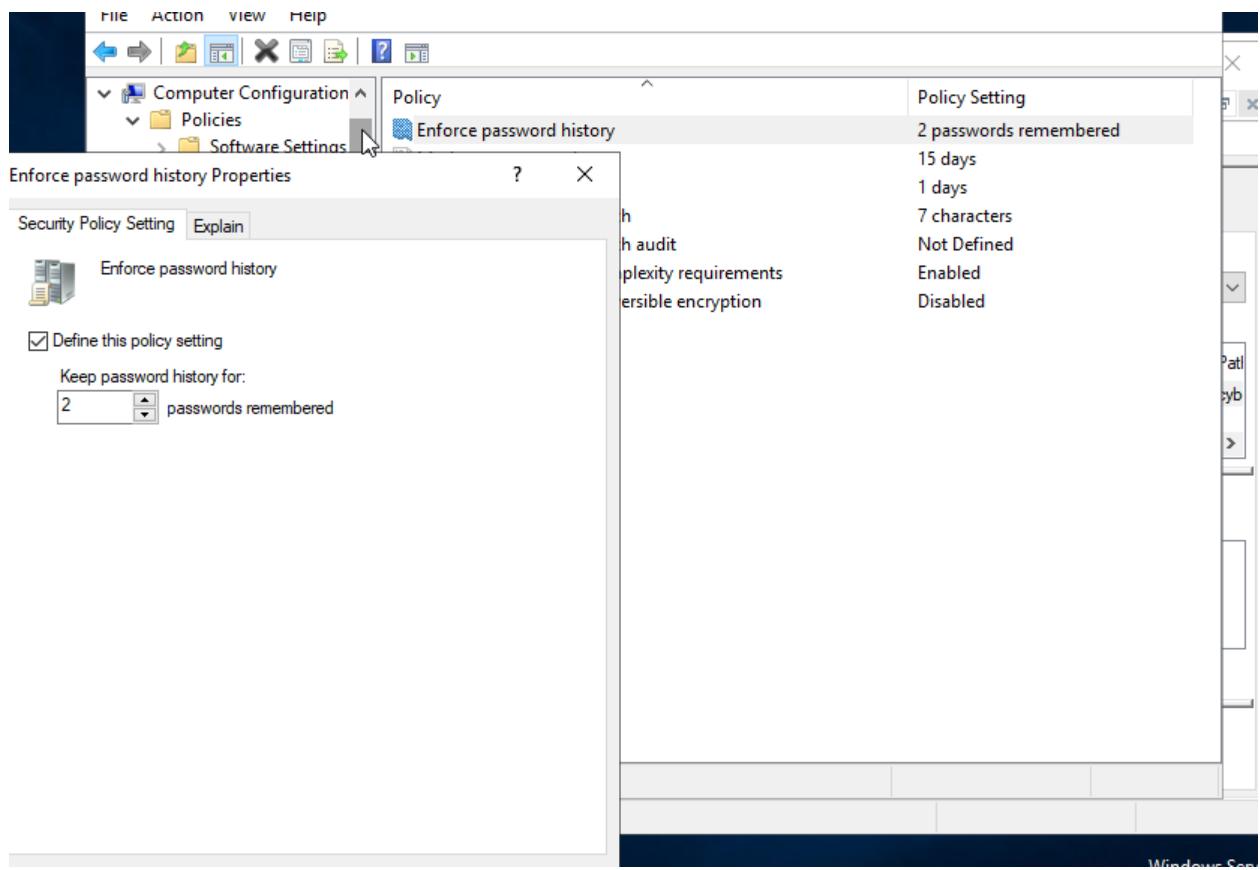
Dentro modificaremos la política password must meet complexity requirements y la dejaremos en enabled.



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.

Para realizar esta política tenemos que entrar a policies >Windows settings > security settings > account policies > password policy.

Dentro modificaremos la sección de enforced password history a 2

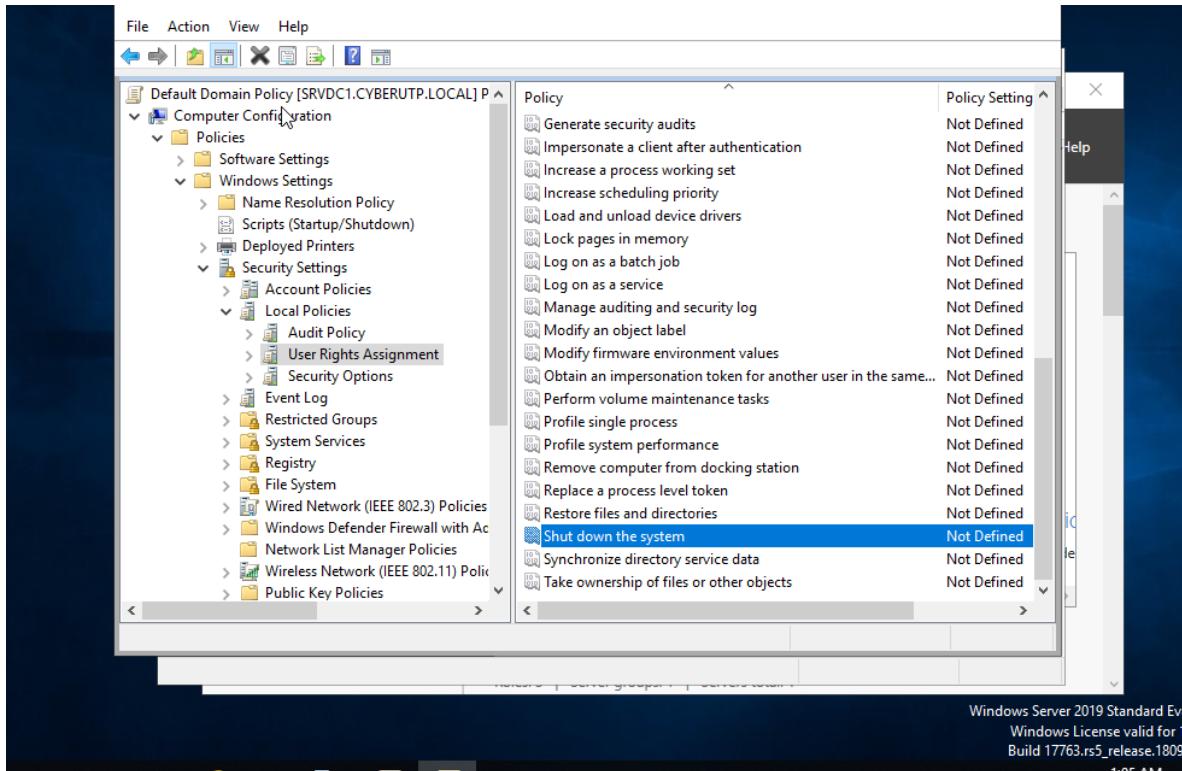


Finalmente tendríamos las políticas de contraseñas completadas

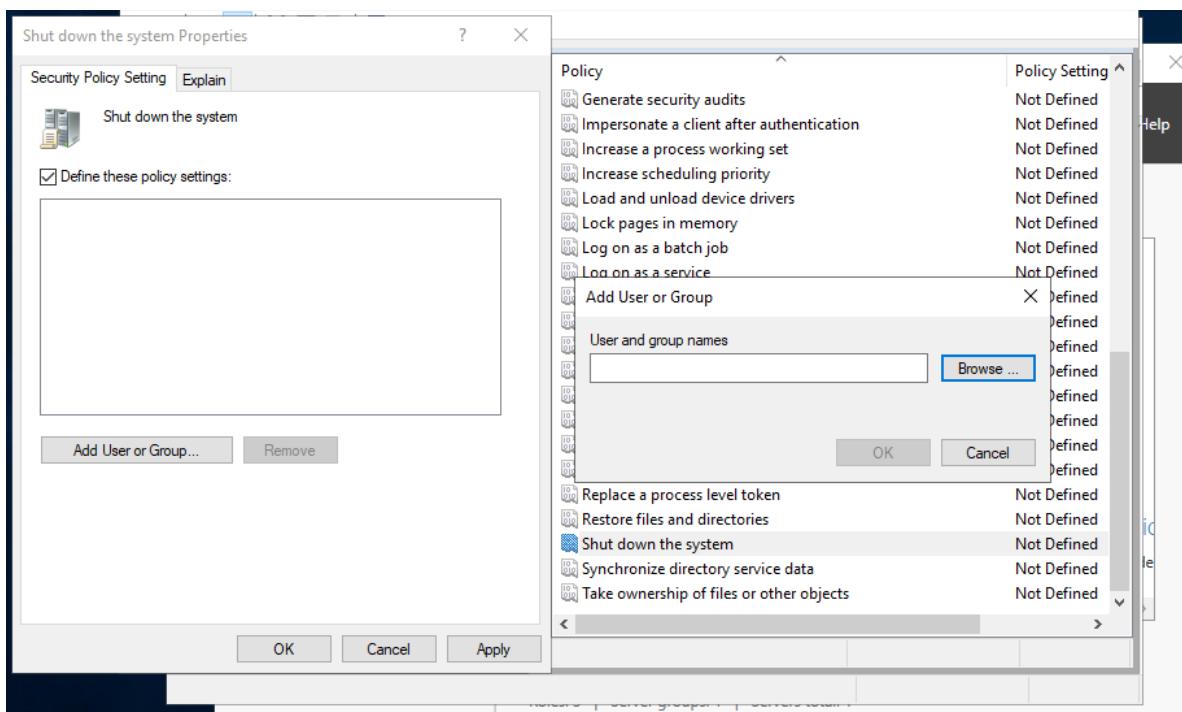
Policy	Policy Setting
Enforce password history	2 passwords remembered
Maximum password age	15 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Los usuarios del grupo Killers pueden apagar la máquina una vez hayan iniciado sesión, (Desde el sistema operativo)

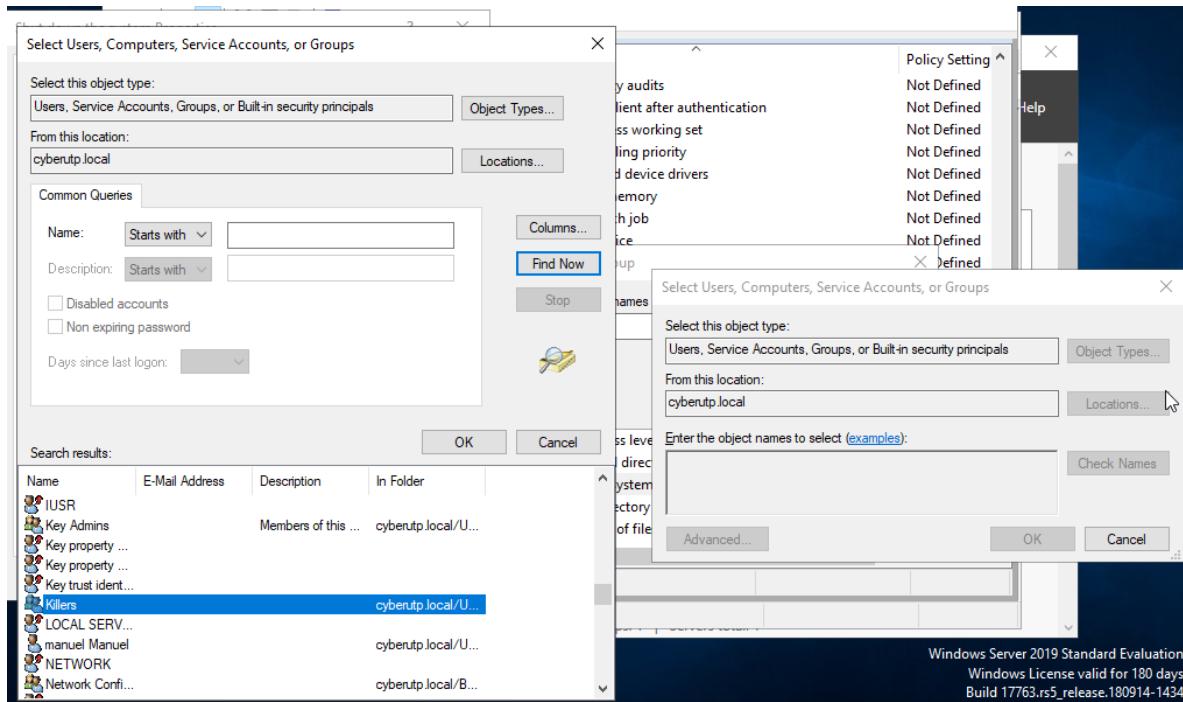
Esto se puede realizar desde policies> Windows settings>security settings > local policies> user rights assignment y modificaremos la que dice user rights assignment



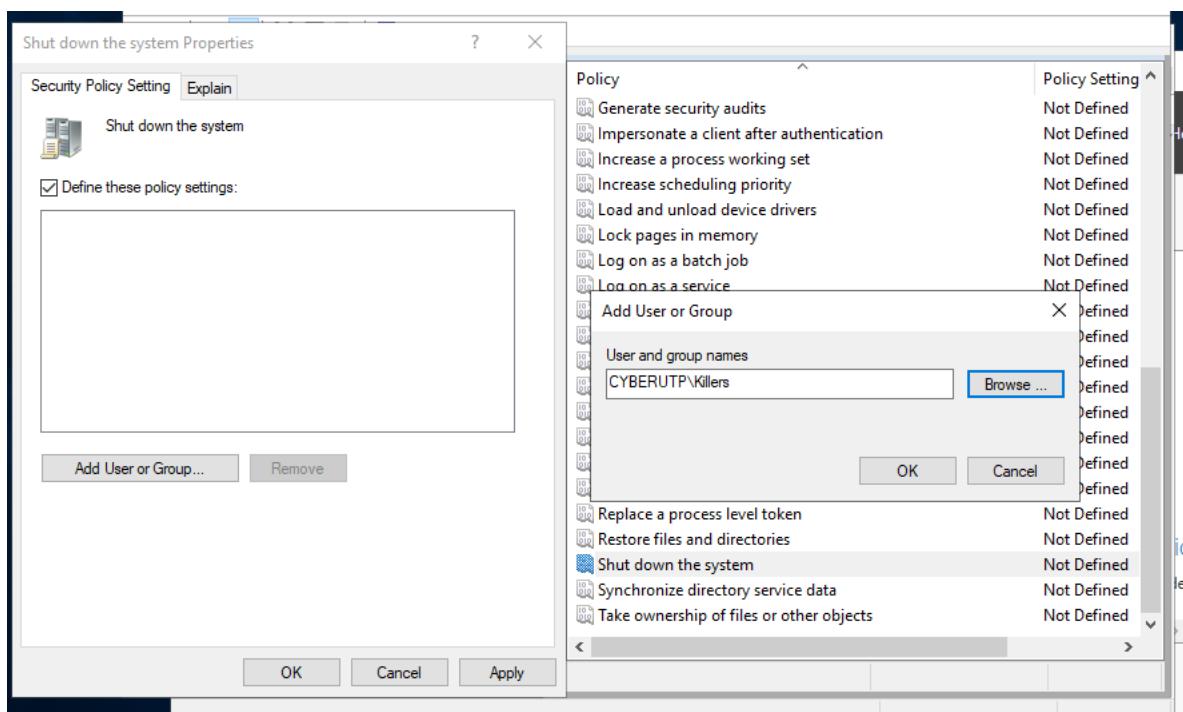
Agregamos con add user or group



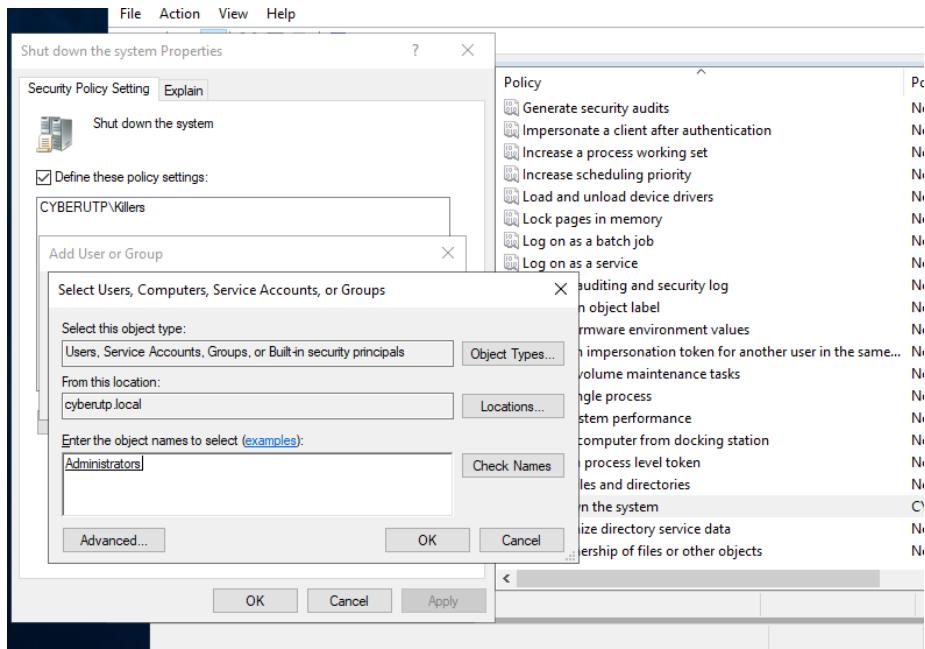
En este caso solo agregaremos a los killers dándole a find now y buscando el grupo



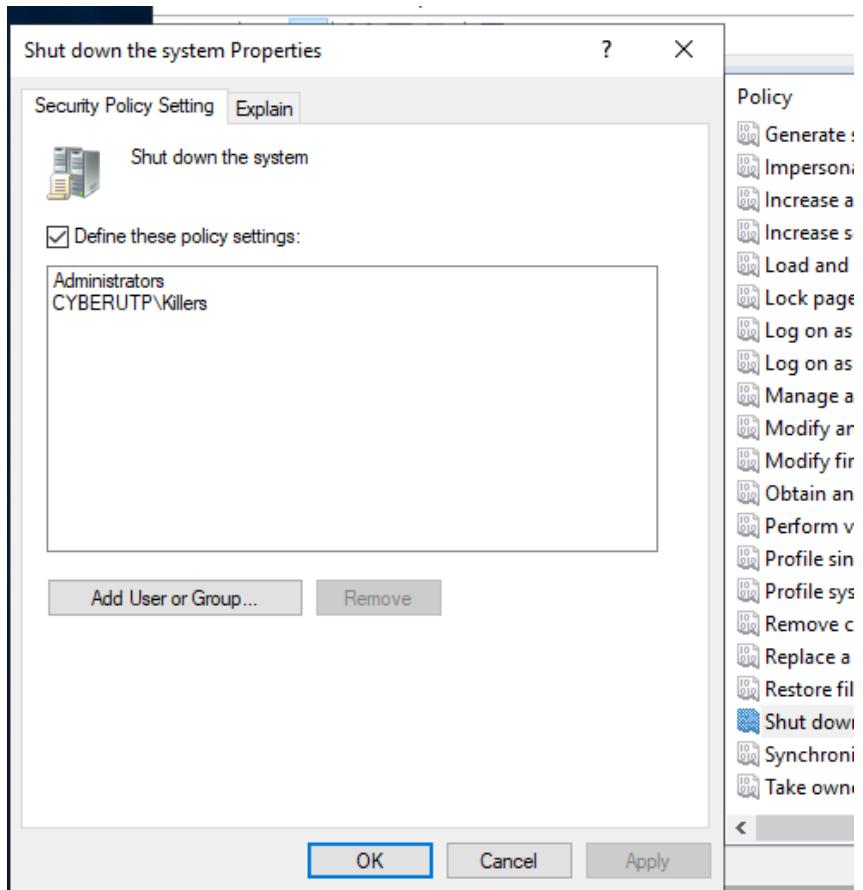
Vemos que se muestra en la pantalla el grupo



En este caso igual agregare al grupo administradores

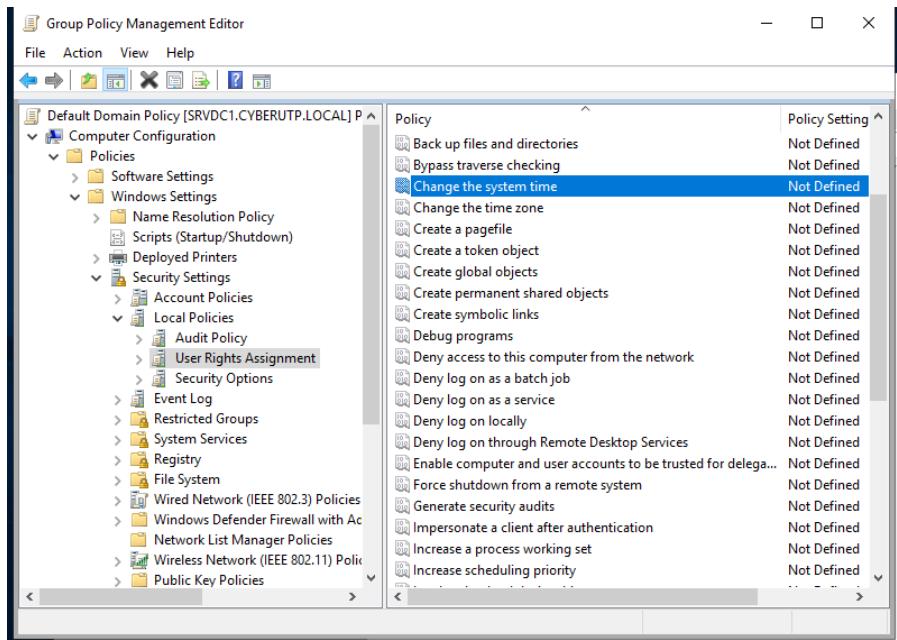


Una vez hecho esto ya tendremos a los dos equipos solo faltaría darle a apply y ok

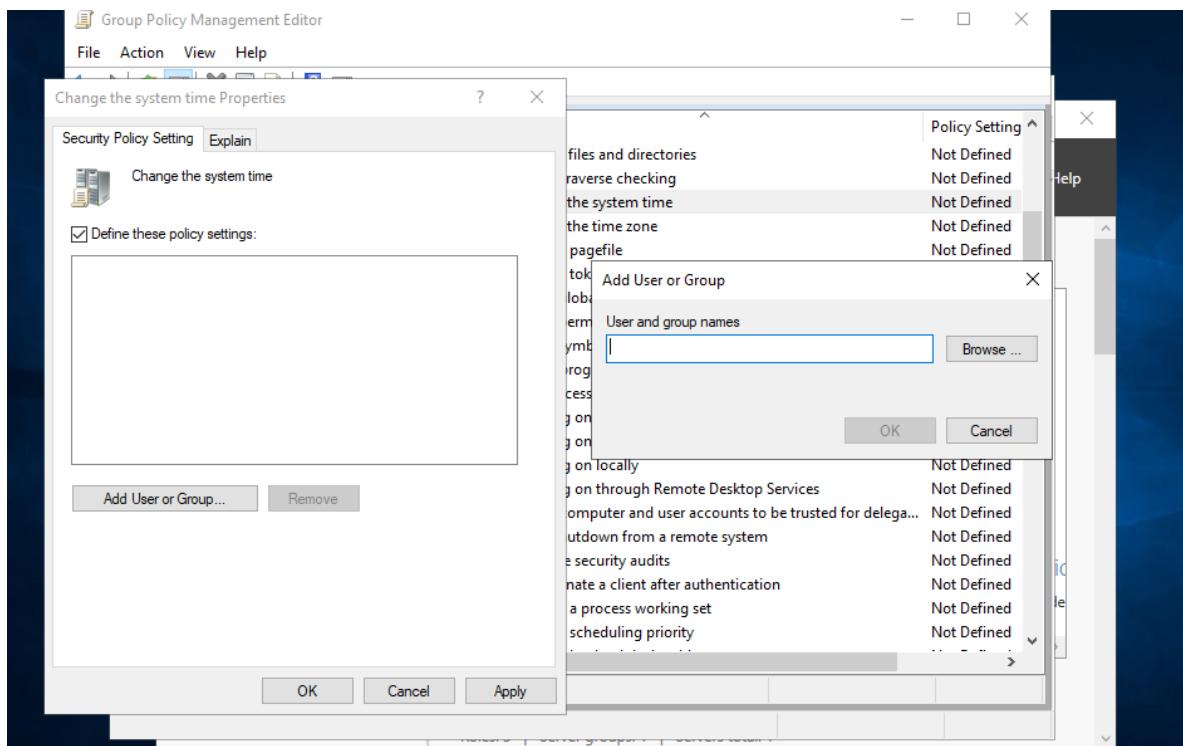


Los usuarios del grupo Timers podrán cambiar la hora de la máquina local.

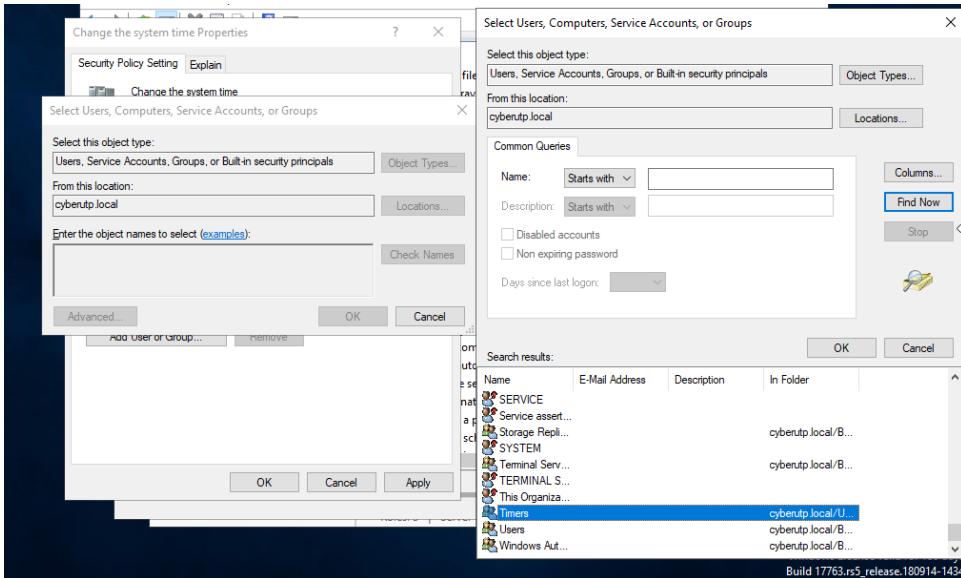
Ahora vamos a hacer que los timers puedan cambiar la hora del sistema en este caso en local policies dentro de user rights assignment modificaremos change the system time.



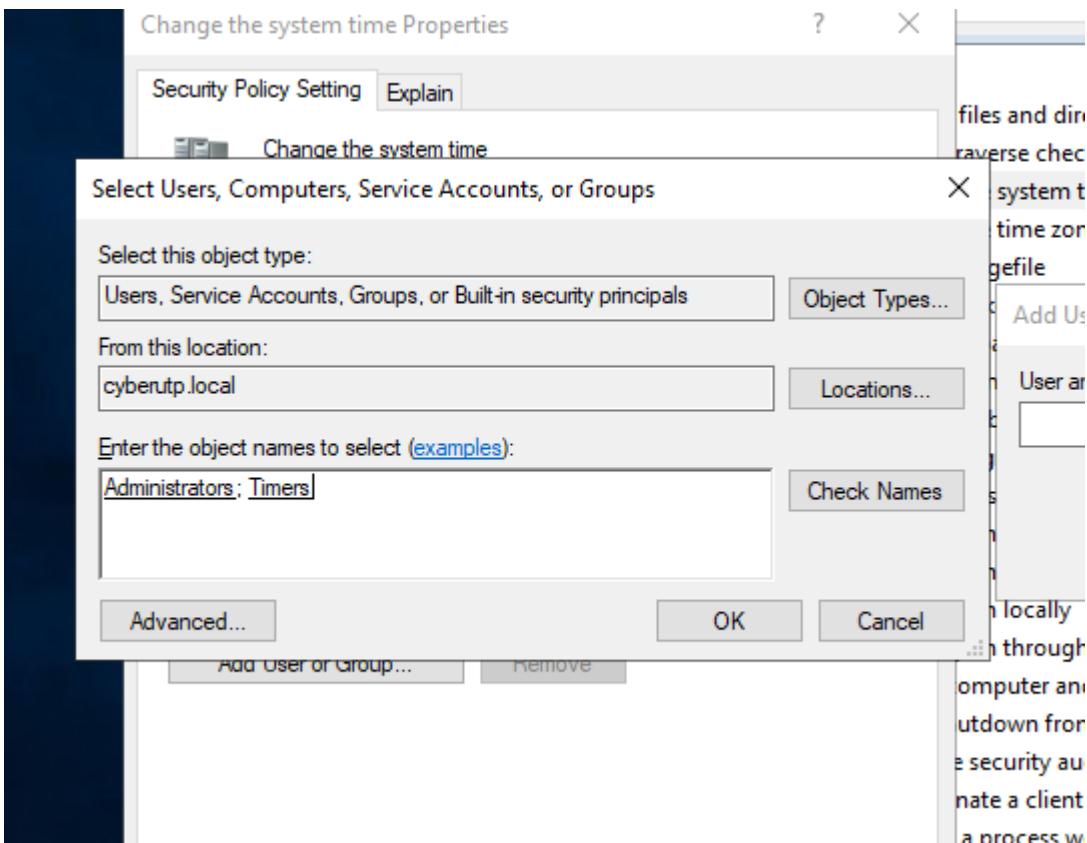
Agregaremos en este caso a los timers y a los administradores



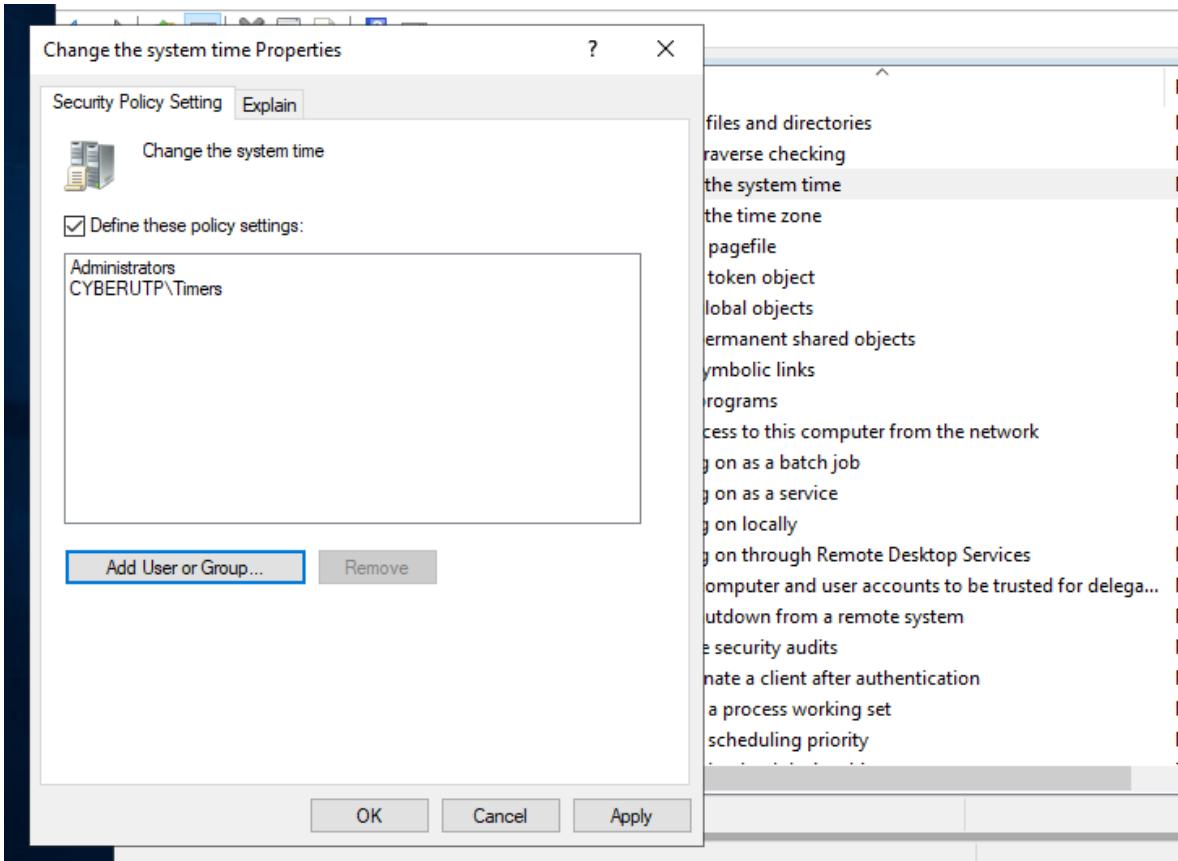
Con advanced y luego find now encontraremos a los timers



Agregamos también a los administradores

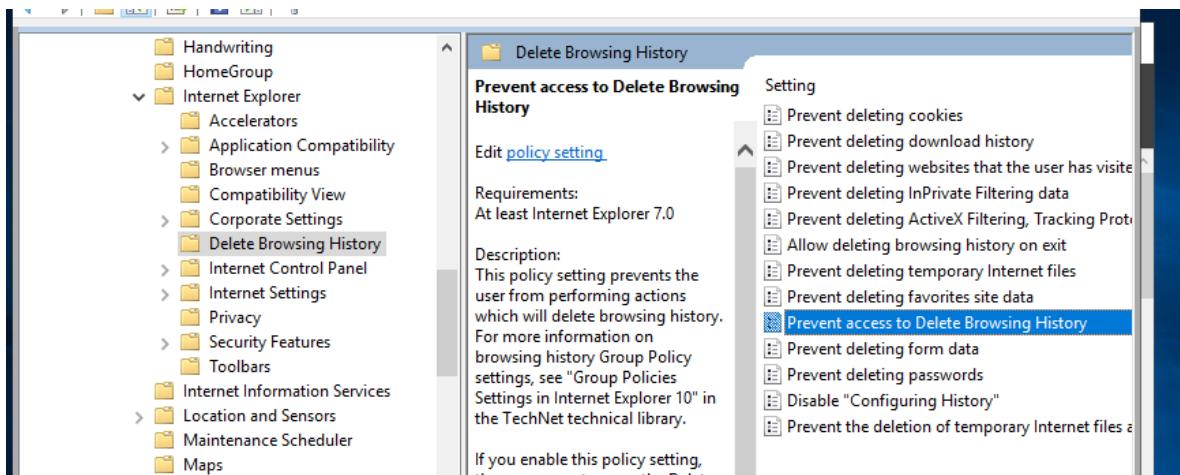


Damos a apply y luego ok con eso habríamos agregado a los administradores

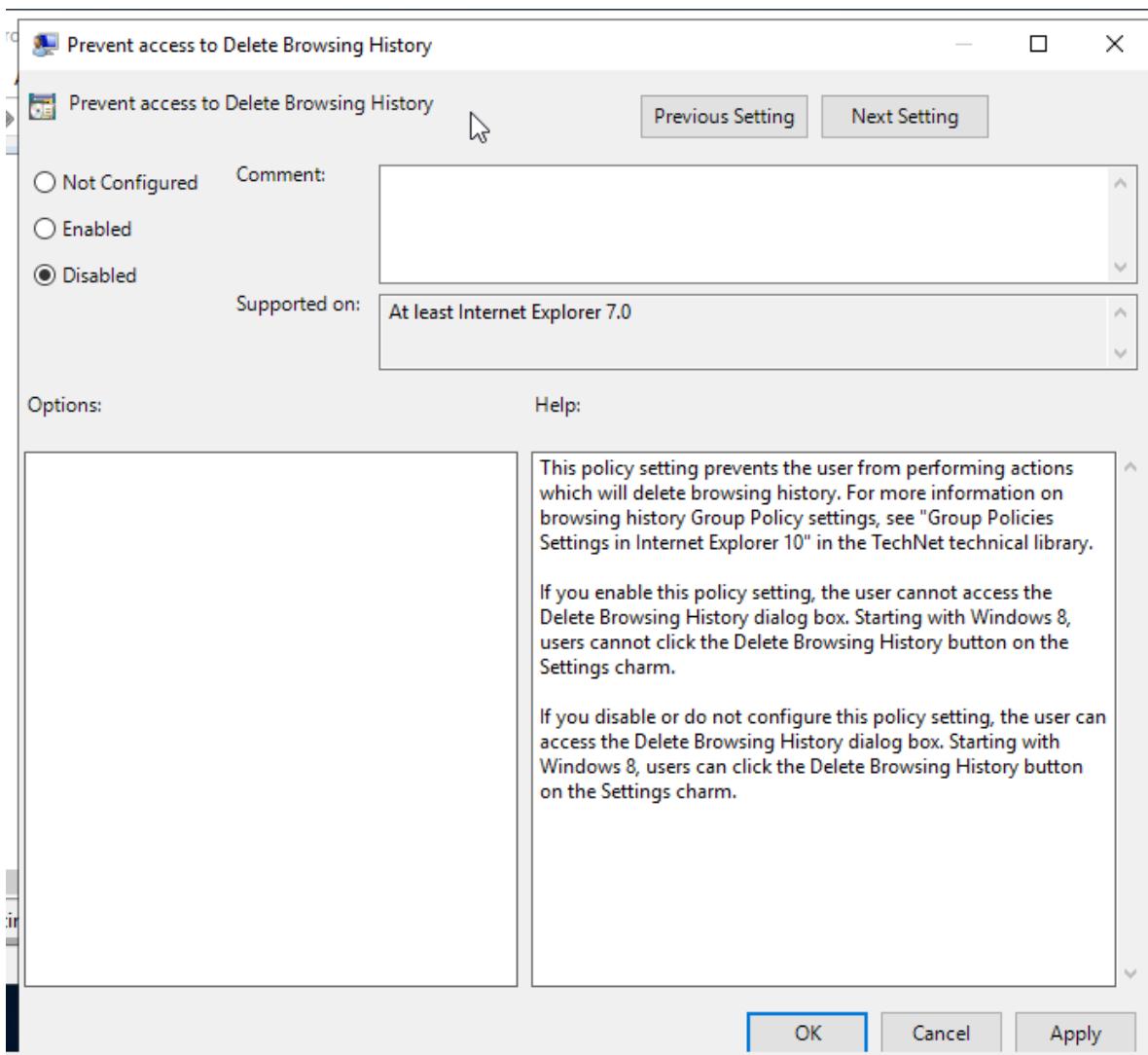


Todos los usuarios tendrán las siguientes restricciones al usar el navegador Internet Explorer:
No podrán eliminar el historial de navegación, No se permitirá el cambio de proxy ya que todos los usuarios usarán el mismo proxy (172.20.49.51:80), Configuración del historial deshabilitada, no permitir el cambio de las directivas de seguridad del navegador

Dentro de delete browser history vamos a modificar la política de prevent acces to delete browsing history

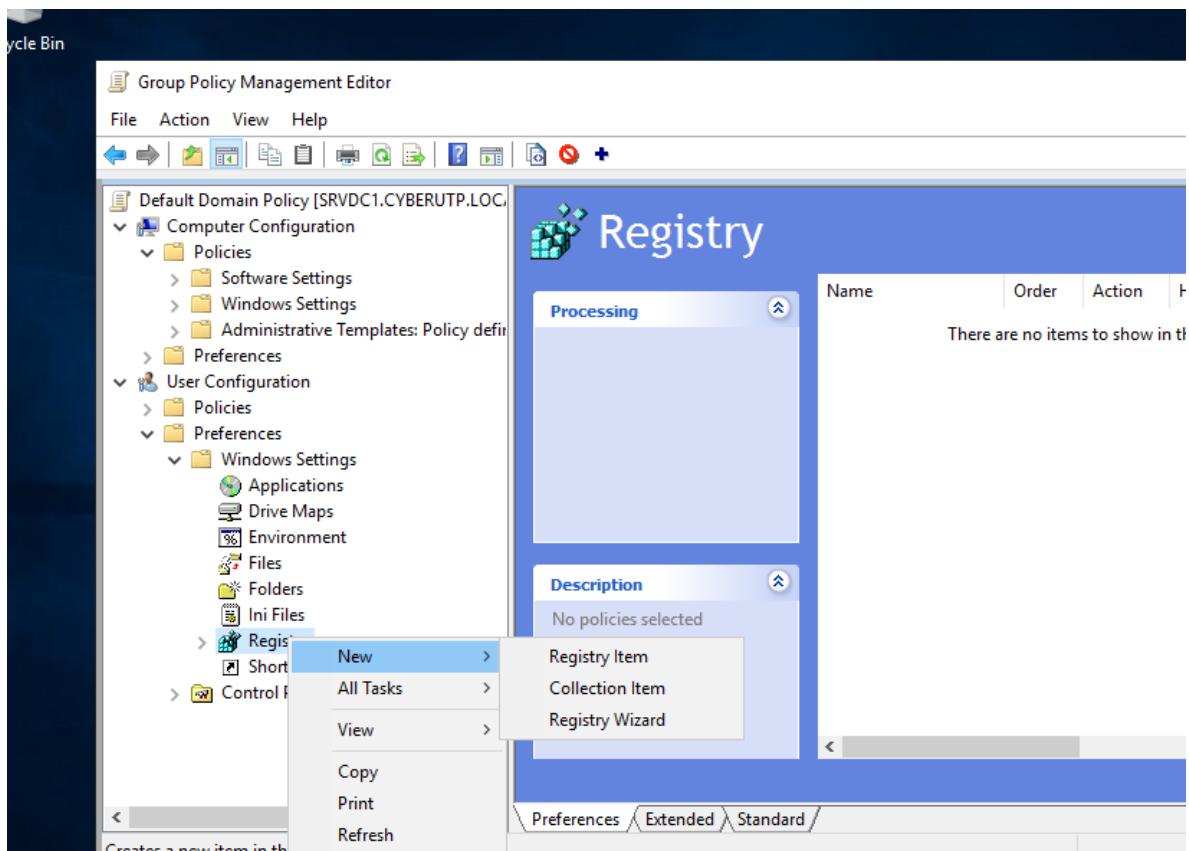


La vamos a deshabilitar



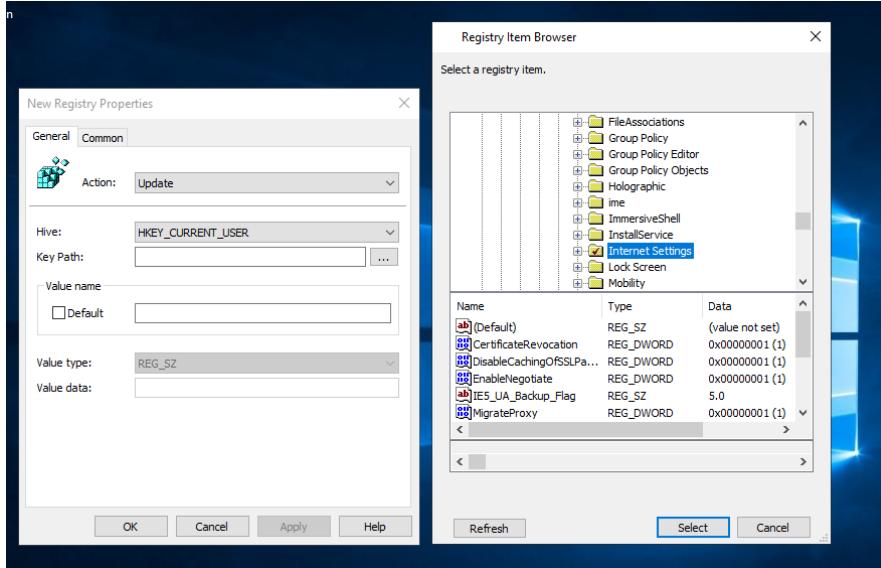
event deleting favorites site data	Not configured
event access to Delete Browsing History	Disabled

Ahora vamos a configurar el proxy por defecto que tendrá todos los dispositivos, para esto vamos dentro de user configuration al registry y crearemos los siguientes archivos

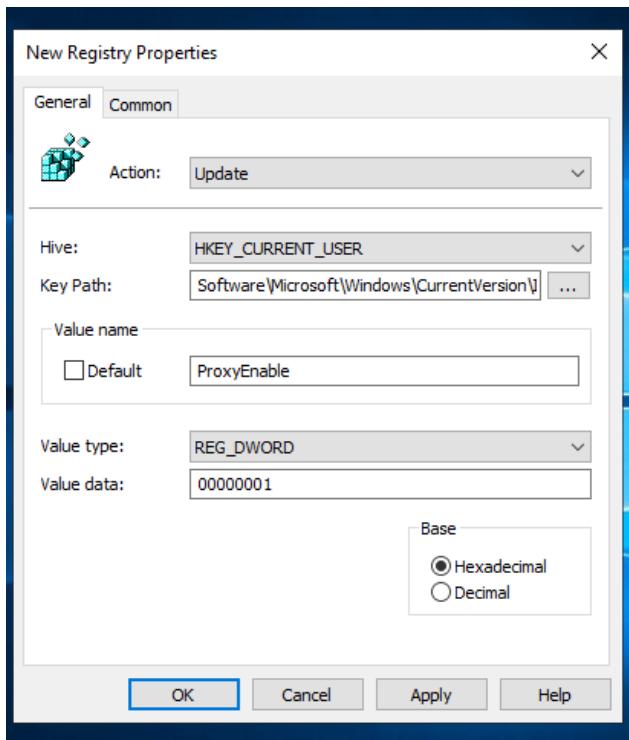


Todas estas modificaciones se harán bajo la siguiente dirección

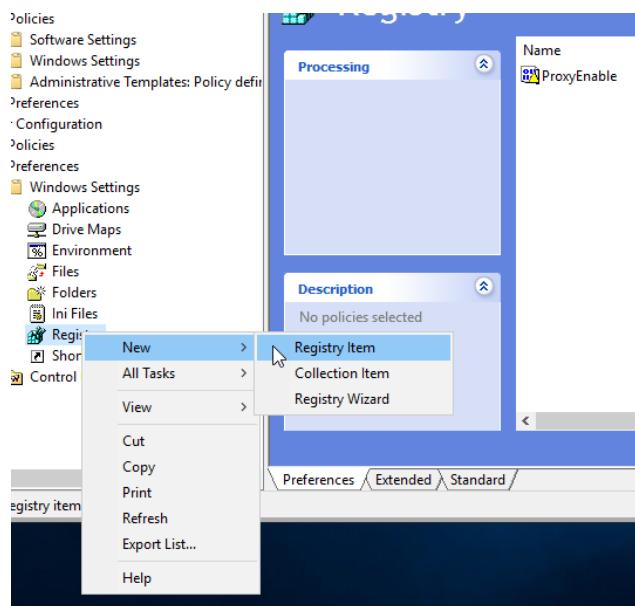
current_user>software>Microsoft>Windows>current versión>internet settings



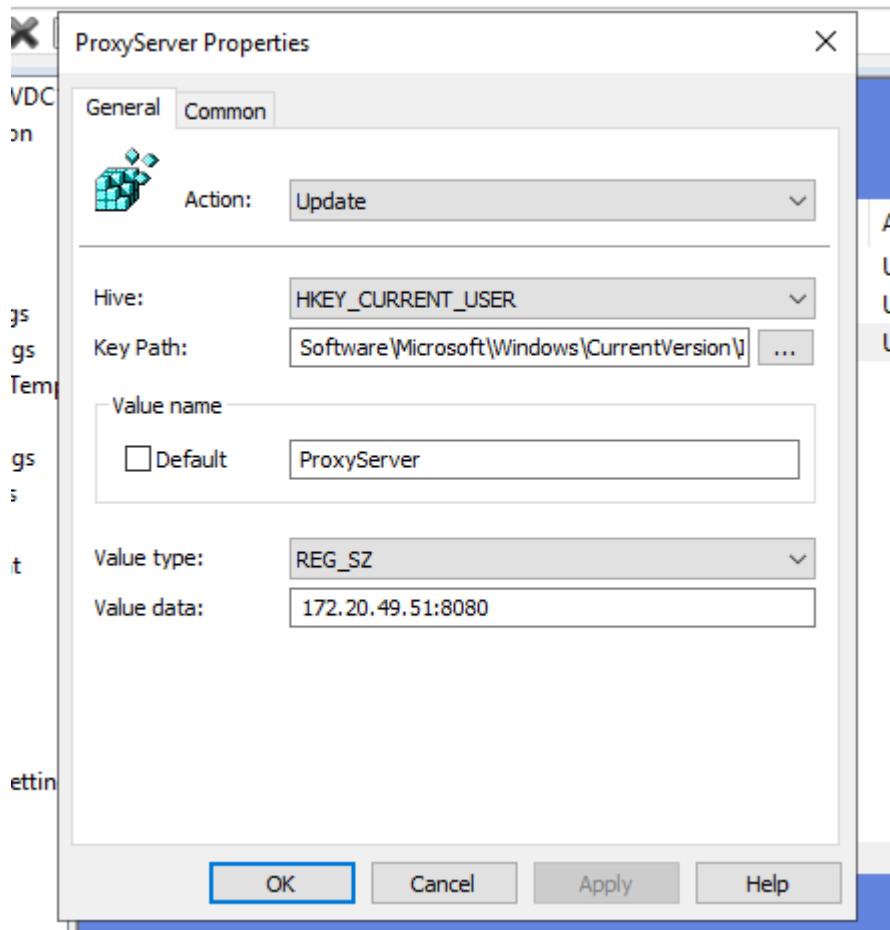
Creamos el proxy enable para levantar el proxy, ponemos el value data 00000001 y un value type de REG_DWORD



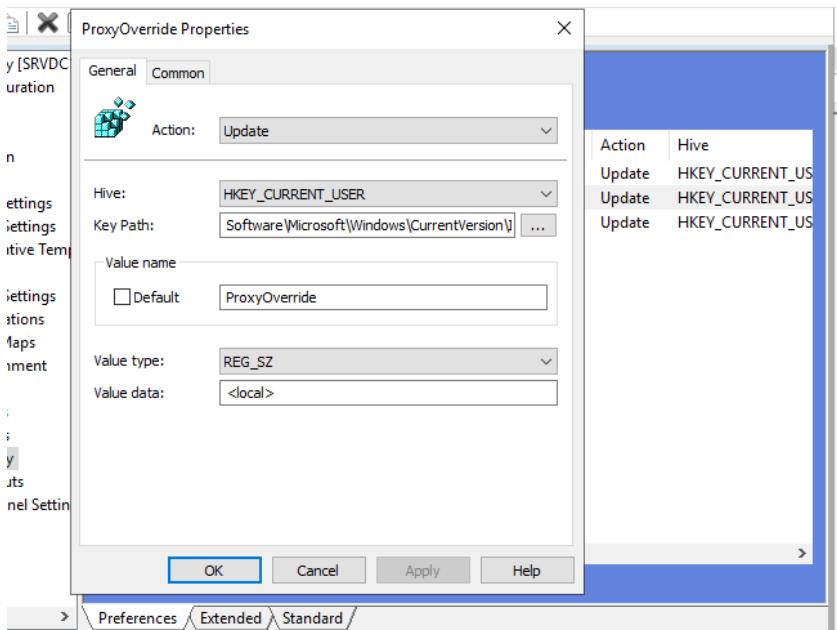
Crearemos otro item



En este caso es el servidor proxy al cual nos queremos conectar por defecto

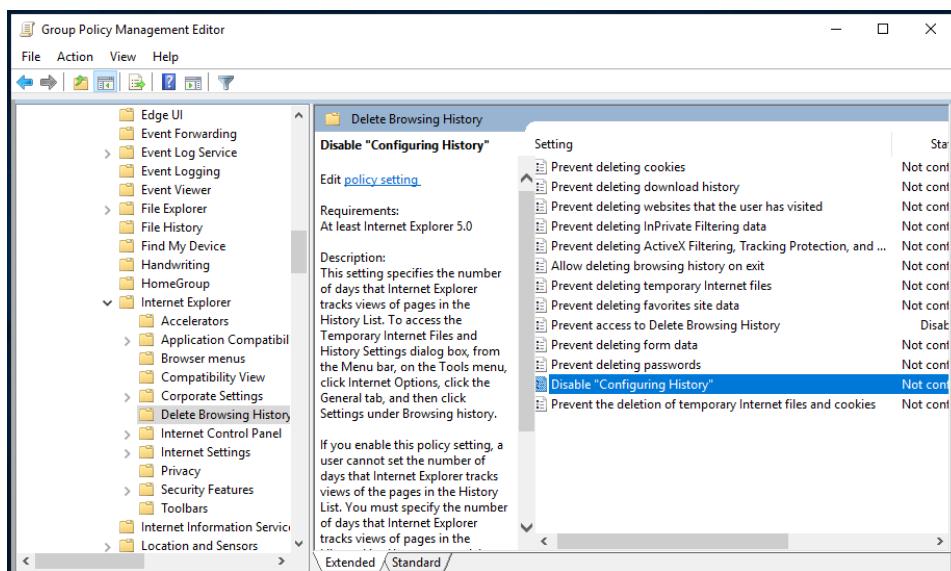


Y luego crearemos el proxy override

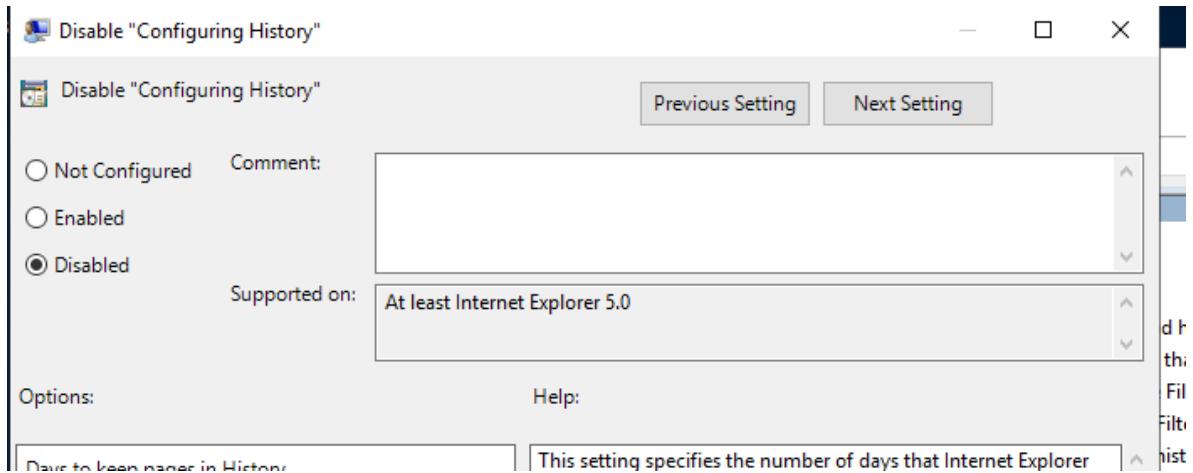


Con eso ya tendríamos el proxy activado

Ahora vamos a deshabilitar la configuración del historial dentro de delete browsng history



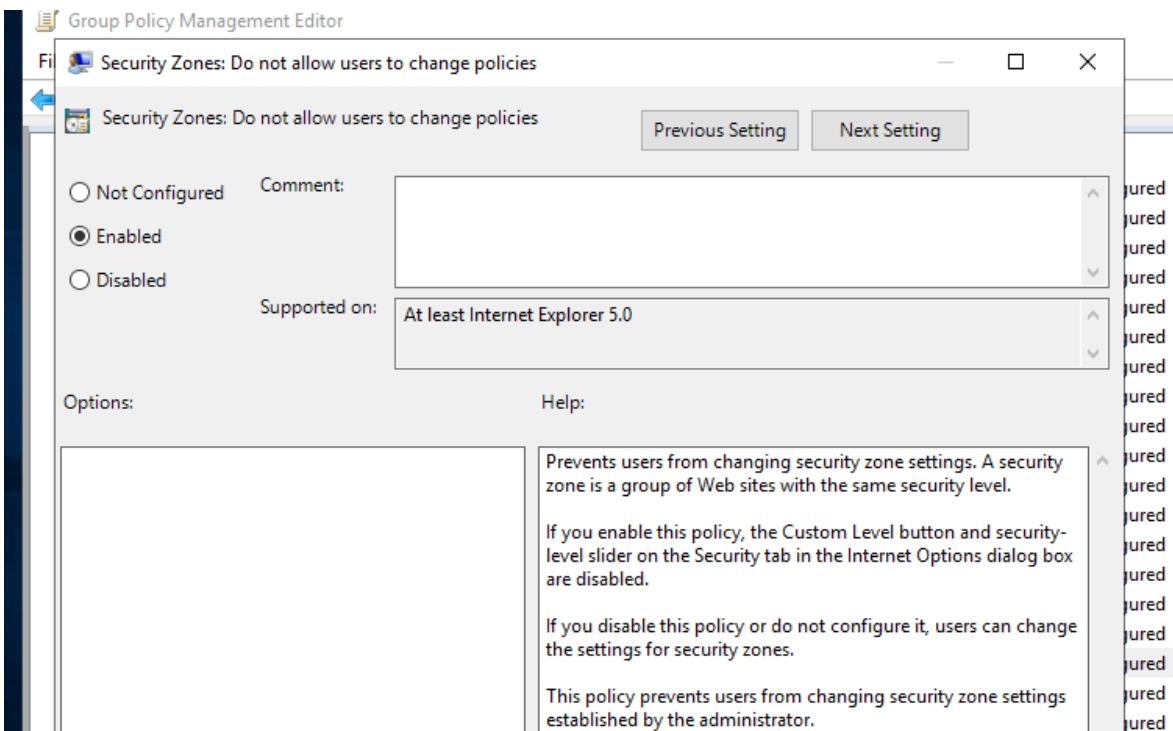
La desabilitamos



Por ultimo vamos a impedir que los usuarios cambien las directivas en internet explorer security zones: do not allow users to change policies

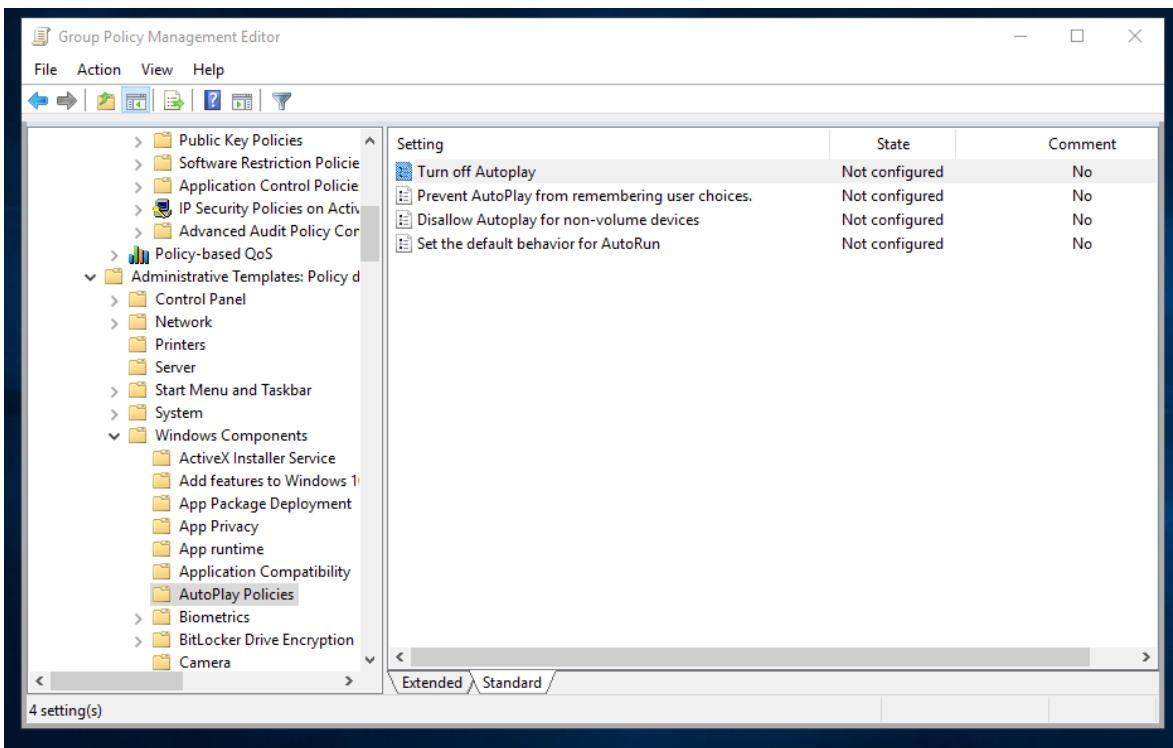
Setting	State	Comment
Disable Periodic Check for Internet Explorer software updates	Not configured	No
Prevent configuration of how windows open	Not configured	No
Specify use of ActiveX Installer Service for installation of Acti...	Not configured	No
Pop-up allow list	Not configured	No
Disable changing Automatic Configuration settings	Not configured	No
Disable changing connection settings	Not configured	No
Send all sites not included in the Enterprise Mode Site List to...	Not configured	No
Prevent managing pop-up exception list	Not configured	No
Turn off pop-up management	Not configured	No
Prevent changing proxy settings	Not configured	No
Turn off the auto-complete feature for web addresses	Not configured	No
Prevent participation in the Customer Experience Improvem...	Not configured	No
Turn off suggestions for all user-installed providers	Not configured	No
Turn off the quick pick menu	Not configured	No
Disable changing secondary home page settings	Not configured	No
Security Zones: Use only machine settings	Not configured	No
Security Zones: Do not allow users to change policies	Not configured	No
Security Zones: Do not allow users to add/delete sites	Not configured	No
Disable software update shell notifications on program laun...	Not configured	No
Show message when opening sites in Microsoft Edge using ...	Not configured	No

71 setting(s)

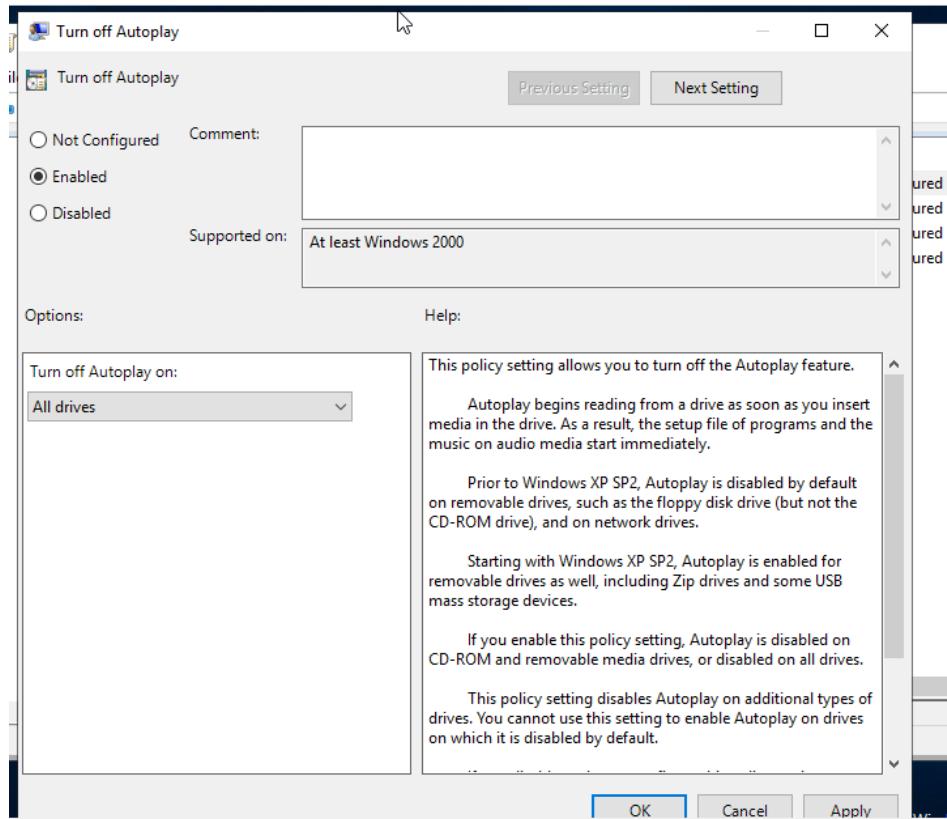


Desactivar la ventana emergente de reproducción automática

Dentro de autoplay policies modificamos el turn off autoplay



Lo habilitamos

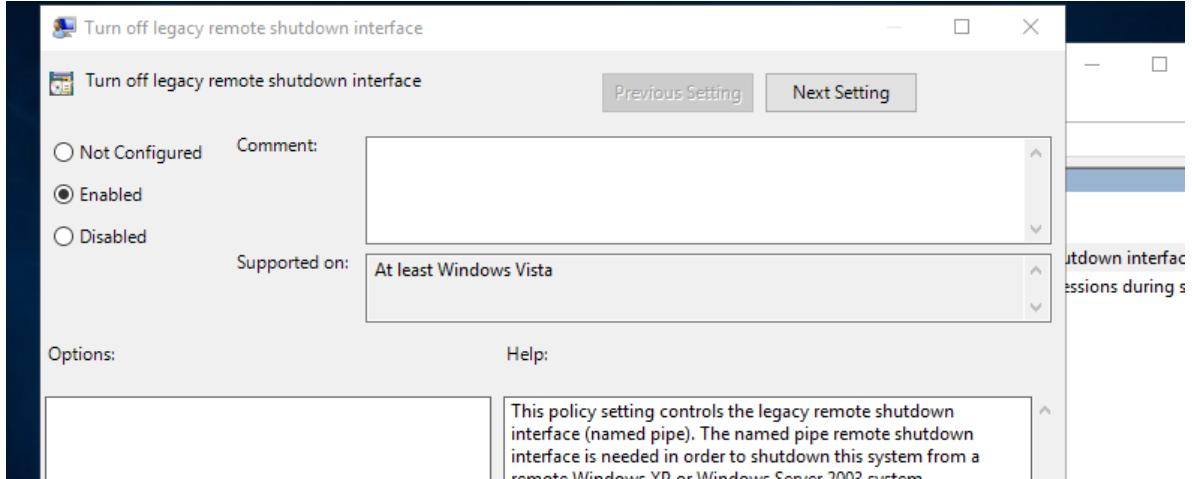


No permitir el apagado remoto de la máquina.

Esto lo modificamos en shutdown options la que dice turn off legacy remote shutdown interface

Turn off legacy remote shutdown interface	Setting
Edit policy setting	Turn off legacy remote shutdown interface
Requirements:	At least Windows Vista
Description:	This policy setting controls the legacy remote shutdown interface (named pipe). The named pipe remote shutdown interface is needed in order to shutdown this system from a remote Windows XP or Windows Server 2003 system.

La habilitamos

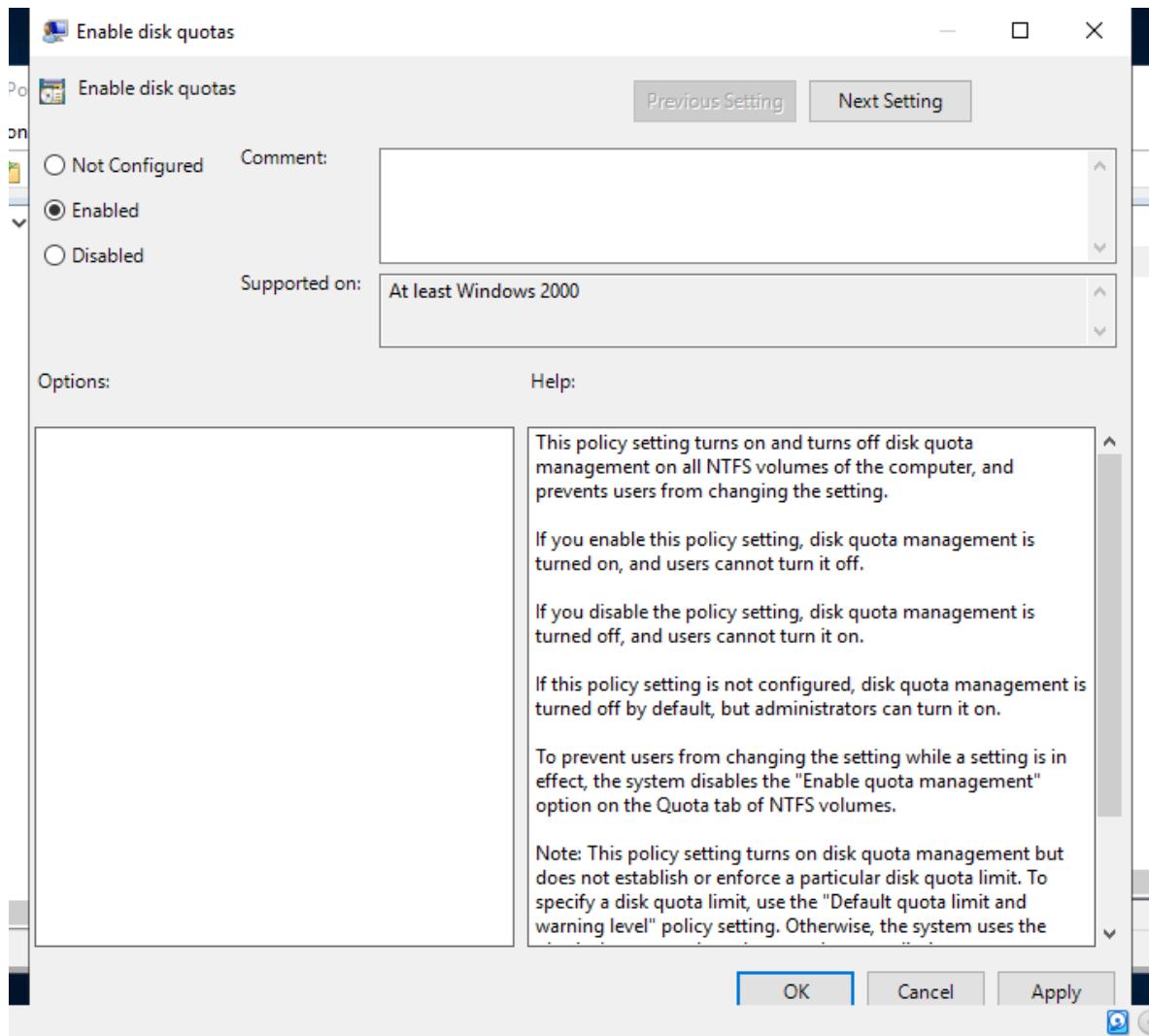


Aplicar cuotas de 50MB para todos los usuarios locales y remotos (Esta es un cuota muy baja y es usada solo para fines académicos)

En disk quotas modificamos la que dice enable disk quotas

Setting	State	Comment
Enable disk quotas	Not configured	No
Enforce disk quota limit	Not configured	No
Specify default quota limit and warning level	Not configured	No
Log event when quota limit is exceeded	Not configured	No
Log event when quota warning level is exceeded	Not configured	No
Apply policy to removable media	Not configured	No

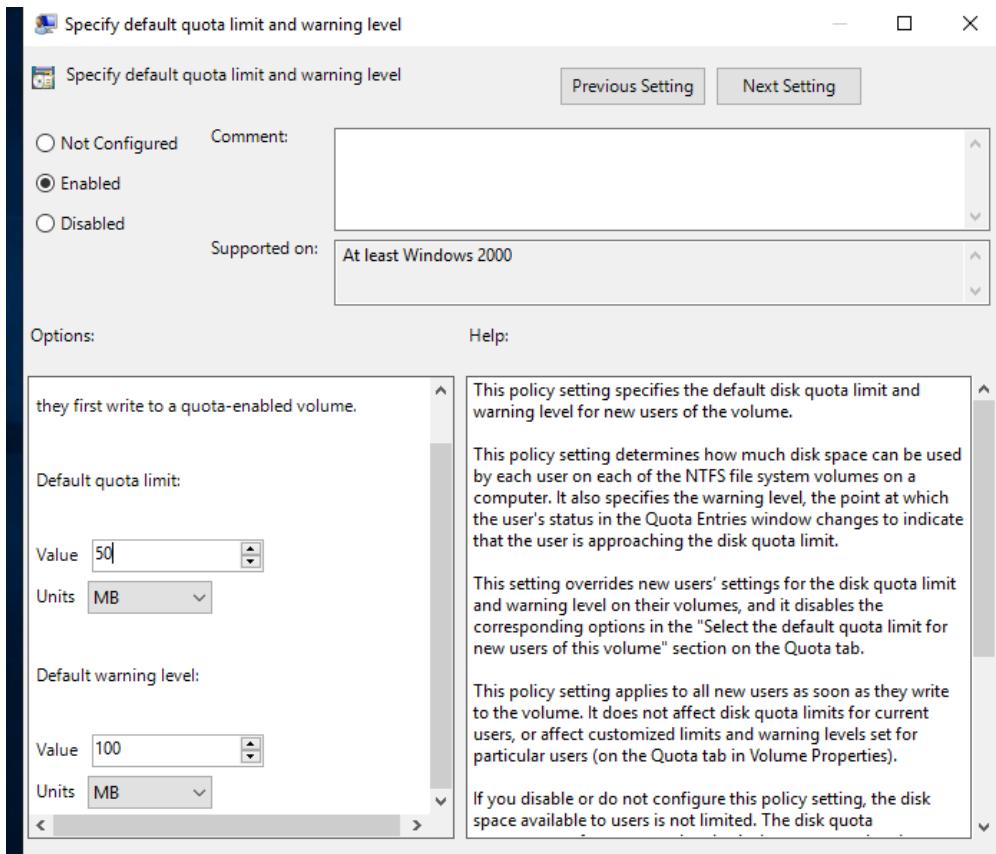
La habilitamos



Luego especificamos el límite de quotas en specify default quota limit

Setting	State
Enable disk quotas	Enabled
Enforce disk quota limit	Not configured
Specify default quota limit and warning level	Not configured
Log event when quota limit is exceeded	Not configured
Log event when quota warning level is exceeded	Not configured
Apply policy to removable media	Not configured

La seteamos en 50 mb



La página principal que se cargará para cada usuario cuando abra su navegador será:

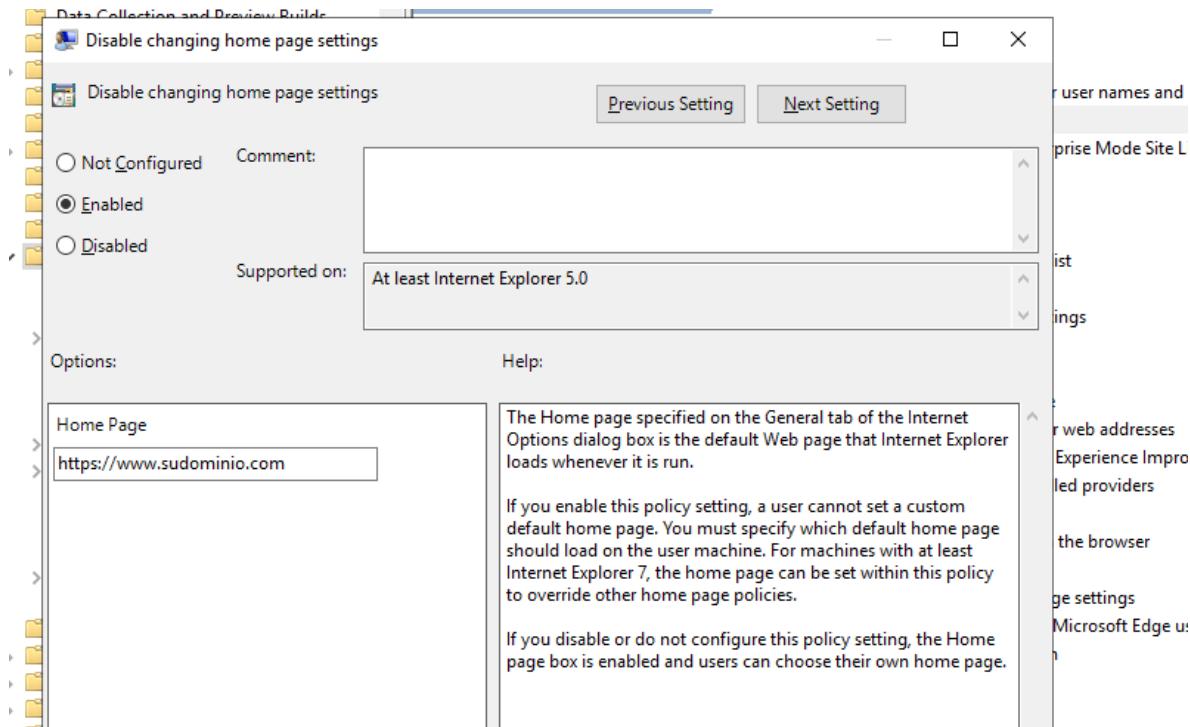
<http://www.sudominio.com> (Página institucional de su empresa)

En internet explorer activamos la que dice disable changing home page settings

Setting	State
Disable AutoComplete for forms	Not configured
Turn on the auto-complete feature for user names and pass...	Not configured
Disable changing home page settings	Enabled
Send all sites not included in the Enterprise Mode Site List to...	Not configured
Disable changing language settings	Not configured
Disable changing link color settings	Not configured
Disable changing Messaging settings	Not configured
Prevent managing pop-up exception list	Not configured
Turn off pop-up management	Not configured
Disable changing Profile Assistant settings	Not configured
Prevent changing proxy settings	Not configured
Disable changing ratings settings	Not configured
Disable the Reset Web Settings feature	Not configured
Turn off the auto-complete feature for web addresses	Not configured
Prevent participation in the Customer Experience Improvem...	Not configured
Turn off suggestions for all user-installed providers	Not configured
Turn off the quick pick menu	Not configured
Search: Disable Find Files via F3 within the browser	Not configured
Search: Disable Search Customization	Not configured

If you disable or do not configure this

Luego de habilitarla ponemos la home page

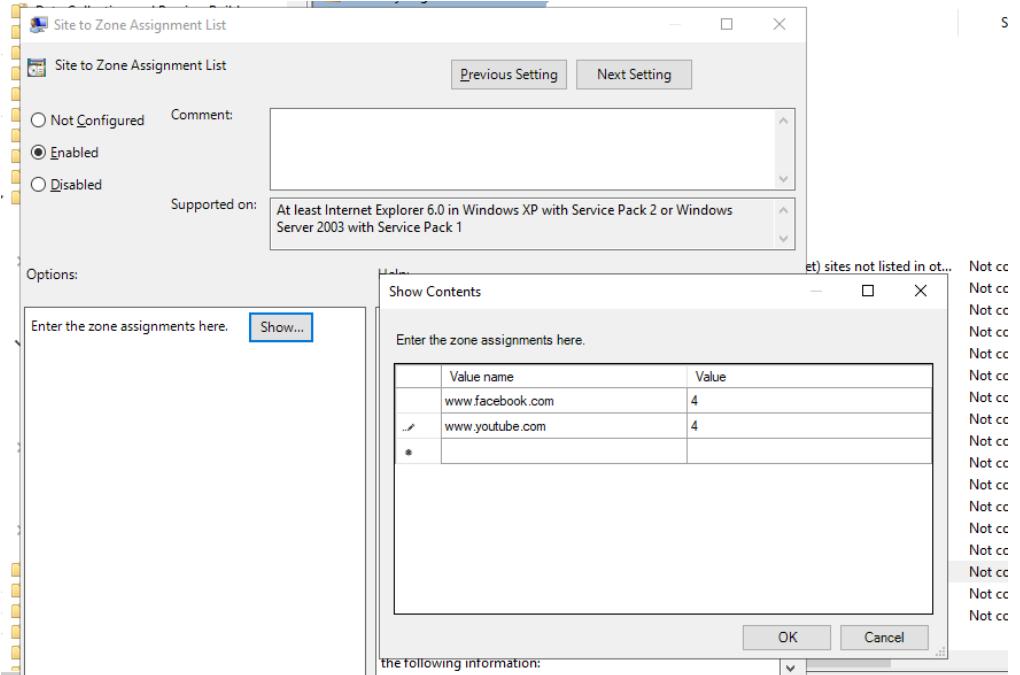


Restringir desde el navegador el acceso a los siguientes sitios: <http://www.facebook.com> y <http://www.youtube.com> por URL, para todos los usuarios.

Tocamos la que dice site to zone assignment list dentro de security page

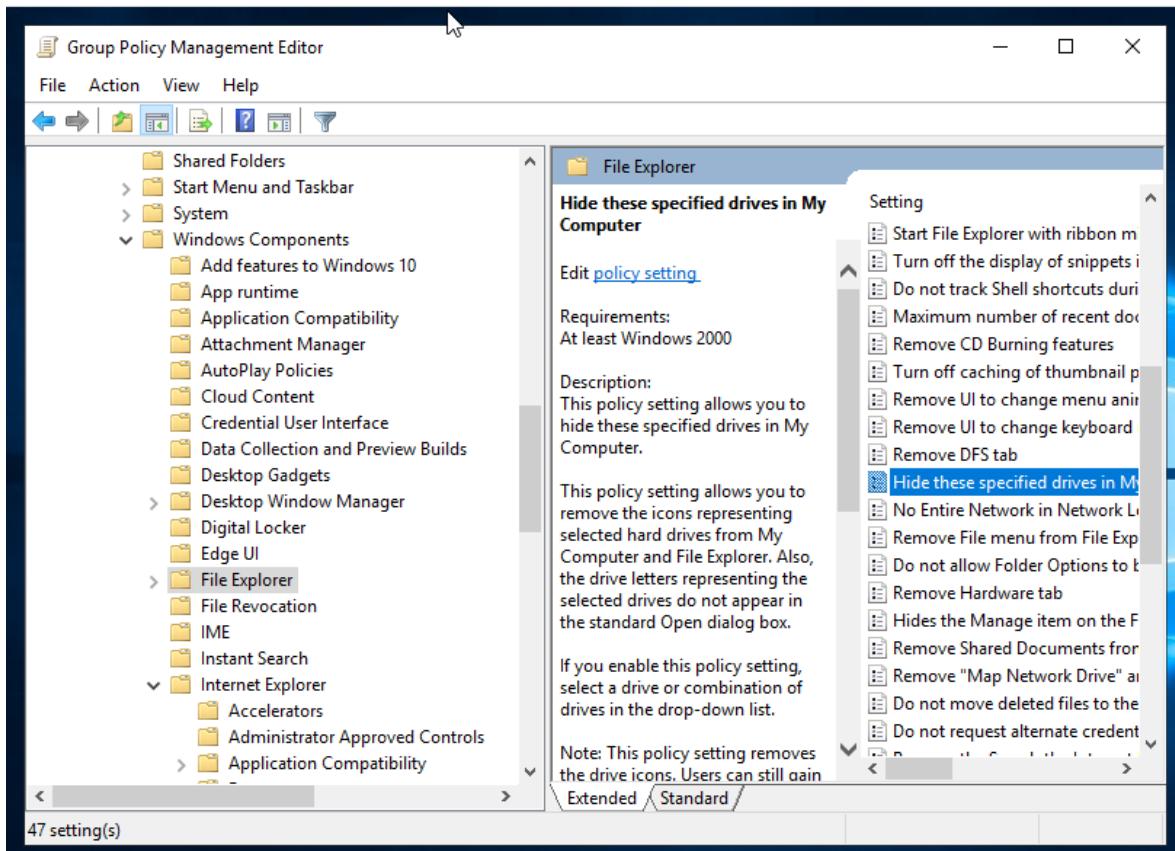
Setting	Status
Intranet Zone	Not configured
Local Machine Zone	Not configured
Locked-Down Internet Zone	Not configured
Locked-Down Intranet Zone	Not configured
Locked-Down Local Machine Zone	Not configured
Locked-Down Restricted Sites Zone	Not configured
Locked-Down Trusted Sites Zone	Not configured
Restricted Sites Zone	Not configured
Trusted Sites Zone	Not configured
Intranet Sites: Include all local (intranet) sites not listed in other zones	Not configured
Locked-Down Internet Zone Template	Not configured
Internet Zone Template	Not configured
Locked-Down Intranet Zone Template	Not configured
Intranet Zone Template	Not configured
Locked-Down Local Machine Zone Template	Not configured
Local Machine Zone Template	Not configured
Locked-Down Restricted Sites Zone Template	Not configured
Restricted Sites Zone Template	Not configured
Locked-Down Trusted Sites Zone Template	Not configured
Trusted Sites Zone Template	Not configured
Turn on certificate address mismatch warning	Not configured
Intranet Sites: Include all sites that bypass the proxy server	Not configured
Intranet Sites: Include all network paths (UNCs)	Not configured
Site to Zone Assignment List	Not configured
Turn on automatic detection of intranet	Not configured
Turn on Notification bar notification for intranet content	Not configured

La habilitamos y agregamos las paginas requeridas

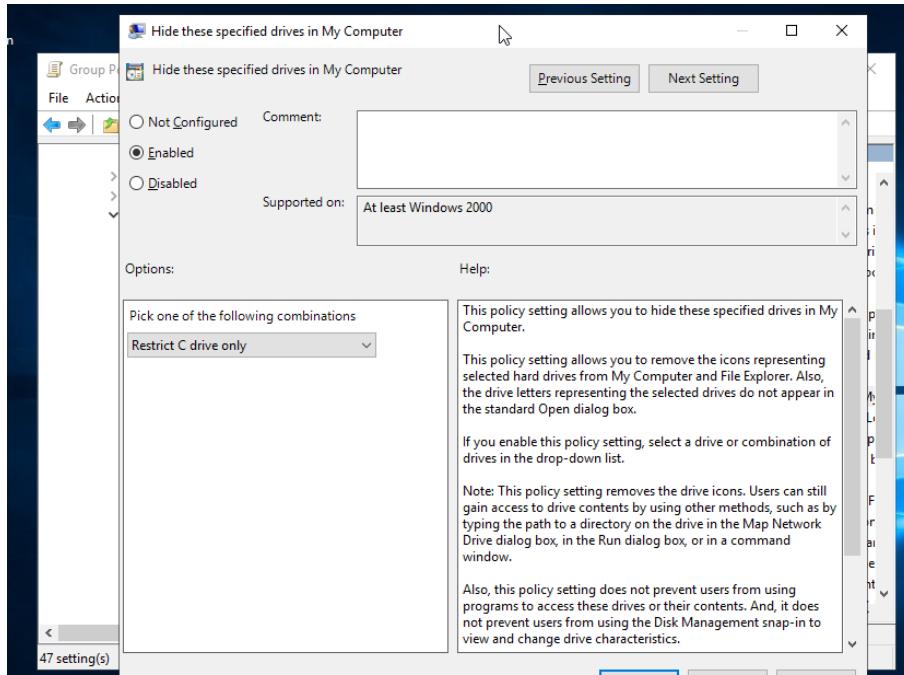


Ocultar la unidad C:\ (NOTA: Esto no restringirá el acceso a dicha unidad)

Para esto tocamos dentro de file explorerr la que dice hide these specified drives in my computer

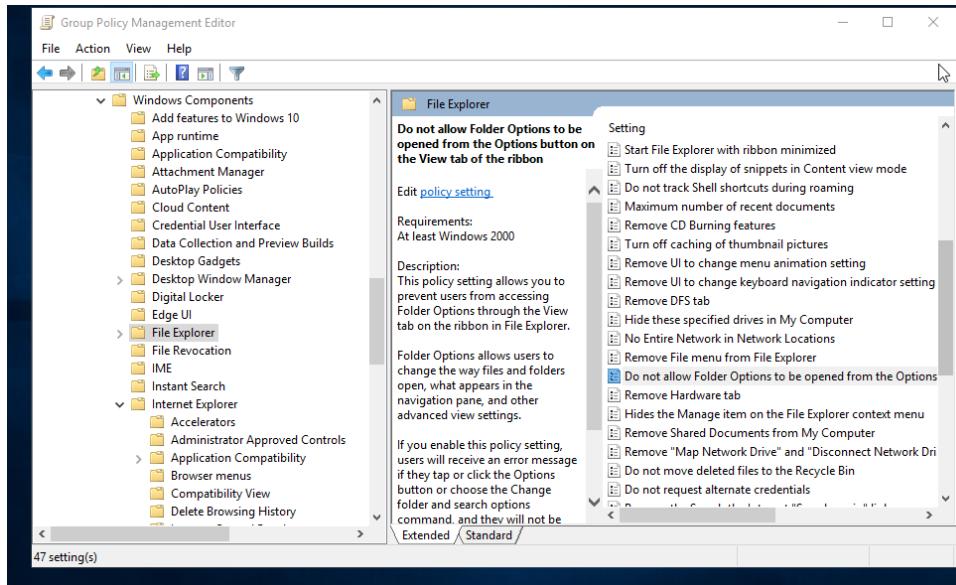


La habilitamos y agregamos el disco que queramos

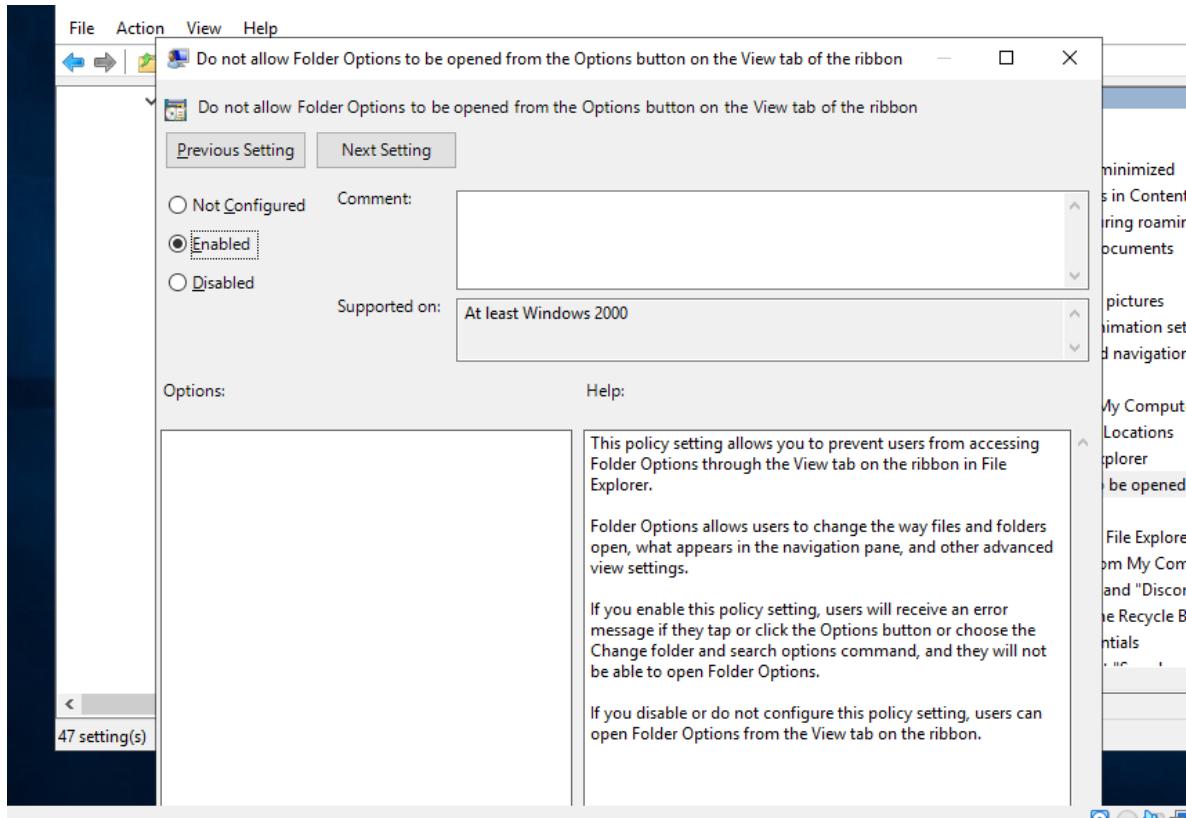


Ocultar el menú de opciones, de la carpeta del menú de herramientas. Esto con el fin de que los usuarios no puedan ver archivos ocultos o cambiar algunas configuraciones de las carpetas

Para esto tocamos la que dice do not allow folder options to be opened from the options... dentro de file explorer

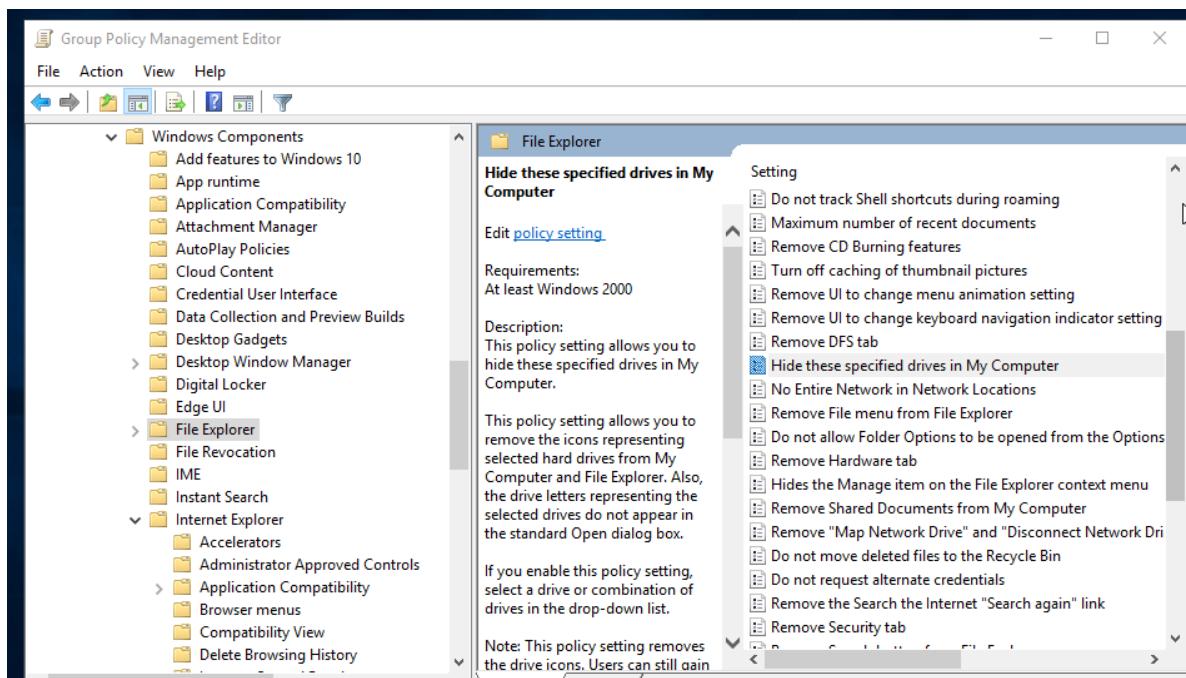


La habilitamos

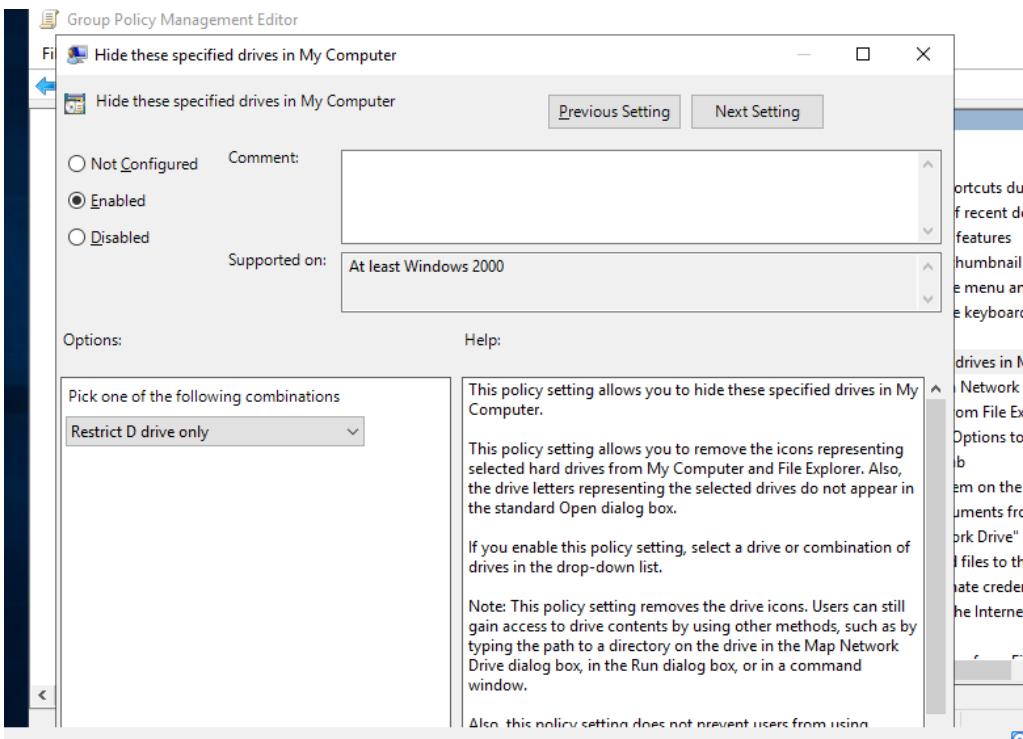


Restringir el acceso a la unidad D:\ desde mi PC

Para esto creamos otra política y vamos al mismo lugar en file explorer que anteriormente en este caso hide these specified drives in my computer y la modificamos

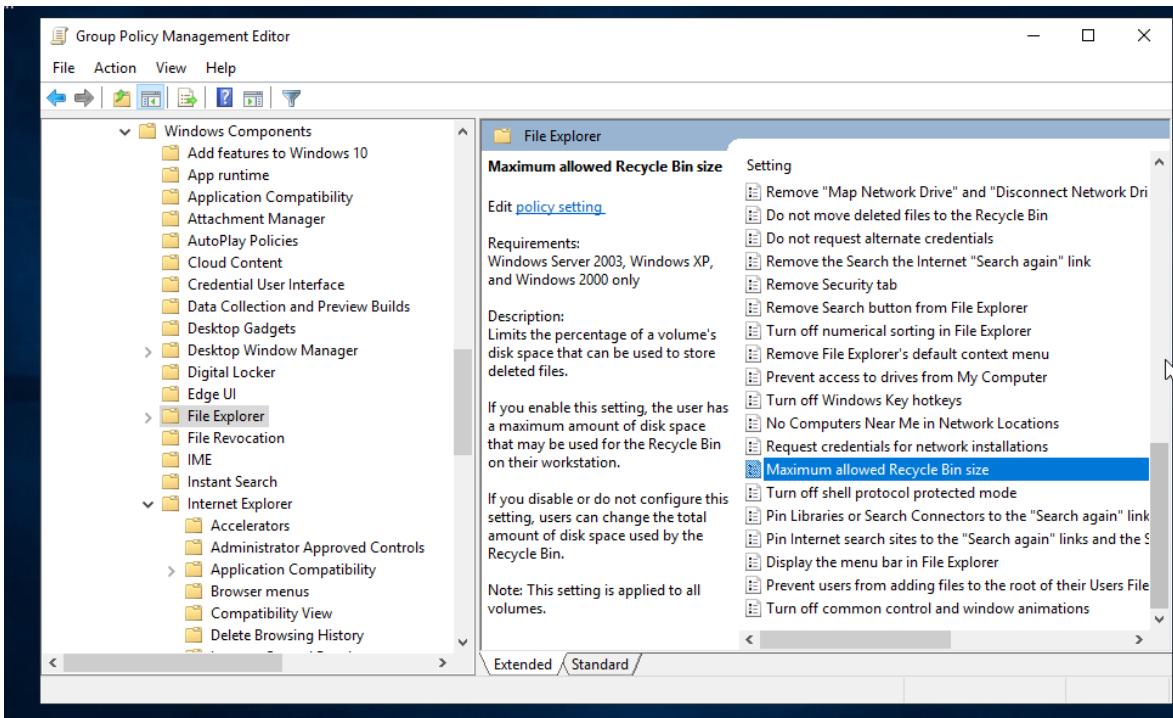


Habilitamos y ponemos el disco d en este caso

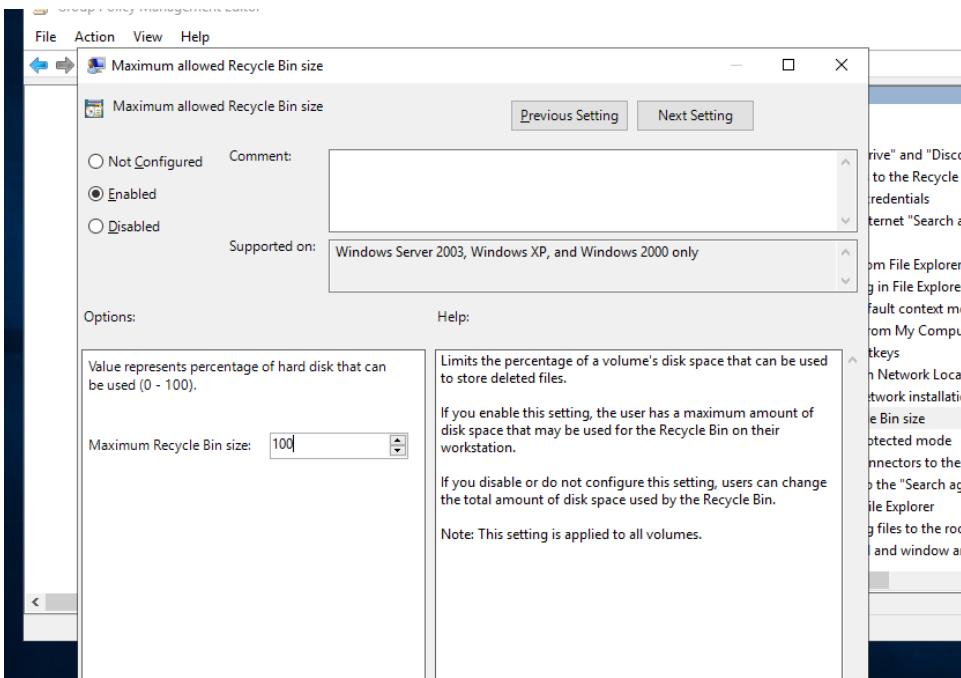


LIMITAR EL TAMAÑO DE LA PAPELERA DE RECICLAJE A 100MB

Para limitar la papelera tocamos dentro de file explorer la que dice maximum allowed recycle bin size

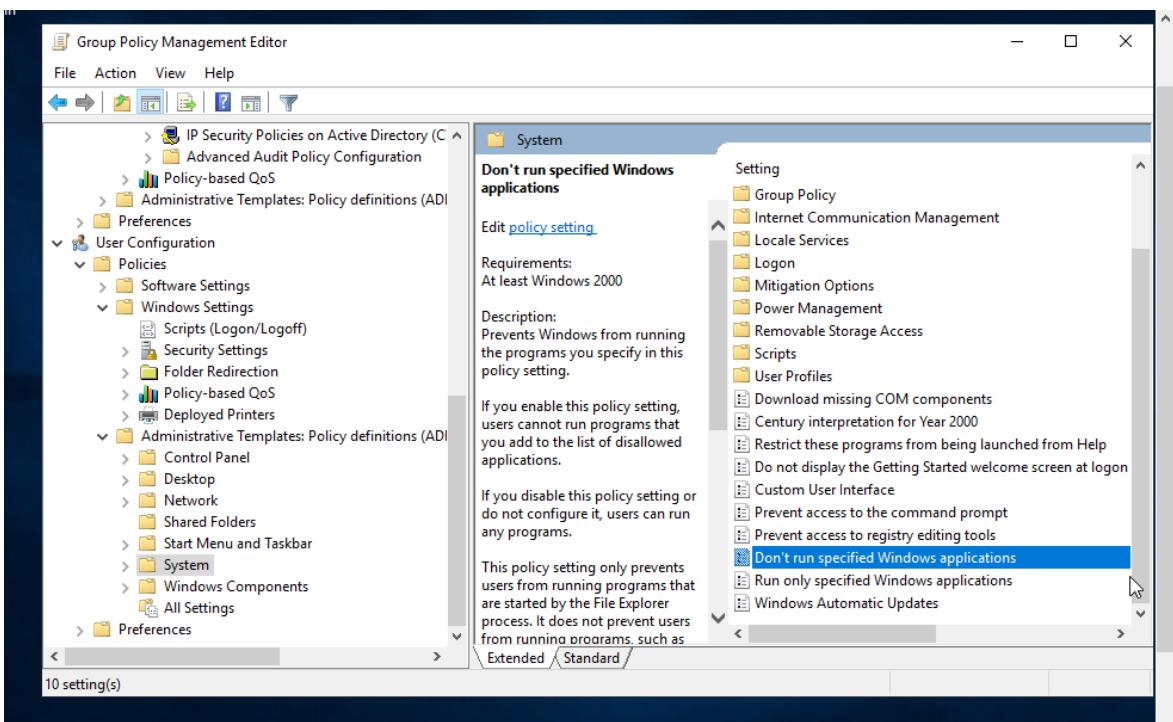


La habilitamos y ponemos 100 mb

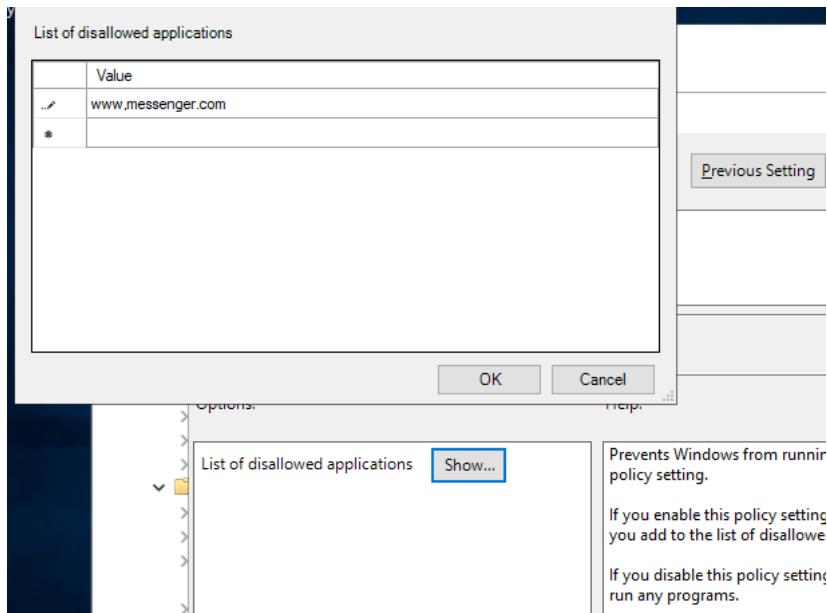


No permitir que se ejecute Messenger

Para esto modificamos dentro de system la que dice don't run specified Windows applications

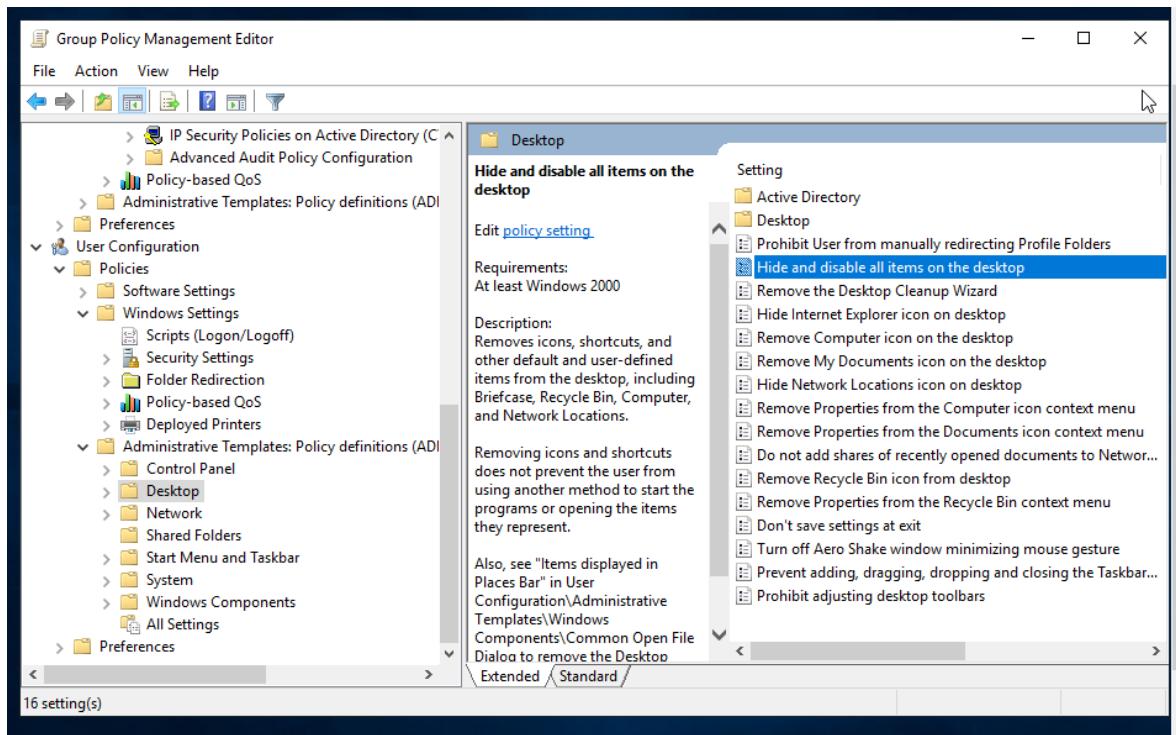


La habilitamos y agregamos www.messenger.com

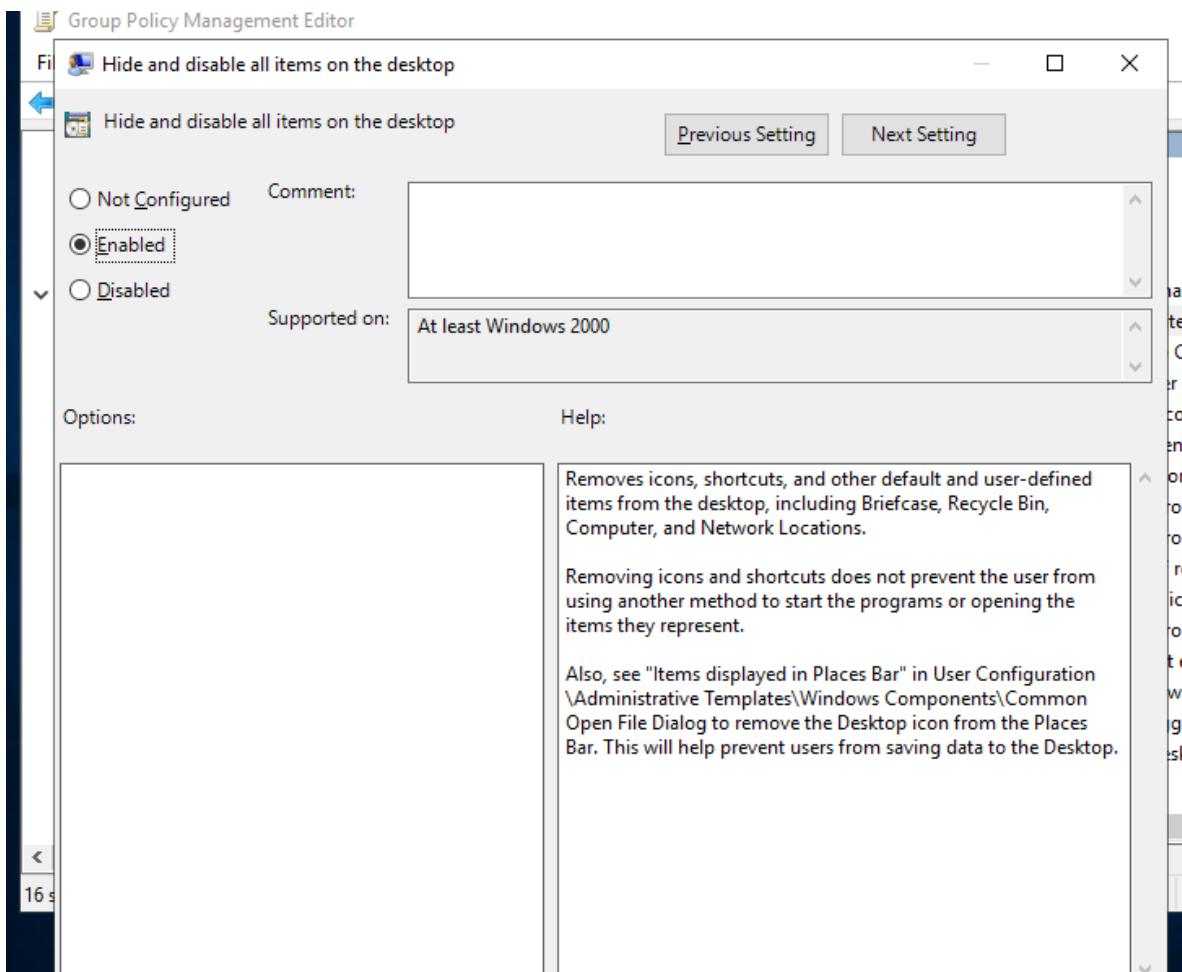


Ocultar todos los elementos del escritorio para todos los usuarios.

Ocultamos todo esto con la de desktop hide and disable all items on the desktop



La habilitamos

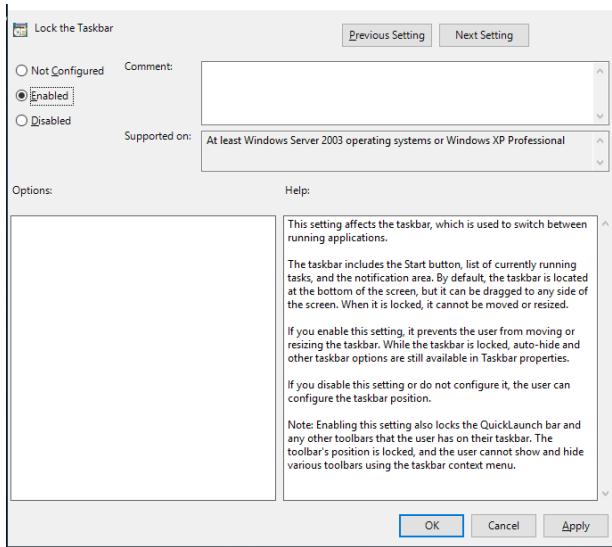


Bloquear la barra de tareas

Bloqueamos la barra de tarea con star menú and taskbar y modificamos la de lock the taskbar

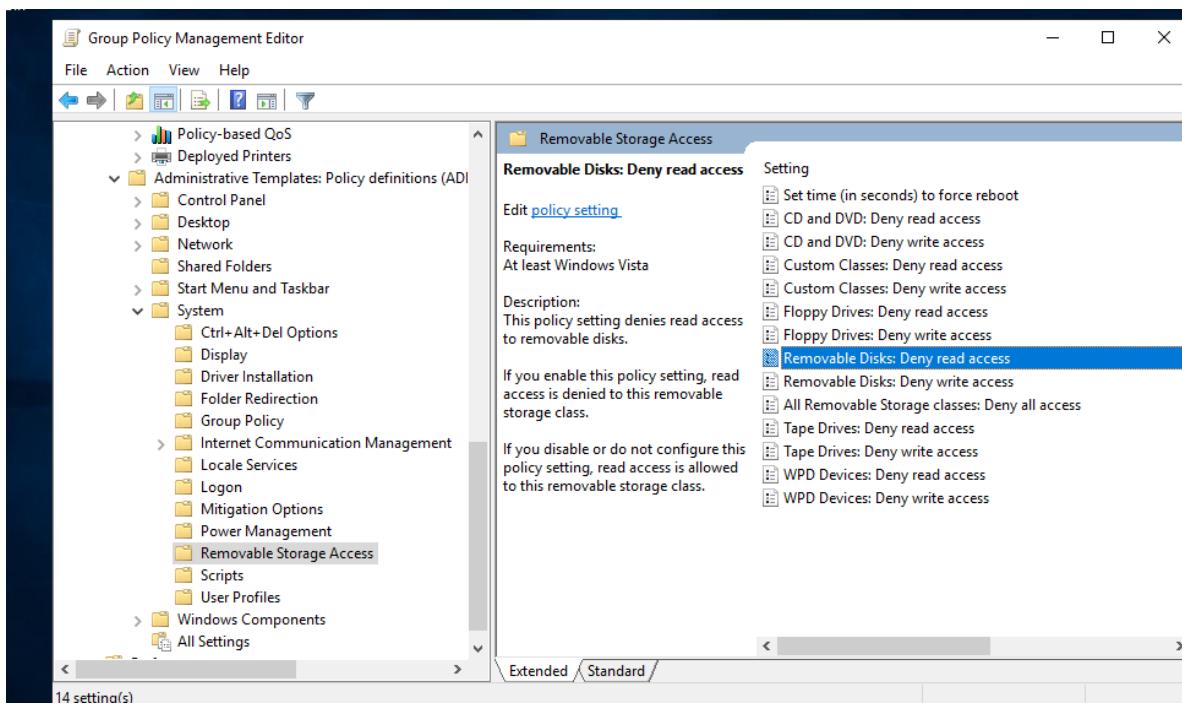
The screenshot shows the Windows Administrative Templates interface under 'Administrative Templates: Policy definitions (AD)'. The 'Start Menu and Taskbar' folder is selected. In the right pane, the 'Lock the Taskbar' policy is highlighted. The description for this policy states that it prevents the user from moving or resizing the taskbar. A list of other policies includes: Clear tile notifications during log on, List desktop apps first in the Apps view, Disable context menus in the Start Menu, Search just apps from the Apps view, Add Logoff to the Start Menu, Force Start to be either full screen size or menu size, Go to the desktop instead of Start when signing in, Gray unavailable Windows Installer programs Start Menu sh, Remove the People Bar from the taskbar, Remove "Recently added" list from Start Menu, Turn off personalized menus, Lock the Taskbar (which is selected), Start Layout, Add "Run in Separate Memory Space" check box to Run dial, and Turn off notification area cleanup.

La habilitamos

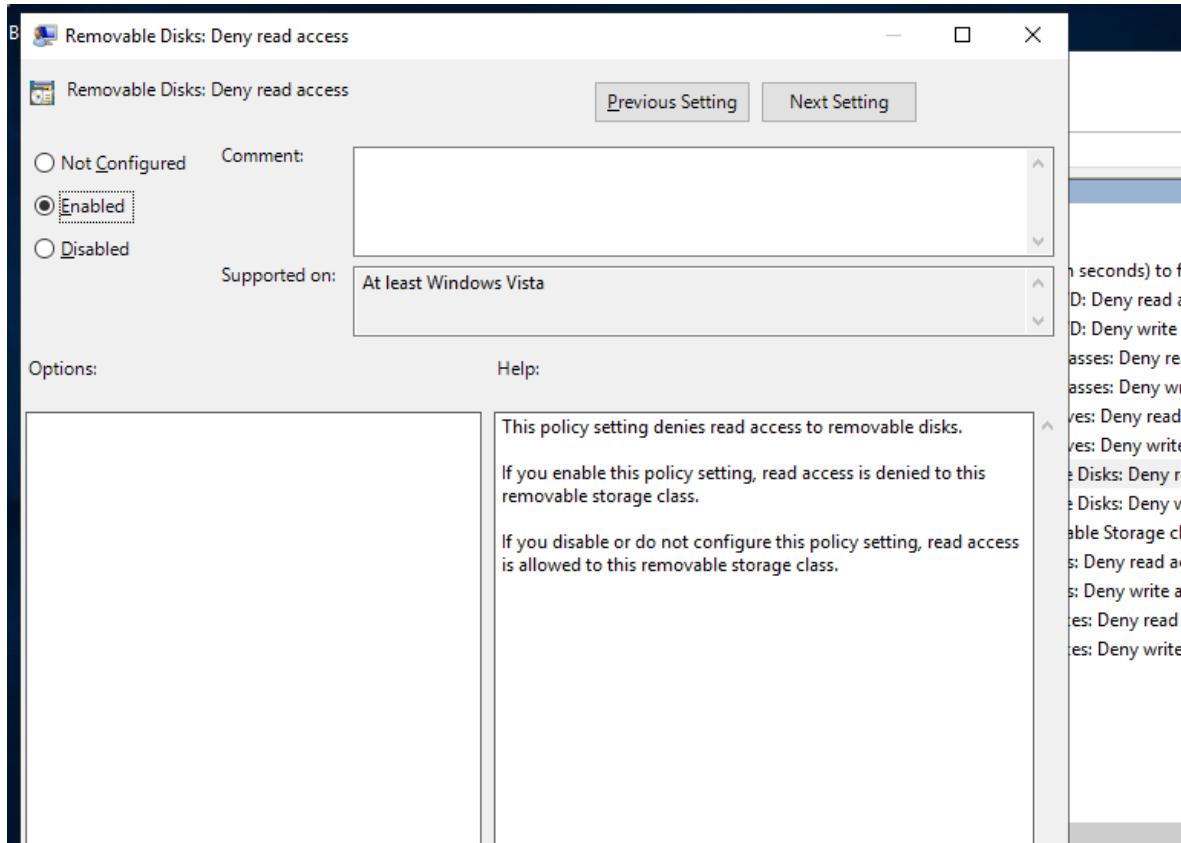


Prohibir el acceso del Lecto-escritura a cualquier medio de almacenamiento extraible.

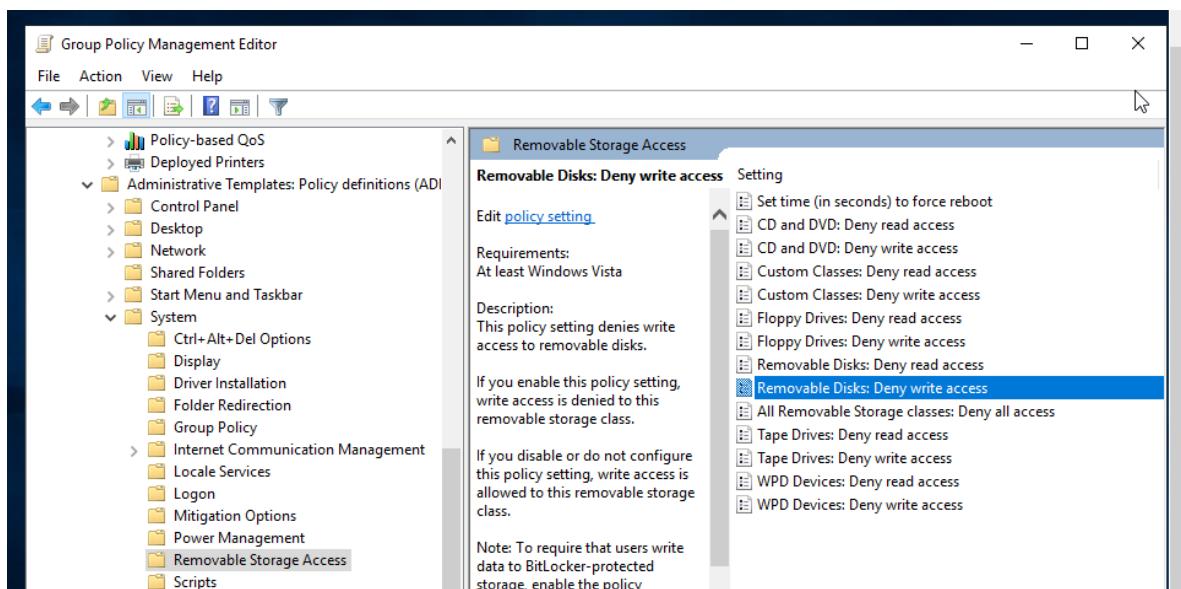
Prohibimos el acceso de lectura en removable storage Access y removable disk: deny read access



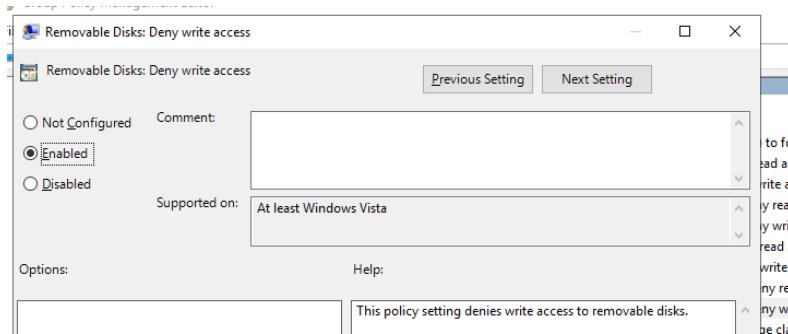
habilitamos



También modificamos la escritura



La habilitamos



Finalmente damos en el command prompt un gpupdate /force para forzar las políticas

```

Administrator: Command Prompt - gpupdate /force
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

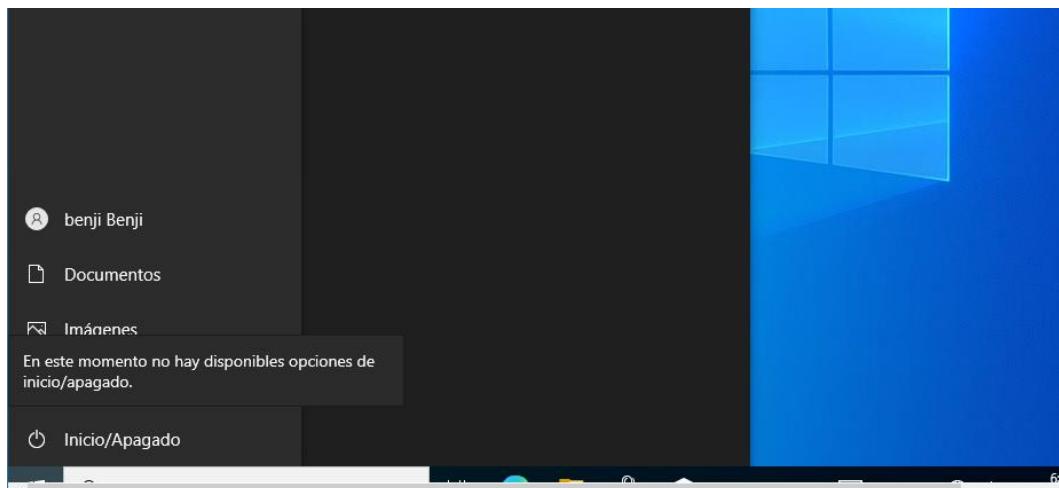
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.

```

Y podemos comprobar si las políticas se aplicaron con un ejemplo sencillo, vimos que los usuarios timers no podían apagar la computadora, entraremos a Benji e intentaremos apagar la computadora y efectivamente este usuario no puede apagar la pc.



Referencias

Iainfoulds. (2023, 9 marzo). *Introducción a Active Directory Domain Services*. Microsoft Learn.

<https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>

Imyuru - Overview. (2001, 17 agosto). GitHub. <https://github.com/imyuru>

MSFT WebCast. (2019, 30 abril). *Configure proxy settings using Group Policy Preferences / Windows Server 2019* [Vídeo]. YouTube. <https://www.youtube.com/watch?v=EJyB-Hh9DYU>

Windows Server 2019 / Microsoft Evaluation Center. (s. f.). <https://www.microsoft.com/en-us/evalcenter/download-windows-server-2019>

Windows Server 2022 : Active Directory : Install : Server World. (s. f.). https://www.server-world.info/en/note?os=Windows_Server_2022&p=active_directory&f=1

[PDF] *Las Directivas de Grupo (GPO) en Windows Server 2008 y 2008 R2 Implementación, funcionalidades, depuración - Free download PDF*. (s. f.). <https://silo.tips/download/las-directivas-de-grupo-gpo-en-windows-server-2008-y-2008-r2-implementacion-func>