

# Implementación y Administración de un Dominio con Active Directory

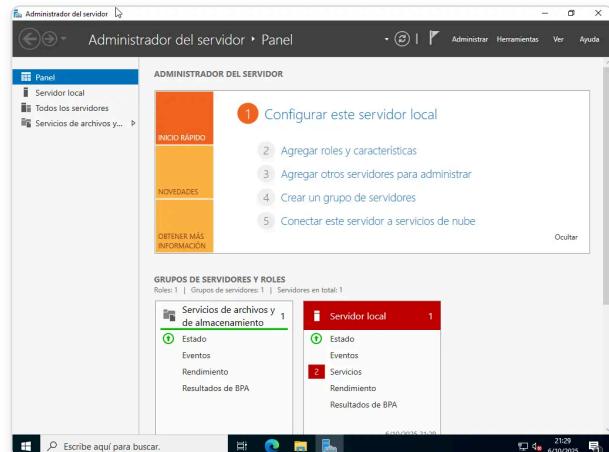
## Fase 1: Configuración Inicial del Servidor

Antes de instalar cualquier rol complejo como Active Directory, es crucial realizar una configuración base del servidor. Esto asegura una base estable, segura y fácil de identificar en la red. Los pasos incluyen establecer un nombre de host descriptivo, configurar una dirección IP estática y asegurarse de que el sistema esté actualizado.

### 1.1: Interfaz Principal del Administrador del Servidor

La imagen muestra el "Administrador del Servidor" (Server Manager), la consola central desde la cual se gestionan la mayoría de los aspectos de un servidor Windows. Esta es la primera pantalla que vemos tras iniciar sesión.

Proporciona un resumen del estado del servidor, los roles instalados, los eventos y el rendimiento. Desde aquí se lanzan los asistentes para agregar o quitar roles y características, y se accede a otras herramientas de administración.



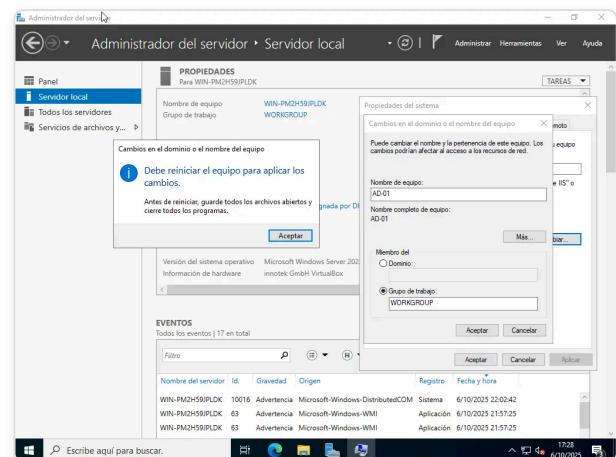
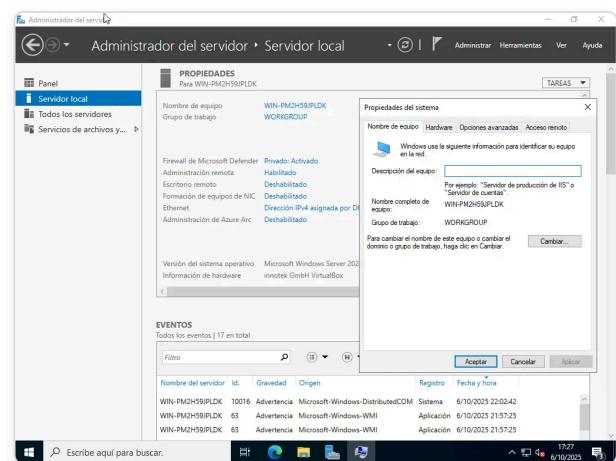
## 1.2: Cambio de Nombre del Servidor

Se procede a cambiar el nombre de host del servidor. Por defecto, Windows asigna un nombre aleatorio y poco descriptivo (ej. **WIN-PM2H59JPLDK**). Se cambia a un nombre significativo: **AD-01**.

Asignar un nombre descriptivo es una práctica fundamental en la administración de sistemas. Facilita la identificación del servidor en la red, en los registros de eventos, en las herramientas de monitoreo y en la documentación. Un nombre como **AD-01** indica claramente su función (Active Directory) y su número de instancia (el primero).

### Cómo:

1. Desde el "Administrador del Servidor", se navega a la sección "Servidor local".
2. Se hace clic en el nombre de equipo actual. Esto abre la ventana de "Propiedades del sistema".
3. En la pestaña "Nombre de equipo", se pulsa el botón "Cambiar...".
4. Se introduce el nuevo nombre (**AD-01**) y se acepta.
5. El sistema informa que es necesario reiniciar para aplicar los cambios, lo cual es un paso obligatorio.

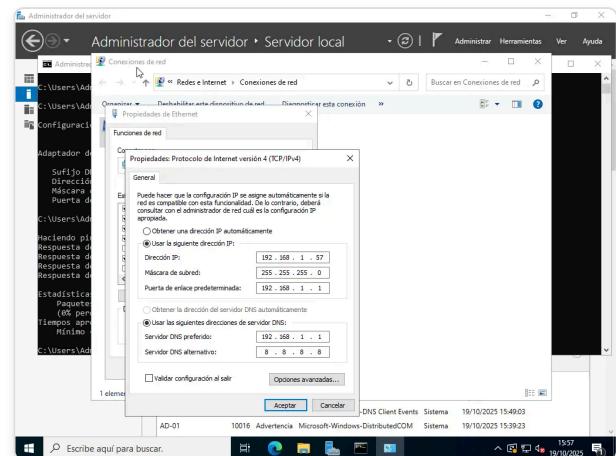
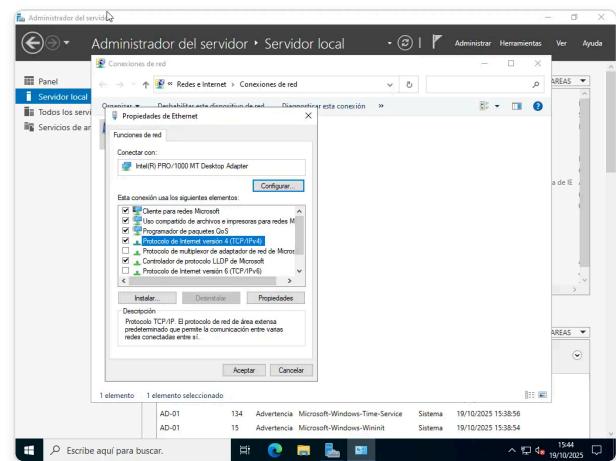
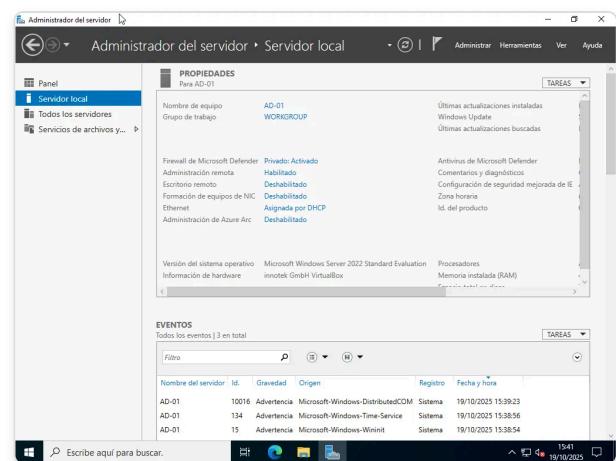


## 1.3: Configuración de Dirección IP Estática

Se configura una dirección IP estática para el adaptador de red del servidor. Se abandona la configuración automática por DHCP y se asignan manualmente la dirección IP, la máscara de subred, la puerta de enlace y los servidores DNS, ya que un Controlador de Dominio debe tener una dirección IP estática, ya que necesitan ser localizables en una dirección predecible y constante.

### Cómo:

1. En "Servidor local", se hace clic en el enlace junto a "Ethernet" (que puede mostrar "Asignada por DHCP"). Esto abre "Conexiones de red".
2. Se hace clic derecho sobre el adaptador de red y se selecciona "Propiedades".
3. Se selecciona "Protocolo de Internet versión 4 (TCP/IPv4)" y se pulsa "Propiedades".
4. Se marca la opción "Usar la siguiente dirección IP" y se rellenan los campos. En este caso:
  - **Dirección IP:** 192.168.1.57
  - **Máscara de subred:** 255.255.255.0
  - **Puerta de enlace predeterminada:** 192.168.1.1
5. De manera crucial, para el servidor DNS, se configura el "Servidor DNS preferido" con la propia dirección IP del servidor (192.168.1.57). Esto es porque, una vez instalado el rol DNS, el servidor se



consultará a sí mismo para la resolución de nombres del dominio. Como DNS alternativo, se puede usar otro controlador de dominio o un DNS público ( 8.8.8.8 ) para la resolución de nombres externos.

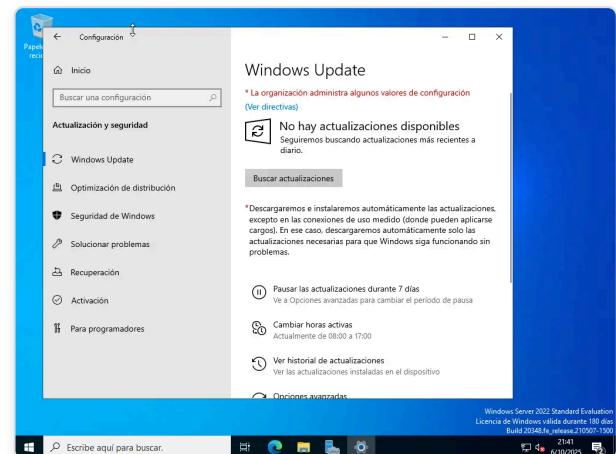
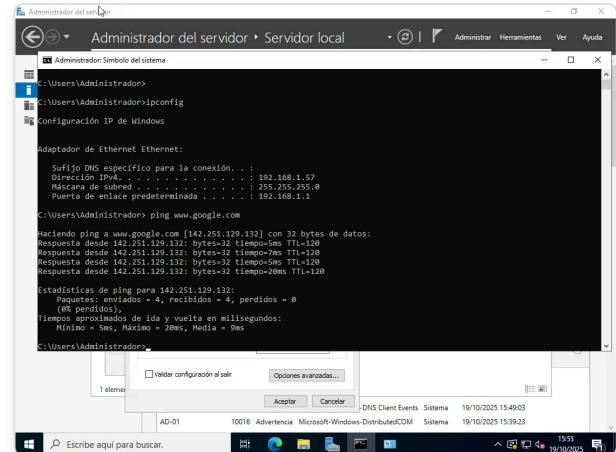
## 1.4: Verificación de Conectividad y Actualizaciones

Tras configurar la IP estática, se verifica que la configuración es correcta y que el servidor tiene conectividad. Además, se revisa el estado de las actualizaciones de Windows.

La verificación es un paso crítico para evitar problemas futuros. Un error en la configuración de red podría aislar al servidor. Los comandos `ipconfig` y `ping` son herramientas de diagnóstico de primer nivel. Por otro lado, instalar todas las actualizaciones de seguridad antes de exponer el servidor a un rol crítico como AD DS es una práctica de seguridad indispensable para mitigar vulnerabilidades conocidas.

### Cómo:

- 1. Verificación de IP:** Se abre una consola de Símbolo del sistema ( cmd ) o PowerShell y se ejecuta el comando `ipconfig`. Esto debe mostrar la dirección IP estática que acabamos de configurar.
- 2. Verificación de Conectividad:** Se ejecuta `ping www.google.com` para confirmar que el servidor tiene acceso a Internet a



través de la puerta de enlace y que la resolución de DNS externa funciona. Una respuesta exitosa confirma que la configuración de red básica es correcta.

**3. Actualizaciones:** Se accede a "Configuración" > "Actualización y seguridad" > "Windows Update" y se hace clic en "Buscar actualizaciones". Se deben instalar todas las actualizaciones críticas y recomendadas. La imagen muestra que la organización gestiona algunas configuraciones, lo que podría ser el resultado de una política de grupo en un entorno ya existente, o una configuración manual.

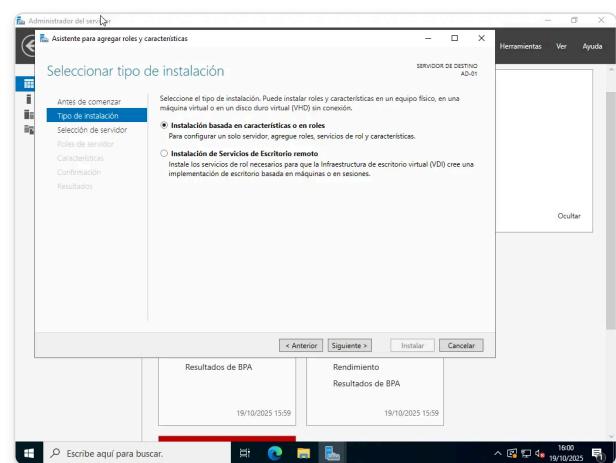
## Fase 2: Instalación y Configuración de Active Directory Domain Services (AD DS)

Esta es la fase central del proyecto. Se instalará el rol de Servicios de Dominio de Active Directory y se promocionará el servidor para que se convierta en el primer Controlador de Dominio de un nuevo bosque y dominio.

### 2.1: Inicio del Asistente para Agregar Roles y Características

Se inicia el proceso para añadir un nuevo rol al servidor a través del "Asistente para agregar roles y características".

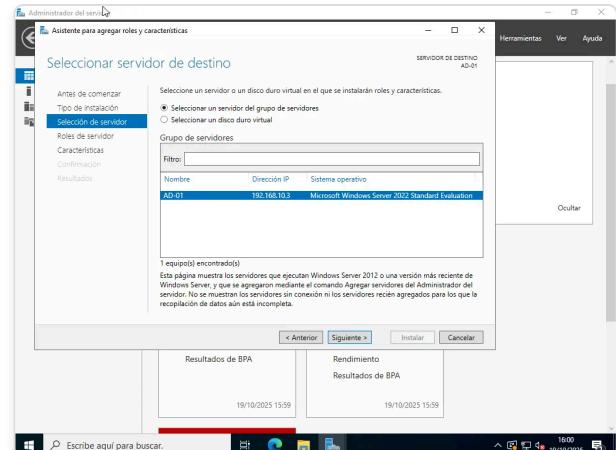
En Windows Server, las funcionalidades se modularizan en "roles" (funciones principales, como servidor web o AD) y "características" (funciones de apoyo, etc). Este asistente guía al



administrador a través de la selección e instalación de estos componentes.

### Cómo:

1. Desde el "Administrador del Servidor", se hace clic en "Administrar" en la esquina superior derecha y se selecciona "Aregar roles y características". Alternativamente, se puede usar el enlace en el panel principal.
2. La primera pantalla del asistente es informativa. Se hace clic en "Siguiente".
3. Se elige el tipo de instalación. Para este caso, se selecciona "Instalación basada en características o en roles", que es la opción estándar para configurar un único servidor. La otra opción es para escenarios de VDI (Virtual Desktop Infrastructure).
4. A continuación, se selecciona el servidor de destino. Como estamos trabajando en el servidor local, AD-01 ya aparece seleccionado en el grupo de servidores.



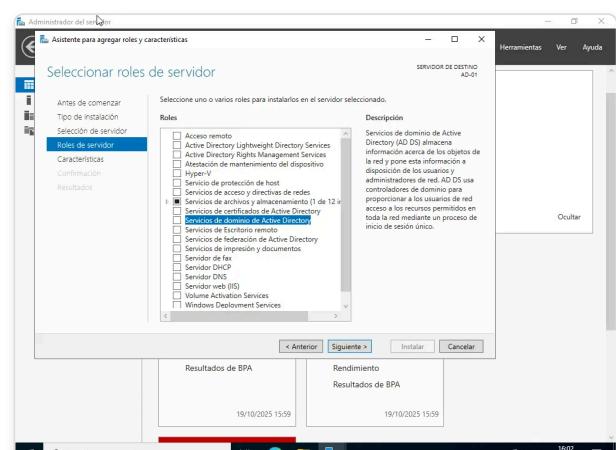
## 2.2: Selección del Rol de Servidor AD DS

En la lista de roles disponibles, se selecciona "Servicios de dominio de Active Directory".

Al seleccionarlo, el sistema detecta que se necesitan herramientas de administración adicionales.

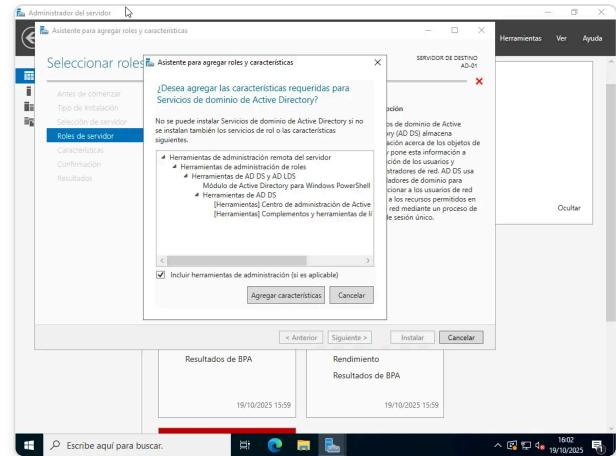
### Cómo:

1. En la pantalla "Seleccionar roles de servidor", se marca la casilla junto a



- "Servicios de dominio de Active Directory".
2. Automáticamente, aparece una ventana emergente que informa sobre las características adicionales requeridas, como las herramientas de administración de AD DS y AD LDS, el módulo de PowerShell para Active Directory, etc. Estas herramientas son esenciales para gestionar el dominio una vez instalado.

3. Se deja marcada la opción "Incluir herramientas de administración (si es aplicable)" y se hace clic en "Agregar características".
4. Se continúa con el asistente, sin necesidad de añadir características adicionales en la siguiente pantalla, y se confirma la instalación.



## Concepto Clave: Active Directory Domain Services (AD DS)

Es el servicio de directorio de Microsoft. Almacena información sobre los objetos de la red (usuarios, equipos, impresoras) y pone esta información a disposición de usuarios y administradores. Su función principal es la autenticación y autorización centralizada, permitiendo un inicio de sesión único (Single Sign-On) para acceder a los recursos de la red.

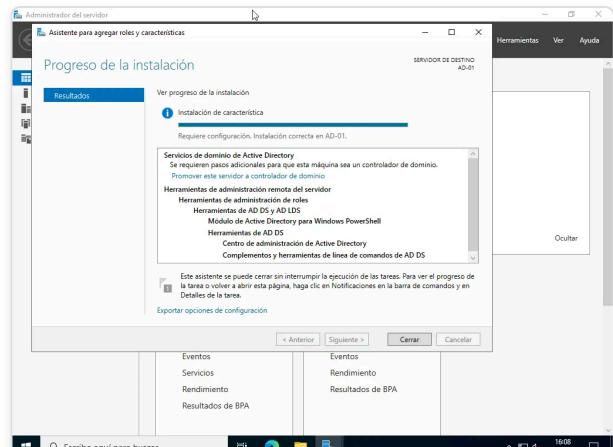
## 2.3: Promoción del Servidor a Controlador de Dominio

Una vez finalizada la instalación de los binarios del rol AD DS, el servidor aún no es un Controlador de Dominio. Es necesario "promocionarlo". La imagen muestra el resultado de la instalación con un enlace clave: "Promover este servidor a controlador de dominio".

La instalación del rol y la configuración del dominio son dos procesos separados. Primero se copian los archivos necesarios (instalación) y luego se configura el entorno del dominio (promoción). Esta separación permite, por ejemplo, preparar múltiples servidores con el rol instalado y promocionarlos más tarde, incluso de forma automatizada.

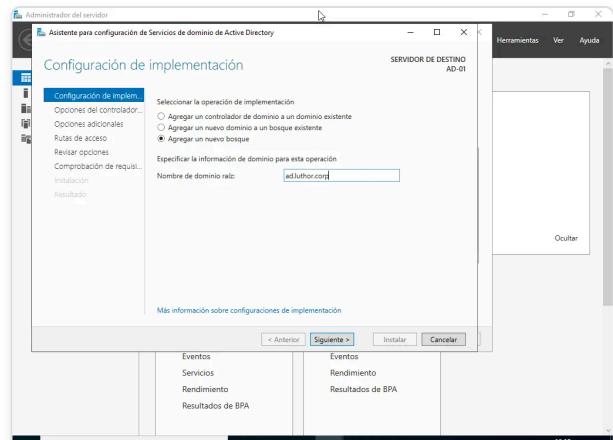
### Cómo:

1. En la pantalla de resultados de la instalación, se hace clic en el enlace azul "Promover este servidor a controlador de dominio".
2. Esto inicia el "Asistente para configuración de Servicios de dominio de Active Directory", que nos guiará en la creación de nuestro dominio.



## 2.4: Configuración del Nuevo Bosque y Dominio

En el primer paso del asistente de promoción, se debe decidir la operación de implementación. Como este es el primer controlador de dominio de la organización, se elige "Aregar un nuevo bosque".



- **Agregar un controlador de dominio a un dominio existente:** Se usa para añadir redundancia o capacidad a un dominio ya creado.
- **Agregar un nuevo dominio a un bosque existente:** Se usa para crear un dominio hijo (ej. `ventas.ad.luthor.corp`) o un nuevo árbol en el bosque.
- **Agregar un nuevo bosque:** Se usa para crear la estructura inicial de Active Directory. El primer dominio que se crea en un bosque se llama "dominio raíz del bosque".

### Cómo:

1. Se selecciona la opción "Aregar un nuevo bosque".
2. Se especifica el "Nombre de dominio raíz".

En este proyecto, se utiliza `ad.luthor.corp`. Es una buena práctica usar un subdominio de un dominio público que la empresa posea (ej. `corp.example.com`) o un dominio no enrutable terminado en `.local` o `.corp` para evitar conflictos con sitios web externos.

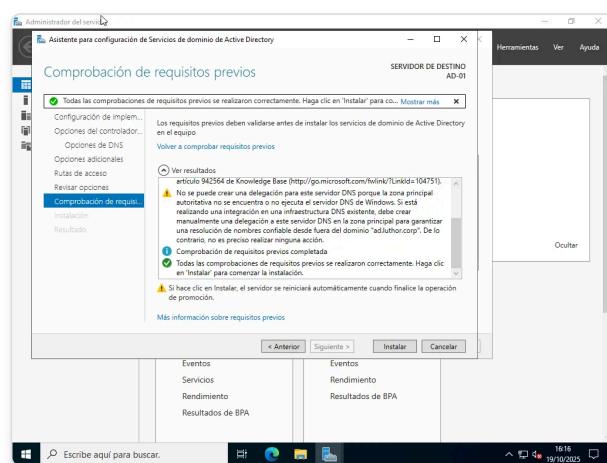
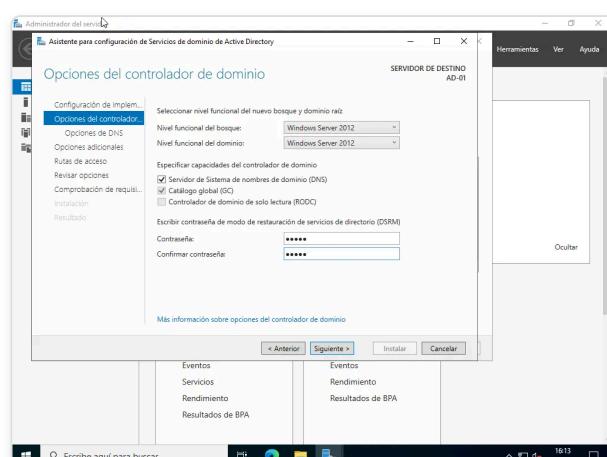
## Conceptos Clave: Bosque, Árbol y Dominio

**Dominio:** Un límite administrativo para objetos como usuarios y equipos. **Árbol:** Una colección de uno o más dominios que comparten un espacio de nombres contiguo (ej. luthor.corp y ventas.luthor.corp). **Bosque:** La estructura de más alto nivel. Es una colección de uno o más árboles que no comparten un espacio de nombres contiguo pero confían entre sí. El primer dominio define el nombre del bosque.

## 2.5: Opciones del Controlador de Dominio y Finalización

Se configuran las opciones funcionales del nuevo dominio y bosque, las capacidades del controlador de dominio y la contraseña de restauración.

- **Nivel funcional:** Determina las características avanzadas de Active Directory disponibles. Un nivel funcional más alto (ej. Windows Server 2016) habilita más funcionalidades, pero requiere que todos los controladores de dominio en el bosque/dominio ejecuten al menos esa versión de Windows Server. Como este es un nuevo bosque, se puede elegir el nivel más alto disponible.
- **Capacidades del DC:** Se especifica si este DC también será un Servidor DNS y/o



un Catálogo Global (GC). El primer DC en un bosque **debe** ser un GC y casi siempre es también un servidor DNS.

- **Contraseña DSRM:** La contraseña del Modo de Restauración de Servicios de Directorio (DSRM) es crucial. Es una contraseña de "último recurso" que se utiliza para arrancar el servidor en un modo especial que permite restaurar o reparar la base de datos de Active Directory. Debe ser segura y estar documentada.

#### Cómo:

1. Se establecen los niveles funcionales de bosque y dominio.
2. Se asegura que las casillas "Servidor de Sistema de nombres de dominio (DNS)" y "Catálogo global (GC)" estén marcadas.
3. Se introduce y confirma una contraseña segura para DSRM.
4. El asistente continúa, realiza una comprobación de requisitos previos. La advertencia sobre la delegación DNS es normal en este escenario, ya que no existe un servidor DNS autoritativo superior.
5. Una vez que la comprobación de requisitos es exitosa, se hace clic en "Instalar". El servidor se reiniciará automáticamente para completar el proceso.

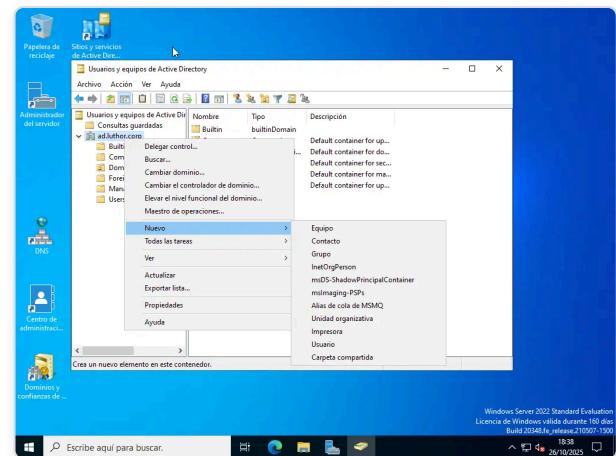
## Fase 3: Administración de Objetos de Active Directory

---

Con el Controlador de Dominio operativo, el siguiente paso es estructurar el directorio creando Unidades Organizativas para delegar la administración y organizar los objetos, y luego crear los usuarios y grupos que poblarán el dominio.

### 3.1: Creación de Unidades Organizativas, Usuarios y Grupos

Se utiliza la consola "Usuarios y equipos de Active Directory" para crear la estructura básica del dominio. La imagen muestra el menú contextual para crear nuevos objetos como Unidades Organizativas (OU), Usuarios y Grupos.



- **Unidades Organizativas (OU):** Son contenedores dentro de un dominio que se utilizan para organizar objetos (usuarios, grupos, equipos) de una manera jerárquica que refleja la estructura de la empresa (por departamento, ubicación geográfica, etc.). Su propósito principal es vincular Directivas de Grupo (GPOs) y delegar permisos administrativos. A diferencia de los contenedores por defecto (como "Users"), a las OUs sí se les pueden aplicar GPOs directamente.
- **Usuarios:** Representan a las personas que necesitarán acceder a los recursos de la red.
- **Grupos:** Simplifican la administración de permisos. En lugar de asignar permisos a cientos de usuarios individualmente, se asignan al grupo, y luego se añaden los usuarios a ese grupo.

#### Cómo:

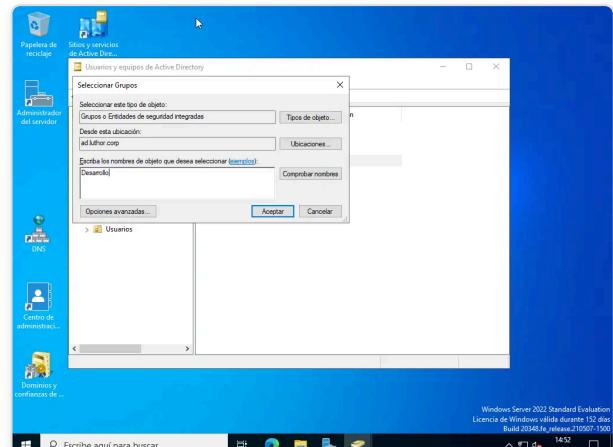
1. Se abre "Usuarios y equipos de Active Directory" desde el menú "Herramientas" del Administrador del Servidor.
2. Se hace clic derecho sobre el dominio (ad.luthor.corp) o sobre otra OU.

3. En el menú contextual, se selecciona "Nuevo" y luego el tipo de objeto a crear: "Unidad organizativa", "Usuario" o "Grupo".
4. Para este proyecto, se crearán OUs como "Usuarios", "Maquinas" y "Grupos" para una mejor organización, y dentro de ellas, los objetos correspondientes.

### 3.2: Anidación de Grupos para Gestión de Permisos

La imagen muestra el proceso de agregar un grupo a otro, una técnica conocida como "anidación de grupos". Aquí, se está buscando el grupo "Desarrollo" para añadirlo como miembro de otro grupo.

La anidación de grupos es una estrategia poderosa para gestionar permisos de forma escalable, siguiendo el modelo **AGDLP** (Accounts -> Global groups -> Domain Local groups -> Permissions) o **AGUDLP** (Accounts -> Global groups -> Universal groups -> Domain Local groups -> Permissions).



- Se agrupan **Cuentas** de usuario (A) en **Grupos Globales** (G) según su función (ej. "Desarrolladores").
- Se asignan **Permisos** (P) a **Grupos Locales de Dominio** (DL) que representan un recurso (ej. "Acceso a Carpeta de Proyectos").
- Finalmente, se anida el Grupo Global en el Grupo Local de Dominio.

Esto desacopla a los usuarios de los permisos, facilitando la administración: si un nuevo

desarrollador se une, solo hay que añadirlo al grupo "Desarrolladores" y automáticamente heredará todos los permisos correctos.

## Cómo:

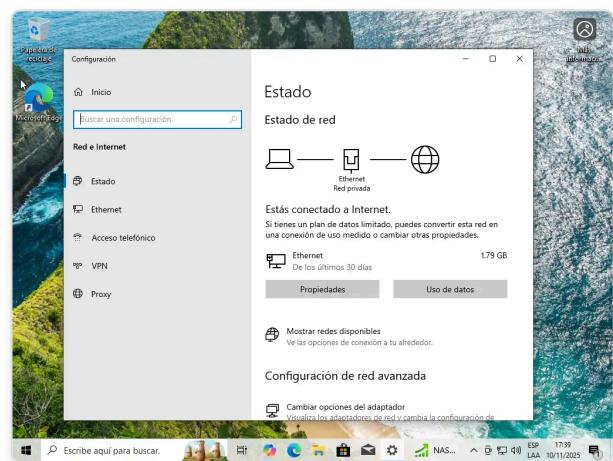
1. Se abren las propiedades del grupo "padre" (al que se le quiere añadir un miembro).
2. Se va a la pestaña "Miembros" y se hace clic en "Aregar".
3. En el cuadro de diálogo "Seleccionar Usuarios, Contactos, Equipos o Grupos", se cambia el "Tipo de objeto" para incluir "Grupos".
4. Se escribe el nombre del grupo a añadir ("Desarrollo") y se hace clic en "Comprobar nombres" para validar que existe, y luego en "Aceptar".

## Fase 4: Configuración del Cliente y Unión al Dominio

Una vez que la infraestructura del dominio está lista, el siguiente paso es integrar los equipos cliente. Esto les permitirá autenticarse contra el dominio y acceder a los recursos de la red de forma centralizada.

### 4.1: Configuración de Red del Equipo Cliente

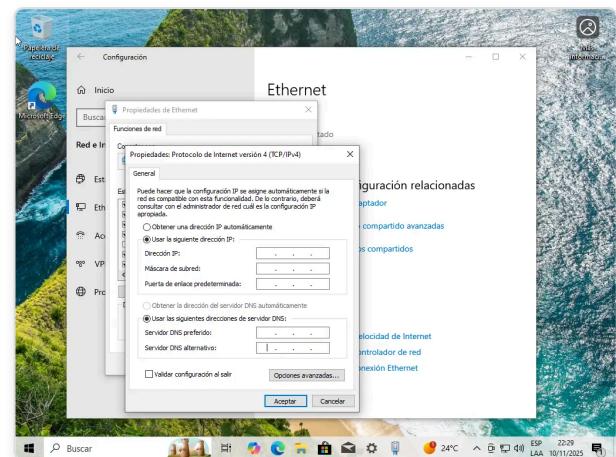
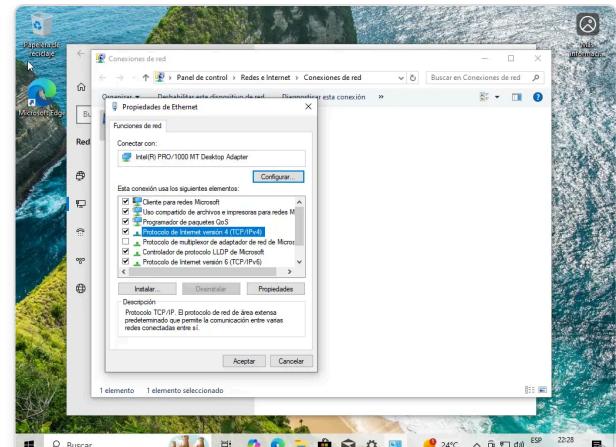
Para que un cliente pueda "encontrar" y comunicarse con el controlador de dominio, su configuración de red debe ser correcta. El punto más crítico es la configuración del **servidor DNS**. El cliente **debe** usar el servidor DNS de Active Directory (es decir, la dirección IP de



nuestro DC, ( 192.168.1.57 ) como su servidor DNS principal. De lo contrario, no podrá resolver los registros SRV necesarios para localizar los servicios del dominio (autenticación, catálogo global, etc.) y la unión al dominio fallará.

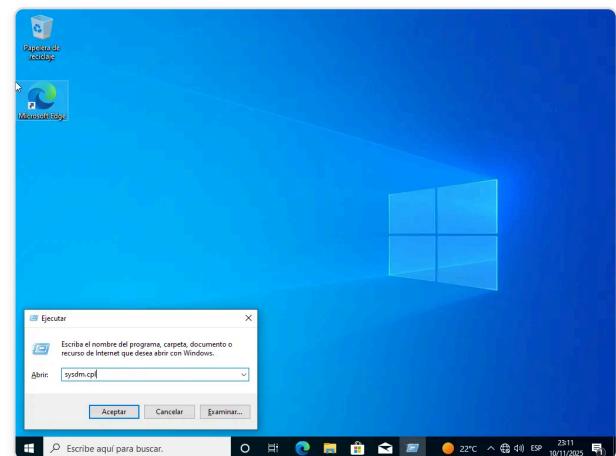
## Cómo:

1. En el equipo cliente, se navega a la configuración de red. Las imágenes muestran el flujo desde el ícono de red en la barra de tareas hasta las propiedades del adaptador.
2. Se accede a las propiedades de "Protocolo de Internet versión 4 (TCP/IPv4)".
3. La dirección IP del cliente puede ser asignada por DHCP (lo más común en redes corporativas) o ser estática. Lo importante es la configuración del DNS.
4. Se selecciona "Usar las siguientes direcciones de servidor DNS" y se introduce la IP del controlador de dominio ( 192.168.1.57 ) como "Servidor DNS preferido". Se puede añadir un DNS público como alternativo para la navegación por Internet.



## 4.2: Unión del Cliente al Dominio

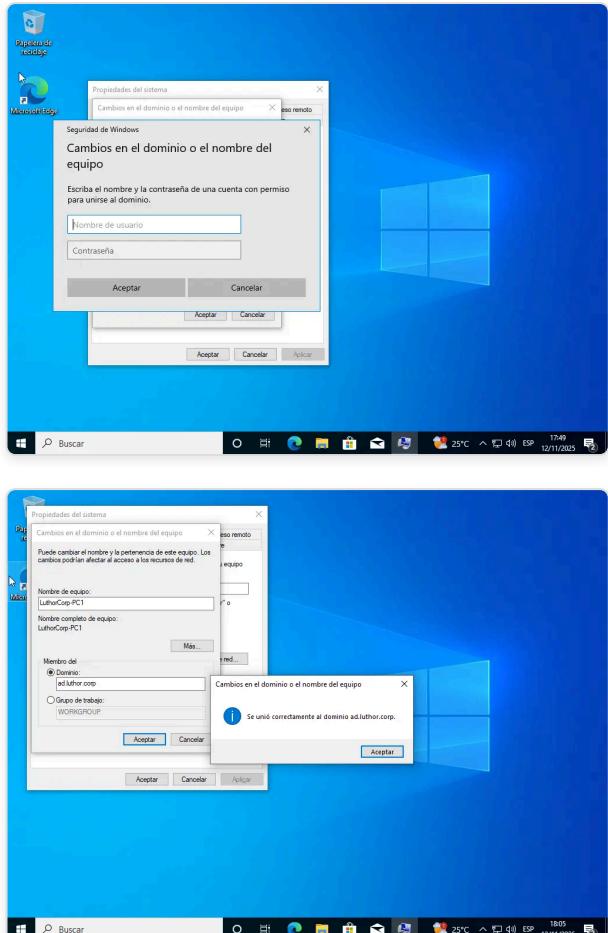
Unir un equipo al dominio crea una cuenta de equipo en Active Directory y establece una relación de confianza. Esto permite que los usuarios del dominio inicien sesión en ese equipo y que el equipo reciba y aplique las



Directivas de Grupo (GPOs) configuradas en el dominio.

## Cómo:

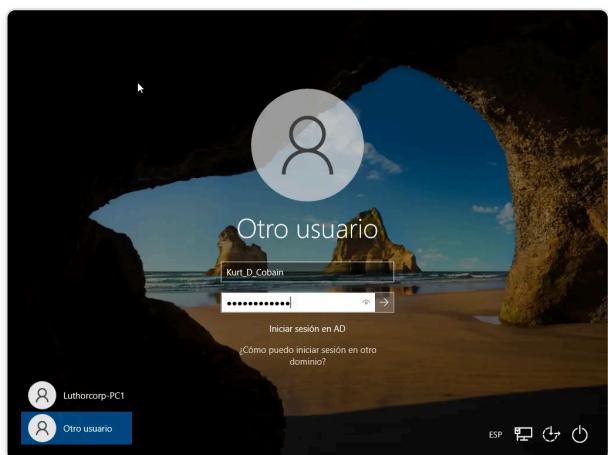
1. Se abre la ventana "Ejecutar" ( Win + R ) y se escribe `sysdm.cpl` para acceder rápidamente a las "Propiedades del sistema".
2. En la pestaña "Nombre de equipo", se hace clic en "Cambiar...".
3. En la sección "Miembro del", se selecciona "Dominio" y se escribe el nombre del dominio: `ad.luthor.corp`.
4. Al hacer clic en "Aceptar", el sistema solicitará las credenciales de una cuenta con permisos para unir equipos al dominio. Por defecto, la cuenta de Administrador del dominio tiene este permiso.
5. Tras introducir las credenciales correctas, aparecerá un mensaje de bienvenida al dominio.
6. El sistema requerirá un reinicio para completar el proceso.



### 4.3: Primer Inicio de Sesión de un Usuario del Dominio

Tras reiniciar el equipo cliente, se inicia sesión por primera vez con una cuenta de usuario creada en Active Directory (en este caso, `Kurt_D_Cobain`).

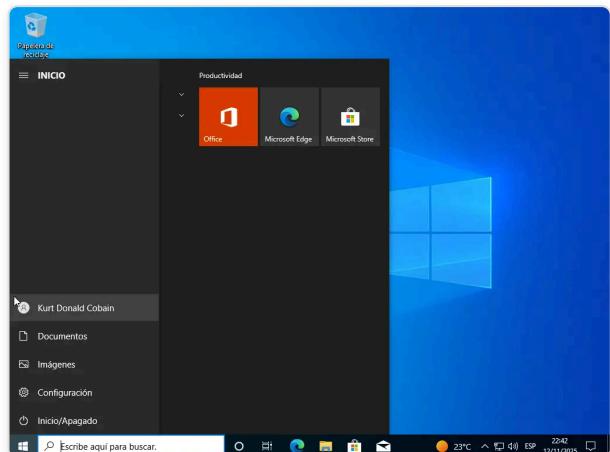
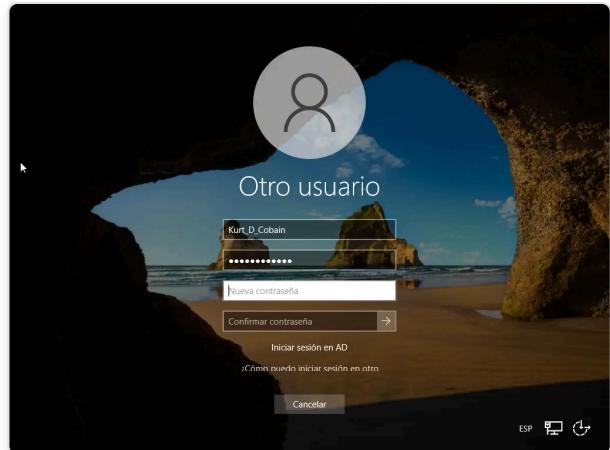
Este paso valida que todo el proceso ha funcionado. El cliente contacta con el controlador de dominio, autentica las credenciales del usuario y crea un perfil local



para él. Es común que en la creación de un usuario en AD se marque la opción "El usuario debe cambiar la contraseña en el siguiente inicio de sesión". Esto fuerza al usuario a establecer una contraseña personal y segura la primera vez que accede.

### Cómo:

1. En la pantalla de inicio de sesión de Windows, se selecciona "Otro usuario".
2. Se introduce el nombre de usuario. Se puede usar el formato `usuario` (si el equipo está en el dominio correcto) o el formato UPN (User Principal Name) `usuario@dominio.corp`.
3. Se introduce la contraseña temporal asignada por el administrador.
4. El sistema detecta que es el primer inicio de sesión y solicita el cambio de contraseña. Se introduce la nueva contraseña y se confirma.
5. Tras el cambio exitoso, Windows procede a crear el perfil de usuario y finalmente muestra el escritorio. El usuario ya está trabajando en un entorno gestionado por el dominio.



## Fase 5: Implementación de Directivas de Grupo (GPO)

Las Directivas de Grupo son una de las herramientas más potentes de Active Directory. Permiten a los administradores definir y aplicar configuraciones de seguridad, software y sistema operativo a usuarios y equipos de forma centralizada.

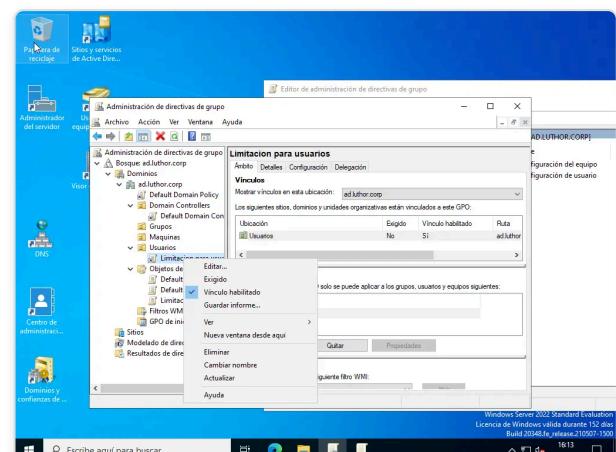
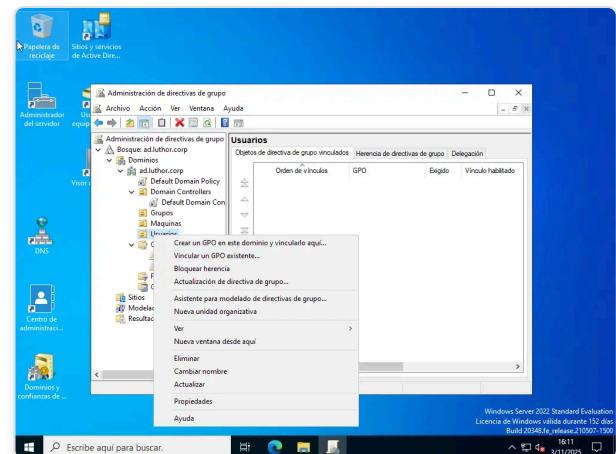
## 5.1: Creación y Vinculación de una Nueva GPO

Se utiliza la "Administración de directivas de grupo" para crear una nueva GPO y vincularla a una Unidad Organizativa (OU).

Las GPOs se aplican a los objetos (usuarios, equipos) que residen dentro del contenedor al que están vinculadas (sitio, dominio o OU). La mejor práctica es vincular las GPOs a las OUs para aplicar configuraciones específicas a grupos de usuarios o equipos. Por ejemplo, una GPO con restricciones para usuarios estándar se vincularía a la OU que contiene a esos usuarios.

### Cómo:

1. Se abre la "Administración de directivas de grupo" desde el menú "Herramientas" del Administrador del Servidor.
2. Se navega hasta la OU a la que se quiere aplicar la política (en la imagen, la OU "Usuarios").
3. Se hace clic derecho sobre la OU y se selecciona "Crear un GPO en este dominio y vincularlo aquí...".
4. Se le da un nombre descriptivo a la GPO, por ejemplo, "Limitacion para usuarios".
5. La nueva GPO aparece ahora vinculada a la OU. En la pestaña "Ámbito" se puede ver este vínculo.



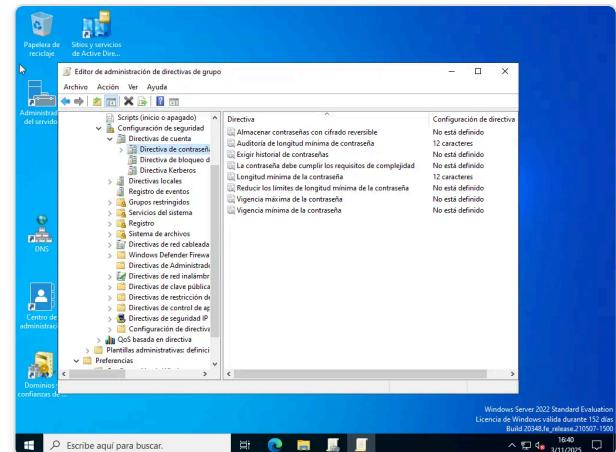
## 5.2: Edición de la GPO para Políticas de Contraseña

Se edita la GPO recién creada para configurar políticas de seguridad, específicamente las relacionadas con las contraseñas.

Fortalecer los requisitos de las contraseñas es una medida de seguridad fundamental. A través de una GPO, se puede exigir una longitud mínima, complejidad (uso de mayúsculas, minúsculas, números y símbolos), un historial para evitar la reutilización y una vigencia máxima para forzar cambios periódicos.

### Cómo:

1. En la consola de "Administración de directivas de grupo", se hace clic derecho sobre la GPO ("Limitacion para usuarios") y se selecciona "Editar...".
2. Esto abre el "Editor de administración de directivas de grupo".
3. Las políticas se dividen en "Configuración de equipo" (se aplican al equipo, sin importar quién inicie sesión) y "Configuración de usuario" (se aplican al usuario, sin importar en qué equipo inicie sesión).
4. Para las políticas de contraseña, se navega a: **Configuración de equipo > Directivas > Configuración de Windows > Configuración de seguridad > Directivas de cuenta > Directiva de contraseña**.



5. En la imagen, se han definido políticas como "Longitud mínima de la contraseña" a 12 caracteres. Se pueden configurar otras como "La contraseña debe cumplir los requisitos de complejidad" (Habilitada) y "Exigir historial de contraseñas" (ej. 24 contraseñas recordadas).

#### **Nota Importante sobre Políticas de Contraseña:**

En un dominio, solo puede haber una política de contraseña efectiva por dominio, y esta debe estar definida en una GPO vinculada a la raíz del dominio (generalmente en la "Default Domain Policy"). Las políticas de contraseña definidas en GPOs vinculadas a OUs no tienen efecto sobre los usuarios de esa OU, a menos que se utilicen "Directivas de contraseña específicas" (Fine-Grained Password Policies), una característica más avanzada. La imagen muestra la configuración, pero su aplicación efectiva dependería de dónde está vinculada la GPO.

## **Fase 6: Configuración de Recursos Compartidos en Red**

Una función clave de un servidor en una red es proporcionar acceso centralizado a archivos y carpetas. En esta fase, se creará una carpeta compartida y se asignarán permisos a un grupo de dominio para controlar el acceso.

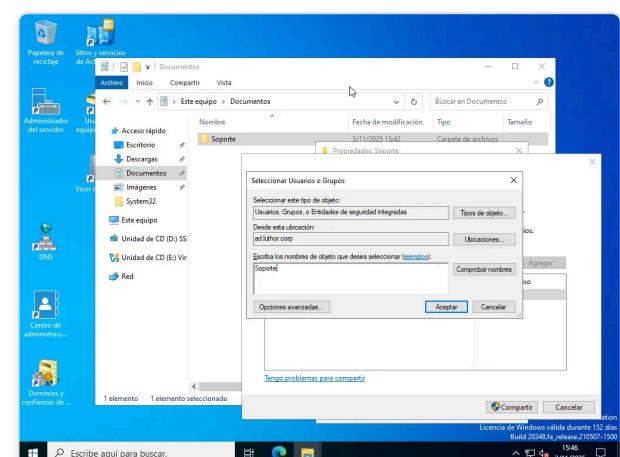
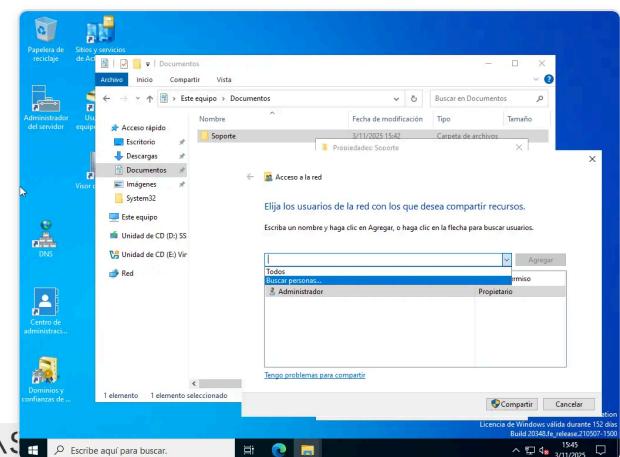
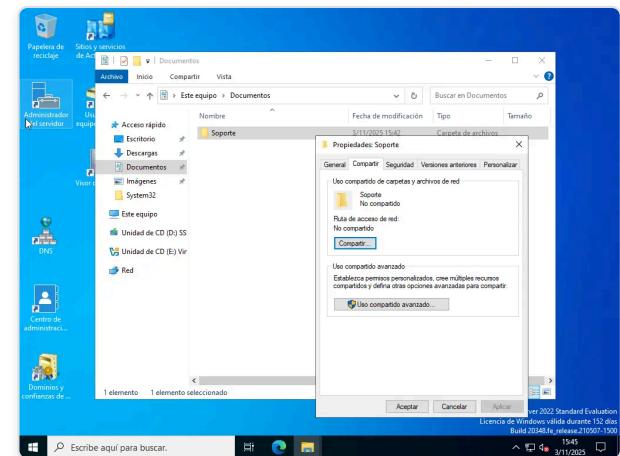
## 6.1: Creación y Compartición de una Carpeta

Se comparte una carpeta local del servidor ("Soporte") para que sea accesible a través de la red.

Compartir carpetas en un servidor centraliza los datos, facilita las copias de seguridad, mejora la colaboración y permite un control de acceso granular. En lugar de tener archivos dispersos en los equipos de los usuarios, se almacenan en un lugar gestionado y seguro.

### Cómo:

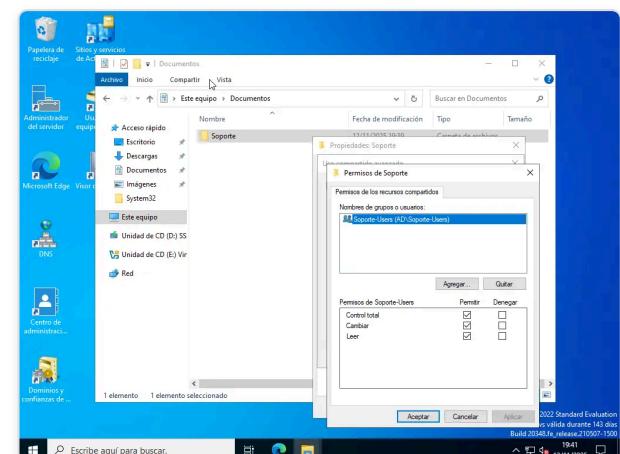
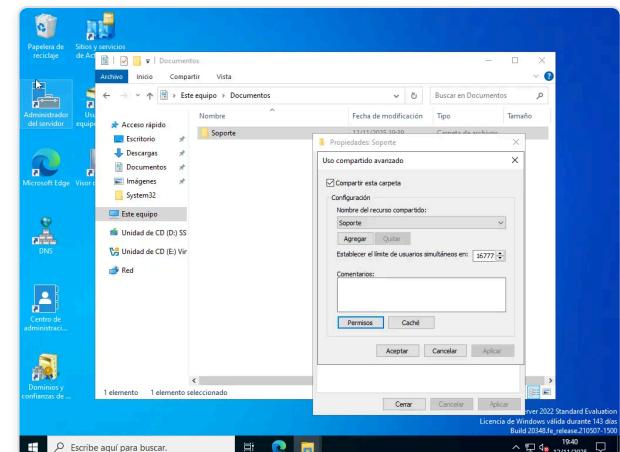
1. Se crea una carpeta en el servidor (ej. `C:\Users\Administrador\Documents\Soporte` (puede ser otra ruta))
2. Se hace clic derecho sobre la carpeta y se selecciona "Propiedades".
3. Se va a la pestaña "Compartir" y se hace clic en "Compartir..." .
4. En el asistente de "Acceso a la red", se puede añadir usuarios o grupos específicos. La imagen muestra cómo se busca y añade un grupo ("Soporte") para darle acceso.
5. Para un control más detallado, se utiliza el "Uso compartido avanzado". Esto permite definir el nombre del recurso compartido (cómo se verá en la red, ej. `\AD-01\Soporte`), establecer un límite de usuarios simultáneos y, lo más importante, acceder a los "Permisos".



## 6.2: Asignación de Permisos de Recurso Compartido

Se configuran los permisos a nivel de recurso compartido ("Share Permissions") para el grupo "Soporte-Users".

El acceso a una carpeta compartida está controlado por dos capas de permisos: **Permisos de Recurso Compartido** y **Permisos NTFS** (de seguridad a nivel de sistema de archivos). El permiso efectivo para un usuario es el **más restrictivo** de los dos. Una práctica común es configurar los permisos de recurso compartido de forma más laxa (ej. "Todos" con "Cambiar") y luego controlar el acceso de forma granular y precisa con los permisos NTFS.



### Cómo:

1. Desde la ventana de "Uso compartido avanzado", se hace clic en "Permisos".
2. Por defecto, el grupo "Todos" puede tener permiso de "Lectura". Es una buena práctica quitar este grupo y añadir explícitamente los grupos que deben tener acceso.
3. Se hace clic en "Agregar...", se busca el grupo de dominio deseado (ej. "Soporte-Users") y se añade.
4. Se seleccionan los permisos para ese grupo. Los permisos de recurso compartido son básicos:
  - **Leer:** Permite ver archivos y carpetas, abrir archivos y ejecutar programas.
  - **Cambiar:** Incluye los permisos de Lectura, y además permite crear,

modificar y eliminar archivos y carpetas.

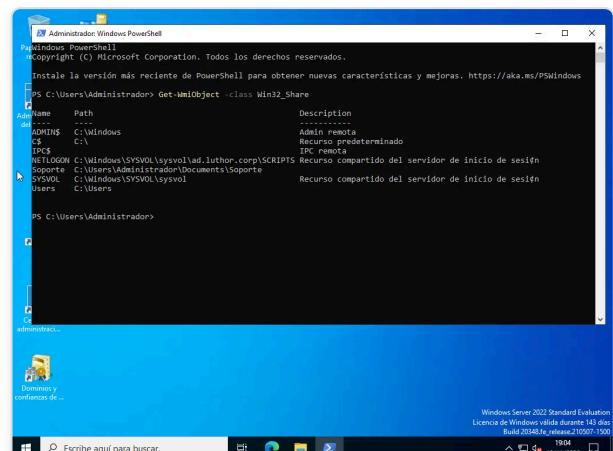
- **Control total:** Incluye los permisos de Cambiar, y además permite cambiar los permisos NTFS (si también se tiene ese derecho en NTFS).

5. En la imagen, se le otorgan los tres permisos al grupo "Soporte-Users".

### 6.3: Verificación de Recursos Compartidos

Se utilizan herramientas de línea de comandos para verificar que la carpeta "Soporte" se ha compartido correctamente en el servidor.

Aunque la interfaz gráfica confirme la creación, verificar desde la línea de comandos es una forma rápida y eficaz de listar todos los recursos compartidos activos en un servidor, incluyendo los recursos administrativos ocultos (como `C$` y `ADMIN$`).



The screenshot shows a Windows Server 2022 Standard Evaluation PowerShell window titled 'Administrador: Windows PowerShell'. The command run is `Get-WmiObject -class Win32_Share`. The output lists several shared resources:

Name	Path	Description
ADMIN\$	C:\Windows	Administrador determinado
C\$	C:\	IPC remota
IPC\$		Recurso compartido del servidor de inicio de sesión
NETLOGON	C:\Windows\SYSTEM32\REFSVOL\Netlogon\ad.luthor.com\USCRPNT	Recurso compartido del servidor de inicio de sesión
Print\$	C:\Windows\PRINTERS\Print\$	Recurso compartido del servidor de inicio de sesión
SYSVOLA	C:\Windows\SYSTEM32\SYSVOL\sysvol	Recurso compartido del servidor de inicio de sesión
Users	C:\Users	

At the bottom right of the window, it says 'Windows Server 2022 Standard Evaluation' and 'Build 20248.10000.210907-1500 1904 12/11/2022'.

#### Cómo:

1. **Con Símbolo del sistema (cmd):** Se ejecuta el comando `net share`. La salida lista todos los recursos compartidos, su ruta local y una descripción. En la imagen, se ve claramente la entrada para "Soporte".
2. **Con Windows PowerShell:** Se ejecuta el cmdlet `Get-WmiObject -class Win32_Share` o el más moderno `Get-SmbShare`. La salida es similar, a menudo

en un formato de objeto más fácil de manipular mediante scripts. Ambas imágenes confirman que el recurso "Soporte" está activo y apunta a la ruta correcta

---

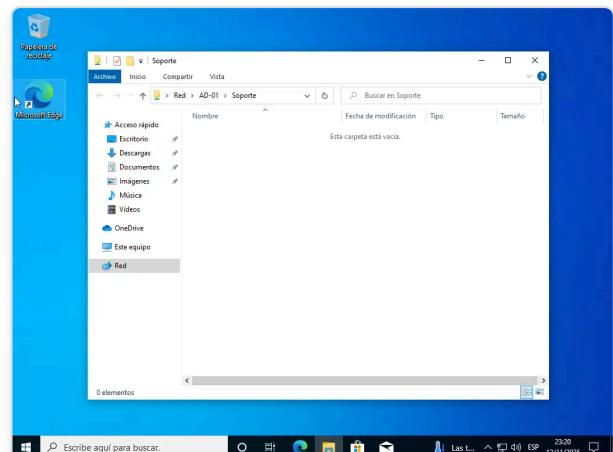
## 6.4: Acceso al Recurso Compartido desde el Cliente

El paso final es acceder a la carpeta compartida desde un equipo cliente que está en el dominio.

Este es el objetivo final de compartir un recurso: que los usuarios autorizados puedan acceder a él de forma transparente desde sus propios equipos. Este paso valida que la configuración de red, la unión al dominio, la pertenencia a grupos y los permisos de recurso compartido funcionan en conjunto correctamente.

### Cómo:

1. En el equipo cliente, con la sesión iniciada como un usuario que pertenece al grupo "Soporte-Users", se abre el Explorador de Archivos.
2. En la barra de direcciones, se escribe la ruta UNC (Universal Naming Convention) del recurso compartido: `\AD-01\Soporte`.  
(`\NombreDelServidor\NombreDelRecurso`).
3. Si todos los permisos son correctos, la carpeta se abrirá. La imagen muestra la carpeta "Soporte" vacía, accesible desde la red. El usuario ahora puede leer, escribir y modificar archivos en esta ubicación



centralizada, según los permisos que se le  
hayan otorgado.