

Entorno empresarial con Active Directory

Este documento porta información teórico-práctica sobre cómo crear un entorno empresarial (básico) en Active Directory. Está hecho con la finalidad de explicar y demostrar la importancia de la gestión, mantenimiento y existencia de la herramienta AD, muy conocida en sistemas operativos Windows. Dicho entorno será utilizado para futuras prácticas relacionadas al hacking ético e implementaciones de distintas políticas de seguridad, con fines educativos.

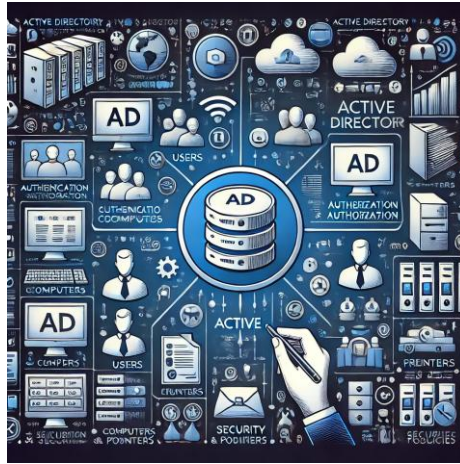
Esta guía ofrece:

- ❖ Creación y gestión de dominios en AD.
- ❖ Cómo agregar máquinas a un dominio de AD.
- ❖ Creación de usuarios, unidades organizativas y políticas en dominios de AD.
- ❖ Instalación y configuración de roles importantes: AD DS, DHCP, DNS.

Sobre el Autor:

- Aidee Miguelina Lorenzo Mejía
- Estudiante de Seguridad Informática. Instituto Tecnológico de Las Américas.
- Creando contenido educativo para ayudar a otros a entender mejor Linux y la ciberseguridad.

Contenido



Entorno empresarial con Active Directory

Introducción.....	5
¿Qué es Windows Server?	5
¿Qué es Active Directory?.....	5
 Instalación de Windows Server	6
 Dominios en AD	11
¿Qué es un dominio de AD?.....	11
Árbol (Tree).....	11
Bosque (Forest)	11
Instalación de AD en Windows Server.....	12
Creación de dominio en AD	15
IP estática para AD	19

Agregar quipos a AD	22
Para cada Sistema Operativo que se conecte a un dominio en una máquina virtual	22
Windows 7	25
Windows 10	27
Windows 11	28
Comprobar los nuevos equipos en el dominio	29
 Objetos en AD	 30
¿Qué es un objeto en AD?	30
 Tipos de objetos	 30
Usuarios	30
Unidades organizativas	30
Grupos	30
Computadoras	30
Políticas de grupo (GPOs)	31
 Administración de objetos en AD	 32
Unidades Organizativas	32
Creación de Unidades Organizativas	32
Eliminar una unidad organizativa	34
Más unidades organizativas	35
Usuarios	37
Creación de Usuarios	37
Propiedades de un usuario	40
Iniciar sesión con un usuario de AD en un equipo del dominio	42
Políticas de Grupo (GPOs)	47

Implementación de políticas	47
Políticas de contraseñas	48
Política de Wallpaper	54
Política de Instalación de Software	63
Políticas de Restricciones a los usuarios	71
 Configuración de Roles en AD	 77
DNS	77
¿Qué es DNS?.....	77
¿Para qué funciona?.....	77
Importancia de DNS en AD.....	77
 Configuración de DNS en AD	 78
Zona de búsqueda directa (Forward Lookup Zone)	78
Zona de búsqueda inversa (Reverse Lookup Zone)	80
Reenviadores DNS	82
 DHCP.....	83
¿Qué es DHCP?.....	83
¿Para qué funciona DHCP?	83
Importancia de DHCP en AD	83
 Configuración de DHCP en AD	 84
Precaución	84
Scope DHCP.....	85
Rango de direcciones.....	86
Direcciones excluidas	87
Tiempo de duración para las direcciones	88
Gateway del DHCP	89
DNS	90
WINS Servers	91
Activación del Scope	92

Reservación de direcciones	93
DHCP para los clientes.....	95
Vistazo al nuevo Scope	97
 Conclusión y reflexión final	 98
Resumen de lo aprendido y reflexión personal.....	98
Importancia en estos temas.....	99

Introducción

¿Qué es Windows Server?

Windows Server es un sistema operativo desarrollado por Microsoft, diseñado específicamente para administrar redes, servidores y servicios en empresas o entornos informáticos más grandes. A diferencia de Windows que se usa normalmente en una computadora personal, Windows Server está hecho para controlar y coordinar múltiples equipos, usuarios y recursos desde un solo lugar.

¿Qué es Active Directory?

Active Directory (AD) es una herramienta de Microsoft que se usa en las computadoras de una red para mantener todo organizado. Sirve para gestionar quién puede usar la red, qué puede hacer y a qué recursos (como archivos, impresoras o programas) puede acceder.

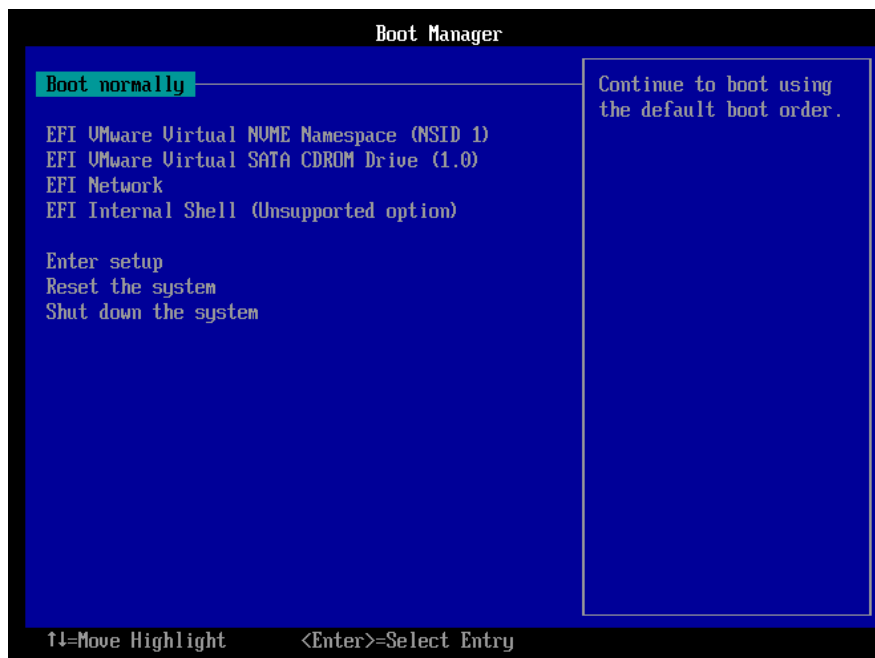
AD actúa como una base de datos donde están los nombres de todas las personas (usuarios), computadoras y dispositivos conectados. También dice qué permisos tiene cada uno, como quién puede abrir ciertos archivos o usar una impresora.

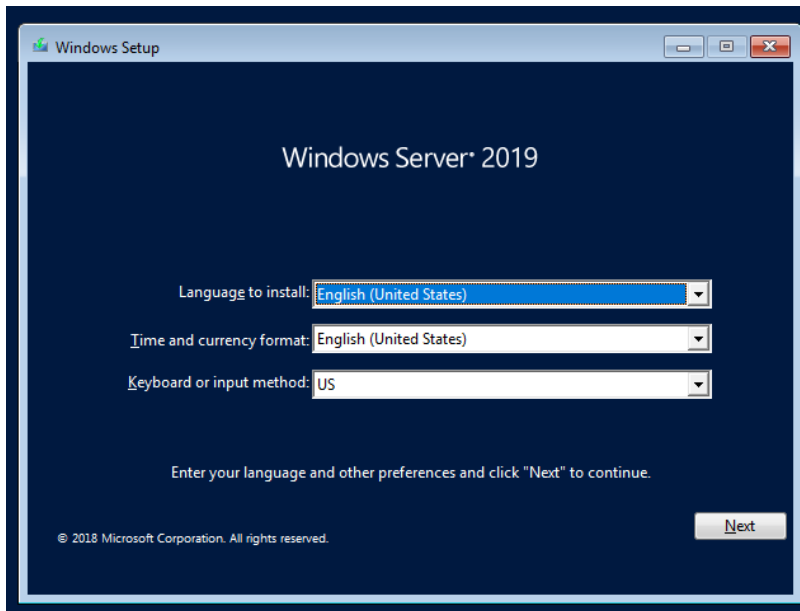
Para que todo funcione de manera organizada, se configuran distintas políticas de seguridad, pero esto y otras cosas se verán a medida que avance el documento.

Instalación de Windows Server

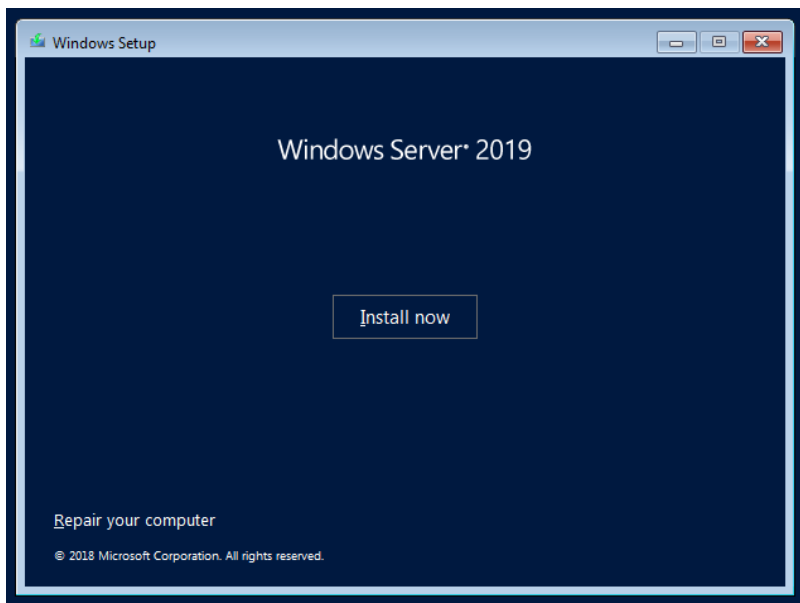
Es posible que esta sea la primera imagen que vea al querer instalar Windows Server en su gestor de MV preferido. En este caso todas las máquinas virtuales utilizadas han sido creadas en VMware. Personalmente desconozco si esto ocurre al utilizar VirtualBox.

Si esta pestaña aparece en su pantalla, deberá seleccionar la opción dos (**SATA CDROM**) con las teclas direccionales. Luego de esto, podrá continuar con la instalación del sistema operativo.

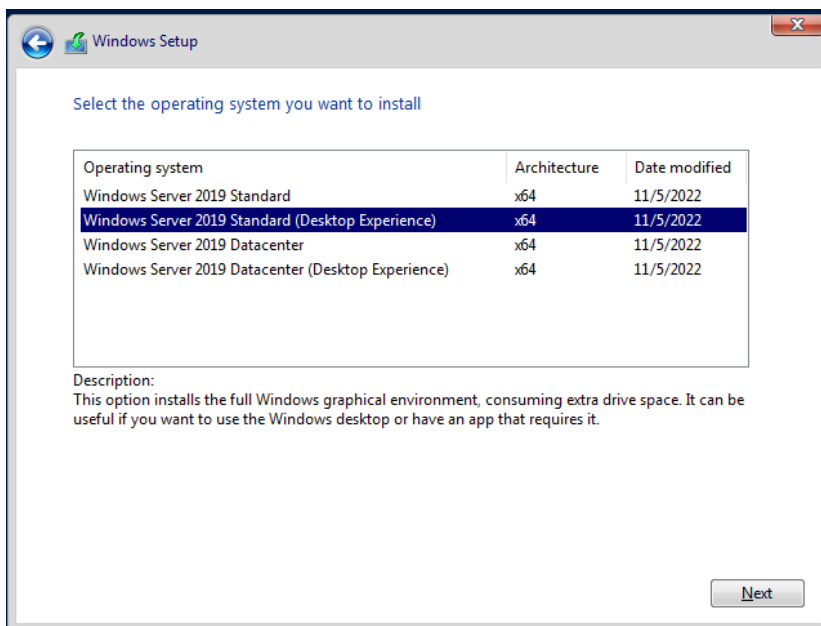
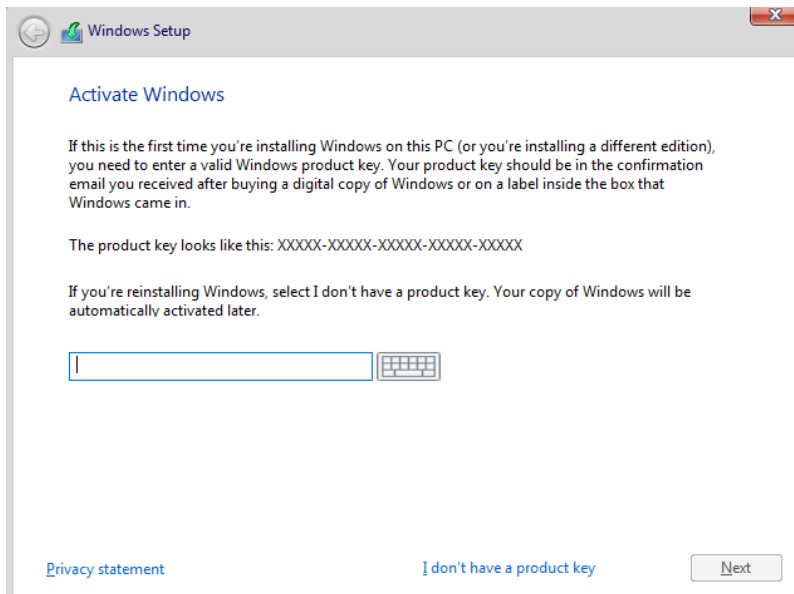




Todos los pasos a partir de acá serán intuitivos para el usuario. Ya que es a través de una interfaz gráfica, leerá y aceptará los términos que sean necesarios para una instalación correcta.

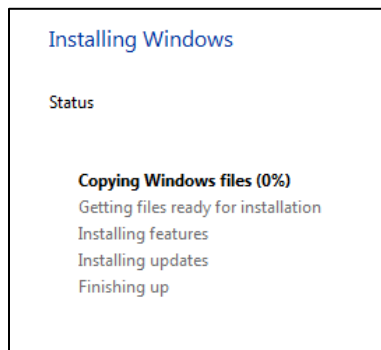
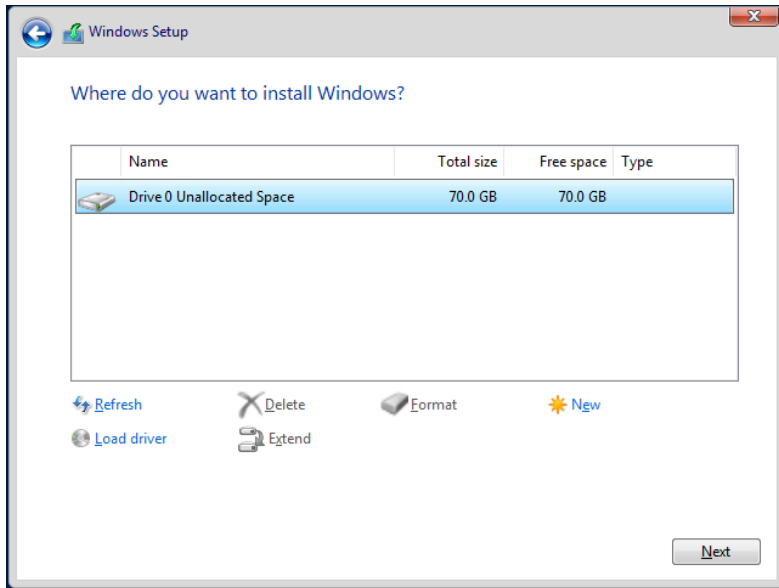


Si cuenta con una clave para activar Windows, lo ideal es colocarlo. De lo contrario puede continuar afirmando que no tiene una clave que poner.



Si lo que busca es tener un entorno pequeño, como es el caso de este documento, su elección será **Estándar**. De lo contrario, si quiere administrar entornos de gran tamaño, lo ideal es seleccionar la opción **Datacenter**. Ambas tienen la opción de ser manejadas por líneas de comando o con GUI (Desktop Experience, como indica la imagen).

Para la personalización de Windows debe seleccionar la segunda opción, de esta forma controla sus particiones.




Customize settings

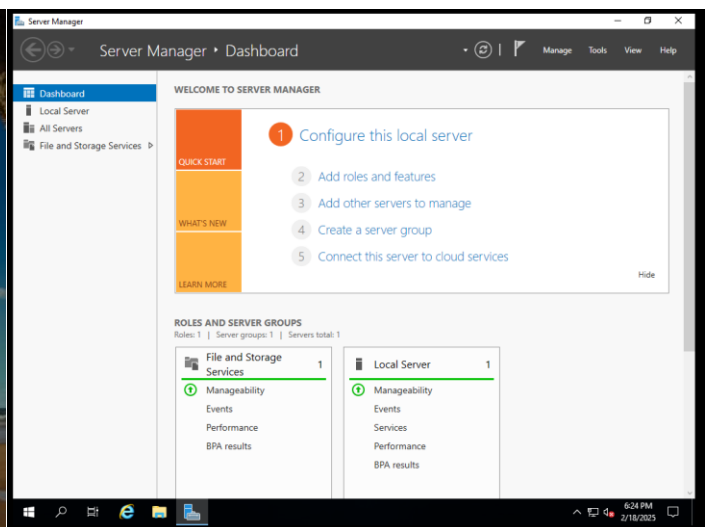
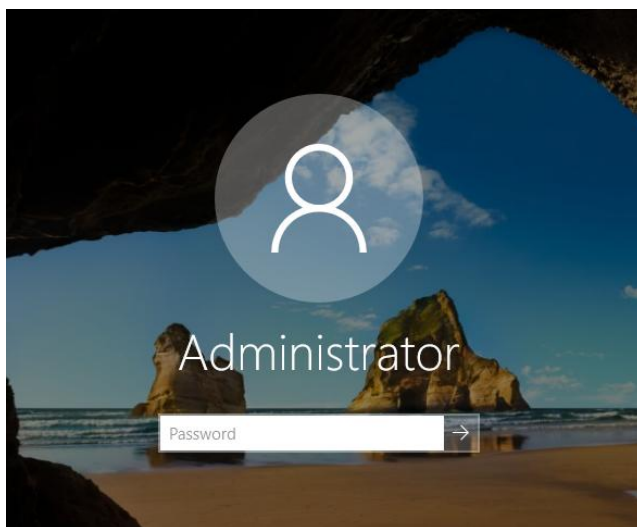
Type a password for the built-in administrator account that you can use to sign in to this computer.

User name

Password

Reenter password

 [Finish](#)



Dominios en AD

Para administrar los equipos, usuarios y otros objetos de nuestra red, es necesario la creación de un dominio. Pero antes, la definición de varios conceptos importantes en AD.

¿Qué es un dominio de AD?

Los dominios en AD son el medio por el cual se administran los distintos objetos (usuarios, equipos, políticas...) vinculados a nuestra red. Cada dominio cuenta con un controlador de dominio (**DC**: Domain Controller en inglés). El DC es el servidor que ejecuta AD y maneja la autenticación y autorización dentro del dominio. Almacena y replica la base de datos de AD.

A partir de los dominios en AD aparecen más conceptos a tener en cuenta.

Árbol (Tree)

En AD se le denomina árbol al conjunto de uno o más dominios que comparten un espacio de nombres contiguos. Es decir, que conectan entre sí de manera lógica y secuencial. Por ejemplo:

- **empresa.com** (dominio raíz)
- **sucursal.empresa.com** (subdominio)

En este caso sucursal.empresa.com es una extensión del nombre del dominio raíz empresa.com. Esto crea una relación jerárquica y continuidad en el espacio de nombres.

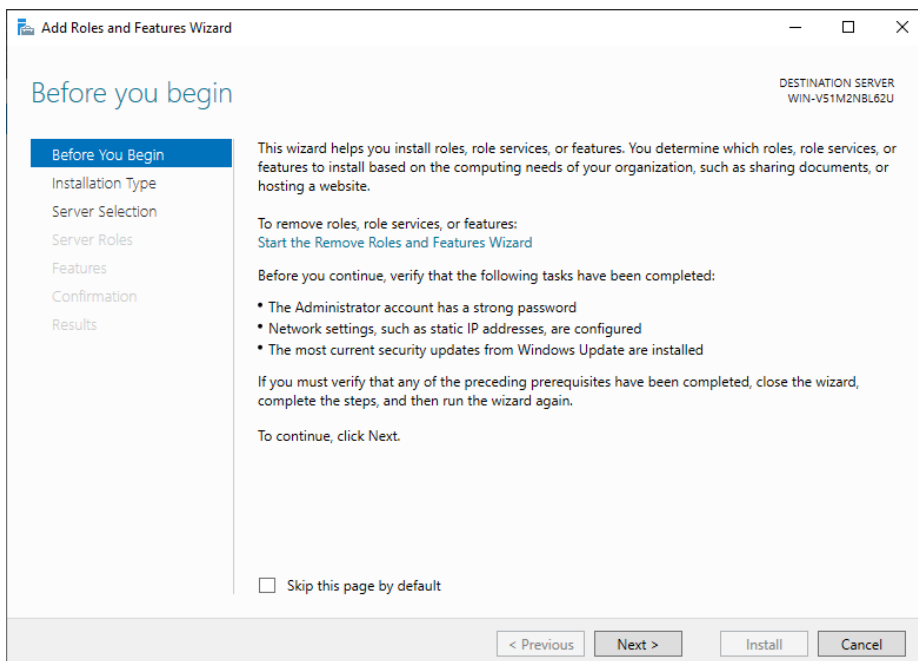
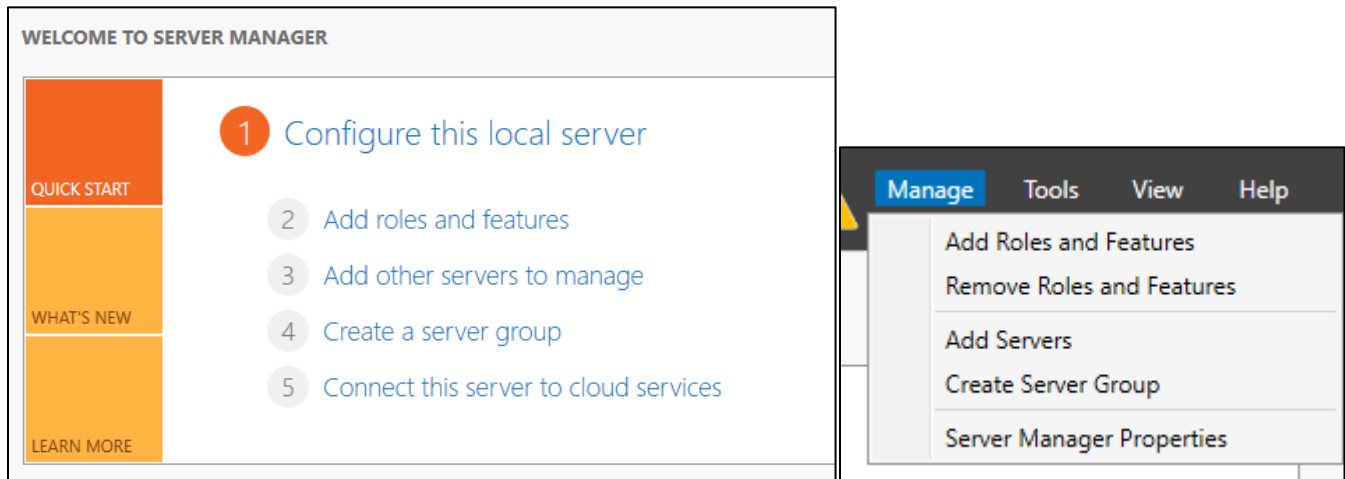
Bosque (Forest)

Es el conjunto más grande en AD. Hace referencia a varios árboles y, puede decirse que representa la totalidad de la infraestructura de AD.

Instalación de AD en Windows Server

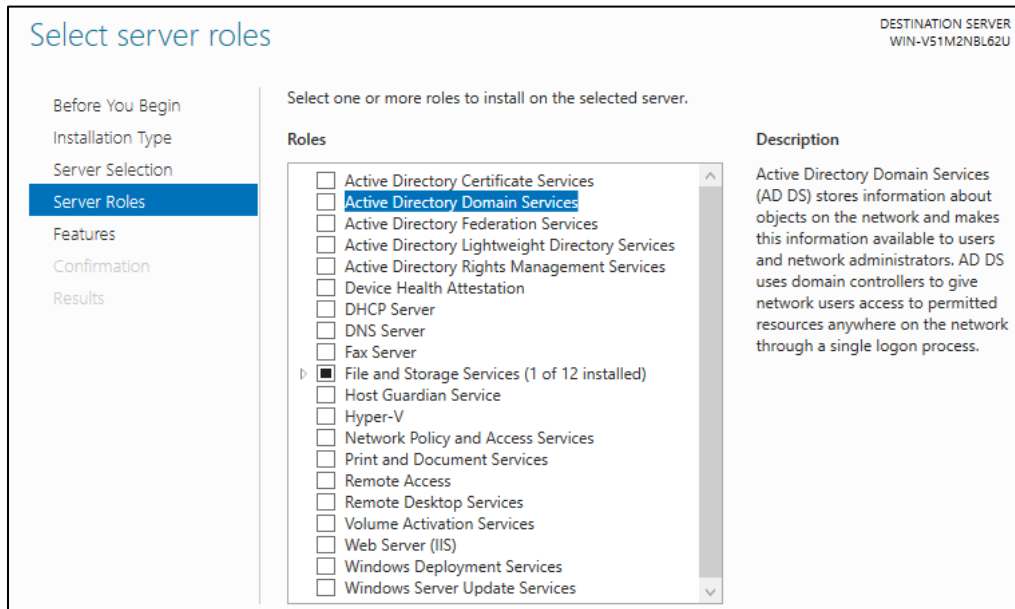
Para llegar a la creación de un dominio, primero hay que pasar por la instalación del rol Active Directory.

En el panel del sistema que sube tan pronto se inicia sesión, se selecciona la opción 2 “**Add roles and deatures**”. Si en alguna ocasión este apartado es eliminado, en la barra superior puede ser agregado.

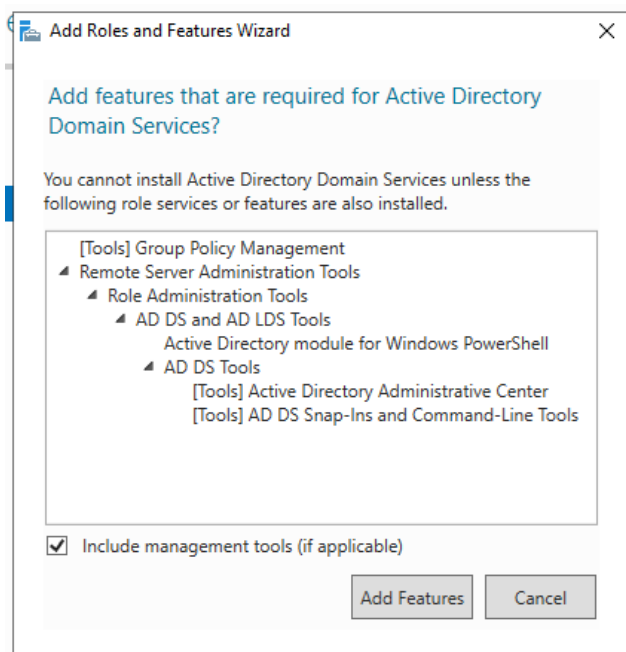


Luego de este cuadro puede continuar dando al botón **Next**, ya que habla sobre el tipo de instalación y el servidor donde se alojará la misma. Como solo tenemos un servidor, podrá continuar con todo por defecto hasta llegar al apartado **Server Roles**.

Active Directory Domain Services es el que nos interesa por el momento. Con solo dar un clic sobre el rol, puede leer una breve descripción al lado. Por el momento solo será seleccionado un rol, pero si quiere agregar más de uno, puede seleccionarlos.



Agregue lo que solicite, ya que son herramientas que utilizará AD.



La casilla de reiniciar en caso de ser necesario, puede ser marcada. En ocasiones el sistema deberá reiniciarse para agregar las nuevas características al sistema. De querer hacerlo de forma manual, puede continuar sin marcar la casilla.

Confirm installation selections DESTINATION SERVER
WIN-VS1M2NBL62U

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results

To install the following roles, role services, or features on selected server, click Install.

☐ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

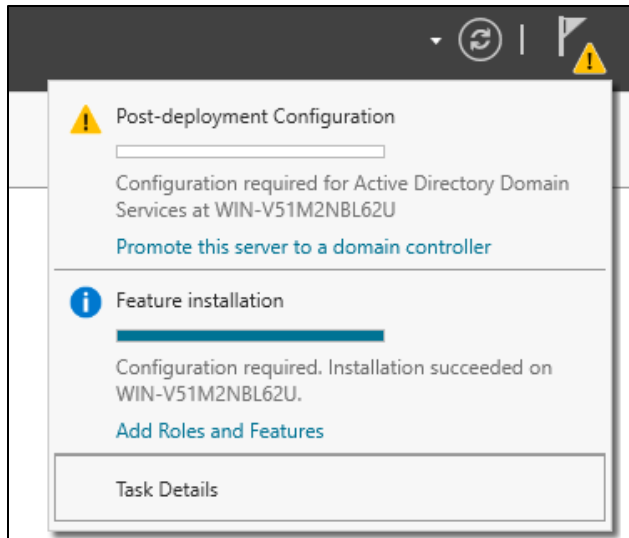
- Active Directory Domain Services
- Group Policy Management
- Remote Server Administration Tools
 - Role Administration Tools
 - AD DS and AD LDS Tools
 - Active Directory module for Windows PowerShell
 - AD DS Tools
 - Active Directory Administrative Center
 - AD DS Snap-Ins and Command-Line Tools

[Export configuration settings](#)
[Specify an alternate source path](#)

< Previous Next > Install Cancel

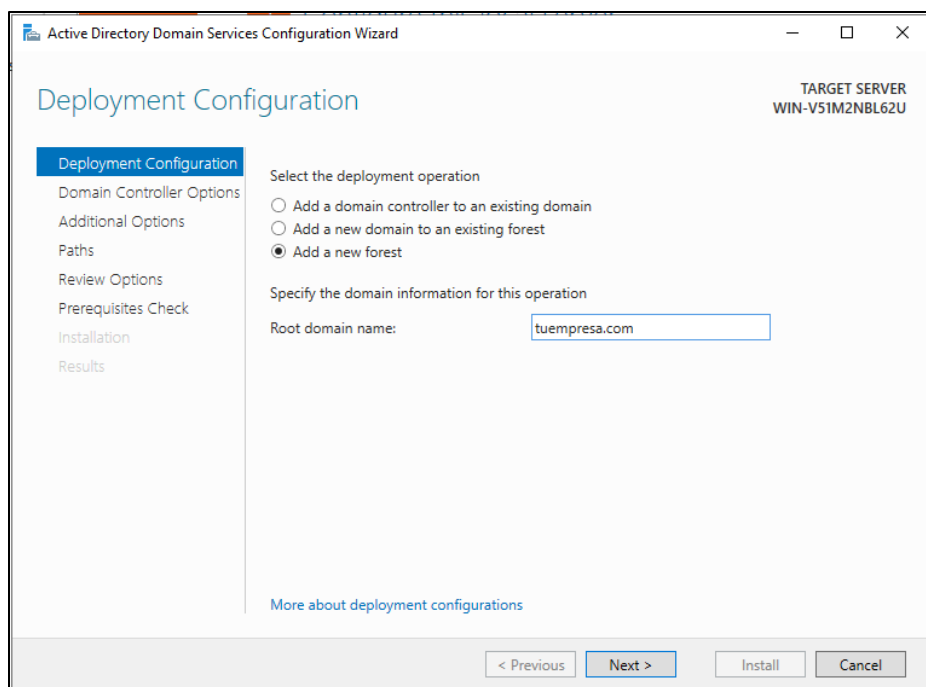
Creación de dominio en AD

Una vez haya terminado la instalación, notará que en la barra superior aparecerá un banderín con un símbolo de emergencia en él. A partir de aquí de donde se configurará el AD para la creación del dominio.

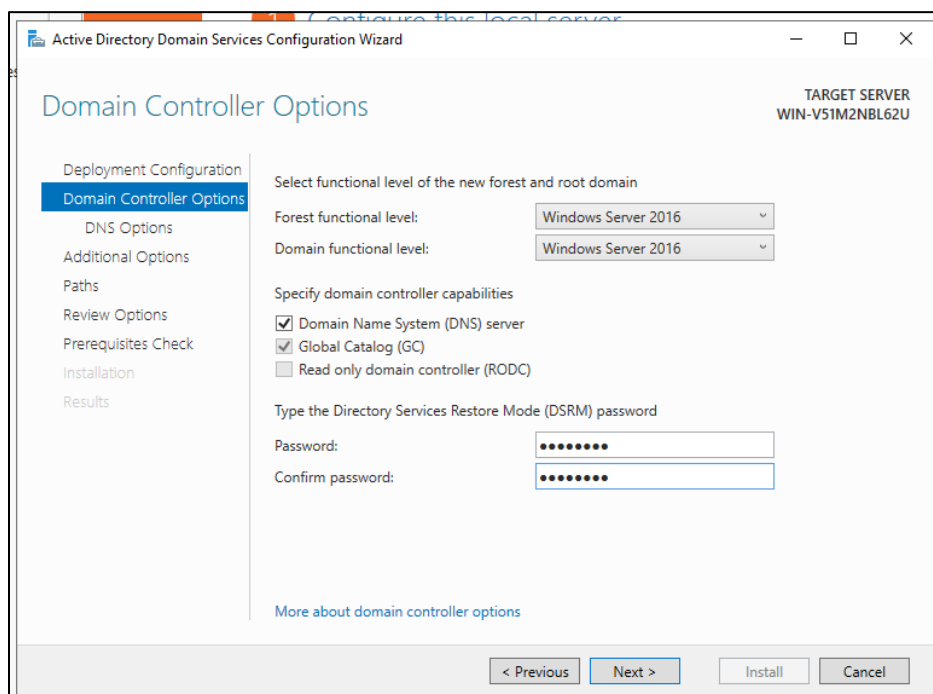


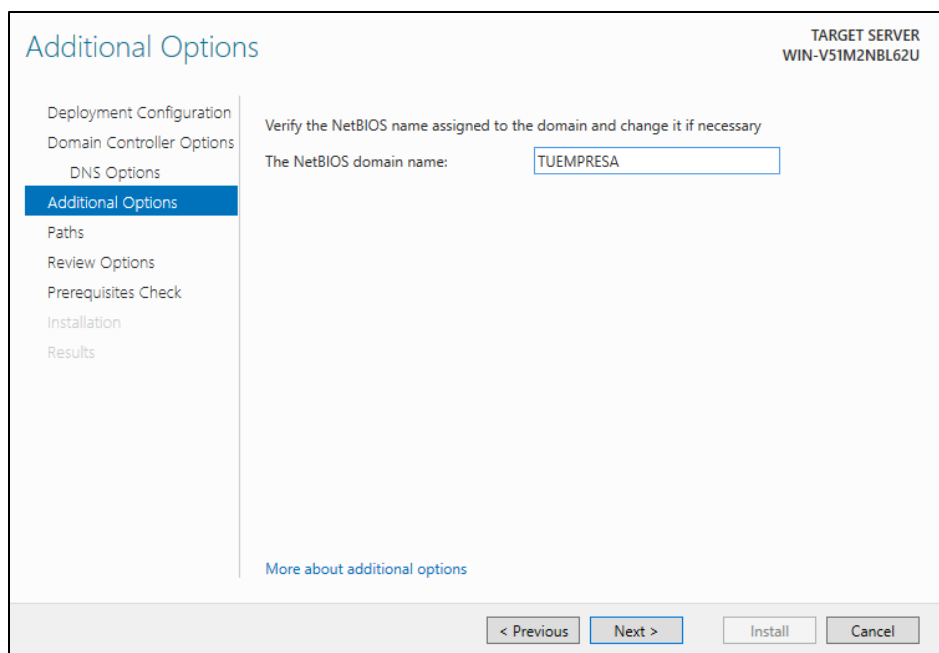
Si no tiene un bosque o un dominio existente, lo ideal es crear un nuevo bosque, y a partir de ahí continuar configurando nuestro dominio.

Para idear el nombre de su dominio, tenga en cuenta de que deberá terminar con (**.algo**). Por ejemplo (**.com, .do, .local...**). No deberá preocuparse por las mayúsculas y minúscula, de forma automática AD lo configurará con mayúsculas; pero luego, usted decidirá si cambia el formato de las letras. Esto servirá para identificar su dominio a la hora de agregar máquinas a su dominio. Tenga en cuenta de que deberá agregar las letras tal como están en este apartado.

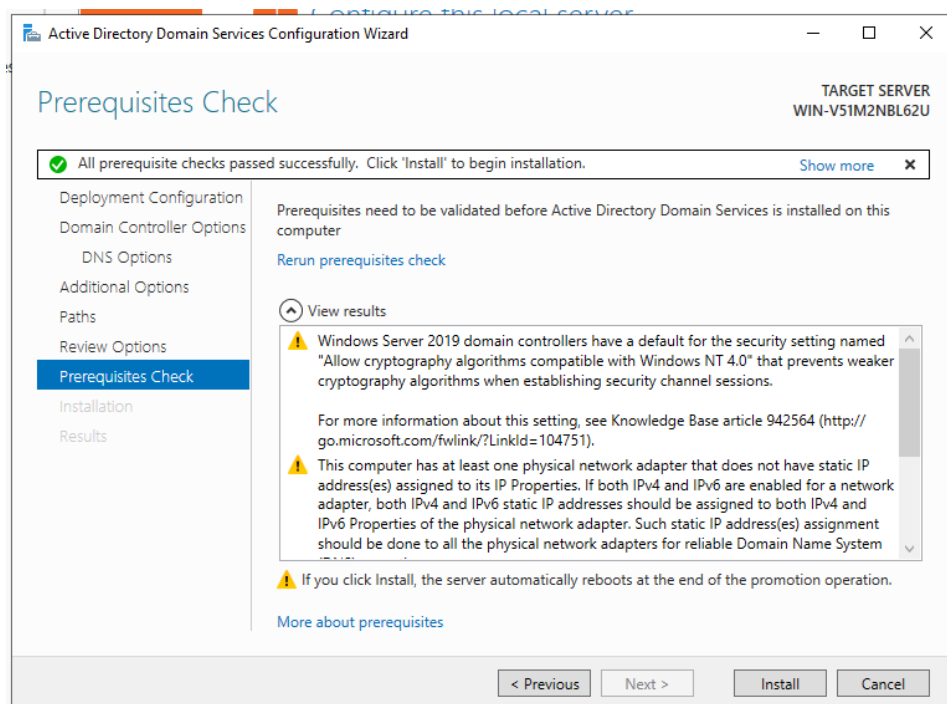


Podrá dejar todas las opciones que siguen por defecto, la configuración de DNS se realizará más adelante junto al DHCP. Lo siguiente será crear una contraseña para el dominio. **Recordar que una contraseña debe ser fuerte a la hora de crear cualquier tipo de credenciales.**





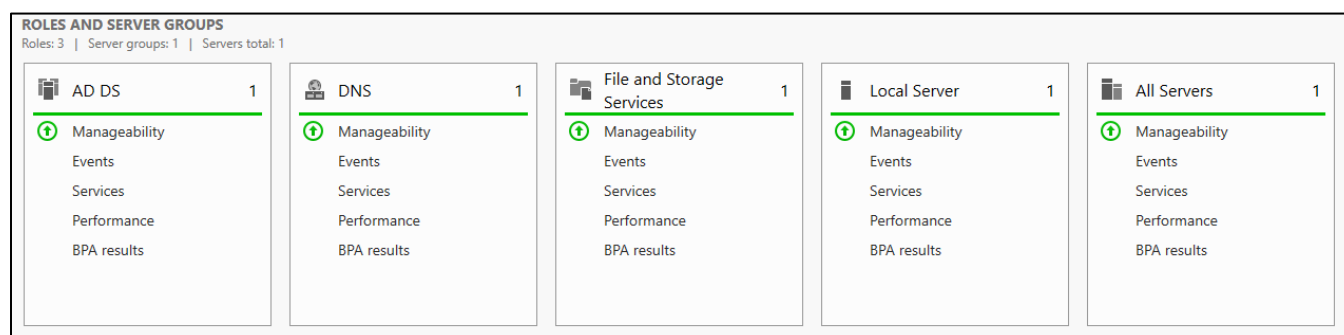
Esta última pestaña es importante. AD nos lanzará algunas advertencias antes de realizar su instalación. Por ejemplo, se pide una IP estática para esto, y es lo que haremos a continuación. Este paso pudo realizarse antes de agregar el rol AD, pero funcionará de igual forma, esto es opcional para hacerlo antes o después. Una vez hecha la instalación el sistema procederá a reiniciarse, lanzando una advertencia que AD ha sido editado o agregado al mismo.



Una vez reiniciado el sistema, el dominio ya estará agregado. Y se verá antes del nombre del usuario que acceda al sistema.

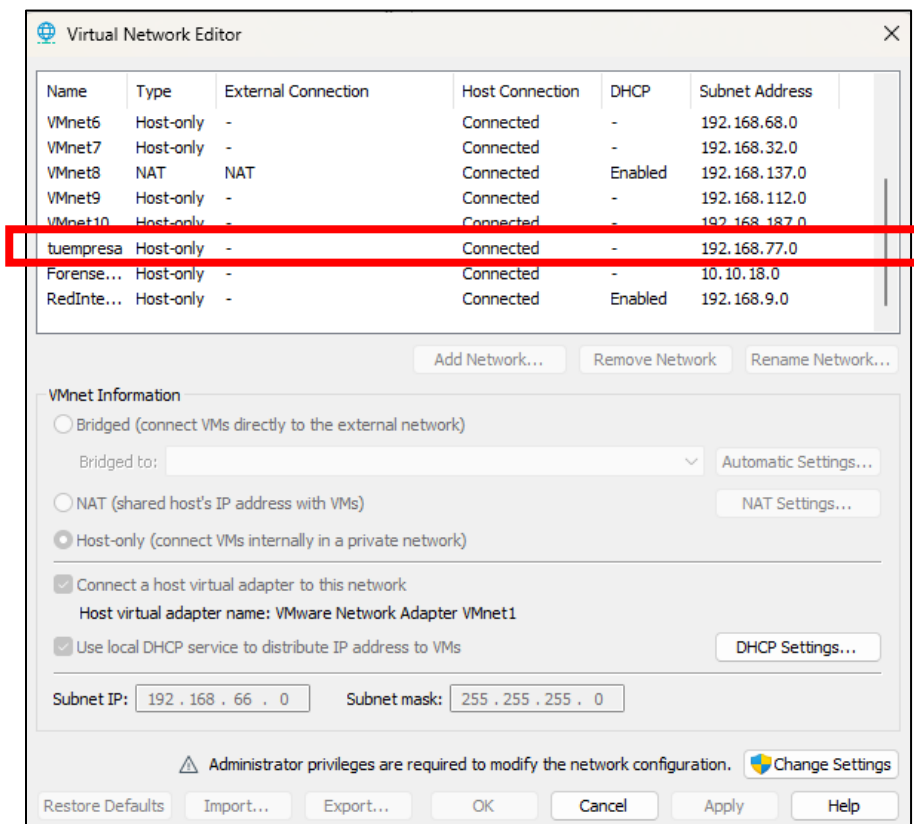


Si necesita otra confirmación de que ya tiene AD y un dominio aplicado, en la sección de roles del servidor, verá el nombre **AD DS** en primera fila.



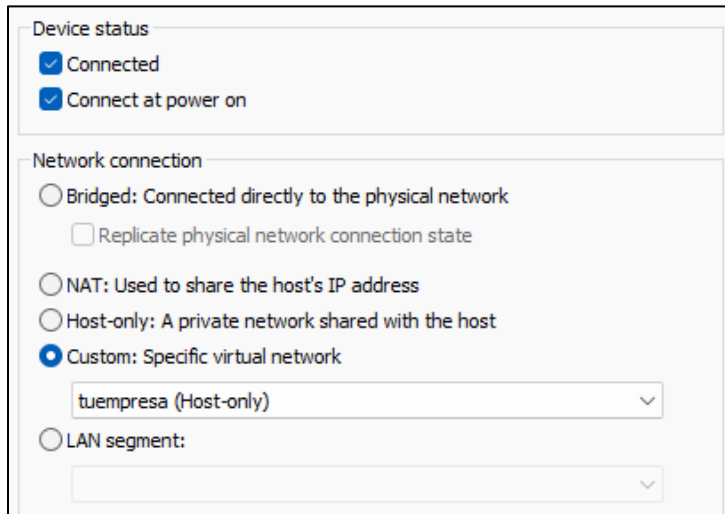
IP estática para AD

Para colocar una IP estática nos encargaremos de configurar una interfaz de Red en VMware, esto para aislar una red única del entorno que estamos creando. Si desconoce los pasos para crear una red, simplemente debe editar la configuración de red en VMware, luego agregar una red nueva, y configurarla a su gusto.

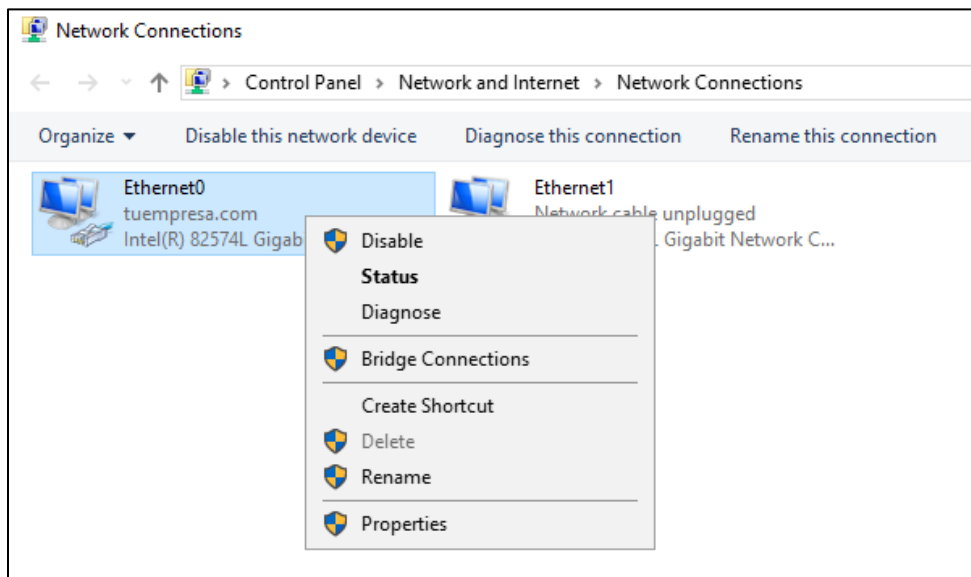


Para editar los parámetros de red deberá contar con permisos de administrador o colocar la contraseña del mismo si se encuentra conectado con otro usuario. En mi caso, deshabilité el DHCP, ya que esa será la red utilizada para configurar el rol recién mencionado y dar IP de forma automática a las demás máquinas del dominio. Esto ayuda a que el DHCP habilitado en la máquina virtual no ofrezca IP, de eso se encargará nuestro dominio. Si todavía no comprende lo explicado, más adelante tendrá más entendimiento sobre esto.

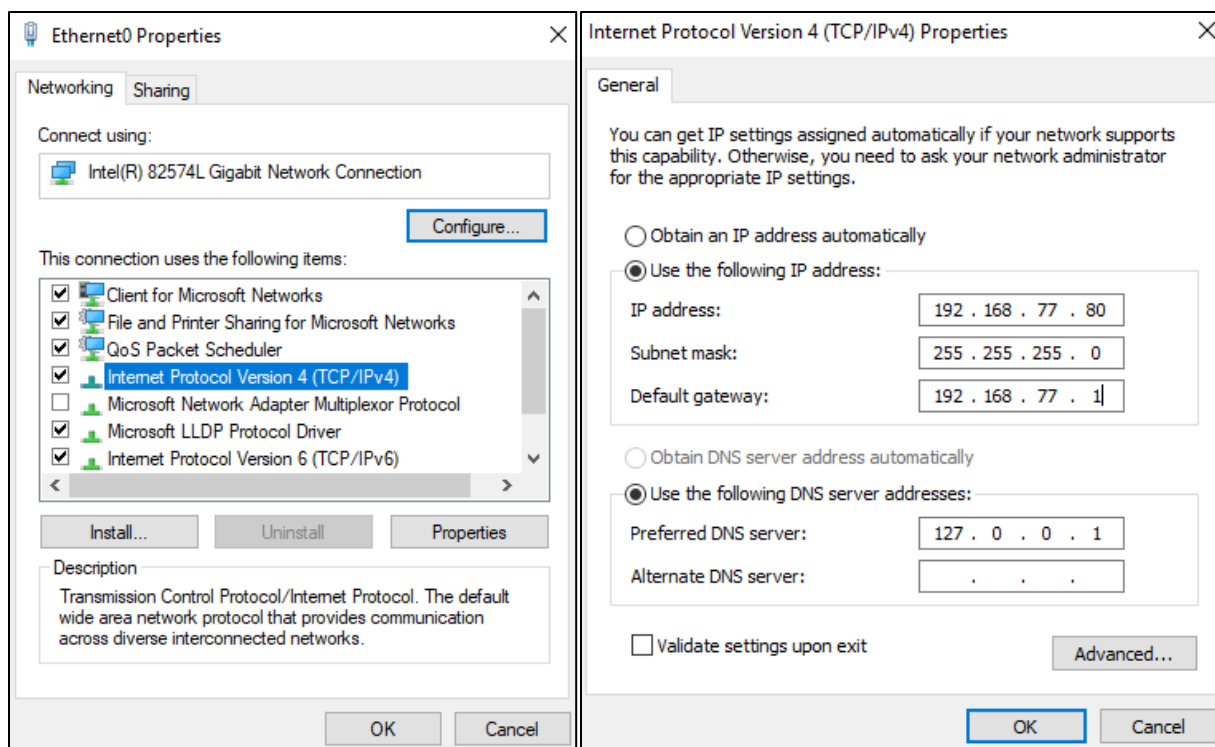
Una vez creada la nueva red, lo recomendable es habilitarla de forma inmediata a su máquina virtual de Windows Server.



De vuelta al servido, debe llegar a la configuración de **Conexiones de Red**.



Una vez dentro, dirigirse a propiedades del conector que desea editar. En este caso el conector está identificado con el nombre del dominio. Posteriormente se dirige a las propiedades del protocolo **IPv4**.



Al estar en esta pestaña debe desactivar la opción de recibir IP de forma automática, y en su lugar colocar una estática. Dentro del parámetro de la red que establecimos más adelante, colocamos una IP. El DNS puede ser cambiado, no afectará.

Para confirmar que la IP ha sido correctamente aplicada, confirme su dirección desde el CMD con el comando **ipconfig**.

```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1c00:5141:a2e4:6186%5
    IPv4 Address. . . . . : 192.168.77.80
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.77.1
```

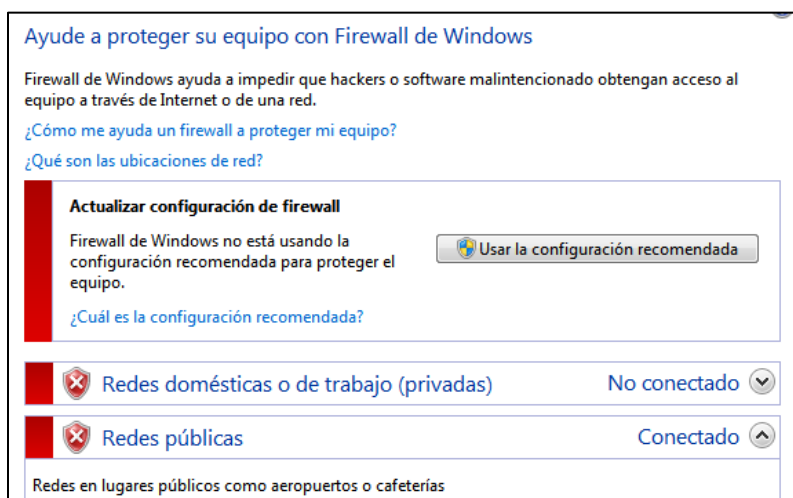
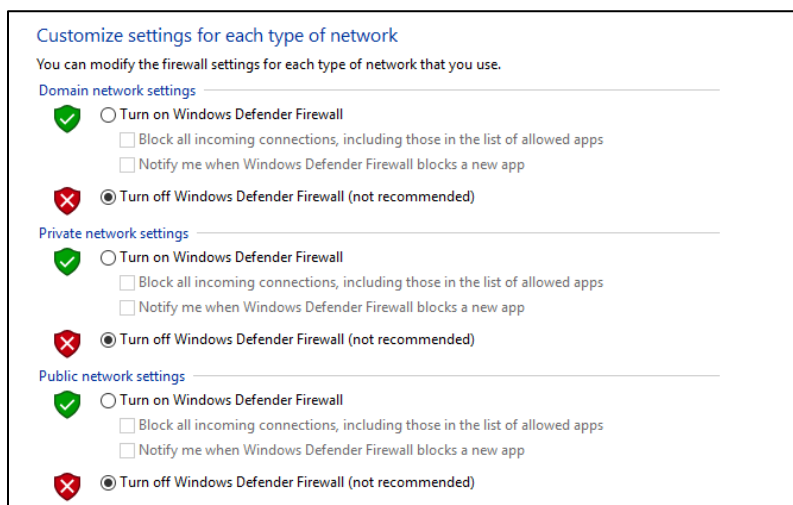
Con esto, nuestro deber con las IP ha terminado, al menos en el servidor.

Agregar quipos a AD

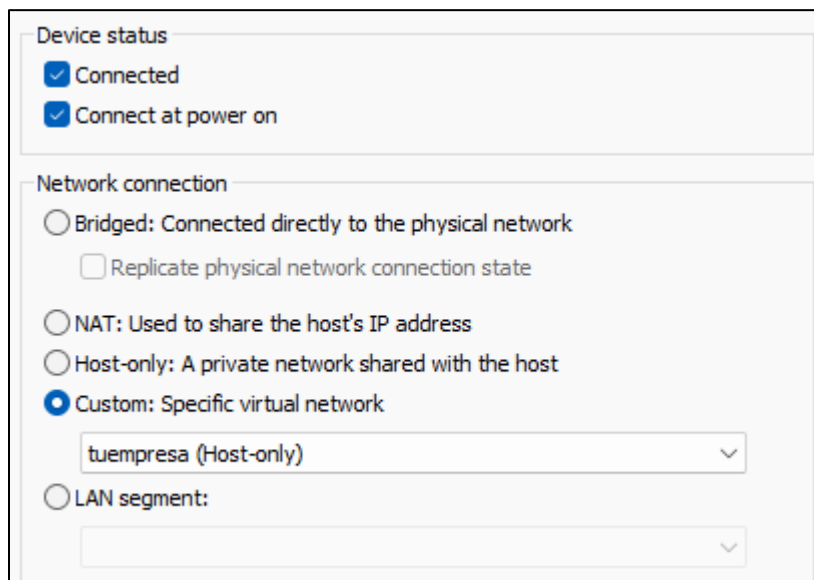
Las máquinas que serán agregadas al dominio tuempresa.com serán: Un Windows7, Windows10, y Windows11.

Para cada Sistema Operativo que se conecte a un dominio en una máquina virtual

1. Si ya ha hecho prácticas de conexión, sabrá que en cada sistema operativo es necesario mantener los firewalls desactivados, para que la conexión no sea detectada como insegura y los pings puedan enviar los paquetes de forma exitosa. Antes de agregar cualquier máquina a un dominio, en VMware o VirtualBox esto debe configurarse de esa forma, incluyendo el servidor de AD.



2. También, cada máquina debe estar conectada a la misma red, de lo contrario el sistema no detectará el dominio. Si trabaja en alguna de las herramientas ya mencionadas para virtualizar, debe crear una red en la que se conectarán todas las máquinas. Por ejemplo, si tiene un adaptador de red con la IP **192.168.77.0** (el caso de este trabajo). Todas las máquinas deben estar conectadas al adaptador configurado con esa red.



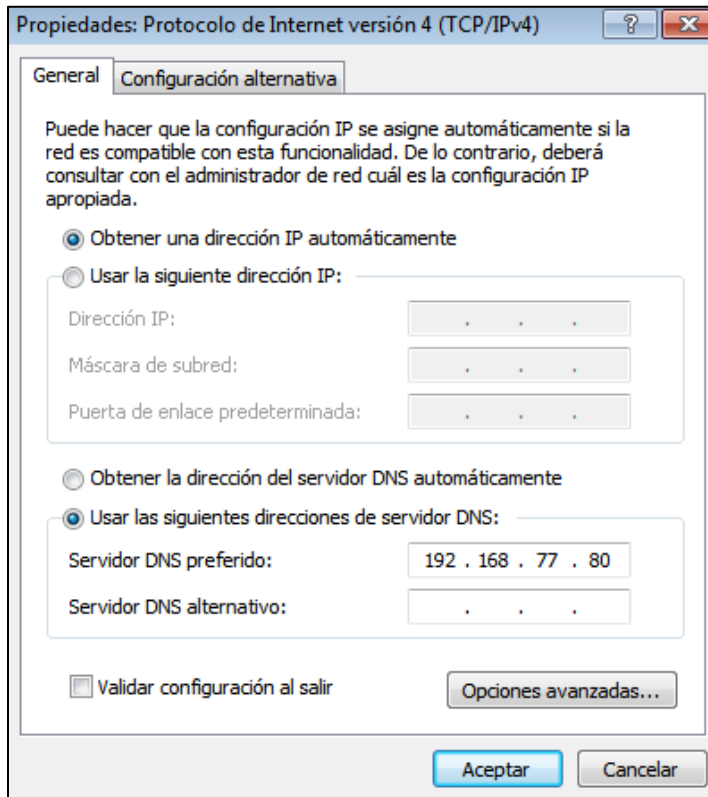
The image shows a network configuration window for a virtual machine. It is divided into two main sections: 'Device status' and 'Network connection'. In the 'Device status' section, there are two checkboxes: 'Connected' and 'Connect at power on', both of which are checked. In the 'Network connection' section, there are four radio button options: 'Bridged: Connected directly to the physical network', 'NAT: Used to share the host's IP address', 'Host-only: A private network shared with the host', and 'Custom: Specific virtual network'. The 'Custom' option is selected. Below the 'Custom' option, there is a dropdown menu that currently displays 'tuempresa (Host-only)'. At the bottom of the 'Network connection' section, there is a 'LAN segment:' label followed by an empty dropdown menu.

TODAS LAS MÁQUINAS QUE DEBAN PERTENECER AL DOMINIO NECESITARÁN ESTAR CONECTADAS A LA MISMA RED.

Si su máquina tiene problemas con detectar el dominio más adelante, tendrá que jugar con los adaptadores de redes, e ir cambiando para comprobar cuál es el correcto. Eso solo en caso de que tengo más de un adaptador conectado y funcionando en su máquina virtual. Si solo tiene uno, no debería haber problemas de conexión.

Recomendación: Desactive todos los adaptadores que tenga en el sistema para ubicar de manera fácil el que conecta el futuro cliente con el servidor de AD.

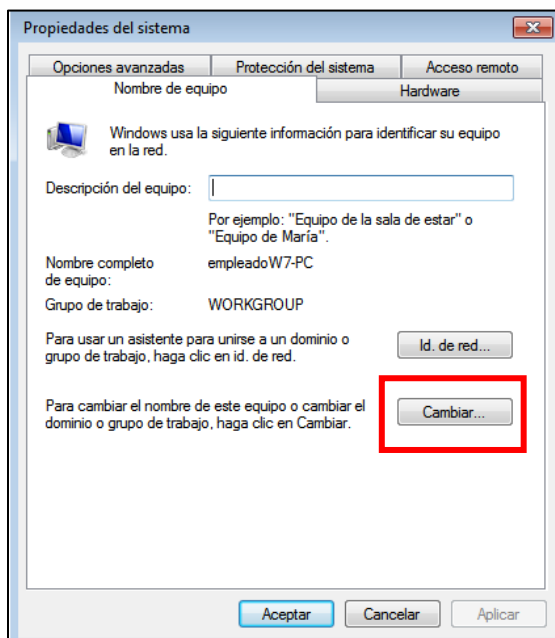
3. Cada máquina, por el momento, deberá contar con una IP estática. De esta forma será posible comunicarse con el servidor, y el dominio será detectado de inmediato. ALGO IMPORTANTE: El DNS debe ser la IP del servidor AD.



Esta máquina todavía no tiene una IP estática configurada, pero el DNS está colocado. Anteriormente ya se había configurado una IP estática, así que la demostración extra estaría de más.

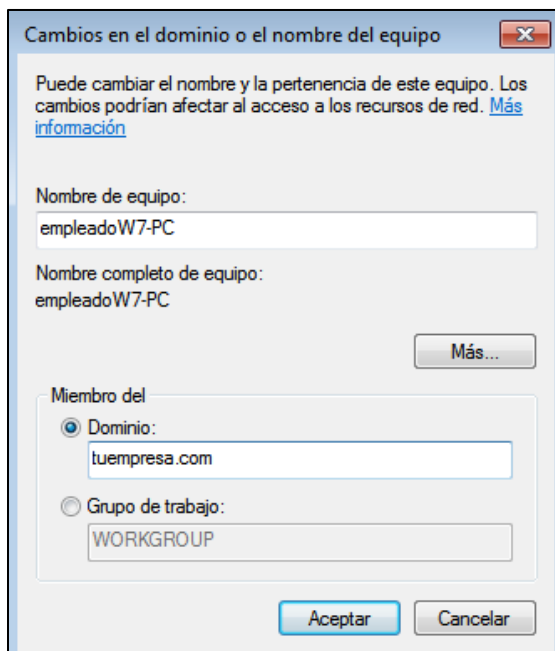
Windows 7

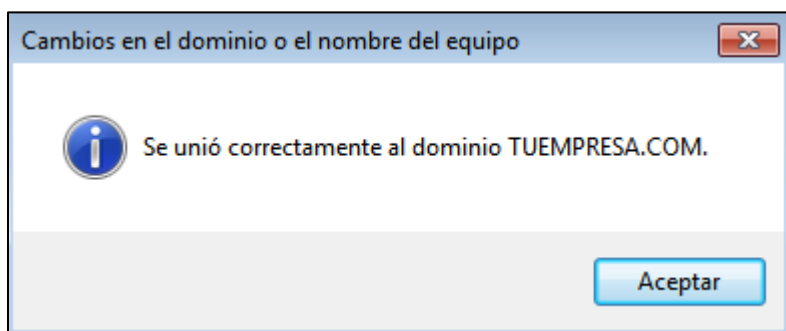
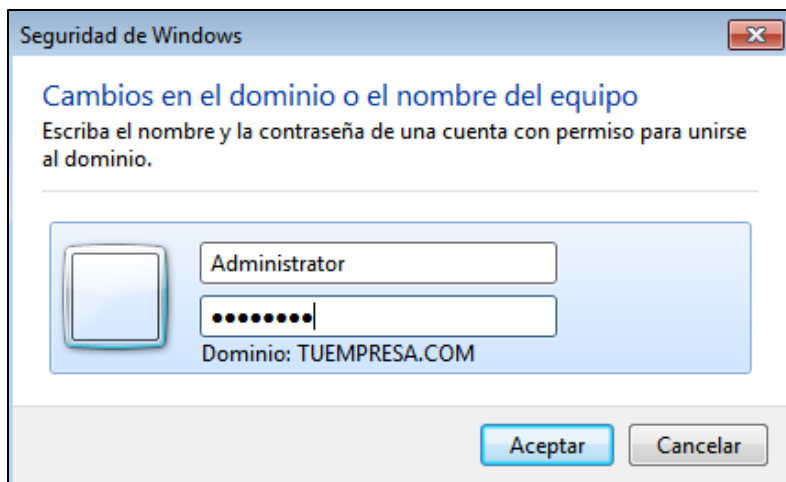
Para agregar una máquina a un dominio el proceso suele ser similar. Desde Windows 7 a Windows 10 el proceso puede ser realizado desde la configuración avanzada del sistema. LA RUTA PARA LLEGAR ES: **Configuración → Sistema → Configuración avanzada → Cambio de nombre** y posteriormente en el apartado tendremos la opción de agregarnos a un dominio.



Si recuerda lo anteriormente mencionado, se mencionó anteriormente que el dominio sería agregado tal y como el AD lo configuró, y usted era libre de cambiarlo. En este caso, escrito con letras minúsculas el sistema no detectará el dominio.

La forma de escribirlo sería **TUEMPRESA.COM**



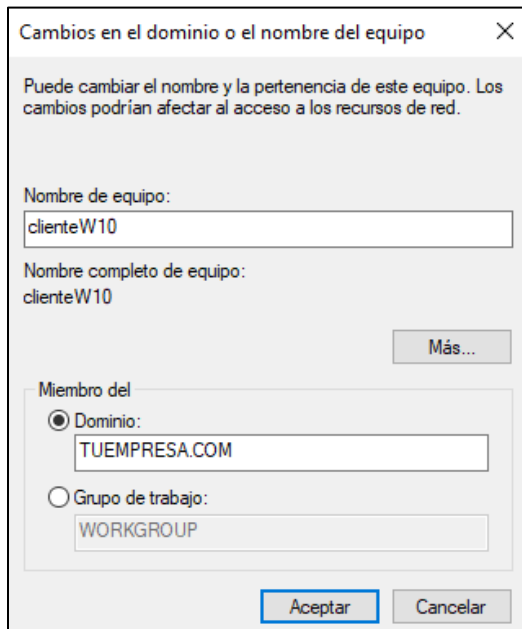


Lo mismo pasa con las credenciales. Si su servidor de AD está en español, deberá escribir el nombre de administrador en el mismo idioma. De lo contrario, como es este caso, deberá hacerlo tal y como lo muestre el sistema: **Administrator**. Más adelante se mostrará un escenario contrario a este.

Y posteriormente la contraseña.

Un mensaje como el de la ilustración deberá mostrarse y, deberá actualizar su máquina en caso de que no pase automáticamente.

Windows 10



Cambios en el dominio o el nombre del equipo

Puede cambiar el nombre y la pertenencia de este equipo. Los cambios podrían afectar al acceso a los recursos de red.

Nombre de equipo:
clienteW10

Nombre completo de equipo:
clienteW10

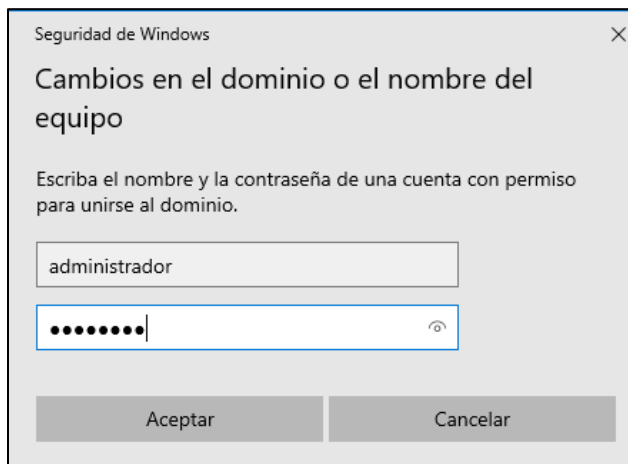
Más...

Miembro del

☒ Dominio:
TUEMPRESA.COM

☐ Grupo de trabajo:
WORKGROUP

Aceptar Cancelar



Seguridad de Windows

Cambios en el dominio o el nombre del equipo

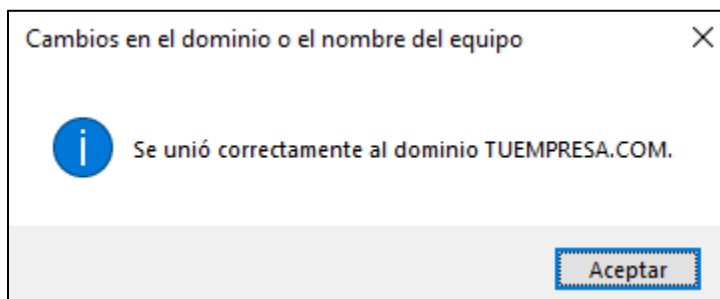
Escriba el nombre y la contraseña de una cuenta con permiso para unirse al dominio.

administrador

.....

Aceptar Cancelar

En este caso, con Windows 10 está bien escrito el nombre del dominio, pero las credenciales no, por lo que no podrá ingresar si no son escritas de la forma correcta.



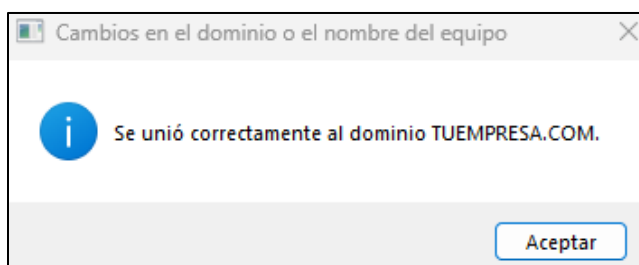
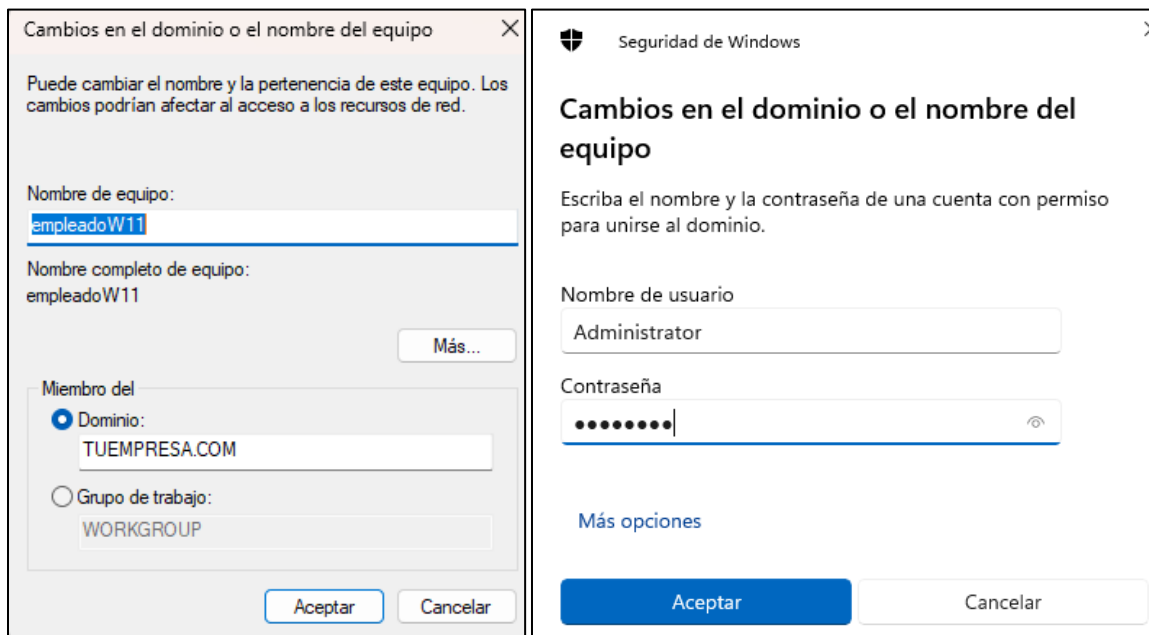
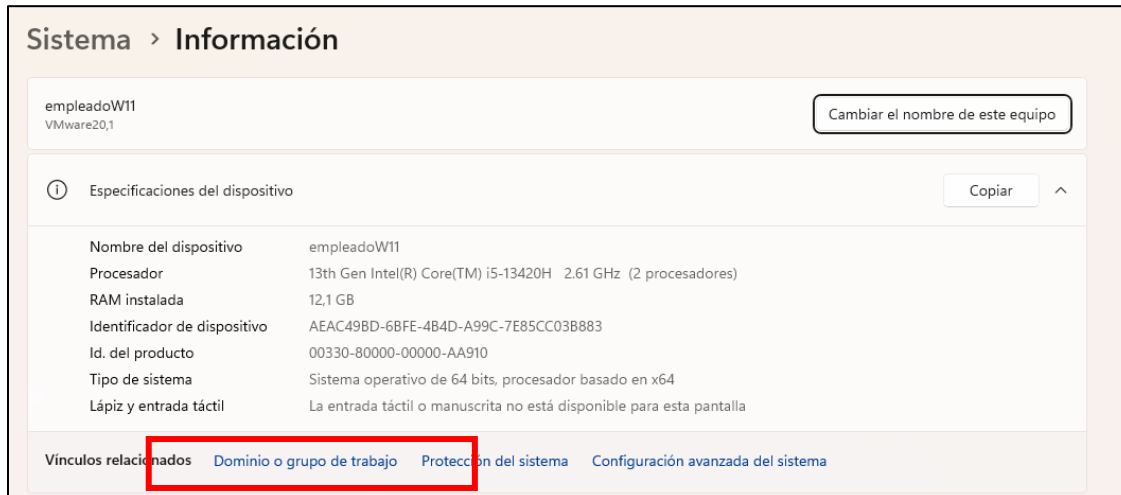
Cambios en el dominio o el nombre del equipo

Se unió correctamente al dominio TUEMPRESA.COM.

Aceptar

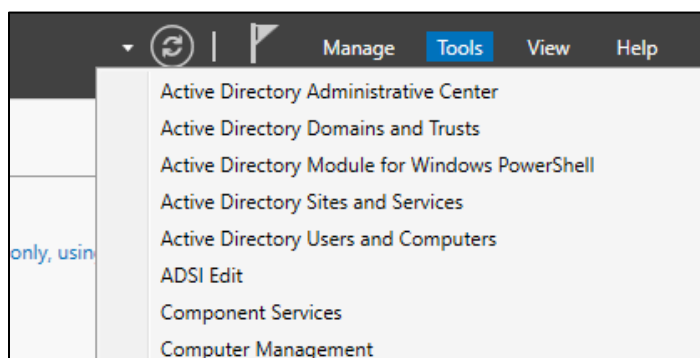
Windows 11

En el caso de Windows 11, puede dificultarse encontrar la opción de agregar la máquina a un dominio. O, puede ser todo lo contrario. Una vez en información avanzada del sistema, encontrará la opción de **Dominio o grupo de trabajo**. Este último escenario plantea todo de forma correcta, sin errores.

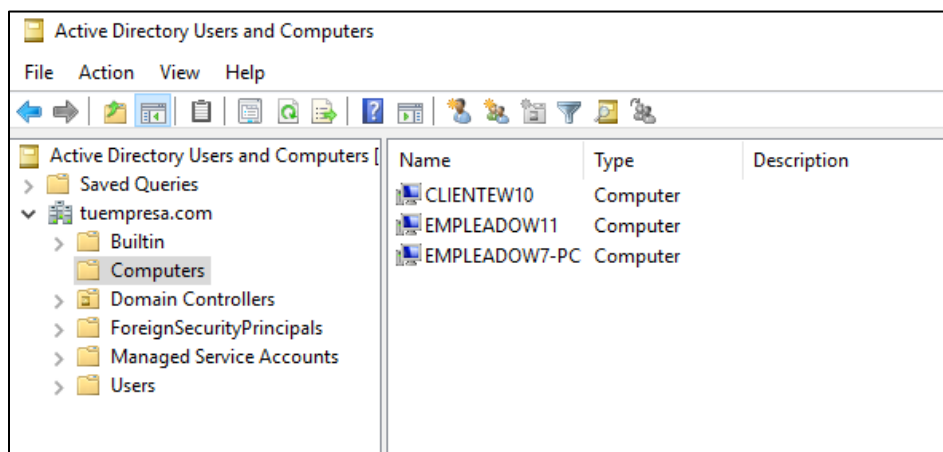


Comprobar los nuevos equipos en el dominio

El paso más sencillo luego de posiblemente mucho “trote”. Directamente en Tools, desde el panel de nuestro Windows Server, podremos confirmar que los equipos se han añadido al dominio. La pestaña es **Active Directory Users and Computers**, si está en inglés. De estar en español sería algo como: **Usuarios y Equipos de Active Directory**. En cualquier caso, independientemente del idioma, estará organizado en orden alfabético.



Una vez en la pestaña de usuarios y equipos, podremos ver debajo de nuestro dominio, en la unidad de **Computers** o **Equipos**, dependiendo del idioma, aquellos equipos que fueron añadidos al dominio.



Si todo está en orden, se puede continuar a la siguiente parte de esta guía. Es momento de agregar usuarios al sistema, y posteriormente configurar más roles y nuevas políticas en el sistema.

NOTA IMPORTANTE: Es recomendable mover los equipos de las carpetas a las que son agregados una vez se unen al dominio. Esto, para evitar complicaciones a la hora de aplicar políticas a cada equipo. Bien pueden moverse a una misma UO o a varias; este ejemplo se verá más adelante.

Objetos en AD

¿Qué es un objeto en AD?

Los objetos de son entidades únicas y específicas que suelen representar un recurso dentro del dominio. Estos objetos suelen variar en su tipo. Usuarios, unidades organizativas, computadoras, grupos... Cada recurso o activo utilizado con un fin, es un objeto en AD.

Tipos de objetos

Usuarios

Sencillamente, un usuario en AD es una cuenta individual que accede a los recursos de un dominio.

Unidades organizativas

Una unidad organizativa es un contenedor objetos en AD. Estas sirven como carpetas que mantienen el orden con los distintos grupos, usuarios y/o equipos que haya en el dominio. Suelen utilizarse para aplicar directamente políticas de seguridad. De esta forma el controlador de dominio no se preocupa por restringir de forma individual a cada usuario.

Grupos

Conjunto de usuarios que compartes permisos.

Computadoras

Equipos añadidos al dominio.

Políticas de grupo (GPOs)

No suelen definirse directamente como objetos en AD, pero suelen estar relacionadas a ello.

Una política de grupo es una regla de acceso, restricción o vinculación, que suelen ser aplicadas a los distintos objetos tradicionales en AD.

Las políticas pueden ser de:

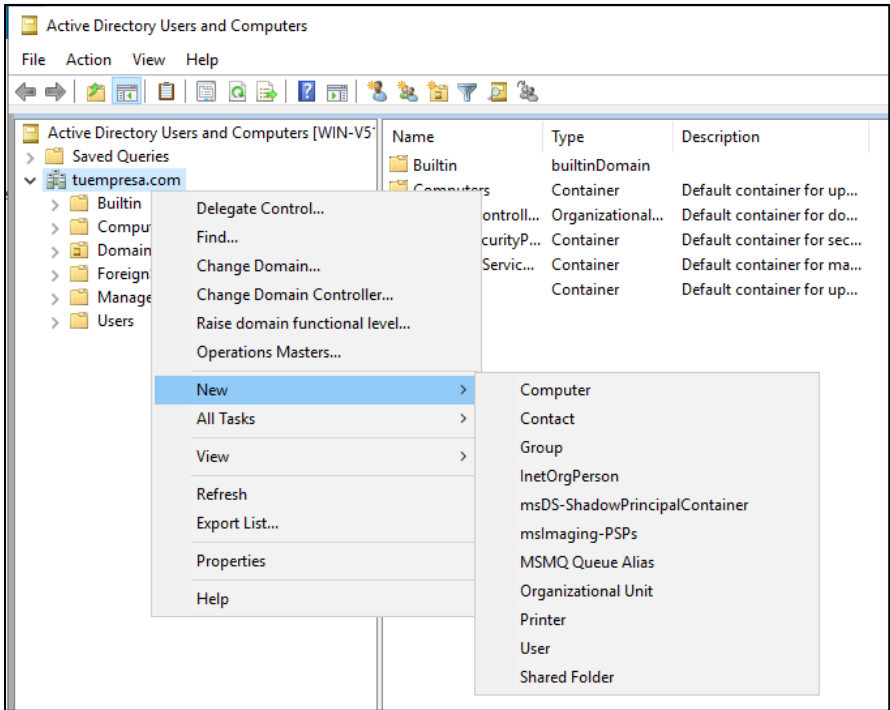
- Restricciones de acceso.
- Seguridad (contraseñas, bloqueos de cuentas, auditoría, etc.).
- Configuración de software (instalación, actualización, eliminación de software).
- Configuración de red y de sistema operativo.

Administración de objetos en AD

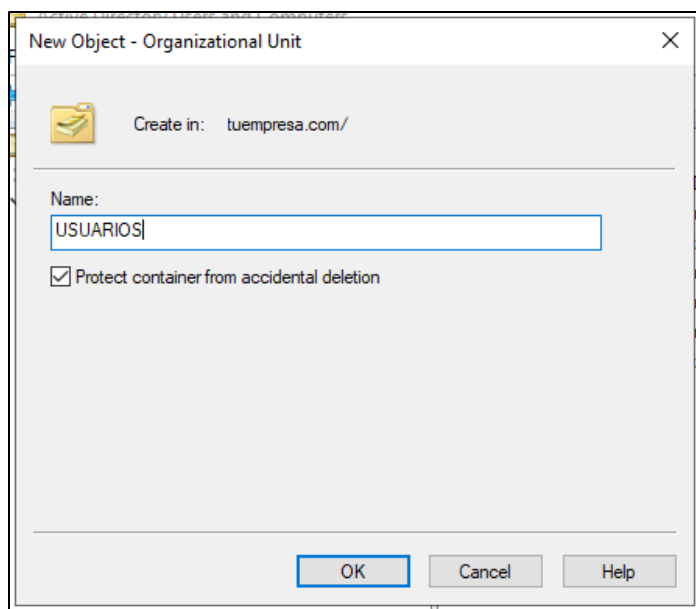
Unidades Organizativas

Creación de Unidades Organizativas

La administración de objetos en AD suele ser sencilla. Tanto como dirigirse a la herramienta **usuarios y equipos de Active Directory**, dar clic derecho sobre el nombre de **dominio**, luego a “nuevo”, y por último a **unidad organizativa**.



Luego, tendremos la oportunidad de nombrar nuestra nueva unidad organizativa. La casilla marcada debajo del cuadro de texto, hace referencia a la **eliminación accidental** de la unidad, y se marca por defecto como medida de seguridad. El administrador de dominio la marcará o no según sus necesidades o las de la empresa. En este caso se quedará marcada, pero si desea deshabilitar esa función, más adelante se mostrará cómo hacerlo.



En total, cuatro unidades organizativas fueron creadas. Donde, una almacena tres más.

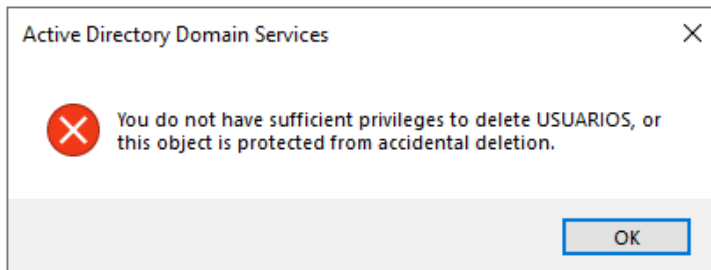
	Name	Type	Description
Active Directory Users and Computers [WIN-V5]			
> Saved Queries			
▼ tuempresa.com			
> Built-in			
> Computers			
> Domain Controllers			
> ForeignSecurityPrincipals			
> Managed Service Accounts			
> Users			
▼ USUARIOS			
> ADMINISTRATIVOS			
> SOPORTE			
> VENTAS			
	SOPORTE	Organizational...	Esta unidad almacena los usuarios encargados del soporte en
	VENTAS	Organizational...	Esta unidad almacena los usuarios encargados de las ventas e
	ADMINISTRATIVOS	Organizational...	Esta unidad almacena los usuarios encargados de los proces

Todas, excepto la unidad **USUARIOS**, tienen la casilla de eliminación accidental sin marcar.

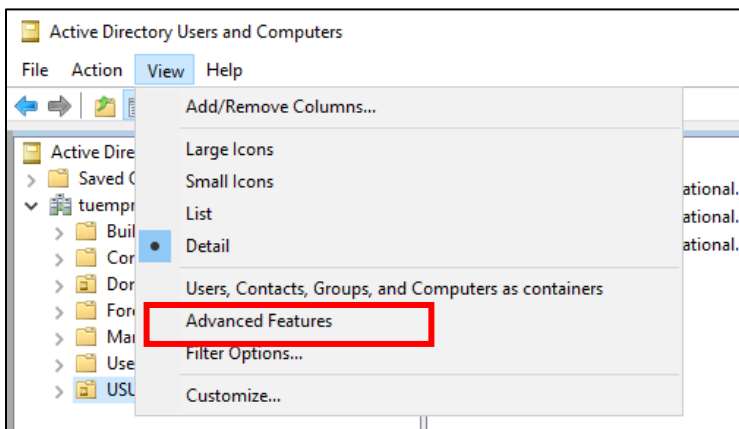
NOTA: Para agregar descripciones y otro tipo de datos, en las **propiedades** de la unidad puede hacerlo.

Eliminar una unidad organizativa

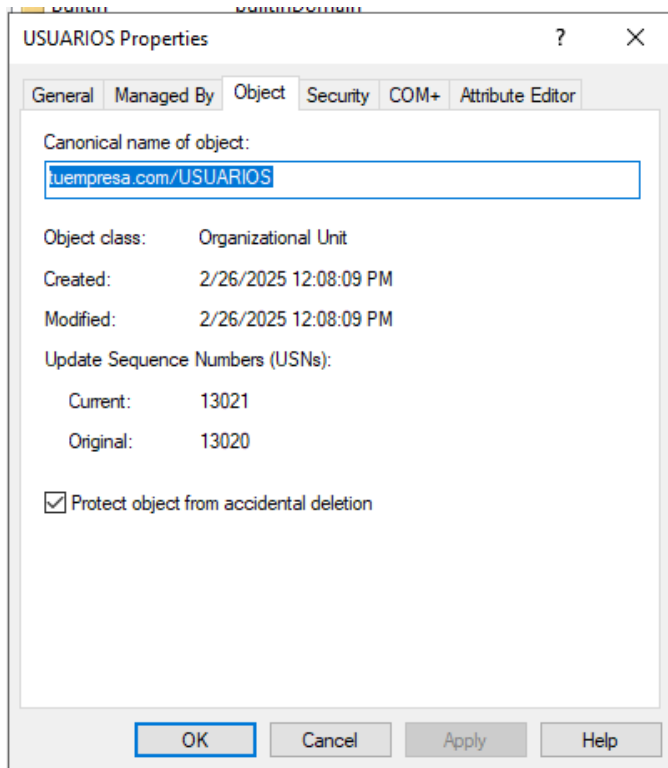
Notará que, al dar clic derecho sobre un objeto, tendrá más de una opción por seleccionar, entre ellas **eliminarlo**. Pero, si la casilla de eliminación accidental está habilitada en una unidad organizativa, le aparecerá el siguiente error.



Para lograr eliminar una UO con éxito, en la barra de opciones superior, en la pestaña **View** o **Vista** (según el idioma), marcará la opción **Advanced Features**.



Una vez marcada la opción, notará que más objetos aparecerán en su dominio, pero no usará nada de eso. Lo que necesita es dirigirse a las propiedades de su UO, donde ahora tendrá la pestaña de **Object** u **Objeto**. De inmediato logrará ver la casilla que busca desmarcar. Una vez aplicados los cambios podrá eliminar la UO sin problemas.

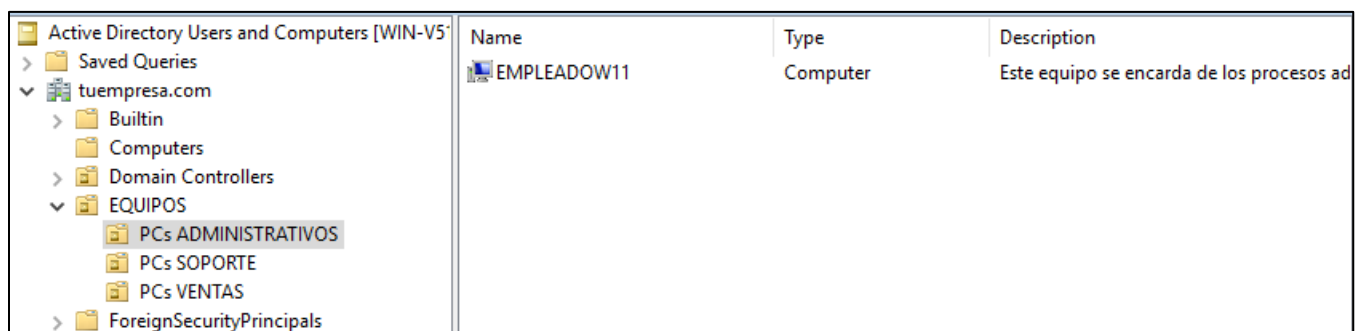


Más unidades organizativas

A continuación, se muestra una ilustración con dos nuevas UO creadas en el dominio tuempresa.com.

Estas fueron: **EQUIPOS** y **GRUPOS**.

Anteriormente se había mencionado algo sobre mover los equipos de aquella carpeta a la que son agregados: **Computers**. En este apartado movimos los equipos a sus UO correspondientes.



Active Directory Users and Computers [WIN-V5]	Name	Type	Description
<ul style="list-style-type: none"> Saved Queries tuempresa.com <ul style="list-style-type: none"> Builtin Computers Domain Controllers EQUIPOS <ul style="list-style-type: none"> PCs ADMINISTRATIVOS PCs SOPORTE PCs VENTAS 	CLIENTEW10	Computer	Este equipo se encarga de dar soporte

Active Directory Users and Computers [WIN-V5]	Name	Type	Description
<ul style="list-style-type: none"> Saved Queries tuempresa.com <ul style="list-style-type: none"> Builtin Computers Domain Controllers EQUIPOS <ul style="list-style-type: none"> PCs ADMINISTRATIVOS PCs SOPORTE PCs VENTAS ForeignSecurityPrincipals 	EMPLEADOW7-PC	Computer	Este equipo es encargado de las ventas

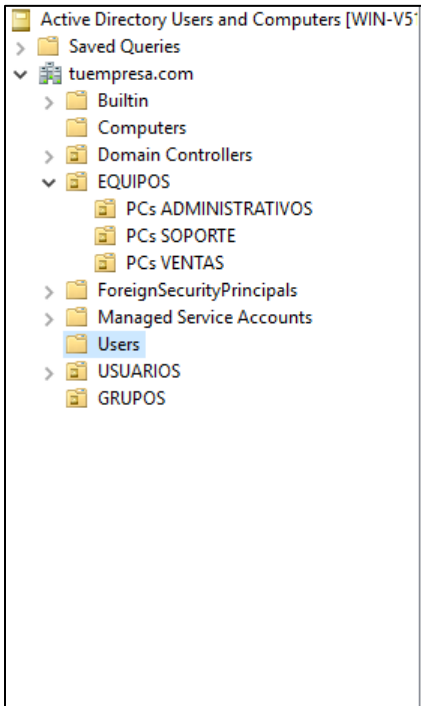
Por el momento no serán utilizados estos grupos. Pero para otorgar permisos de acceso y demás, también para encontrar usuarios con facilidad, suelen ser muy útiles.

Active Directory Users and Computers [WIN-V5]	Name	Type	Description
<ul style="list-style-type: none"> Saved Queries tuempresa.com <ul style="list-style-type: none"> Builtin Computers Domain Controllers EQUIPOS <ul style="list-style-type: none"> PCs ADMINISTRATIVOS PCs SOPORTE PCs VENTAS ForeignSecurityPrincipals Managed Service Accounts Users USUARIOS <ul style="list-style-type: none"> GRUPOS 	<ul style="list-style-type: none"> Admins-Ventas Usuarios-Ventas Admins-Soporte Usuarios-Soporte Admins-Administrativos Usuarios-Administrativos 	<ul style="list-style-type: none"> Security Group - Global Security Group - Global Security Group - Global Security Group - Global Security Group - Global Security Group - Global 	<ul style="list-style-type: none"> Usuarios con permisos avanzados Usuarios regulares de Ventas Usuarios con permisos avanzados Usuarios regulares de Soportes Usuarios con permisos avanzados Usuarios regulares de Administrativos

Usuarios

Creación de Usuarios

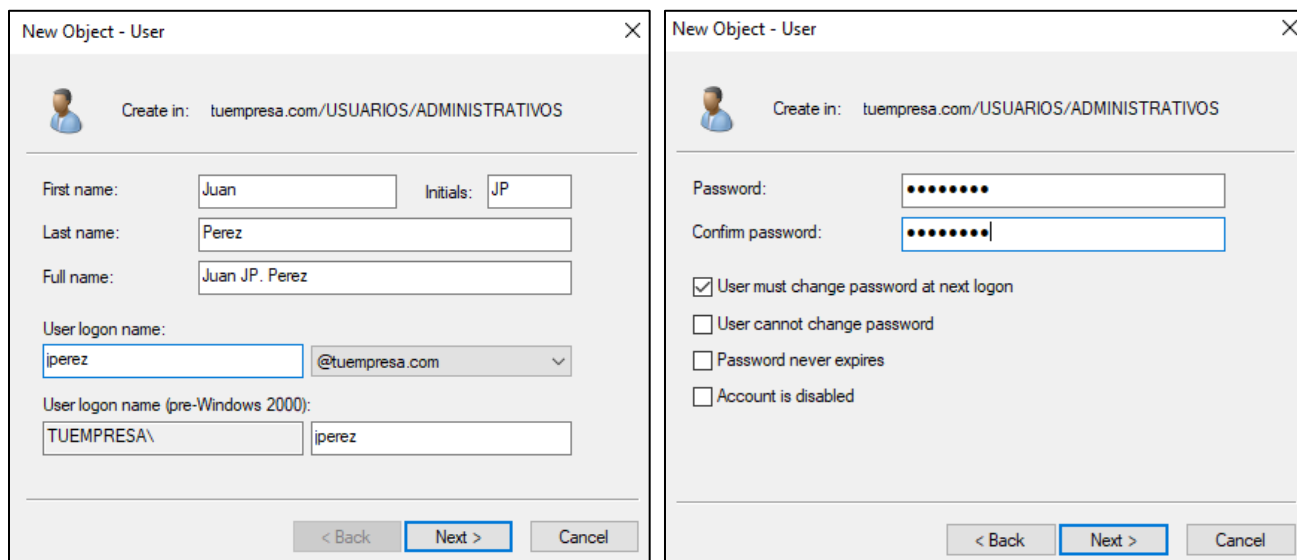
Los usuarios son una parte importante en AD, anteriormente ya se habló sobre ello. Su creación puede hacerse en distintas partes. Bien puede ser en el grupo Usuarios, que de por sí ya está creado en el dominio, o, en una unidad organizativa específica.

	Name	Type	Description
	RAS and IAS Servers	Security Group - Do...	Servers in this group can acc
	Cloneable Domain Controllers	Security Group - Global	Members of this group that
	Enterprise Key Admins	Security Group - Univ...	Members of this group can
	Key Admins	Security Group - Global	Members of this group can
	Enterprise Read-only Domain ...	Security Group - Univ...	Members of this group are R
	Read-only Domain Controllers	Security Group - Global	Members of this group are R
	Cert Publishers	Security Group - Do...	Members of this group are p
	Protected Users	Security Group - Global	Members of this group are a
	Denied RODC Password Replic...	Security Group - Do...	Members in this group cann
	Group Policy Creator Owners	Security Group - Global	Members in this group can
	Allowed RODC Password Repli...	Security Group - Do...	Members in this group can f
	DnsUpdateProxy	Security Group - Global	DNS clients who are permitt
	DnsAdmins	Security Group - Do...	DNS Administrators Group
	Schema Admins	Security Group - Univ...	Designated administrators o
	Enterprise Admins	Security Group - Univ...	Designated administrators o
	Domain Admins	Security Group - Global	Designated administrators o
	Guest	User	Built-in account for guest ac
	Administrator	User	Built-in account for adminis
	Domain Computers	Security Group - Global	All workstations and servers
	Domain Users	Security Group - Global	All domain users
	Domain Guests	Security Group - Global	All domain guests
	Domain Controllers	Security Group - Global	All domain controllers in the

Podrá identificar carpetas que ya trajo del dominio y las Unidades Organizativas. Las carpetas que ya vienen, a excepción de **Domain Controllers** (que tiene el equipo servidor de AD), no tienen diseño alguno en sus íconos. A diferencia de las UO, que tienen una especie de ícono en la misma carpeta.

En este caso, crearemos usuarios en unidades organizativas específicas. Pero, si desea hacerlo desde el grupo usuarios, podrá moverlos a otro objeto sin problema alguno.

La creación de usuarios en AD se basa en dos pasos. Lo inicial ya se conoce, clic derecho en cualquier unidad organizativa o espacio en el que quiera crearse el usuario. A partir de eso, aparecerán los siguientes cuadros.



The image displays two sequential screenshots of the 'New Object - User' dialog box in Active Directory. The first screenshot shows the 'Name' tab, where the user's details are entered: First name (Juan), Last name (Perez), Initials (JP), Full name (Juan JP. Perez), User logon name (jperez), and User logon name (pre-Windows 2000) (TUEMPRESA\jperez). The second screenshot shows the 'Password' tab, where the user's password is set: Password (masked with dots) and Confirm password (masked with dots). It also includes checkboxes for 'User must change password at next logon' (checked), 'User cannot change password', 'Password never expires', and 'Account is disabled'.

Este será el único usuario donde se llenarán todos los campos solicitados. No es necesario acaparar cada cuadro de texto, al menos no el de **Initials**, ya que **Full Name** se completa de forma automática con **First Name** y **Last Name**.

La única casilla marcada en el apartado de contraseñas para el usuario es **Cambiarla en el siguiente inicio de sesión**. Esto quiere decir que, en cuanto el usuario inicie sesión luego de su creación, la contraseña deberá ser cambiada por el mismo.

Esta es una **medida de seguridad**. En ocasiones las empresas crean los usuarios con contraseñas únicas para todos; si el usuario continúa con la misma, sería un peligro para la información. Para evitar esto, se aplican medidas como esta, además de políticas como: **contraseñas únicas y fuertes**, para que los usuarios no utilicen la misma contraseña y aprendan a crear contraseñas fuertes.

Active Directory Users and Computers [WIN]	Name	Type	Description
<ul style="list-style-type: none"> Saved Queries tuempresa.com <ul style="list-style-type: none"> Builtin Computers Domain Controllers EQUIPOS ForeignSecurityPrincipals Managed Service Accounts Users USUARIOS <ul style="list-style-type: none"> ADMINISTRATIVOS SOPORTE VENTAS GRUPOS 	<ul style="list-style-type: none"> Juan JP. Perez María Sanchez Ana Martinez Laura Ramirez Sofia Herrera 	<ul style="list-style-type: none"> User User User User User 	

Active Directory Users and Computers [WIN]	Name	Type	Description
<ul style="list-style-type: none"> Saved Queries tuempresa.com <ul style="list-style-type: none"> Builtin Computers Domain Controllers EQUIPOS ForeignSecurityPrincipals Managed Service Accounts Users USUARIOS <ul style="list-style-type: none"> ADMINISTRATIVOS SOPORTE VENTAS GRUPOS 	<ul style="list-style-type: none"> Luis Torres Valeria Castro Miguel Jimenez Daniela Ortiz Andres Morales 	<ul style="list-style-type: none"> User User User User User 	

Active Directory Users and Computers [WIN]	Name	Type	Description
<ul style="list-style-type: none"> Saved Queries tuempresa.com <ul style="list-style-type: none"> Builtin Computers Domain Controllers EQUIPOS ForeignSecurityPrincipals Managed Service Accounts Users USUARIOS <ul style="list-style-type: none"> ADMINISTRATIVOS SOPORTE VENTAS GRUPOS 	<ul style="list-style-type: none"> Gabriela Vega Mariana Navarro Ricardo Paredes Patricia Mendez Pedro Sanchez 	<ul style="list-style-type: none"> User User User User User 	

En este escenario, todos los usuarios fueron creados con esa única casilla marcada y una misma contraseña, la cual deberá ser cambiada tan pronto sean registrados en un equipo. Si se quiere cambiar esta opción, basta con ir a las propiedades del usuario y desmarcar dicha casilla.

Propiedades de un usuario

Para validar o cambiar información sobre un usuario, el lugar al cual se debe acudir a las propiedades del mismo. Esta opción abarca múltiples pestañas que ayudan a la configuración de los usuarios.

Si quiere confirmar o cambiar:

- Nombre completo del usuario
- Nombre para iniciar sesión
- Grupos a los que pertenece
- Contraseña
- Habilitar o deshabilitar su cuenta
- Información personal (dirección, puesto de trabajo, número de teléfono...)
- Entre otras opciones. Todo se hace desde propiedades.

Ejemplos:

Información general del usuario

The screenshot shows the 'Miguel Jimenez Properties' dialog box with the 'General' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are tabs: 'Remote control', 'Remote Desktop Services Profile', 'COM+', 'Member Of', 'Dial-in', 'Environment', 'Sessions', 'General', 'Address', 'Account', 'Profile', 'Telephones', and 'Organization'. The 'General' tab is active, showing a user icon and the name 'Miguel Jimenez'. Below this are fields for 'First name' (containing 'Miguel'), 'Last name' (containing 'Jimenez'), 'Display name' (containing 'Miguel Jimenez'), 'Description', 'Office', 'Telephone number', 'E-mail', and 'Web page'. At the bottom are buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

Información de la cuenta

The screenshot shows the 'Miguel Jimenez Properties' dialog box with the 'Account' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are tabs: 'Member Of', 'Dial-in', 'Environment', 'Sessions', 'Remote control', 'Remote Desktop Services Profile', 'COM+', 'General', 'Address', 'Account', 'Profile', 'Telephones', and 'Organization'. The 'Account' tab is active, showing fields for 'User logon name' (containing 'miguel') and 'User logon name (pre-Windows 2000):' (containing 'TUEMPRESA\miguel'). Below these are buttons for 'Logon Hours...' and 'Log On To...'. There is a checkbox for 'Unlock account'. Under 'Account options', there are checkboxes for 'User must change password at next logon' (checked), 'User cannot change password', 'Password never expires', and 'Store password using reversible encryption'. Under 'Account expires', there is a radio button for 'Never' (selected) and a radio button for 'End of:' with a date field showing 'Friday, March 28, 2025'. At the bottom are buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

Grupos a los que pertenece

Miguel Jimenez Properties

General Address Account Profile Telephones Organization

Remote control Remote Desktop Services Profile COM+

Member Of Dial-in Environment Sessions

Member of:

Name	Active Directory Domain Services Folder
Domain Users	tuempresa.com/Users

Add... Remove

Primary group: Domain Users

Set Primary Group There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

OK Cancel Apply Help

Teléfonos

Miguel Jimenez Properties

Member Of Dial-in Environment Sessions

Remote control Remote Desktop Services Profile COM+

General Address Account Profile Telephones Organization

User login name: miguel @tuempresa.com

User login name (pre-Windows 2000): TUEMPRESA\ miguel

Login Hours... Log On To...

☐ Unlock account

Account options:

- ☒ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Store password using reversible encryption

Account expires

☒ Never

☐ End of: Friday , March 28, 2025

OK Cancel Apply Help

Si desea mover, eliminar o hacer otras acciones con los usuarios, basta con dar clic derecho sobre el mismo.

Iniciar sesión con un usuario de AD en un equipo del dominio

Para iniciar sesión con un usuario del dominio, es necesario recordar el nombre que le fue asignado para dicha acción al momento de crearlo. De no tenerlo claro, deberá revisarlo en la pestaña de **cuenta** en propiedades.

Iniciaremos sesión en los equipos correspondientes de cada usuario:

Equipo de Ventas (Windows 7) --- Pedro Sánchez

Equipo de Soporte (Windows 10) --- Miguel Jiménez

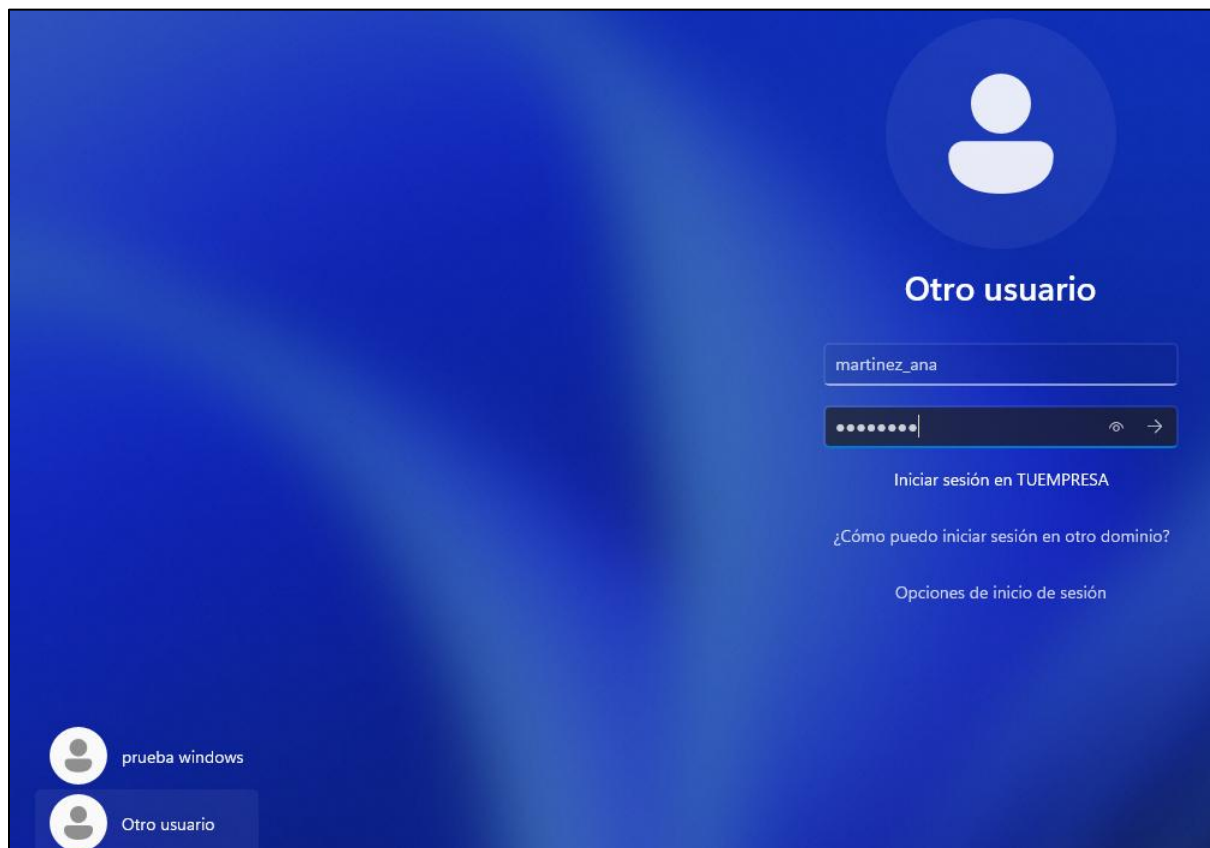
Equipo de Administración (Windows 11) --- Ana Martínez

Equipo de Administración (Windows 11) --- Ana Martínez

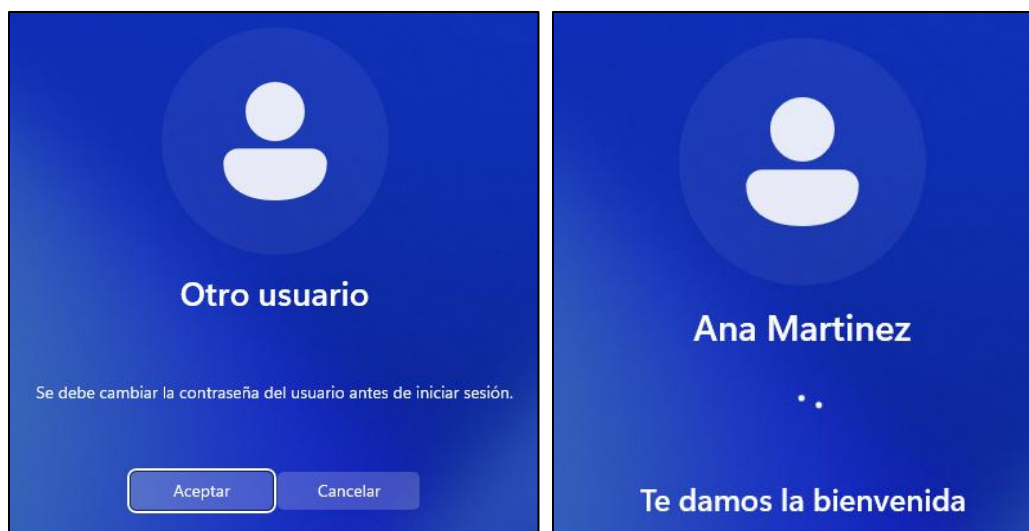
En cada usuario verificares con qué nombre debemos iniciar sesión

User logon name:	
<input type="text" value="martinez_ana"/>	<input type="text" value="@tuempresa.com"/>
User logon name (pre-Windows 2000):	
<input type="text" value="TUEMPRESA\"/>	<input type="text" value="martinez_ana"/>

Luego, ubicar el equipo al cual pertenece el usuario. Una vez ubicado, no es más que colocar el nombre correspondiente donde se solicita.



Si antes de adherir el equipo al dominio, tenía un usuario, deberá clicar **Otro usuario** para ingresar las credenciales.



Si el dominio ya tiene establecida una política de contraseñas fuertes, se deberán tener en cuenta los parámetros que solicite la política en cuestión. Esto puede incluir: longitud de contraseña; combinación de caracteres, letras y números...

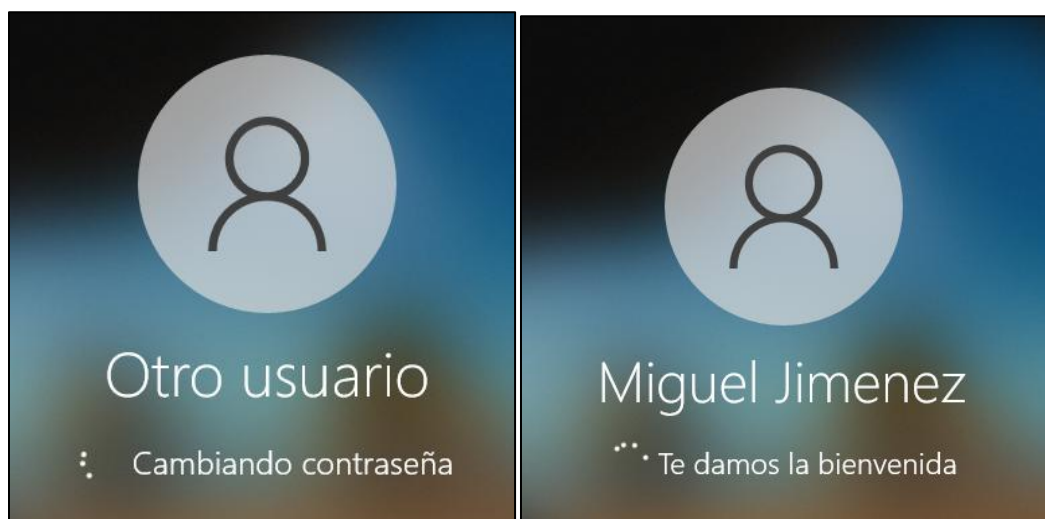
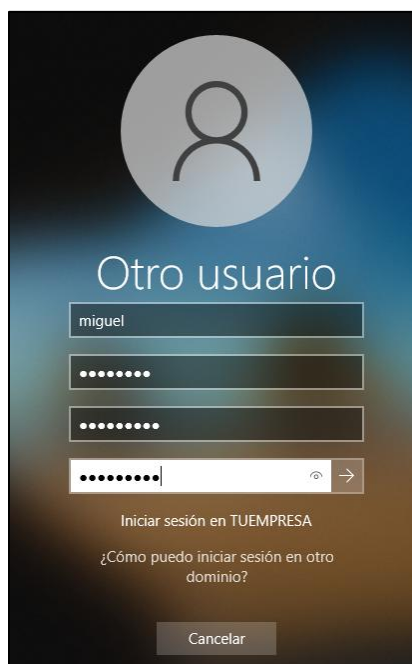
Una vez la sesión sea iniciada, el equipo comenzará a ser configurado. Nuevamente, si el dominio tiene establecidas varias políticas, estas serán aplicadas tan pronto el usuario se registre. Esto incluye: Políticas de fondo de pantalla, carpetas compartidas, horario, restricciones y acceso, entre otras...

Equipo de Soporte (Windows 10) --- Miguel Jiménez

User logon name:

@tuempresa.com

User logon name (pre-Windows 2000):

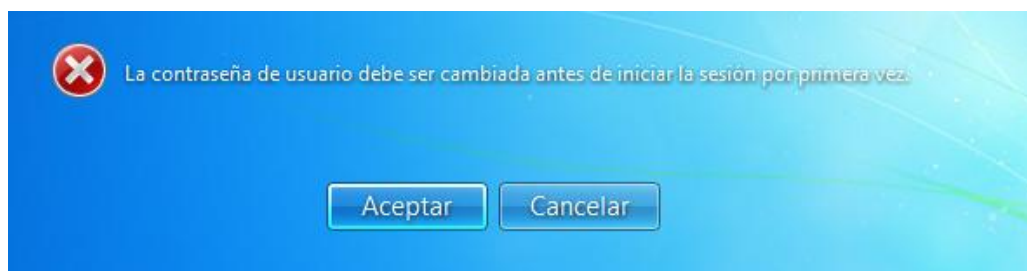


Equipo de Ventas (Windows 7) --- Pedro Sánchez

User logon name:

@tuempresa.com

User logon name (pre-Windows 2000):



A Windows 7 login screen with a blue background. It features four input fields: the first contains "PS", the second and third are filled with dots, and the fourth is also filled with dots and has a cursor at the end. To the right of the fourth field is a blue circular button with a white right-pointing arrow. Below the fields, the text reads: "Iniciar sesión en: TUEMPRESA" and "¿Cómo puedo iniciar sesión en otro dominio?".

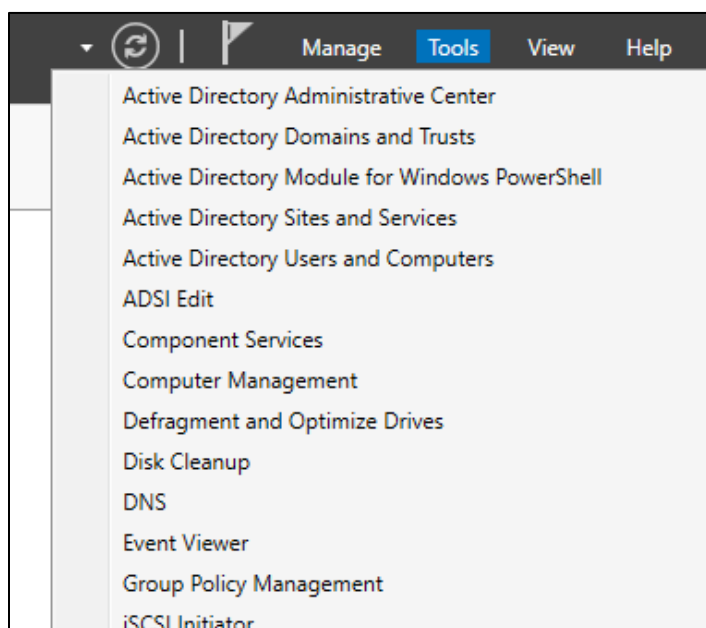


Políticas de Grupo (GPOs)

Implementación de políticas

La implementación de políticas varía según el tipo de política que sean. Estas pueden ser a nivel de dominio, a nivel de usuario o unidades organizativas, a nivel de sitios, etc.

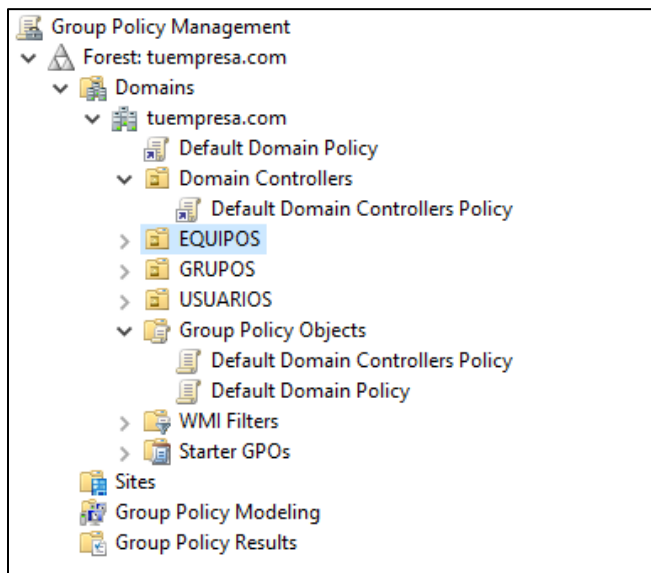
Cuando se trata de políticas de dominio, suele editarse la política por defecto que trae el mismo. Pero, por motivos de seguridad y evitar confusiones, lo recomendado es hacer las políticas de forma individual, en caso de que sean varias. En este escenario se configurará cada política de forma individual, siempre y cuando sean de distintas categorías.



Políticas de contraseñas

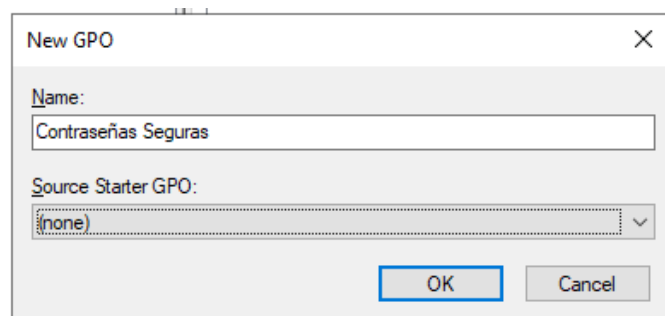
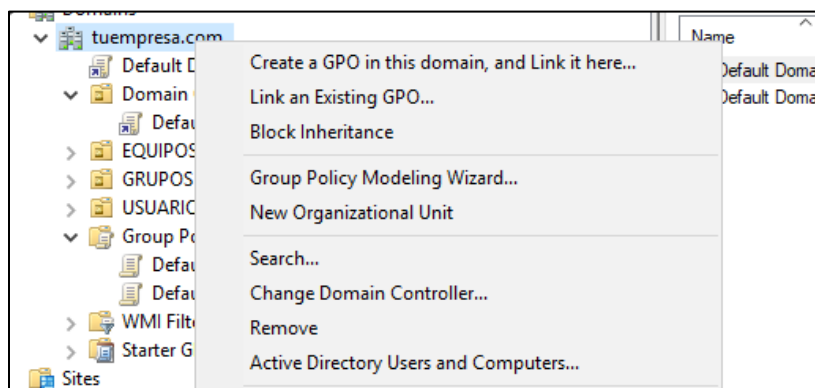
Las políticas de contraseñas son utilizadas para aumentar los parámetros de seguridad. Estas pueden ir desde la longitud mínima de caracteres, hasta la complejidad de su composición. En este escenario crearemos una política únicamente para las contraseñas; aunque, se mencionó anteriormente que también puede configurarse en la política por defecto que trae el dominio.

En la siguiente ilustración vemos la estructura de nuestro dominio. Donde, desde el nombre tuempresa.com aparecen todas las UO, sitios y otros grupos del dominio. También, junto a estos se aprecian las políticas vinculadas a cada objeto, si es que tienen.

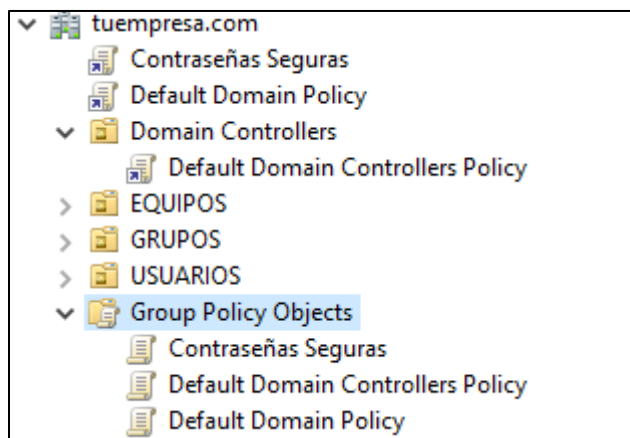


La creación de una política se puede realizar de dos formas: Una: crearla y vincularla directamente en la UO o grupo que deseemos. Esto aumenta las posibilidades de que la política sea creada y aplicada en el lugar correspondiente. Dos: crearlas en la carpeta **Group Policy Objects** u **Objetos de directiva de grupo**. Esta carpeta contiene TODAS las políticas creadas en el dominio, sin importar si están vinculadas o no a alguna UO. De no tener una política vinculada a algún grupo, esta acción puede realizarse al dar clic derecho sobre la política, y elegir la opción de vincular y luego adherirla a un objeto.

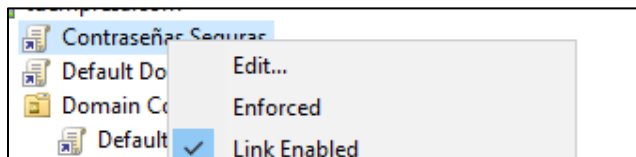
En ocasiones es mejor crear las políticas desde la carpeta **Group Policy Objects**, recomendable si dicha política será aplicada a más de una UO. Pero, como esta política será aplicada para todos los usuarios del dominio, se vinculará directamente al mismo.



Una vez creada la política, aparecerá tanto en el grupo donde fue vinculada como en la carpeta GPO. Si solo fue creada en la GPO, aparecerá únicamente en ese apartado.



Para configurar la política, debe dar clic derecho sobre ella, y oprimir **Edit** o **Editar**. Esto es importante, ya que una política no se crea previamente configurada a pesar del nombre que le otorguemos.



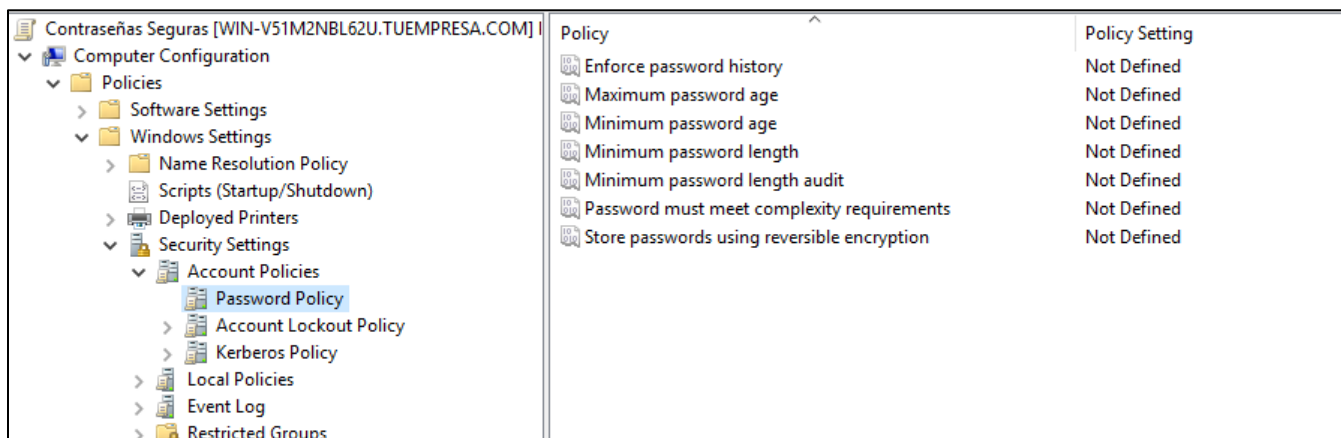
Al oprimir el botón tendremos una pestaña nueva ante nosotros, es hora de ubicar a qué será aplicada, si a los equipos, o a los usuarios.

Antes de aplicar una política se debe planificar con detenimiento todo sobre su configuración y vinculación. Se deben tener en cuenta todos los puntos relevantes. ¿A quiénes será aplicada? ¿De qué tipo será? ¿Cuáles parámetros tendrá?

Para este tipo de políticas debemos dirigirnos a **Computer Configuration → Windows Settings → Security Settings → Account Policy → Password Policy**.

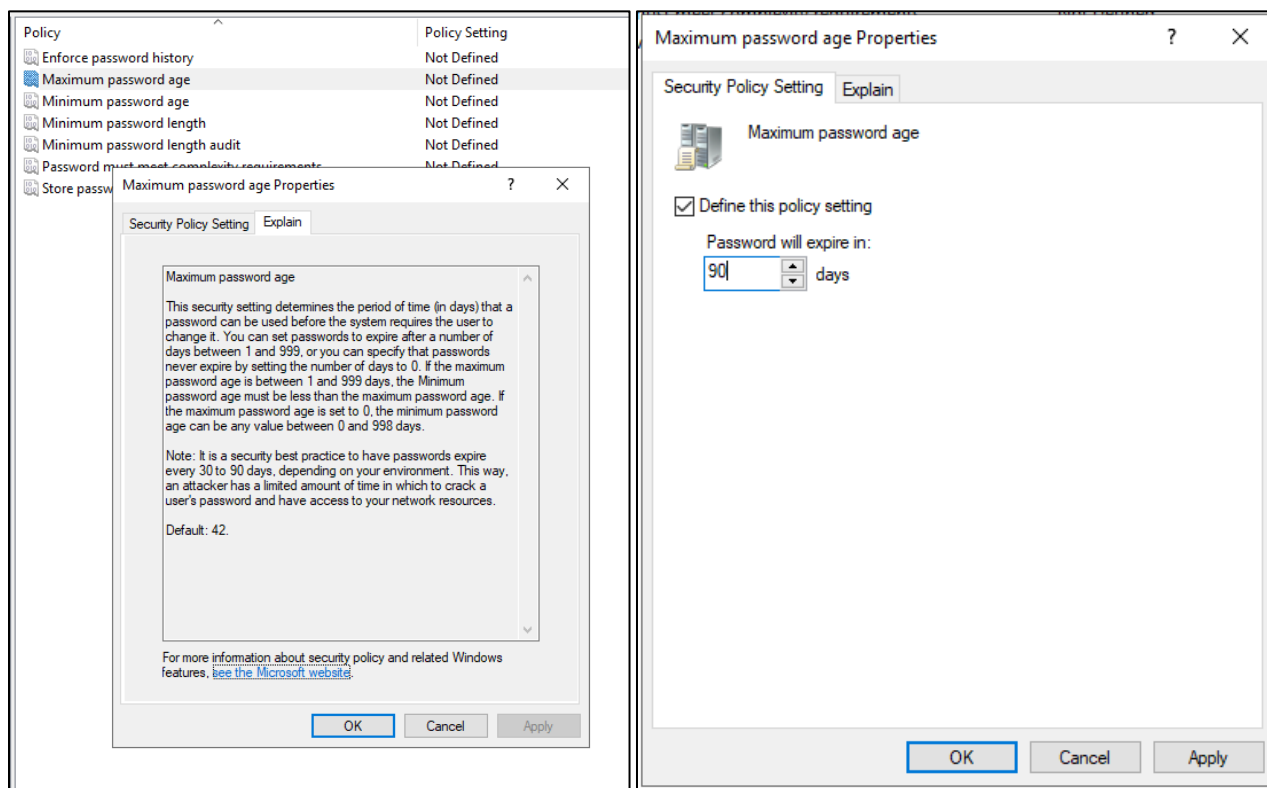
Como se mencionó antes, debemos saber a qué será aplicada nuestra política. A juzgar por la dirección antes de llegar a la configuración necesarias, nos damos cuenta de que tiene sentido lo que estamos buscando: aplicar políticas de contraseña a las cuentas de los equipos de nuestros usuarios.

En el apartado tendremos más de una opción donde, al dar clic podremos habilitar o deshabilitar ciertos parámetros para la política, y también ver sus distintas definiciones, en caso de que solo estemos aplicando las políticas como práctica.

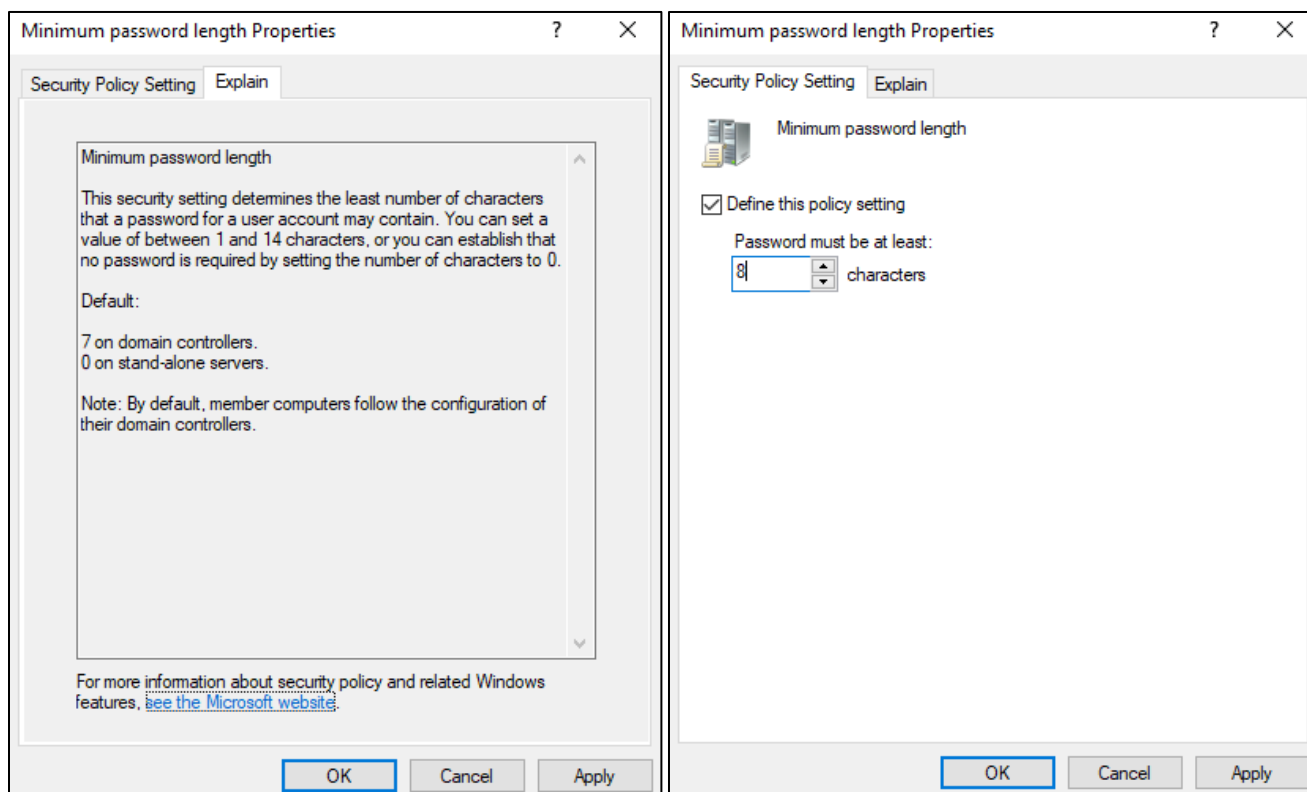


A continuación, se abrirán los cuadros de texto donde podremos configurar a gusto propio o por demanda, los requisitos de seguridad que tendrán nuestra política. Cada parámetro será mostrado con su definición y configuración.

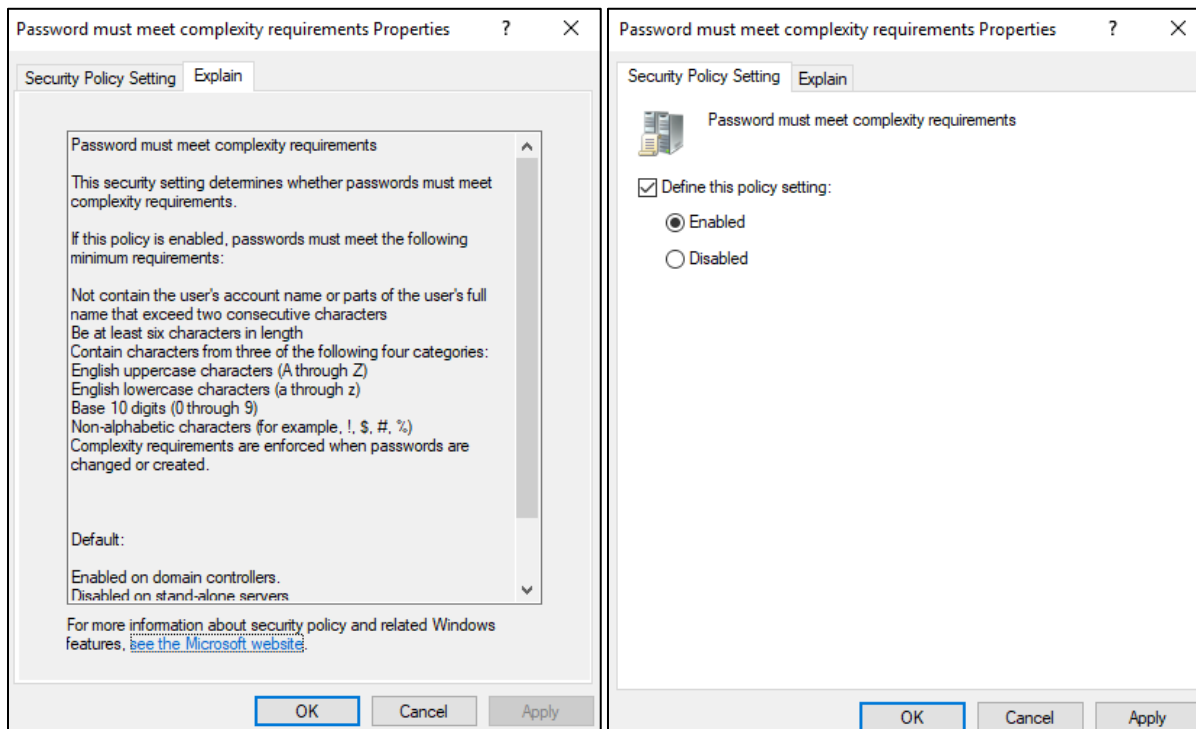
Primero, configuraremos los días máximos para que expire una contraseña. Lo ideal es que estas sean cambiadas cada tres o cuatro meses; para evitar su prolongación de habilitación. Automáticamente el parámetro mínimo se establecerá en 30 días; por lo que no deberá configurar esa parte si no lo desea.



Lo siguiente a configurar será la longitud mínima de la contraseña. Esto, para evitar que los usuarios creen contraseñas cortas. Lo recomendable siempre es que la longitud mínima sea de 12 o 14 caracteres. Pero, como se mencionó antes, este escenario será utilizado para pruebas de hacking ético; a propósito, se configurarán las políticas de seguridad tan débil como se pueda y algunas serán ignoradas. Todo con el objetivo de demostrar la importancia de las políticas en una empresa.



Lo último que será configurado en esta política es la combinación de caracteres para aumentar la complejidad de las nuevas contraseñas. Los usuarios tendrán la obligación de ocupar números, letras de todo tamaño, y símbolos para la creación de sus contraseñas. Con esto, en caso de algún ataque, será difícil para la amenaza descifrar con facilidad las credenciales de un usuario final.



Para aplicar las políticas y que las máquinas correspondientes reciban lo necesario, desde el **cmd** en nuestro Windows Server será escrito el comando **gpupdate /force**. Esto hará que las políticas sean actualizadas en tiempo real sin necesidad de reiniciar el sistema.

En ocasiones este comando podrá ser aplicado desde algunos clientes, dependiendo el tipo de política. Y, una que otra vez requerirá reiniciar el sistema de forma obligatoria para su aplicación, pero este no es el caso. Ahora, el sistema solicitará a los usuarios en cada cambio de contraseña, cumplir con lo necesario.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(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>
```

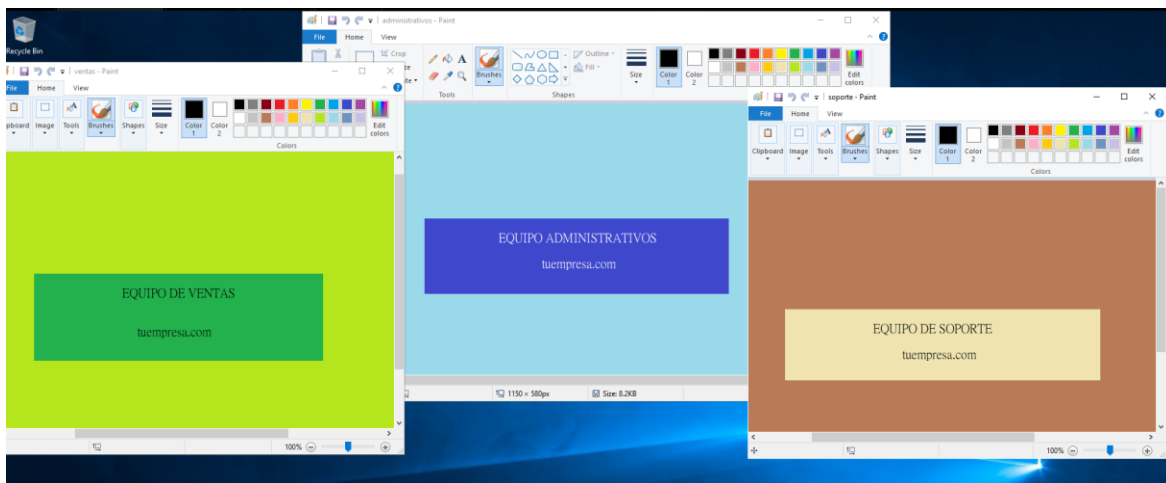
Política de Wallpaper

Wallpaper significa “fondo de pantalla” en inglés. Esta política es utilizada para asignar fondos de pantallas a los distintos equipos que hayan vinculados a la red de AD. Se configura y aplica nivel de usuario en el apartado de políticas de grupos.

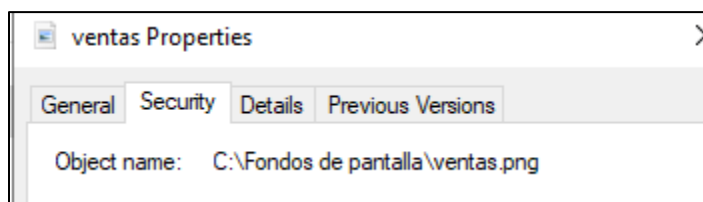
Como no es posible asignar una sola política para varios fondos de pantallas en distintos equipos (por el momento no porto ese tipo de información), en este trabajo se asignará una política por equipo. Es decir, habrá tres políticas de Wallpaper.

Antes de iniciar con la implementación de la política, se deben tener en cuenta varias cosas.

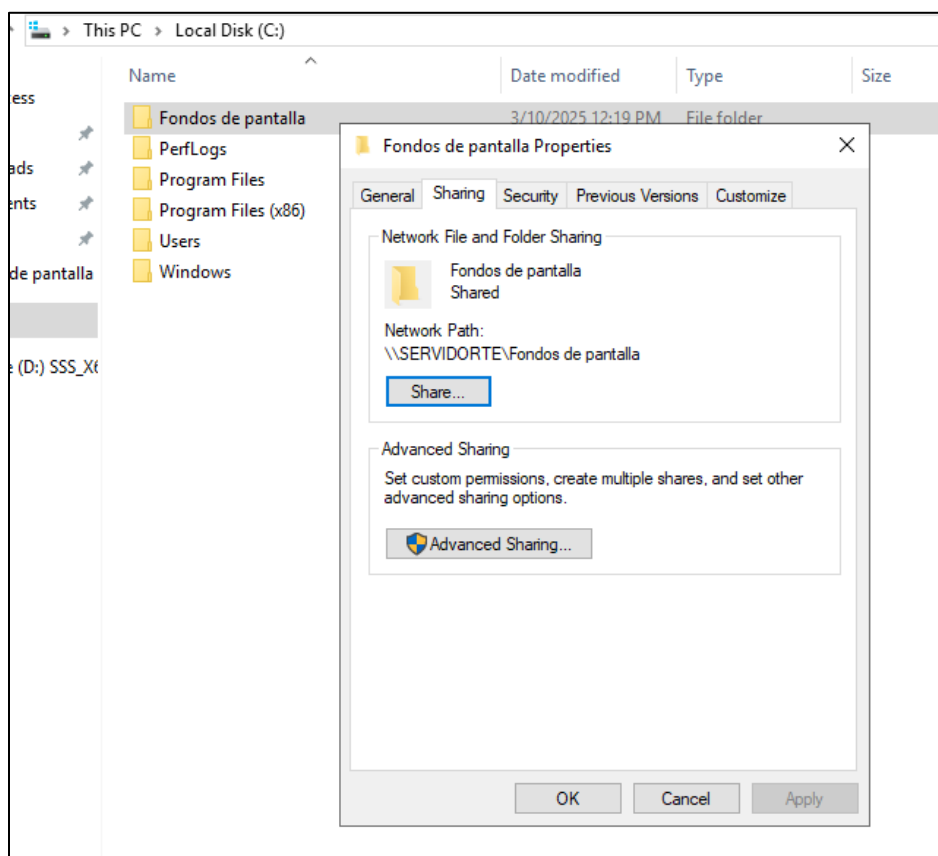
1. Debe tener un fondo de pantalla listo. Este puede ser una imagen creada o descargada. En este caso, creé un fondo de pantalla para cada equipo: Ventas, Soporte y Administrativos.



2. Debe guardar los fondos de pantalla en un directorio que le sea fácil de ubicar, ya que la dirección de la imagen será necesaria en la configuración de la política. En las propiedades de la imagen podrá ver la información.



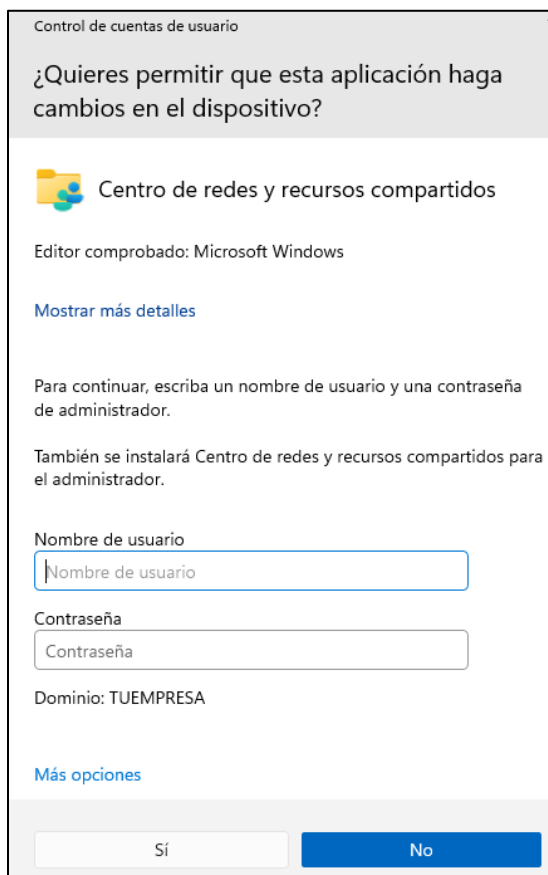
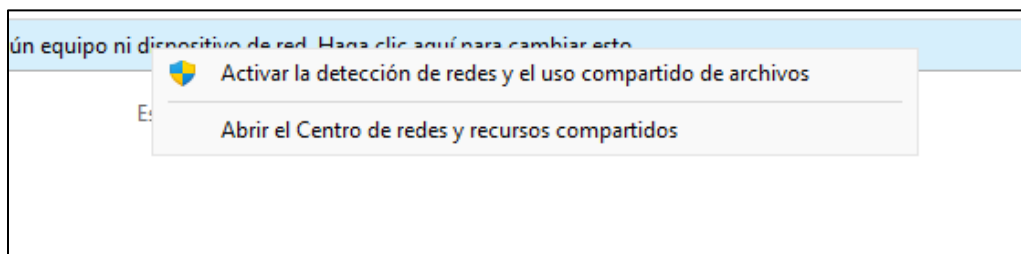
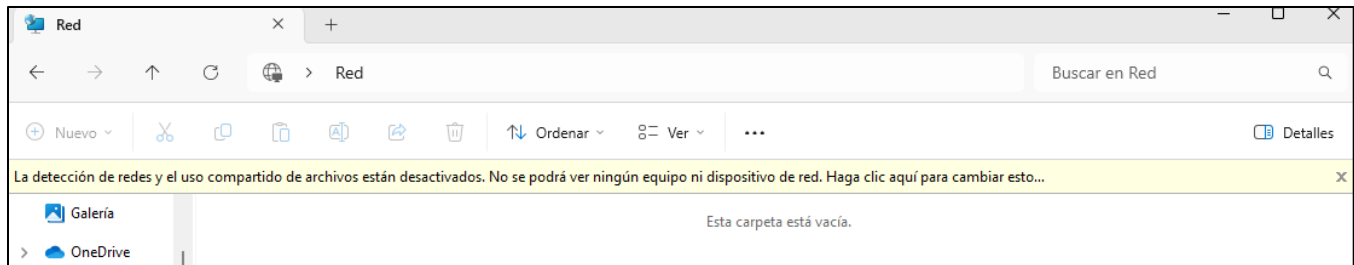
3. Asegurarse de que la carpeta donde las imágenes están siendo almacenadas se comparta con los dispositivos en la red. Esto asegura que los equipos a configurar ubiquen el fondo de pantalla. Para lograrlo, en propiedades de la carpeta está la pestaña de compartir. Una vez dentro de la opción, compartirá con todos los usuarios, o, si lo desea, con usuarios en específico.

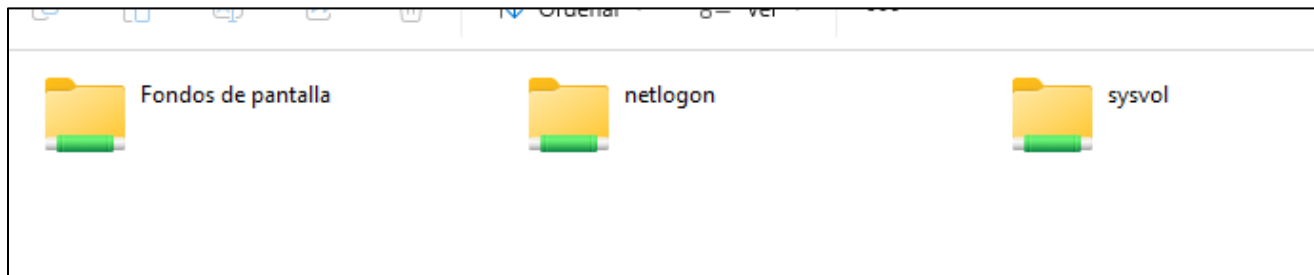
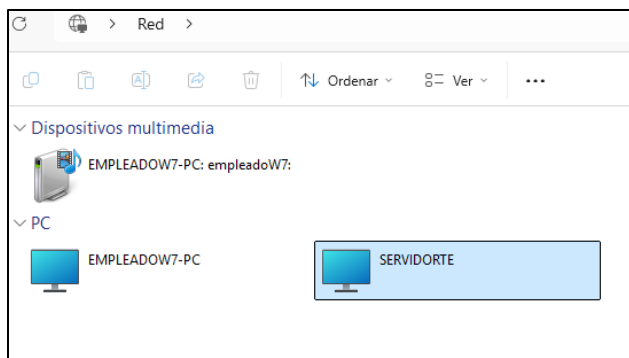


<input type="text"/> <input type="button" value="Add"/>	
Name	Permission Level
Administrator	Read/Write ▼
Administrators	Owner
Everyone	Read ▼

Para activar la función de lograr ver más dispositivos en la red desde otro equipo del dominio, puede hacerlo desde el explorador de archivos. En este ejemplo lo haremos desde Windows 11.

Esto debería aparecer cuando intenta buscar dispositivos en **Red**. Siga los siguientes pasos de forma intuitiva.





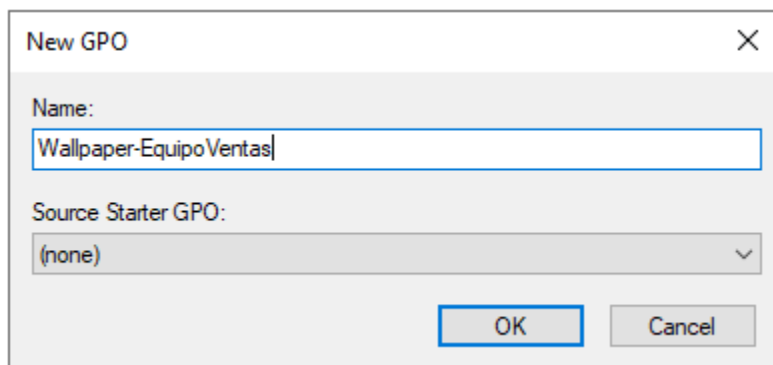
Si al ingresar al directorio aparecen las imágenes de los fondos de pantalla, entonces está compartiendo de forma correcta la carpeta. Otra forma de comprobarlo es ingresar en el explorador de archivos la dirección de compartido que se le ofrece en las propiedades de las imágenes en el servidor. Si esta le abre, entonces puede proceder con la implementación de la política.

4. No es tan necesario, pero si estará realizando políticas a nivel empresarial, es importante conocer las dimensiones de las imágenes. Esto, para saber qué tan centralizada deberá estar la imagen.

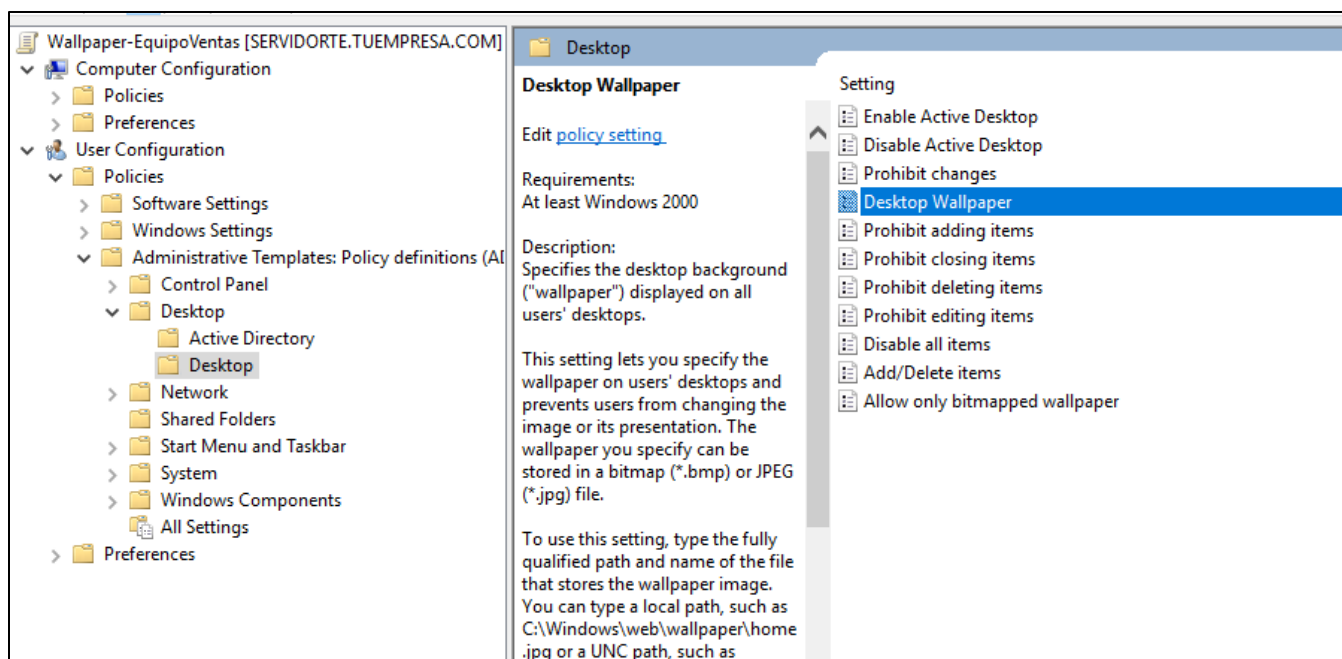
Ahora sí, a crear e implementar la política de Wallpaper.

Cada política fue creada en la carpeta de Objetos de Políticas de Grupo. Como ya se ha explicado, puede crearlas directamente en las UO correspondientes. Pero en este caso las vincularemos una vez sean configuradas.

La primera política en ser creada será la del equipo de ventas.



Luego, Desde User Configuration, dirigirse a Administrative Templates → Desktop → Desktop. Y en este apartado configurares tres parámetros.



Los tres habilitados en la imagen serán los configurados. Si gusta, solo configure el seleccionado en la ilustración, los otros dos han sido habilitados para evitar cambios por partes de los usuarios. En las mismas políticas podrá leer su definición.

Setting	State	Comment
Enable Active Desktop	Enabled	No
Disable Active Desktop	Not configured	No
Prohibit changes	Enabled	No
Desktop Wallpaper	Enabled	No
Prohibit adding items	Not configured	No

La que nos interesa ajusta es la Desktop Wallpaper. En esta, se definirá la dirección de la imagen una vez sea habilitado el parámetro. Para definir de forma correcta la dirección de la imagen, tenga en cuenta lo siguiente: **NO COPIE LA DIRECCION DESDE EL DISCO C:**, ya que los equipos interpretarán que la imagen está en su mismo sistema.

En cambio, tenga a mano el nombre de su servidor, este será usado para este apartado. La dirección será algo como esto:

\\SERVIDORTE\Fondos de pantalla

Seguido de ella, el nombre de la imagen más su extensión.

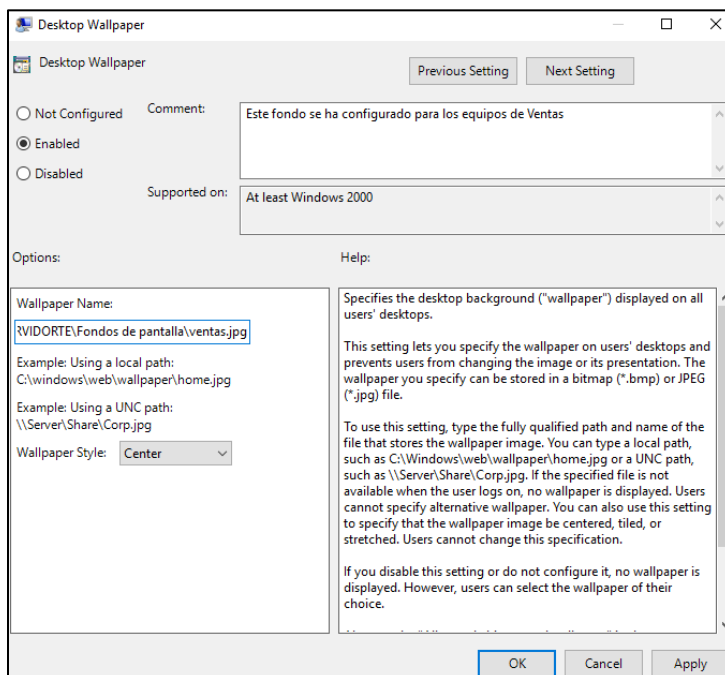
EJEMPLO:

```
Untitled - Notepad
File Edit Format View Help
\\SERVIDORTE\Fondos de pantalla\ventas.jpg

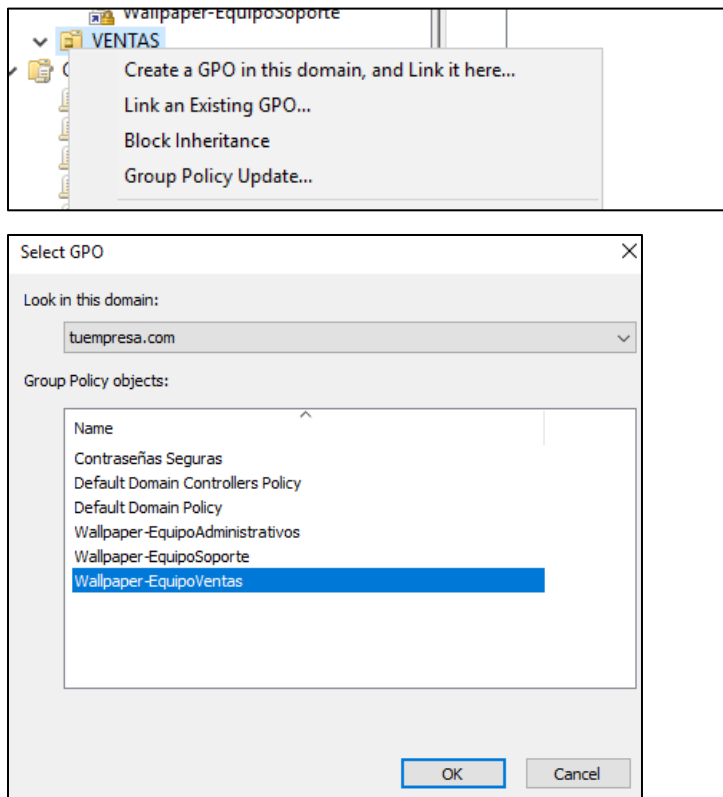
\\SERVIDORTE\Fondos de pantalla\soporte.jpg

\\SERVIDORTE\Fondos de pantalla\ventas.jpg
```

Una vez definidas las direcciones necesarias, deberán ser colocadas en el recuadro del parámetro de la política.



La política ya está configurada, ahora es momento de vincularla a las UO correspondientes. Para vincularla no es más que dar clic derecho sobre una unidad organizativa y luego a la opción de vincularla a la política correspondiente.



Una vez con todo esto, podrá ejecutar el siguiente comando para aplicar la política. Proceda a hacer lo mismo para los demás equipos.

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

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

También deberá ejecutarlo en los demás equipos donde aplique la política, para garantizar su implementación. También, utilizar: `gpresult /r` para ver un resumen de las políticas aplicadas en dicho equipo. Cuando lo ejecute en su Windows 10, 7, 11... podrá ver en configuración de usuario el nombre de la política si este fue aplicado correctamente.

Para que los cambios se apliquen deberá reiniciar los equipos. Al iniciar sesión, los fondos de pantallas serán aplicados.

```
CONFIGURACIÓN DE USUARIO
-----
CN=Miguel Jimenez,OU=SOPORTE,OU=USUARIOS,DC=tuempresa,DC=com
Última vez que se aplicó la Directiva de grupo: 10/03/2025 a las 21:11:49
Directivas de grupo aplicadas desdeSERVIDORTE.tuempresa.com
Umbral del vínculo de baja velocidad de las Directivas de grupo:500 kbps
Nombre de dominio:          TUEMPRESA
Tipo de dominio:            Windows 2008 o posterior

Objetos de directiva de grupo aplicados
-----
Wallpaper-EquipoSoporte

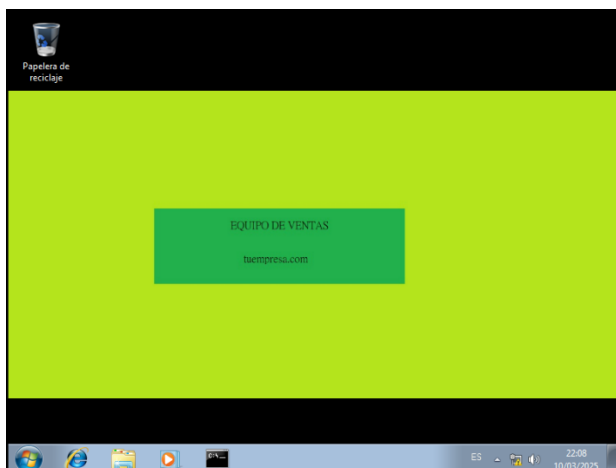
Los objetos GPO siguientes no se aplicaron porque fueron filtrados
-----
Directiva de grupo local
```



```
CONFIGURACIÓN DE USUARIO
-----
CN=Pedro Sanchez,OU=VENTAS,OU=USUARIOS,DC=tuempresa,DC=com
Última vez que se aplicó la Directiva de grupo: 10/03/2025 a las 21:17
Directivas de grupo aplicadas desdeSERVIDORTE.tuempresa.com
Umbral del vínculo de baja velocidad de las Directivas de grupo:500 kb
Nombre de dominio:          TUEMPRESA
Tipo de dominio:            Windows 2000

Objetos de directiva de grupo aplicados
-----
Wallpaper-EquipoVentas

Los objetos GPO siguientes no se aplicaron porque fueron filtrados
-----
Directiva de grupo local
Filtrar: No aplicado <vacío>
```



```
Objetos de directiva de grupo aplicados
-----
Wallpaper-EquipoAdministrativos

Los objetos GPO siguientes no se aplicaron porque fueron filtrados
-----
Directiva de grupo local
  Filtrar: No aplicado (vacío)

El usuario es parte de los siguientes Grupos de seguridad
-----
Domain Users
Todos
Usuarios
```

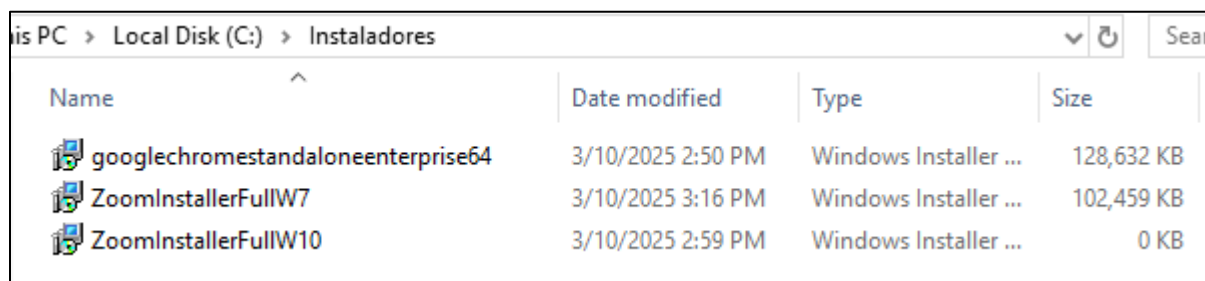


Política de Instalación de Software

La instalación de Software es una práctica importante cuando se trata de la implementación de políticas en Windows Server. Ya sea para evitar retrasos con los distintos clientes, o para asegurarse de que nadie tenga más de lo que necesita, es necesario aprender a implementarla por lo menos de forma básica. Algo importante a tener en cuenta, al aplicarse directamente al dominio, los programas también le serán instalados al administrador.

Para la configuración de esta política se deben tener en cuenta varias cosas:

1. Tener descargados los instaladores necesarios para esta política. En este caso solo se instalarán Google Chrome y Zoom. Ambos programas serán descargados con la extensión **.msi**. Estos son encontrados en internet con sus respectivos nombres.

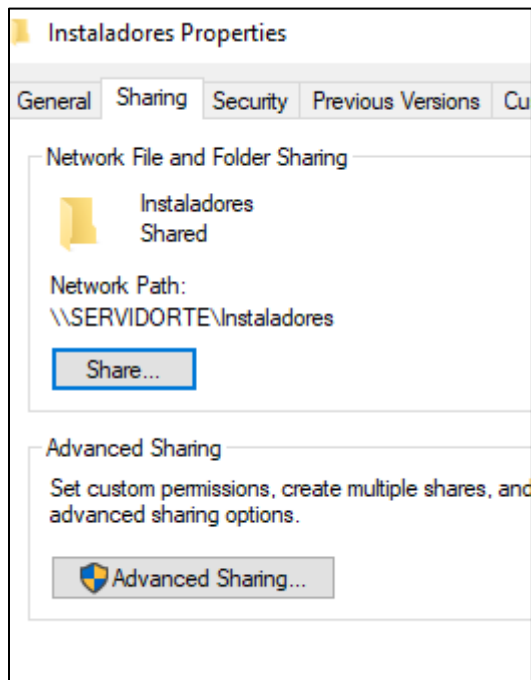


Name	Date modified	Type	Size
googlechromestandaloneenterprise64	3/10/2025 2:50 PM	Windows Installer ...	128,632 KB
ZoomInstallerFullW7	3/10/2025 3:16 PM	Windows Installer ...	102,459 KB
ZoomInstallerFullW10	3/10/2025 2:59 PM	Windows Installer ...	0 KB

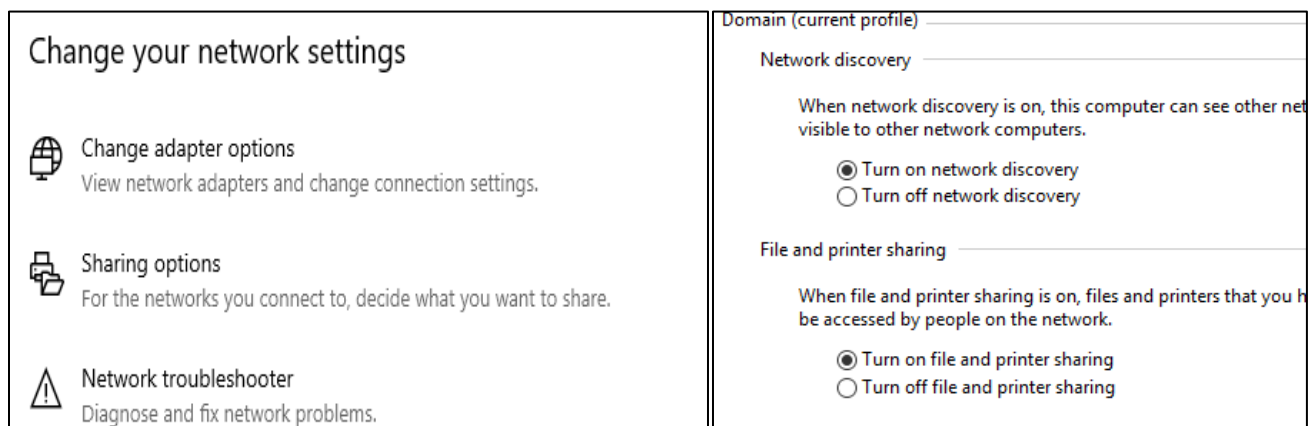
NOTA: Se ven dos instaladores de Zoom para Windows 7 y Windows 10. Pero, por cuestiones de error, uno no logró ser instalado.

2. La carpeta donde se almacenen estos instaladores debe ser fácil de ubicar, su dirección será utilizada para buscar los paquetes en el servidor. Como se ve en la ilustración anterior, todos los paquetes fueron guardados en el disco local, luego en una carpeta llamada **Instaladores**.

3. La carpeta donde se almacenen estos paquetes debe ser compartida con todos en la red, como anteriormente se configuraron las imágenes para los fondos de pantalla. De esta forma la carpeta contará con una dirección de directorio del servidor.

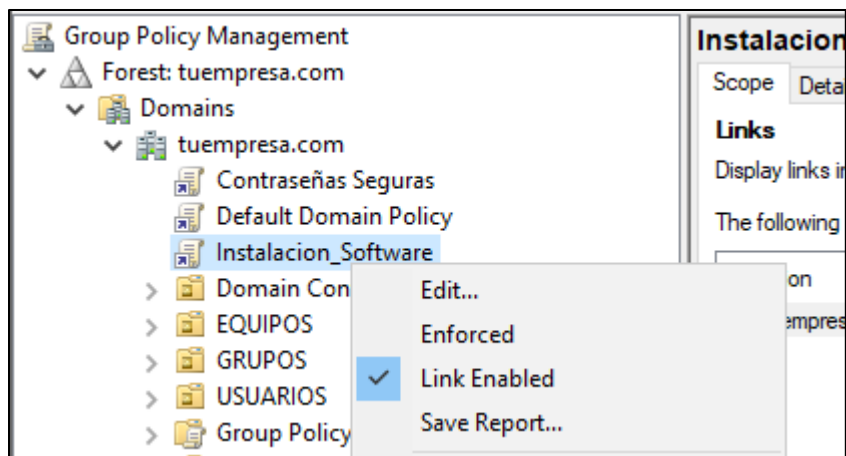


4. En configuración de redes, deberá tener las opciones de “**compartir**” todas activas. En especial aquellas conexiones relacionadas a su domino.

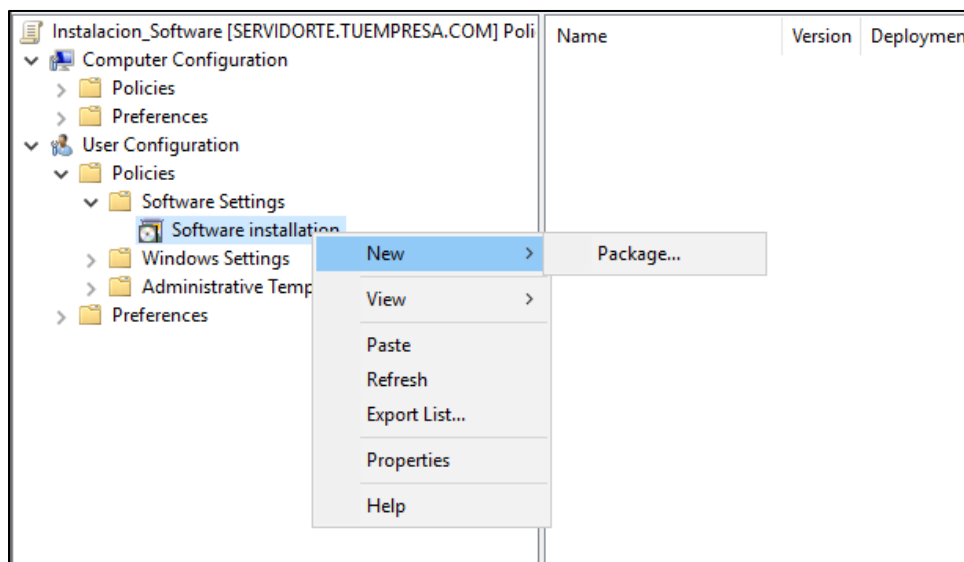


Con esto ya configurado, se puede continuar con la implementación de la política.

En este caso, la política será creada directamente en el dominio. Esto, para que todos los equipos y usuarios tengan consigo los softwares instalados. De querer que solo una parte tenga cierta cantidad o tipos de software, puede implementar estar de manera individual a la UO que desee o requiera su empresa.

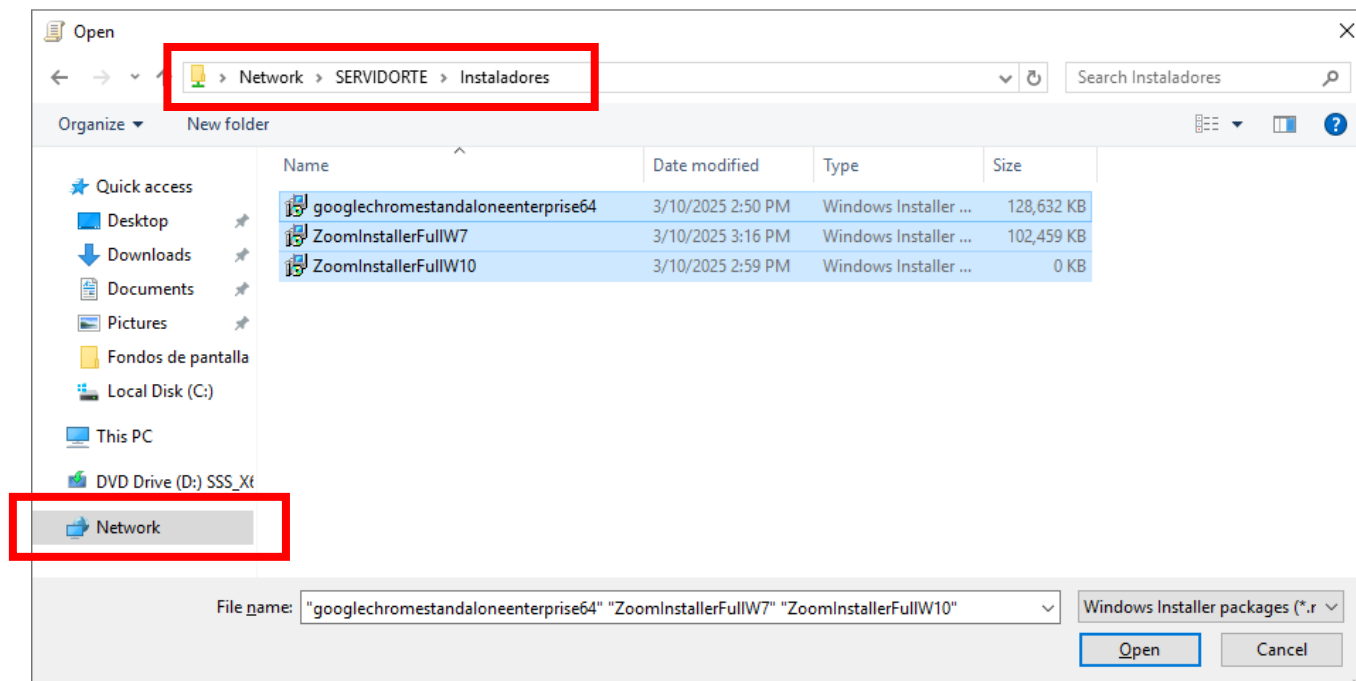


La ubicación para la instalación de Software es: **Configuración de usuario → Políticas → Configuración de Software.**

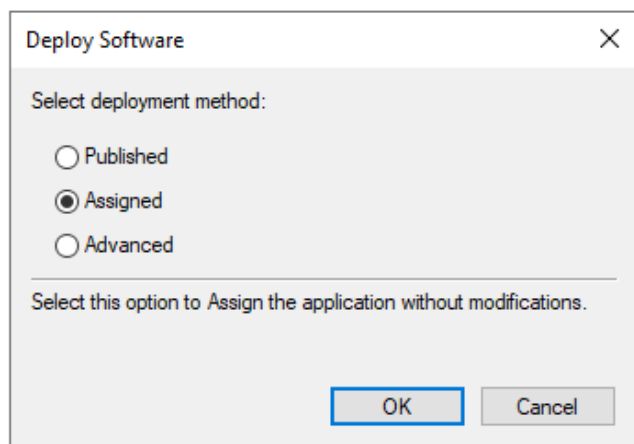


Una vez se encuentre en ese apartado, dando clic derecho sobre el recuadro que ve en la ilustración, o en el recuadro en blanco que le de su interfaz, podrá agregar nuevos paquetes de instalación.

Al momento de optar por agregar un nuevo paquete, el explorador de archivos le dará la oportunidad de buscarlo entre todos los directorios. Deber tener en cuenta que, la dirección deberá buscarla desde su Red o Network. Esto, para que la dirección de su paquete sea reconocida con la del servidor, y no con la de la máquina. Los recuadros marcan desde dónde fueron buscados los paquetes de instalación.



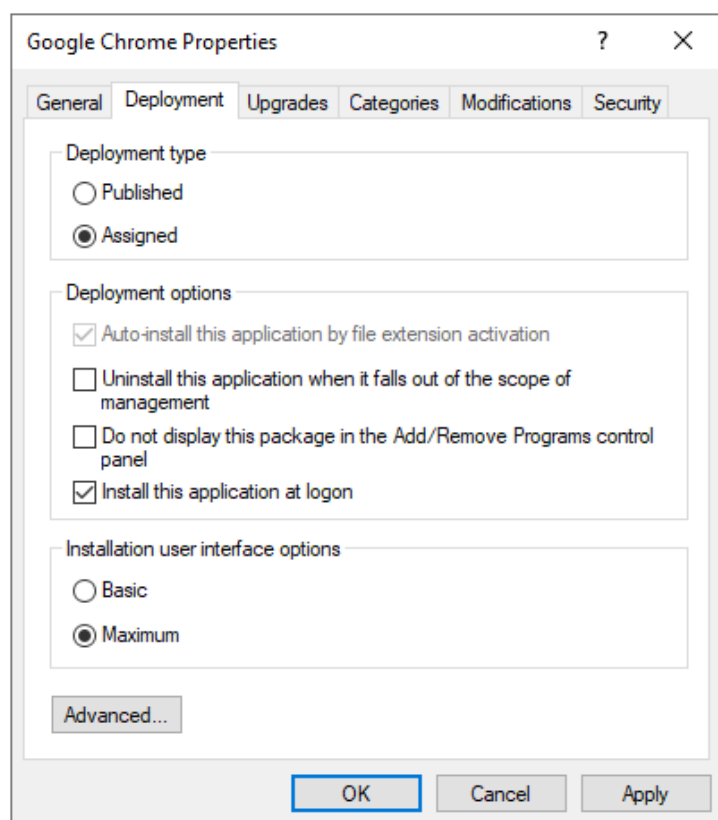
De buscar los paquetes en su disco local directamente, el sistema lo marcará con una dirección inválida, ya que ningún dispositivo de su dominio lo reconocerá como propiedad del servidor, sino que lo buscarán en sus mismos discos. Vea que al momento de agregar los paquetes será con la dirección del servidor, aquella que se ve al momento de compartir la carpeta con todos. Antes de ser agregados, aparecerá el siguiente cuadro de diálogo, donde debe marcarlo como **asignado**, para que así el sistema lo detecte como un programa **obligatorio** para los usuarios. Puede que después el paquete tarde en aparecer en la interfaz.



Name	Version	Deployment st...	Source
Google Chrome	70.213	Assigned	\\SERVIDORTE\Instaladores\googlechromestandaloneenterprise64.msi
Zoom (32-bit)	5.17	Assigned	\\SERVIDORTE\Instaladores\ZoomInstallerFullW7.msi

Podrá agregar todos los paquetes a la vez, o uno por uno. Independientemente de la forma que elija, si agrega cinco paquetes le aparecerán cinco recuadros como el anterior.

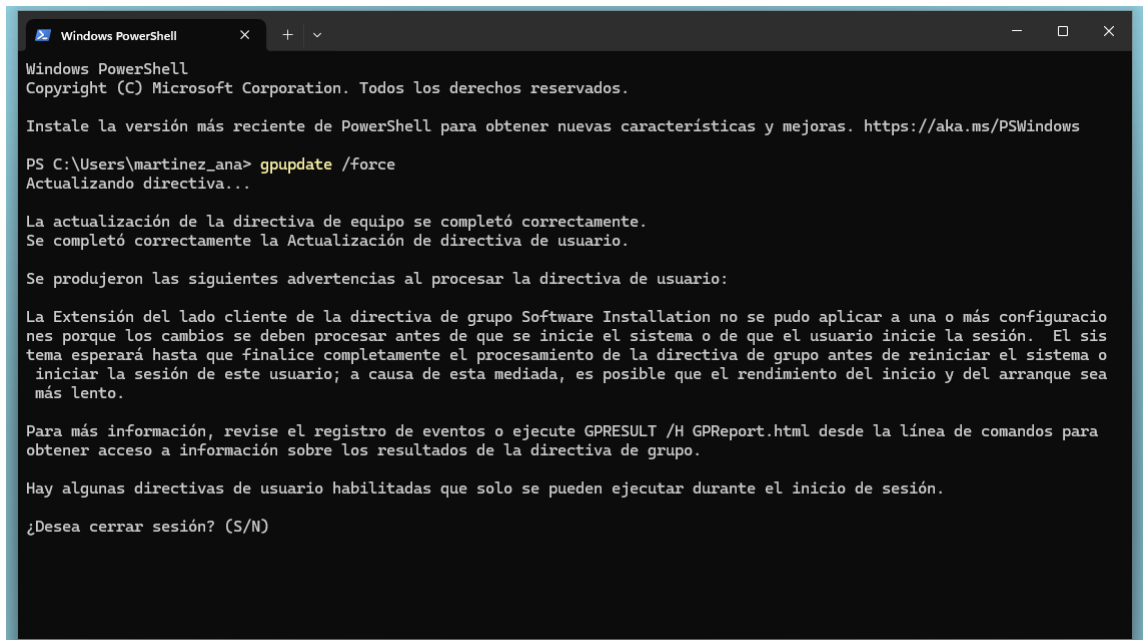
Como último paso en la configuración de estos paquetes, debe ir a propiedades de cada paquete y, en la pestaña **Deployment** seleccionará o marcará que sean instalados al momento de iniciar sesión. Esto hará que cada programa sea agregado a sus usuarios al momento de volver a iniciar sesión. Claro, puede marcar otras casillas según sus necesidades, pero en este caso solo se marcó esta. Si todavía no lo tiene marcado como asignado, en este apartado también podrá hacerlo.



Con todo lo demás visto, la política está completamente configurada. Para reflejar la implementación debe escribir en el CMD de cada usuario **gpupdate /force** para que esta sea forzada y así se reinicie el sistema y los programas sean instalados.

Claro, si no desea ver esta política de inmediato, puede esperar a que su usuario vuelva a abrir sesión.

Este mensaje debe aparecer en su CMD al ejecutar el comando:



```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\Users\martinez_ana> gpupdate /force
Actualizando directiva...

La actualización de la directiva de equipo se completó correctamente.
Se completó correctamente la Actualización de directiva de usuario.

Se produjeron las siguientes advertencias al procesar la directiva de usuario:

La Extensión del lado cliente de la directiva de grupo Software Installation no se pudo aplicar a una o más configuraciones porque los cambios se deben procesar antes de que se inicie el sistema o de que el usuario inicie la sesión. El sistema esperará hasta que finalice completamente el procesamiento de la directiva de grupo antes de reiniciar el sistema o iniciar la sesión de este usuario; a causa de esta mediada, es posible que el rendimiento del inicio y del arranque sea más lento.

Para más información, revise el registro de eventos o ejecute GPRESET /H GPREport.html desde la línea de comandos para obtener acceso a información sobre los resultados de la directiva de grupo.

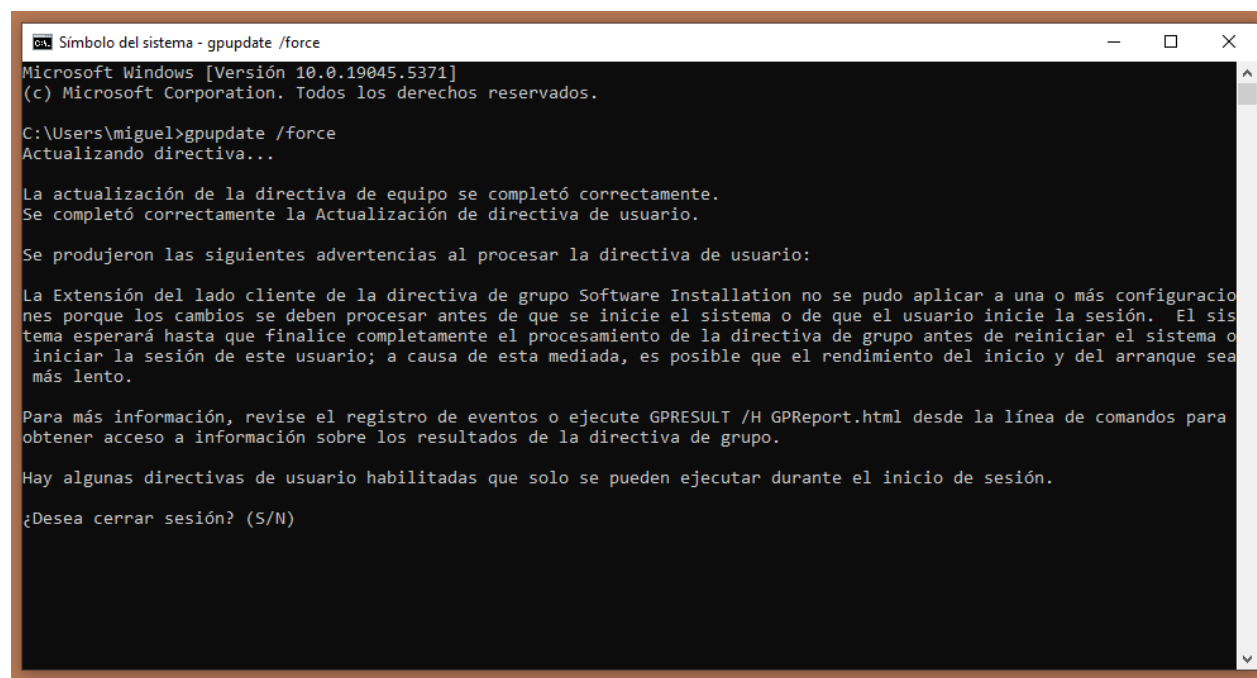
Hay algunas directivas de usuario habilitadas que solo se pueden ejecutar durante el inicio de sesión.

¿Desea cerrar sesión? (S/N)
```

Y luego de darle el permiso de cerrar sesión, con S, tendrá la opción de ingresar su contraseña luego de unos segundos. Tardará en iniciar, ya que mientras el usuario ingresa, el programa se va instalando.



En Windows 10 y Windows 7 se ve de forma similar.



```
Símbolo del sistema - gpupdate /force
Microsoft Windows [Versión 10.0.19045.5371]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\miguel>gpupdate /force
Actualizando directiva...

La actualización de la directiva de equipo se completó correctamente.
Se completó correctamente la Actualización de directiva de usuario.

Se produjeron las siguientes advertencias al procesar la directiva de usuario:

La Extensión del lado cliente de la directiva de grupo Software Installation no se pudo aplicar a una o más configuraciones porque los cambios se deben procesar antes de que se inicie el sistema o de que el usuario inicie la sesión. El sistema esperará hasta que finalice completamente el procesamiento de la directiva de grupo antes de reiniciar el sistema o iniciar la sesión de este usuario; a causa de esta mediada, es posible que el rendimiento del inicio y del arranque sea más lento.

Para más información, revise el registro de eventos o ejecute GPRESULT /H GPReport.html desde la línea de comandos para obtener acceso a información sobre los resultados de la directiva de grupo.

Hay algunas directivas de usuario habilitadas que solo se pueden ejecutar durante el inicio de sesión.

¿Desea cerrar sesión? (S/N)
```



```
Simbolo del sistema - gpupdate /force
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Users\PS>gpupdate /force
Actualizando directiva...

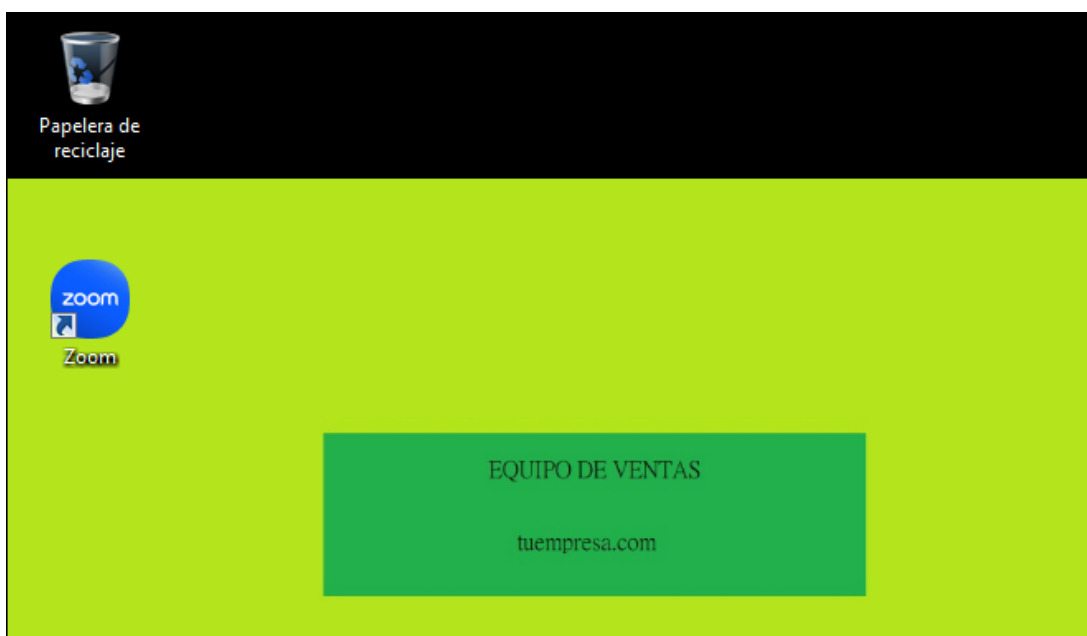
Se completó correctamente la Actualización de directiva de usuario.

Se produjeron las siguientes advertencias al procesar la directiva de usuario:

La Extensión del lado cliente de la directiva de grupo Software Installation no se pudo aplicar a una o más configuraciones porque los cambios se deben procesar antes de que se inicie el sistema o de que el usuario inicie la sesión. El sistema esperará hasta que finalice completamente el procesamiento de la directiva de grupo antes de reiniciar el sistema o iniciar la sesión de este usuario; a causa de esta mediada, es posible que el rendimiento del inicio y del arranque sea más lento.
La actualización de la directiva de equipo se completó correctamente.

Para más información, revise el registro de eventos o ejecute GPREPUL /H GPREport.html desde la línea de comandos para obtener acceso a la información sobre los resultados de la directiva de grupo.
Ciertas directivas de Usuario están habilitadas para que puedan ejecutarse sólo durante el inicio de sesión.

¿Cerrar sesión?. (S/N)S_
```



Lamentablemente Windows 7 no corrió con suerte a la hora de instalar Chrome. Es un SO casi obsoleto, por lo que las versiones instaladas en esta práctica no son compatibles. Si desea practicar con otros softwares posiblemente compatibles para W7, es libre de hacerlo. En este caso se omite eso, ya que el objetivo es solo mostrar la implementación de esta política. Muy posiblemente al ejecutar el mismo comando que los demás en el CMD, le mencione un error.

Políticas de Restricciones a los usuarios

Estas son las políticas más sencillas de configurar, y son perfectas para practicar si se es principiante en Active Directory. En este caso, las políticas son aleatorias, son varias. Y usted también es invitado a practicar con las que más les llamen la atención.

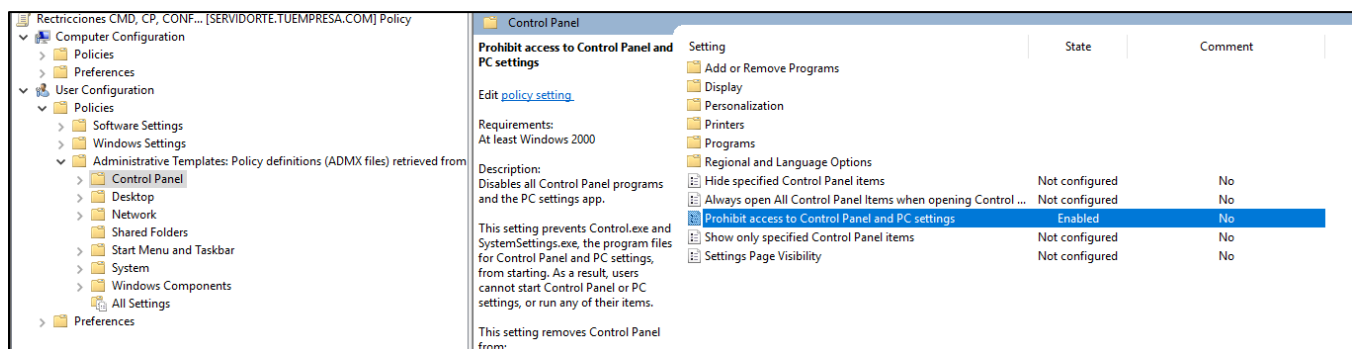
Las políticas anteriormente configuradas fueron para acostumbrarlo a la implementación de políticas comunes en algunas empresas. Estas son para divertirlo un rato. Lo más tedioso pasó. Esta es su oportunidad de buscar entre las muchas políticas de usuarios y equipos las que más le gusten; de esta forma aprende a buscar en el mar de AD, también, la diferencia que hay entre las políticas de Equipo y de Usuario.

En este caso, planificará primero qué hará con cada política. En lo personal, bloquearé el CMD, configuración y el panel de control a los usuarios de ventas. Como se mencionó al inicio, son los que se registrarán en la máquina de Windows 7; ya que no será utilizada para mucho, mantendré esas restricciones para la misma. En Windows 10 bloquearé algunas funciones con respecto a la instalación de software, y en W11 bloquearé el uso de unidades USB.

ASEGÚRESE DE HACER ZOOM CON LAS SIGUIENTES IMÁGENES.

Windows 7:

Prohibir el acceso al Control Panel.



Prohibir el acceso al command prompt (CMD).

Restricciones CMD, CP, CONF... [SERVIDORTE.TUEMPRESA.COM] Policy	
Computer Configuration	
Policies	
Preferences	
User Configuration	
Policies	
Software Settings	
Windows Settings	
Administrative Templates: Policy definitions (ADMX files) retrieved from	
Control Panel	
Desktop	
Network	
Shared Folders	
Start Menu and Taskbar	
System	
Windows Components	
All Settings	
Preferences	

Setting	State	Comment
Prevent access to the command prompt		
Edit policy setting .		
Requirements:		
At least Windows 2000		
Description:		
This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determines whether batch files (.cmd and .bat) can run on the computer.		
If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.		
If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally.		
Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop		
Setting		
Ctrl+Alt+Del Options		
Display		
Driver Installation		
Folder Redirection		
Group Policy		
Internet Communication Management		
Locale Services		
Logon		
Mitigation Options		
Power Management		
Removable Storage Access		
Scripts		
User Profiles		
Download missing COM components	Not configured	No
Century interpretation for Year 2000	Not configured	No
Restrict these programs from being launched from Help	Not configured	No
Do not display the Getting Started welcome screen at logon	Not configured	No
Custom User Interface	Not configured	No
Prevent access to the command prompt	Enabled	No
Prevent access to registry editing tools	Not configured	No
Don't run specified Windows applications	Not configured	No
Run only specified Windows applications	Not configured	No
Windows Automatic Updates	Not configured	No

Desactivar la personalización del menú.

Restricciones CMD, CP, CONF... [SERVIDORTE.TUEMPRESA.COM] Policy	
Computer Configuration	
Policies	
Preferences	
User Configuration	
Policies	
Software Settings	
Windows Settings	
Administrative Templates: Policy definitions (ADMX files) retrieved from	
Control Panel	
Desktop	
Network	
Shared Folders	
Start Menu and Taskbar	
Notifications	
System	
Windows Components	
All Settings	
Preferences	

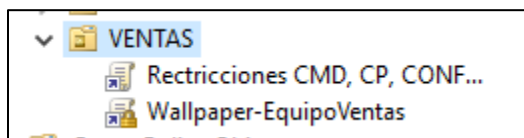
Setting	State	Comment
Turn off personalized menus		
Edit policy setting .		
Requirements:		
Windows Server 2008, Windows Server 2003, Windows Vista, Windows XP, and Windows 2000		
Description:		
Disables personalized menus.		
Windows personalizes long menus by moving recently used items to the top of the menu and hiding items that have not been used recently. Users can display the hidden items by clicking an arrow to extend the menu.		
If you enable this setting, the system does not personalize menus. All menu items appear and remain in standard order. Also, this setting removes the "Use Personalized Menus" option so users do not try to change the setting while a setting is in effect.		
Setting		
Notifications		
Add Search Internet link to Start Menu	Not configured	No
Clear history of recently opened documents on exit	Not configured	No
Clear the recent programs list for new users	Not configured	No
Clear tile notifications during log on	Not configured	No
List desktop apps first in the Apps view	Not configured	No
Disable context menus in the Start Menu	Not configured	No
Search just apps from the Apps view	Not configured	No
Add Logoff to the Start Menu	Not configured	No
Force Start to be either full screen size or menu size	Not configured	No
Go to the desktop instead of Start when signing in	Not configured	No
Gray unavailable Windows Installer programs Start Menu shortcuts	Not configured	No
Remove the People Bar from the taskbar	Not configured	No
Remove "Recently added" list from Start Menu	Not configured	No
Turn off personalized menus	Enabled	No
Lock the Taskbar	Not configured	No
Start Layout	Not configured	No
Add "Run in Separate Memory Space" check box to Run dialog box	Not configured	No
Turn off notification area cleanup	Not configured	No
Remove Balloon Tips on Start Menu items	Not configured	No
Prevent users from customizing their Start Screen	Not configured	No

Remover "ejecutar" del menú.

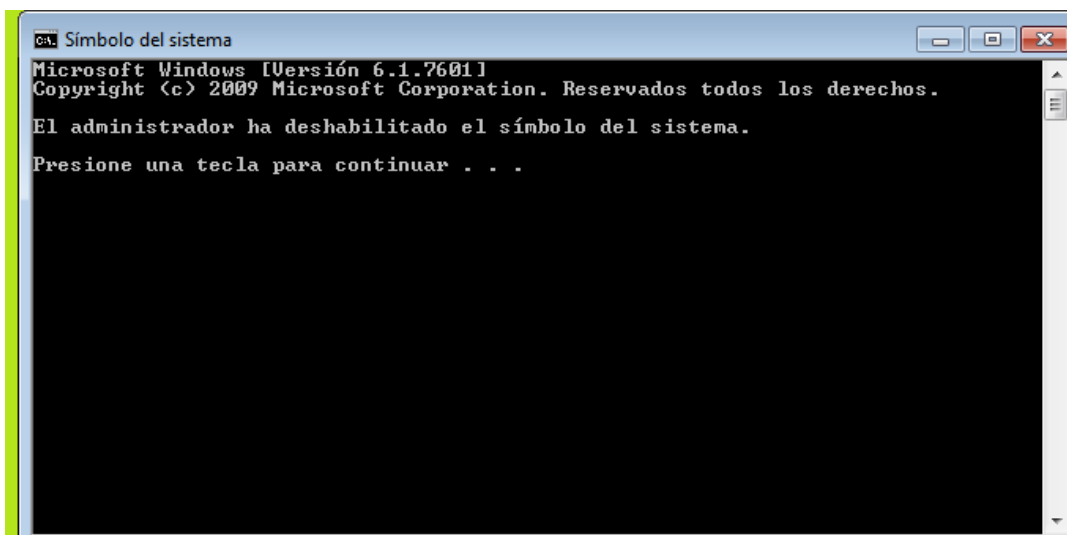
Restricciones CMD, CP, CONF... [SERVIDORTE.TUEMPRESA.COM] Policy	
Computer Configuration	
Policies	
Preferences	
User Configuration	
Policies	
Software Settings	
Windows Settings	
Administrative Templates: Policy definitions (ADMX files) retrieved from	
Control Panel	
Desktop	
Network	
Shared Folders	
Start Menu and Taskbar	
System	
Windows Components	
All Settings	
Preferences	

Setting	State	Comment
Remove the Run command from the Start menu	Not configured	No
Remove the People Bar from the taskbar	Not configured	No
Remove "Recently added" list from Start Menu	Not configured	No
Turn off personalized menus	Enabled	No
Lock the Taskbar	Not configured	No
Start Layout	Not configured	No
Add "Run in Separate Memory Space" check box to Run dialog box	Not configured	No
Turn off notification area cleanup	Not configured	No
Remove Balloon Tips on Start Menu items	Not configured	No
Prevent users from customizing their Start Screen	Not configured	No
Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands	Not configured	No
Remove common program groups from Start Menu	Not configured	No
Remove Favorites menu from Start Menu	Not configured	No
Remove Search link from Start Menu	Not configured	No
Remove frequent programs list from the Start Menu	Not configured	No
Remove Games link from Start Menu	Not configured	No
Remove Help menu from Start Menu	Not configured	No
Turn off user tracking	Not configured	No
Remove All Programs list from the Start menu	Not configured	No
Remove Network Connections from Start Menu	Not configured	No
Remove pinned programs list from the Start Menu	Not configured	No
Do not keep history of recently opened documents	Not configured	No
Remove Recent Items menu from Start Menu	Not configured	No
Do not use the search-based method when resolving shell shortcuts	Not configured	No
Do not use the tracking-based method when resolving shell shortcuts	Not configured	No
Remove Run menu from Start Menu	Enabled	No
Remove Default Programs link from the Start menu.	Not configured	No
Remove Documents icon from Start Menu	Not configured	No
Remove Music icon from Start Menu	Not configured	No

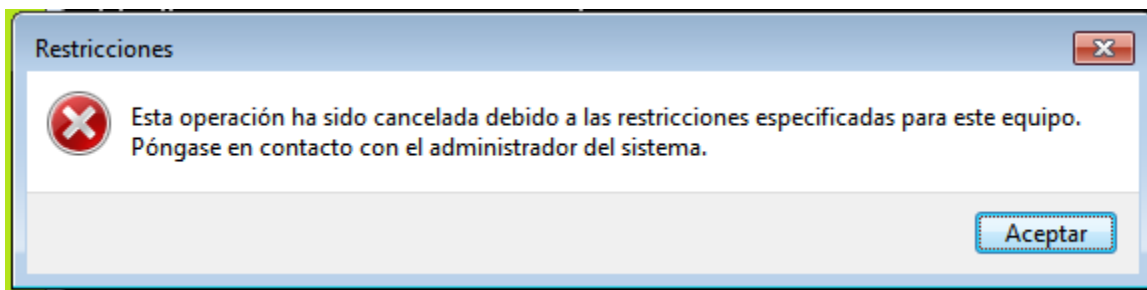
Cuando termine de configurar las políticas a su antojo, podrá anclarla a la UO que desee.



Visualización de las políticas:

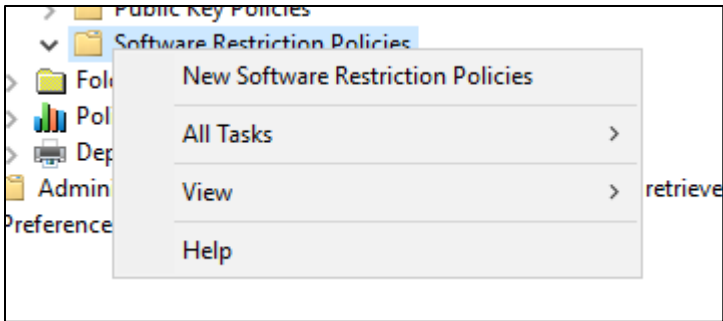


Ahora, cada que quiera acceder al **Control Panel** por cualquier vía, oprima **Windows + R**, o elija la opción de **personalizar** en el menú que tiene al hacer clic derecho sobre el escritorio... le aparecerá el siguiente mensaje:

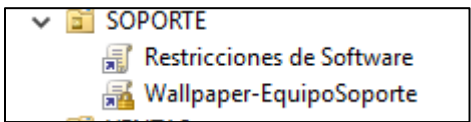
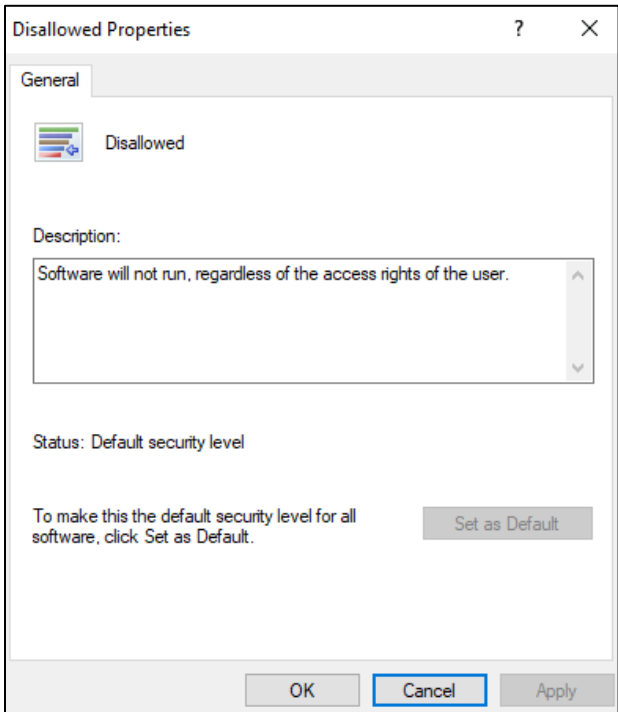


Windows 10:

Es muy probable que al querer aplicar políticas de software aparezca un mensaje de advertencia. En ese caso, solo se crearán nuevas políticas de este tipo.



Name	Description
Disabled	Software will not run, regardless of the access rights of the user.
Basic User	Allows programs to execute as a user that does not have Administrator access rights, but can still access resources accessible by normal users.
Unrestricted	Software access rights are determined by the access rights of the user.



En este caso, al querer abrir Microsoft Edge, aparece el siguiente mensaje:

El administrador del sistema bloqueó esta aplicación.

Ponte en contacto con el administrador del sistema para que te dé más información.

Copiar al Portapapeles

Cerrar

Windows 11:

En Windows 11 solo fue aplicada la política para evitar el uso de unidades de almacenamiento extraíble.

Start Menu and Taskbar

System

Ctrl+Alt+Del Options

Display

Driver Installation

Folder Redirection

Group Policy

Internet Communication Management

Locale Services

Login

Mitigation Options

Power Management

Removable Storage Access

Scripts

User Profiles

Windows Components

All Settings

Preferences

This policy setting takes precedence over any individual removable storage policy settings. To manage individual classes, use the policy settings available for each class.

If you enable this policy setting, no access is allowed to any removable storage class.

If you disable or do not configure this policy setting, write and read accesses are allowed to all removable storage classes.

Removable Disks: Deny write access

Not configured

No

All Removable Storage classes: Deny all access

Enabled

No

Tape Drives: Deny read access

Not configured

No

Tape Drives: Deny write access

Not configured

No

WPD Devices: Deny read access

Not configured

No

WPD Devices: Deny write access

Not configured

No

ADMINISTRATIVOS

Restricciones unidades extraíbles

Wallpaper-EquipoAdministrativos

Al esta ser aplicada, el sistema no permitirá que se visualice el contenido de cualquier unidad de almacenamiento extraíble que se conecte a la máquina.

Galería

OneDrive

Escritorio

Descargas

Documentos

Imágenes

Música

Videos

Este equipo

VENTOY (E:)

Red

Acceso rápido

Escritorio

Almacenado

Imágenes

Almacenado

Favoritos

Después de marcar algunos

Reciente

Después de abrir algunos archivos, aquí te mostraremos los más recientes.

Ubicación no disponible

No se puede obtener acceso a E:\.

Acceso denegado.

Aceptar

Configuración de Roles en AD

DNS

¿Qué es DNS?

Conocido como **Sistema de Nombres de Dominio**, es un servicio utilizado para traducir nombre de dominio en direcciones IP. Es decir, que en lugar de recordar direcciones como **192.168.1.1**, los usuarios pueden optar por escribir nombres fáciles de recordar. **Facebook.com**, **Youtube.com**, **Instagram.com** son algunos ejemplos. DNS se encarga de encontrar la dirección correcta a través de estos nombres. En este caso, el dominio de este trabajo es **tuempresa.com**, mientras que su ip es **192.168.77.80**. En lugar de escribir esa dirección, el cliente podrá comunicarse con el servidor a través del nombre de dominio.

¿Para qué funciona?

DNS facilita la comunicación en redes, permitiendo que los dispositivos encuentren servidores y servicios sin necesidad de conocer sus direcciones IP. Es fundamental para acceder a sitios web, enviar correos electrónicos y conectarse a servidores dentro de una red.

Importancia de DNS en AD.

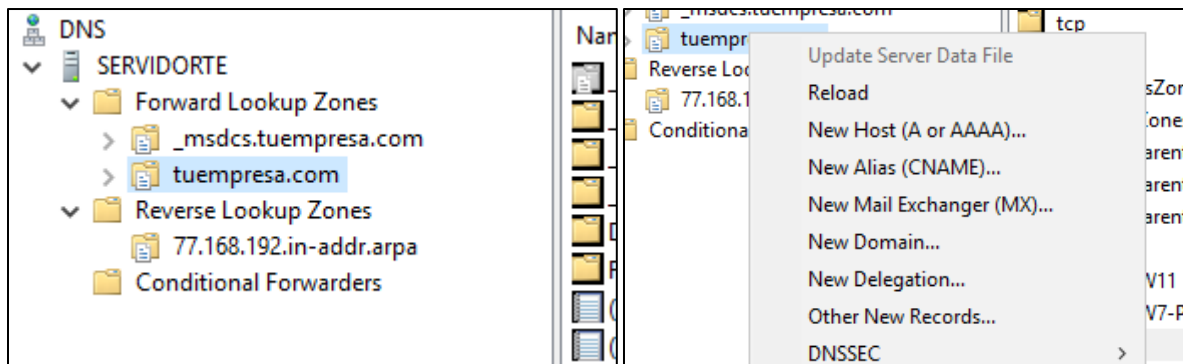
En un entorno de Active Directory (AD), DNS es esencial porque permite que los equipos y servidores dentro de la red se ubiquen entre sí. AD depende de DNS para el inicio de sesión de usuarios, la localización de controladores de dominio y la correcta resolución de nombres en la red. Sin un DNS bien configurado, muchos servicios de AD no funcionarían correctamente.

Configuración de DNS en AD

Zona de búsqueda directa (Forward Lookup Zone)

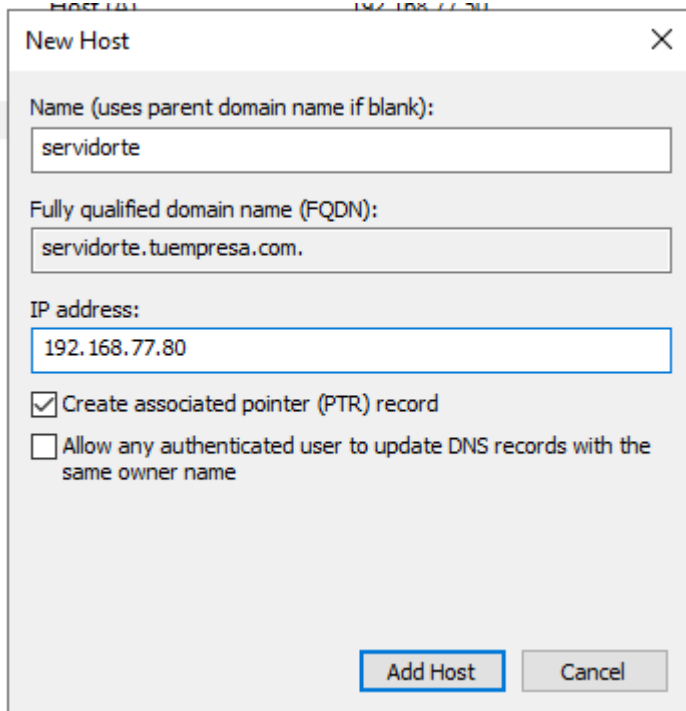
Esta zona permite la resolución de nombres a direcciones IP. Al ingresar **servidorte.tuempresa.com**, el servidor DNS traduce ese nombre a la IP **192.168.77.80**. Es fundamental para que los equipos en la red encuentren los servicios de Active Directory.

Ya debe poder buscar las herramientas en AD sin problema alguno. En la barra, debe buscar el ya mencionado DNS. Una vez dentro, se encontrará con la siguiente estructura, la que se muestra en la primera ilustración. Seguido de eso, para crear una nueva zona puede hacer clic derecho sobre la carpeta **Forward Lookup Zone**, pero el DNS ya habrá sido creado al momento de instalar AD DS. En su lugar, configuraremos un nuevo **host** con nuestra IP del servidor.



De clic derecho sobre el nombre de su dominio, posteriormente en **Nuevo Host (A o AAA)**.

Llenar los campos será pan comido. En el campo Nombre, de preferencia, debe escribir el nombre de su servidor. De esta forma podrá recordar más fácil el nombre completo. También, en el campo de **Dirección IP**, la que pertenece a su servidor de AD. Con todo ya lleno, debe marcar la primera casilla, de crear un **PTR**.



Esto puede llenarlo cuantas veces quiera para poder ubicar su dominio y la conexión del mismo entre clientes. Para este trabajo, solo se hará un ejemplo en cada zona.

Para confirmar que la zona ha sido configurada correctamente, desde su CMD, en cualquier máquina del dominio, trate de dar ping al nombre completo de su zona. Más adelante se mostrarán otras formas de confirmarlo.

```
C:\Users\Administrator>ping SERVIDORTE.tuempresa.com

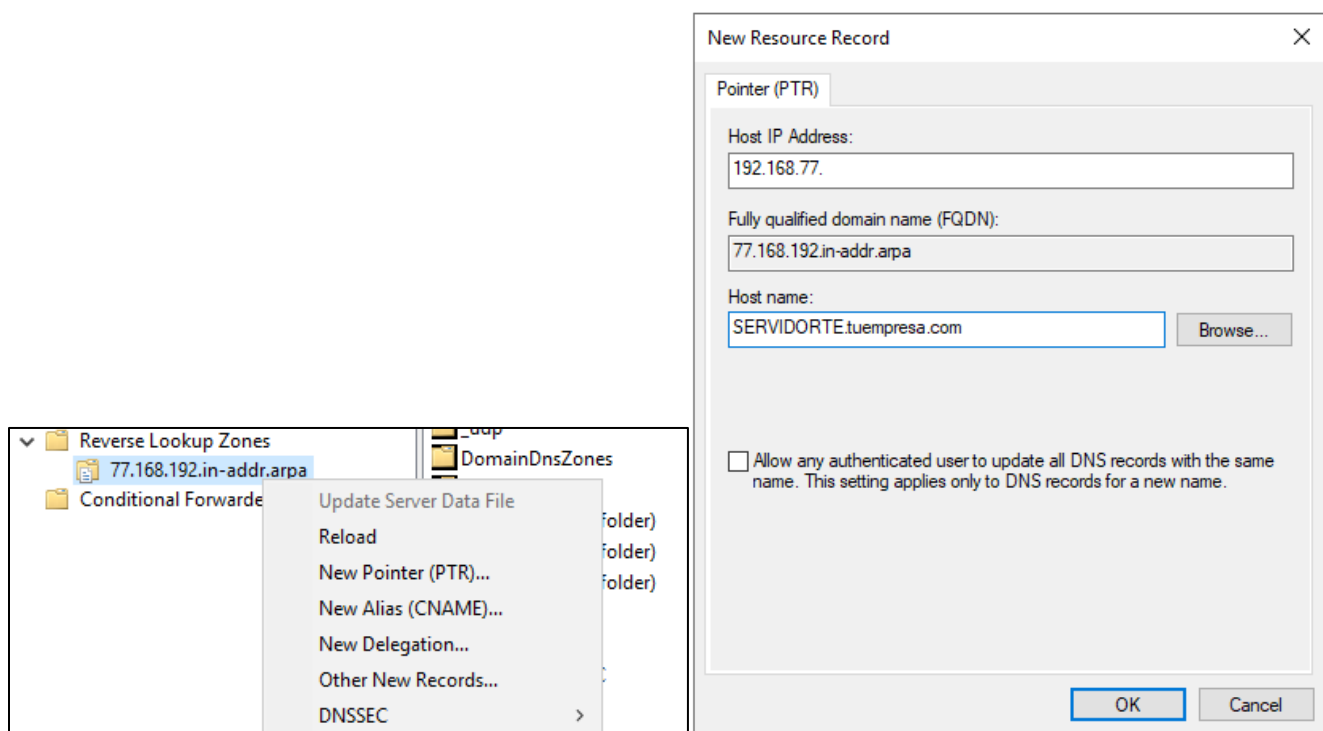
Pinging SERVIDORTE.tuempresa.com [fe80::1c00:5141:a2e4:6186%12] with 32 bytes of data:
Reply from fe80::1c00:5141:a2e4:6186%12: time<1ms
Reply from fe80::1c00:5141:a2e4:6186%12: time<1ms
Reply from fe80::1c00:5141:a2e4:6186%12: time<1ms
Reply from fe80::1c00:5141:a2e4:6186%12: time<1ms

Ping statistics for fe80::1c00:5141:a2e4:6186%12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```


Zona de búsqueda inversa (Reverse Lookup Zone)

En este caso, esta zona permite la resolución inversa, es decir, convertir una dirección IP en un nombre de dominio. Si un dispositivo conoce la IP **192.168.77.80**, puede consultar DNS para saber que pertenece a **servidorte.tuempresa.com**. Es útil para la seguridad y la gestión de la red, ya que permite identificar qué dispositivos están conectados.

El aparatado de Zona inversa tendrá un registro hecho, dentro del mismo dará clic para crear un nuevo **PTR**.



Para mostrar el ejemplo, se dejó el primer campo tal cual aparece al seleccionar la opción ya mencionada. Debe llenar el último octeto de su ip con la correspondiente a su servidor. Y, el campo de **Host name** debe llenar de acuerdo al nombre ya configurado que dejó en la zona directa.

Al terminarlo aparecerá el nuevo PTR en su interfaz gráfica. Si aparece otro host, como algún cliente del dominio (así como se ve en la ilustración), no se preocupe. Esto puede cambiar si configura el DHCP de su dominio, o si hace algún cambio en el DNS de otras máquinas.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[6], servidorte.tuempresa.com., hostmaster.tuempresa.com.	static
(same as parent folder)	Name Server (NS)	servidorte.tuempresa.com.	static
192.168.77.50	Pointer (PTR)	clienteW10.tuempresa.com.	3/14/2025 3:00:00 PM
192.168.77.80	Pointer (PTR)	SERVIDORTE.tuempresa.com.	static

Para confirmar que ha configurado la zona correctamente, escriba el siguiente comando en el CMD.

```
C:\Users\Administrator>nslookup 192.168.77.80
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Name:     SERVIDORTE.tuempresa.com
Address:  192.168.77.80
```

Y para la zona directa:

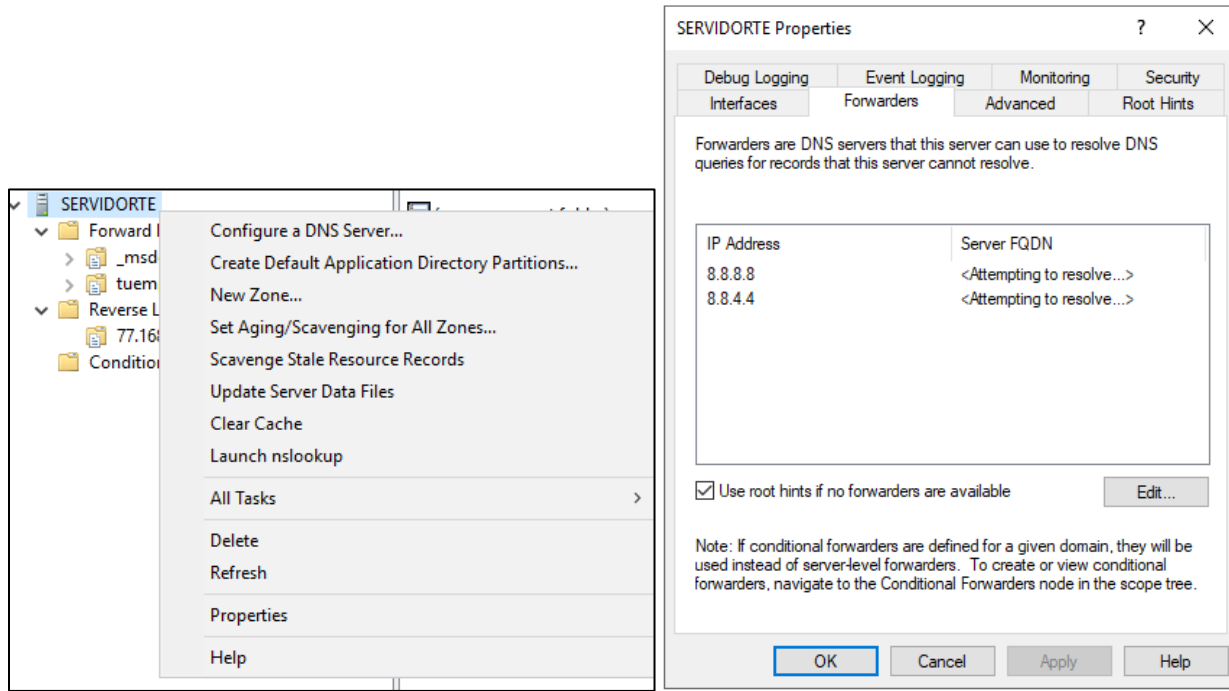
```
C:\Users\Administrator>nslookup SERVIDORTE.tuempresa.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Name:     SERVIDORTE.tuempresa.com
Address:  192.168.77.80
```

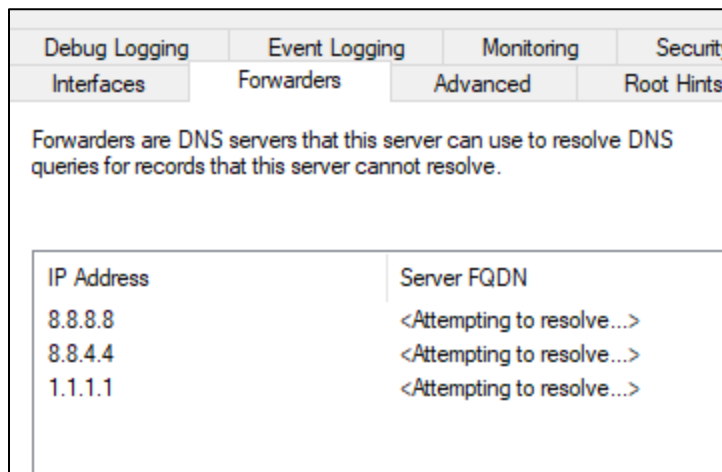
Desde el servidor o cualquier cliente puede hacer estas comprobaciones, debería ser el mismo resultado para todos.

Reenviadores DNS

Esto es opcional, pero puede ayudar si se necesita acceso a Internet desde algún cliente con DNS.



En este apartado ya se tenían dos configurados, pero puede agregar más al oprimir **Edit**.



DHCP

¿Qué es DHCP?

Es el **Protocolo de Configuración Dinámica de Host**, un servicio que asigna direcciones IP **automáticamente** a los dispositivos en una red. En lugar de configurar manualmente cada equipo, DHCP les proporciona una IP y otros parámetros de red de forma automática.

¿Para qué funciona DHCP?

DHCP facilita la administración de direcciones IP al asignarlas de manera dinámica y evitar conflictos. También proporciona información esencial como la puerta de enlace (**Gateway**), servidores **DNS** y otros detalles de configuración de red.

Importancia de DHCP en AD

En un entorno con Active Directory, DHCP es fundamental para garantizar que los dispositivos de la red reciban configuraciones correctas y puedan comunicarse con los servidores. Además, puede integrarse con DNS para registrar automáticamente los equipos en la red, facilitando su identificación y administración.

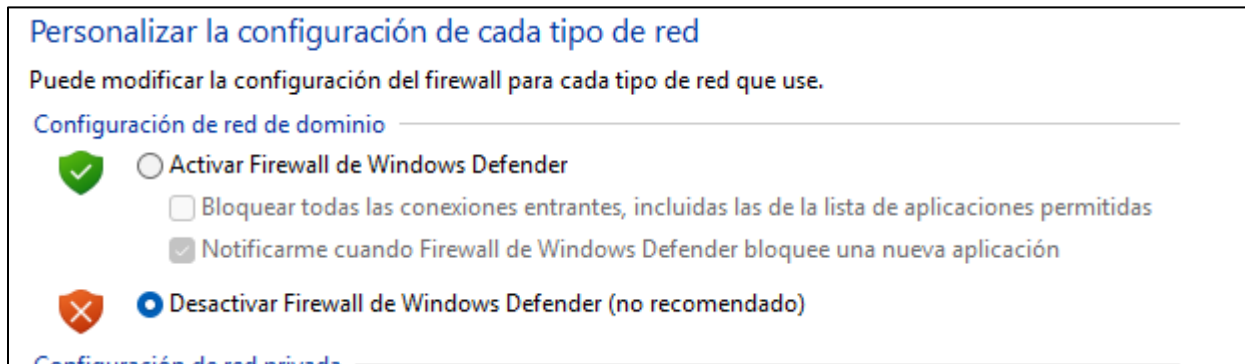
Configuración de DHCP en AD

Precaución

Antes de empezar a configurar el Pool en DHCP, es necesario hacer lo siguiente en TODAS las máquinas del dominio, las cuales recibirán direcciones de este servicio.

Como anteriormente ya se ha ingresado a configuraciones de Firewall para desactivarlo, deberá realizar nuevamente esta acción. Al enlazar un nuevo dispositivo a un dominio, se activa una nueva función de firewall, la cual es para la red de dominio. Mayormente, esta opción se activa sin notificarle al usuario, lo cual puede interferir con ciertas configuraciones. En este caso, si no se desactiva, el DHCP no será reconocido por los clientes.

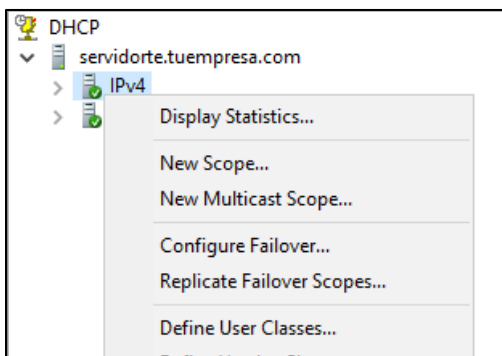
Aunque no siempre está activa, lo ideal es confirmar antes de comenzar a configurar, ya que podría ser un estorbo después, y no reconocería de dónde viene el error.



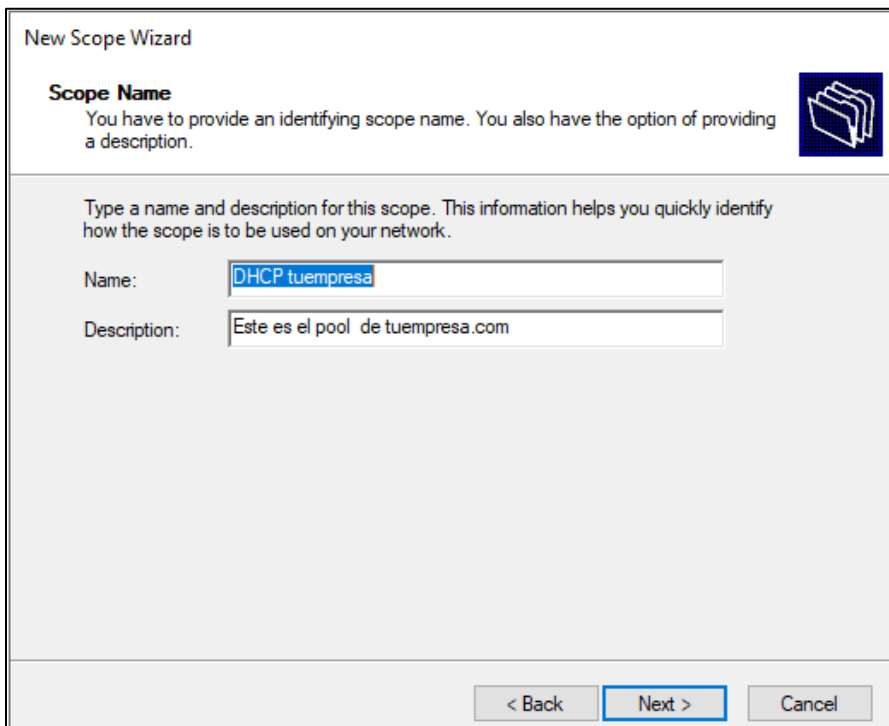
Scope DHCP

La creación del Scope DHCP se divide en varias partes. Durante la creación y configuración del mismo se pasa por el rango de IP, exclusión de direcciones, configuración de puerta de enlace... Todo se verá a continuación.

El primer paso es ingresar a la configuración de DHCP a través de la barra de herramientas. En el servidor DHCP verá las opciones de IPv4 e IPv6. Es este trabajo solo se configurará IPv4. De clic derecho sobre el mismo, y seleccione la opción New Scope.



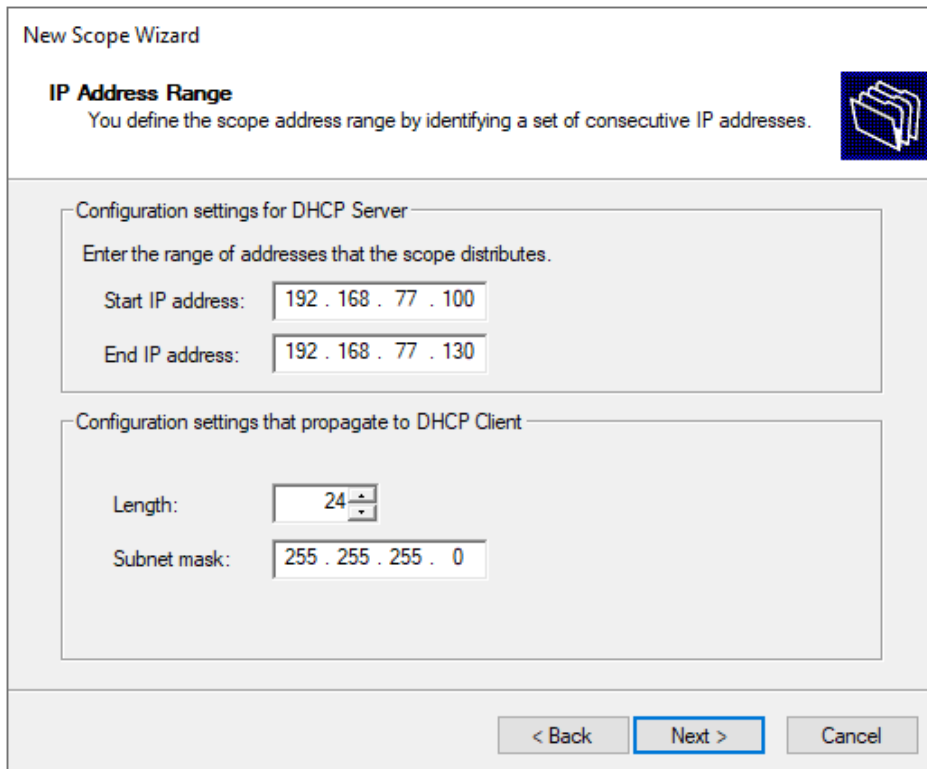
Con esto, colocará el nombre y/o descripción de su Scope DHCP.



Rango de direcciones

Más adelante se nos solicitará el rango que queremos otorgar a nuestro direccionamiento. Es decir, desde qué IP a cuál queremos que nuestro DHCP imparta direcciones. En este caso, se configuró para que brinde 30 direcciones desde el rango 192.168.77.100 – 192.168.77.130.

De forma automática el Scope configura la longitud y máscara de red, dependiendo el rango que le otorgue. Claro está, todo esto lo configurará según lo necesario para su empresa o su práctica.



New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 77 . 100

End IP address: 192 . 168 . 77 . 130

Configuration settings that propagate to DHCP Client

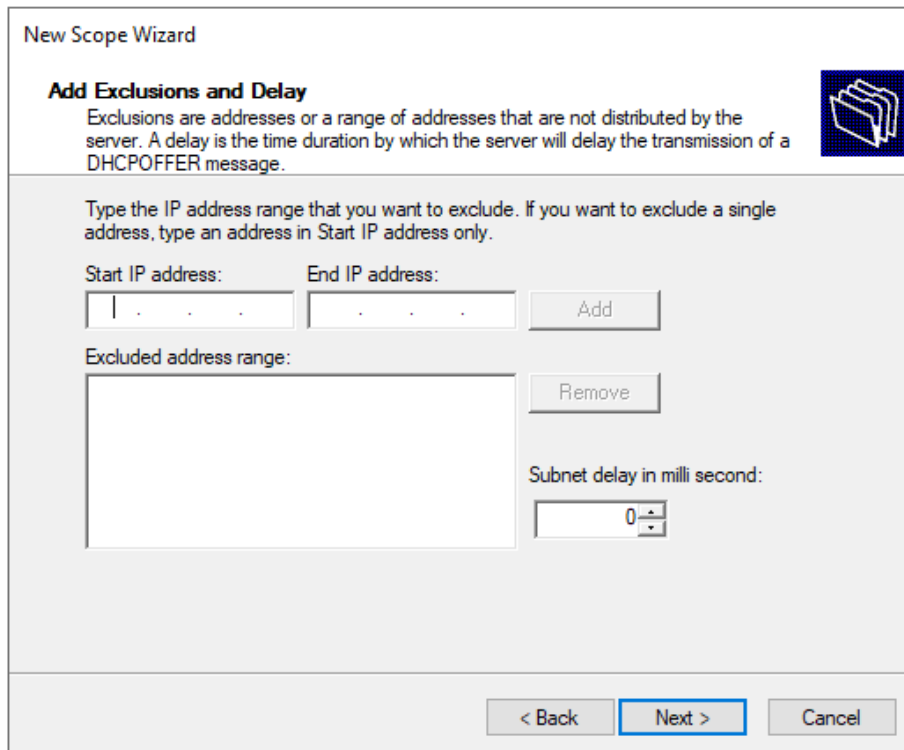
Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

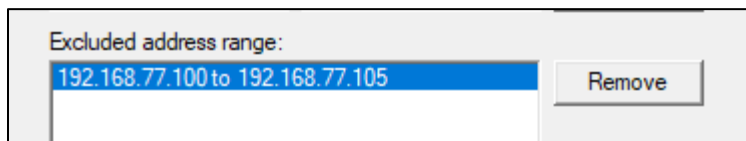
Direcciones excluidas

Esto no suele configurarse para simples prácticas. Pero, si lo desea, este es su momento. Por lo general, las direcciones excluidas se utilizan para evitar conflictos en la red. Estas direcciones no serán otorgadas dinámicamente a los clientes; preferiblemente se dejan para aquellos dispositivos que serán configurados con IPs estáticas, como impresoras.



The image shows a screenshot of the 'New Scope Wizard' window, specifically the 'Add Exclusions and Delay' step. The window has a title bar 'New Scope Wizard' and a subtitle 'Add Exclusions and Delay'. Below the subtitle, there is a description: 'Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.' To the right of this text is a folder icon. The main area of the window contains instructions: 'Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.' Below this, there are two input fields: 'Start IP address:' and 'End IP address:'. The 'Start IP address:' field contains '1' followed by three dots. The 'End IP address:' field contains three dots. To the right of these fields is an 'Add' button. Below the 'Add' button is a 'Remove' button. To the left of the 'Remove' button is a large text area labeled 'Excluded address range:'. To the right of the 'Remove' button is a 'Subnet delay in milli second:' label and a spinner box containing the number '0'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

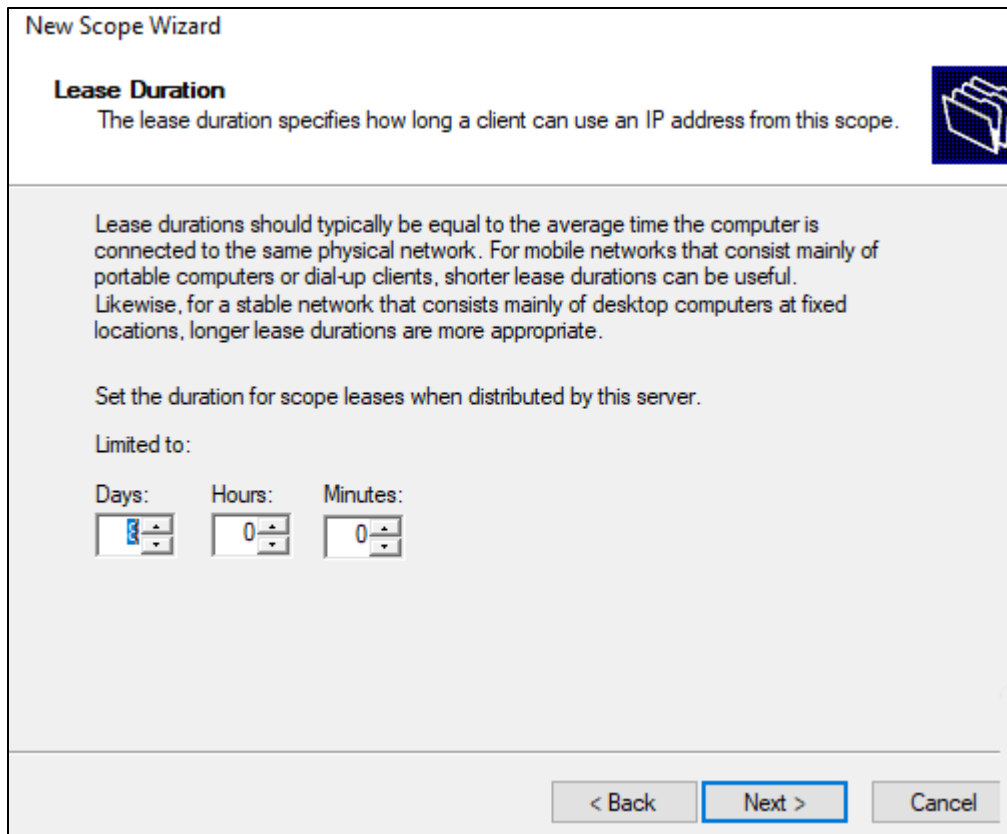
En este caso, solo se excluyeron cinco direcciones. Las primeras cinco del rango.



The image shows a close-up of the 'Excluded address range:' list box. It contains a single entry: '192.168.77.100 to 192.168.77.105'. The entry is highlighted with a blue background. To the right of the list box is a 'Remove' button.

Tiempo de duración para las direcciones

Por temas de seguridad, el DHCP no otorga direcciones dinámicas por un tiempo prolongado. Lo ideal sería dejar la configuración por defecto, 8 días. Pero si lo desea, puede cambiar este parámetro.



New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days: 8 Hours: 0 Minutes: 0

< Back Next > Cancel

Gateway del DHCP

Esta ventana le aparecerá. Si desea configurar todo de enseguida, puede continuar. De lo contrario, su recorrido por este trabajo ha terminado.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

☒ Yes, I want to configure these options now


☐ No, I will configure these options later

Toda configuración de direcciones IP necesita una puerta de enlace. En este caso, agregará la que tiene en su servidor que, por lo general es la primera IP de su rango. Puede que no sea necesario que la agregue, ya que podría aparecerle una vez acceda a este paso.

New Scope Wizard

Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.



To add an IP address for a router used by clients, enter the address below.

IP address:

.

.

.

192.168.77.1

Add

Remove

Up

Down

< Back

Next >

Cancel

DNS

También es posible que aparezca un servidor DNS ya configurado en este apartado. Independiente de, agregue la IP de su servidor. Esto, para que de inmediato los dispositivos sean configurados con el DNS del servidor en su DHCP.

New Scope Wizard

Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

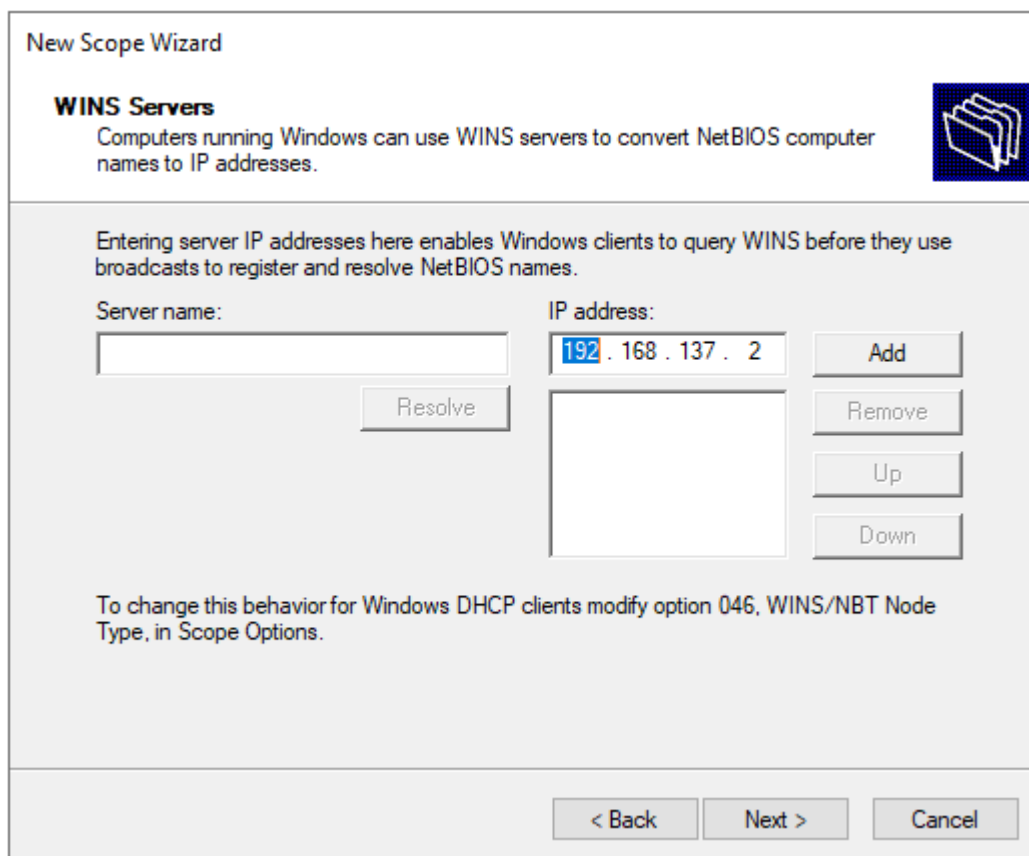
Server name:	IP address:	
<input type="text"/>	<input type="text" value=" . . ."/>	<input type="button" value="Add"/>
<input type="button" value="Resolve"/>	8.8.8.8 192.168.77.80	<input type="button" value="Remove"/>
		<input type="button" value="Up"/>
		<input type="button" value="Down"/>

< Back Next > Cancel

WINS Servers

Windows Internet Name Service es un servicio de resolución de nombres desarrollado por Microsoft que convierte nombres de equipos NetBIOS en direcciones IP. Permite que los dispositivos con nombres NetBIOS en redes Windows se comuniquen entre sí sin necesidad de usar direcciones IP.

Con el tiempo esto ha dejado de utilizarse, en su lugar ha sido reemplazado con DNS en los entornos modernos que no dependen de NetBIOS. En este caso no será configurado, puede removerlo si así lo desea.



New Scope Wizard

WINS Servers
Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.

Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.

Server name:

IP address:

To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.

Activación del Scope

New Scope Wizard

Activate Scope
Clients can obtain address leases only if a scope is activated.

Do you want to activate this scope now?

☒ Yes, I want to activate this scope now

☐ No, I will activate this scope later

< Back Next > Cancel

New Scope Wizard

Completing the New Scope Wizard
You have successfully completed the New Scope wizard.

To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.

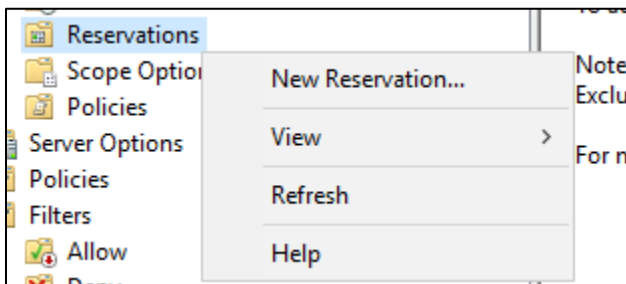
To close this wizard, click Finish.

< Back Finish Cancel

Reservación de direcciones

La reserva de dirección en DHCP es una configuración que asigna una dirección **IP específica** a un dispositivo en la red de manera permanente, basada en su dirección **MAC**. Evita conflictos al asegurar que la IP reservada no se asigne a otro equipo.

En esta práctica solo se hará reserva de la IP del servidor. Cuando haya terminado de configurar el Scope, le será fácil ver la opción, y ahí podrá hacer una nueva reserva.



Ya se mencionó que necesita la MAC de la máquina para esta reserva. Para encontrar la dirección física de su máquina, basta con el comando **ipconfig /all**, y en el último apartado la encontrará. Cópiela o memorícela para ingresarla al siguiente formulario.

```
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-54-0D-41
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::1c00:5141:a2e4:6186%12(Preferred)
IPv4 Address. . . . . : 192.168.77.80(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.77.1
DHCPv6 IAID . . . . . : 83889193
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-47-29-1B-00-0C-29-54-0D-41
DNS Servers . . . . . : ::1
                        8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Administrator>
```

New Reservation ? X

Provide information for a reserved client.

Reservation name:

IP address:

MAC address:

Description:


Supported types

☒ Both

☐ DHCP

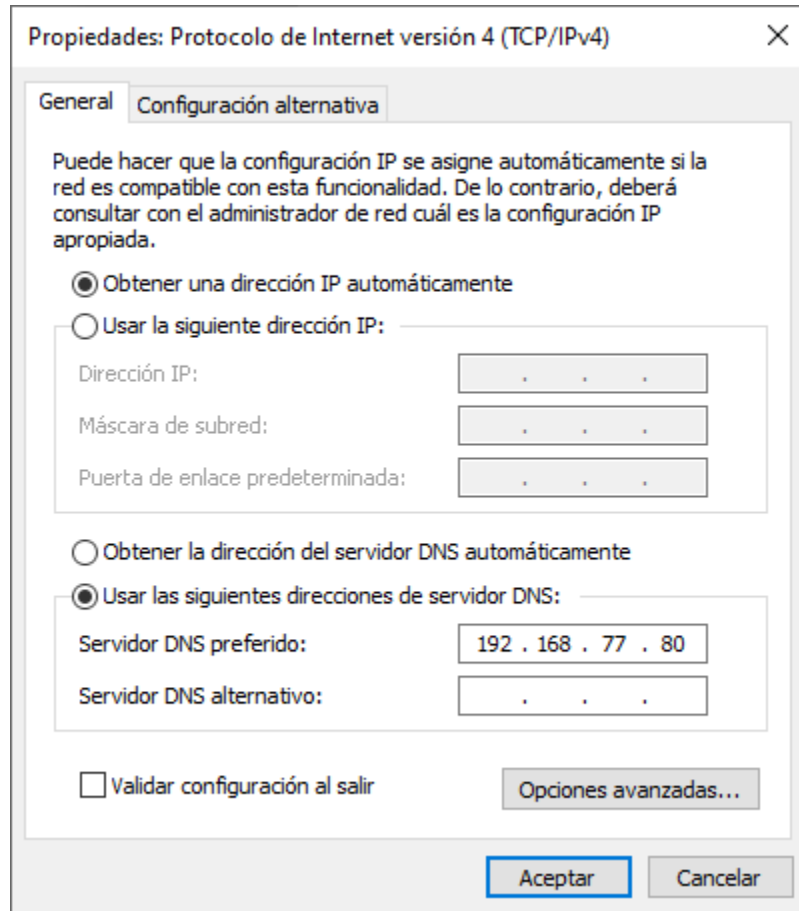
☐ BOOTP

Add Close

Reservations
 [192.168.77.80] SERVIDORTE

DHCP para los clientes

Para activar este protocolo en cada cliente del domino, no basta más que ir a la configuración de red de cada máquina y, donde antes se habían puesto direcciones IP estáticas, se activará la opción de recibir IP de forma automática.



Opcionalmente puede dejar el DNS como está. Ya que lo tiene configurado, no tiene por qué tocarlo.

Ahora, deberá notar que, no de inmediato recibirá su nueva dirección IP. Por lo que es necesario ejecutar un comando desde el CMD. Este comando es: **ipconfig /renew**. Esto hará que la configuración de red busque una nueva dirección dentro del pool DHCP. Y si está configurado correctamente, deberá darle la primera dirección disponible.


```

PS C:\Users\martinez_ana> ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet0:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::d361:deb1:b311:4e15%7
    Dirección IPv4 de configuración automática: 169.254.59.165
    Máscara de subred . . . . . : 255.255.0.0
    Puerta de enlace predeterminada . . . . . :
PS C:\Users\martinez_ana> ipconfig /renew

Configuración IP de Windows

Adaptador de Ethernet Ethernet0:

    Sufijo DNS específico para la conexión. . . : tuempresa.com
    Vínculo: dirección IPv6 local. . . : fe80::d361:deb1:b311:4e15%7
    Dirección IPv4. . . . . : 192.168.77.106
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.77.1
PS C:\Users\martinez_ana>

```

Como anteriormente se configuró la exclusión de cinco direcciones, la primera en lista es la **.6**, como ve en la ilustración.

```

C:\Users\miguel>ipconfig /renew

Configuración IP de Windows

Adaptador de Ethernet Ethernet0:

    Sufijo DNS específico para la conexión. . . : tuempresa.com
    Vínculo: dirección IPv6 local. . . : fe80::8a46:d34d:d58d:3886%14
    Dirección IPv4. . . . . : 192.168.77.107
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.77.1

C:\Users\PS>ipconfig /renew

Configuración IP de Windows

Error al liberar la interfaz Loopback Pseudo-Interface 1 : El sistema
ncontrar el archivo especificado.

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . . : tuempresa.com
    Vínculo: dirección IPv6 local. . . : fe80::39e0:436b:6299:a1cd%11
    Dirección IPv4. . . . . : 192.168.77.108
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.77.1

Adaptador de túnel isatap.tuempresa.com:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . : tuempresa.com
C:\Users\PS>

```

Vistazo al nuevo Scope

Y su Scope debería verse así:

DHCP		Client IP Address	Name	Lease Expiration	Type
servidorte.tuempresa.com	IPv4	192.168.77.106	empleadoW11.tuempresa.com	3/25/2025 12:27:51 PM	DHCP
	Scope [192.168.77.0] DHCP tuempresa	192.168.77.107	clienteW10.tuempresa.com	3/25/2025 12:38:29 PM	DHCP
	Address Pool	192.168.77.108	empleadoW7-PC.tuempresa.com	3/25/2025 12:43:41 PM	DHCP
	Address Leases				
	Reservations				
	Scope Options				
	Policies				

DHCP		Start IP Address	End IP Address	Description
servidorte.tuempresa.com	IPv4	192.168.77.100	192.168.77.130	Address range for distribution
	Scope [192.168.77.0] DHCP tuempresa	192.168.77.100	192.168.77.105	IP Addresses excluded from distribution
	Address Pool			
	Address Leases			

DHCP		Option Name	Vendor	Value	Policy Name
servidorte.tuempresa.com	IPv4	003 Router	Standard	192.168.77.1	None
	Scope [192.168.77.0] DHCP tuempresa	006 DNS Servers	Standard	8.8.8.8, 192.168.77.80	None
	Address Pool	015 DNS Domain Name	Standard	tuempresa.com	None
	Address Leases				

Conclusión y reflexión final

Resumen de lo aprendido y reflexión personal

La implementación de Active Directory en un entorno empresarial permite una gestión centralizada y eficiente de usuarios, equipos y recursos, asegurando mayor seguridad y control dentro de la organización. La correcta instalación y configuración de AD en Windows Server, junto con la integración de DNS y DHCP, proporciona una infraestructura estable donde la administración de dominios, árboles y bosques facilita la escalabilidad y organización de la red. La asignación de IPs estáticas y la incorporación de equipos al dominio garantizan una comunicación fluida entre los dispositivos, optimizando el uso de los recursos de red.

Las GPOs (Políticas de Grupo) son esenciales para establecer restricciones y configuraciones de seguridad, permitiendo la automatización de tareas como la gestión de contraseñas, la personalización del entorno de trabajo y la instalación de software. La administración de objetos en AD, como usuarios, grupos y unidades organizativas, facilita el control y asignación de permisos dentro de la empresa, asegurando que cada usuario tenga acceso solo a los recursos necesarios para su función.

Como opinión personal, esta práctica aportó a la diversión y el conocimiento. Trabajar con Active Directory puede ser tedioso al inicio, pero una vez hay familiarización con los procesos, todo se hace más sencillo. Jugar con las políticas de grupo nos hace ver hasta dónde puede restringirse un sistema, y hasta dónde es bueno dar libertades al usuario. Configurar DNS y DHCP nos permite ver cómo las redes trabajan en cuestiones de segundos cosas que, podrían ser eternas para una mano humana.

Importancia en estos temas

La gestión eficiente de los sistemas y recursos dentro de una organización es fundamental para garantizar un entorno de trabajo seguro, organizado y escalable. La implementación de tecnologías adecuadas permite centralizar la administración, optimizar los procesos y reducir la carga operativa, facilitando la supervisión y el control de la infraestructura. Esto no solo mejora la seguridad y el acceso a la información, sino que también permite una mejor distribución de los recursos, asegurando que cada usuario tenga las herramientas necesarias para desempeñar sus funciones de manera eficiente. La automatización y estandarización de configuraciones dentro de una red empresarial contribuyen a la estabilidad y el rendimiento del sistema, evitando problemas de compatibilidad y asegurando una experiencia uniforme para los usuarios. Contar con un entorno bien estructurado permite responder de manera ágil a los cambios y necesidades de la organización, minimizando riesgos y mejorando la productividad. Una administración efectiva de estos aspectos no solo fortalece la infraestructura tecnológica, sino que también impulsa el crecimiento y la innovación dentro de las empresas.