

« Scripting en Windows. PowerShell

Administracion del servicio de
directorio en Windows con
PowerShell »

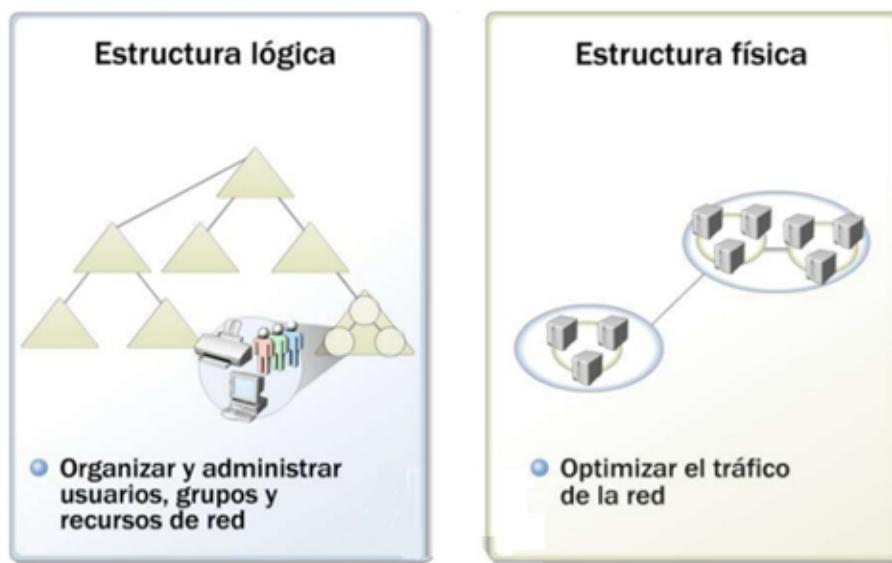
Windows Server - Directorio Activo

- 1. Conceptos básicos de Active Directory
 - 1.1 Componentes lógicos del Directorio Activo
 - 1.2 Componentes físicos del Directorio Activo
- 2. Instalación de Active Directory
 - 2.1 Instalación de Active Directory mediante el Administrador del Servidor
 - 2.2 Verificación de la instalación
 - 2.3 Unir un cliente Windows a un dominio
- 3. Degradar un controlador de dominio desde la interfaz gráfica
- 4. Gestión del directorio activo a través de la interfaz gráfica
 - 4.1 Cuentas de usuario y equipo
 - 4.2 Cuentas de grupo
 - 4.2.1 Tipos de grupos
 - 4.2.2 Ámbitos de un grupo
 - 4.3 Unidades organizativas
 - 4.4 Directivas de grupo
 - 4.4.1 Creación de una nueva directiva
 - 4.4.2 Vinculación de una directiva a una Unidad Organizativa
 - 4.4.3 Orden de prioridad de las directivas de grupo
 - 4.5 Permisos
 - 4.5.1 Permisos de recursos compartidos
 - 4.5.2 Permisos NTFS
 - 4.6 Perfiles

1. Conceptos básicos de Active Directory

El **Directorio Activo** (también conocido como **Active Directory** en inglés) es un servicio de directorio de red desarrollado por Microsoft. Su objetivo principal radica en proporcionar un servicio centralizado para la gestión y organización de recursos de red, como usuarios, grupos, impresoras y otros dispositivos, facilitando así la administración, autenticación y autorización en entornos empresariales de manera eficiente y segura.

El Directorio Activo incluye componentes **lógicos y físicos**.



1.1 Componentes lógicos del Directorio Activo

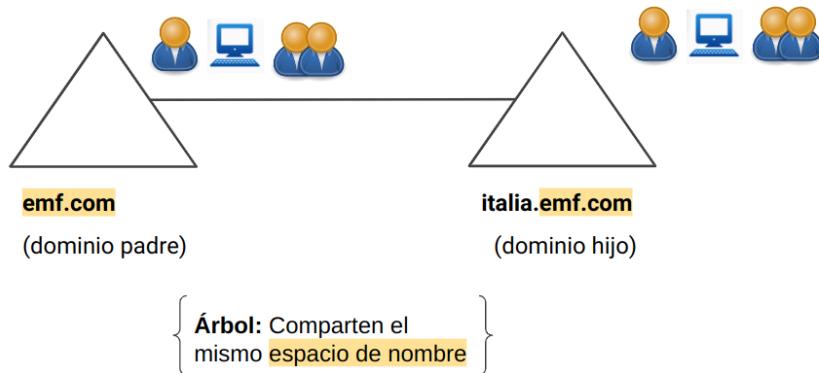
La **estructura lógica** se centra en la administración de los recursos de la red organizativa, independientemente de la ubicación física de dichos recursos, y de la topología de las redes subyacentes.

Los componentes de la estructura lógica del Directorio Activo son:

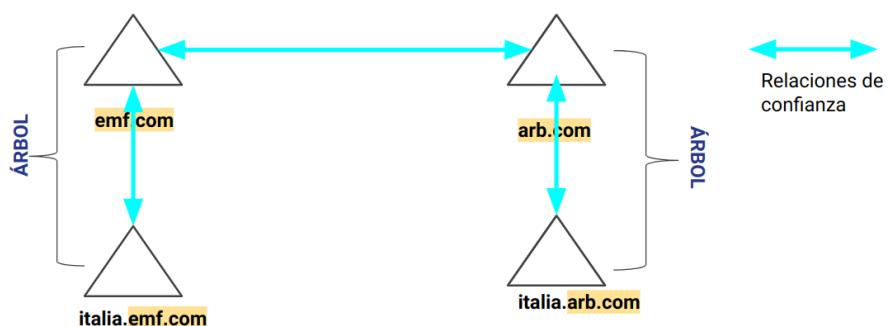
- **Objetos:** Son los componentes básicos de la estructura lógica representan a usuarios y recursos como equipos e impresoras. Las clases de objetos son esquemas o plantillas

de los tipos de objetos que pueden crear en el directorio activo.

- **Unidades organizativas:** Es un contenedor para organizar los objetos en un dominio, a la que se pueden asignar valores de configuración de directivas de grupo.
- **Dominios (Domain):** Colección de objetos: usuarios, grupos, equipos, etc. Se representa por un nombre de dominio DNS. Ejemplo: empresa.local
- **Árboles de dominios (Tree):** Los árboles están compuestos por uno o varios dominios. Estos dominios están dentro del mismo espacio de nombres.



- **Bosque (Forest):** Colección de árboles. Los dominios dentro de un bosque establecen relaciones de confianza, y esto les permite compartir recursos. Los dominios dentro del bosque no comparten el mismo espacio de nombres.



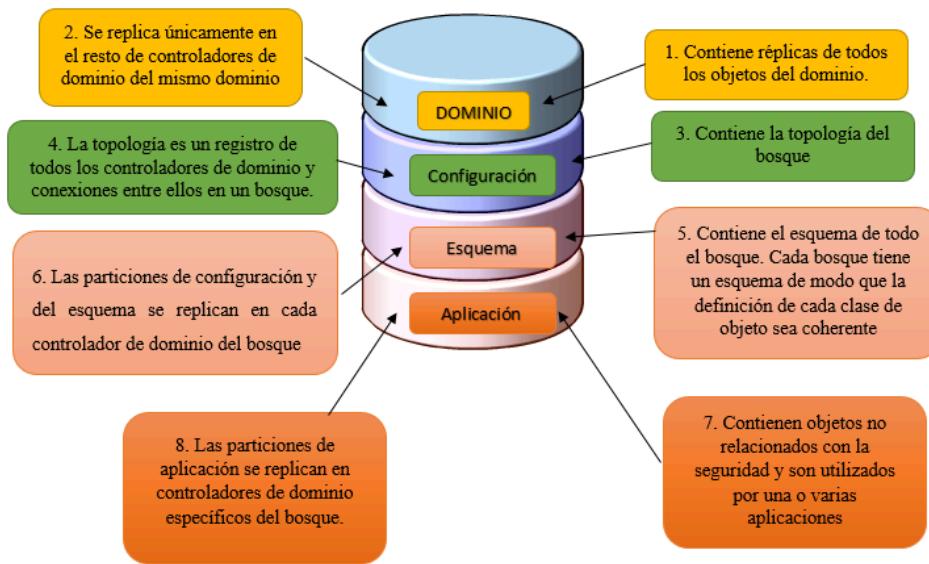
1.2 Componentes físicos del Directorio Activo

Los elementos de la estructura física son los siguientes:

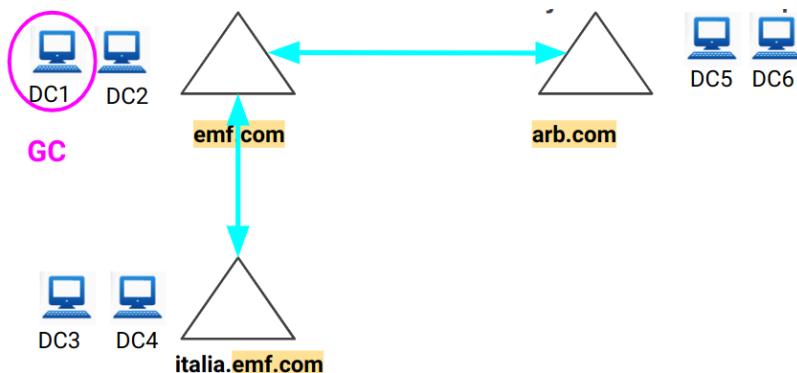
- **Sitios:** En una red física, un sitio representa un conjunto de equipos conectados mediante una línea de alta velocidad, como una red de área local. En AD, los sitios representan la estructura física, o topología de red. Es importante distinguir entre sitios y dominios. Los sitios representan la estructura física de red, mientras que los dominios representan la estructura lógica de la organización.
- **Controlador de dominio (Domain Controller):** Es el servidor ejecutando Windows Server con el directorio activo instalado, que contiene la base de datos de objetos del directorio para un determinado dominio.

Cada **controlador de dominio** contiene varias particiones del Directorio Activo:

1. **Particiones del dominio:** contienen las réplicas de todos los objetos en ese dominio. Esta partición se replica solamente a otros Controladores de Dominio del mismo dominio.
2. **Particiones de configuración:** contienen la topología del bosque. La topología que es el esquema de conexión de los sitios, registra todas las conexiones de los controladores de dominio en el mismo bosque.
3. **Particiones del esquema:** contiene el esquema del bosque. Cada bosque tiene un esquema para que la definición de cada clase del objeto sea única. Las particiones de configuración y esquema se replican en cada Controlador de Dominio del bosque.
4. **Particiones de aplicaciones:** contienen los objetos relacionados a la seguridad y se utilizan en las aplicaciones. Se replican en Controladores de Dominio especificados en el bosque.



- **Catálogo Global (Global Catalog)**: Es un servidor que almacena una copia completa de todos los objetos del directorio para su dominio host y una copia parcial de solo lectura de todos los objetos del resto de dominios del bosque.



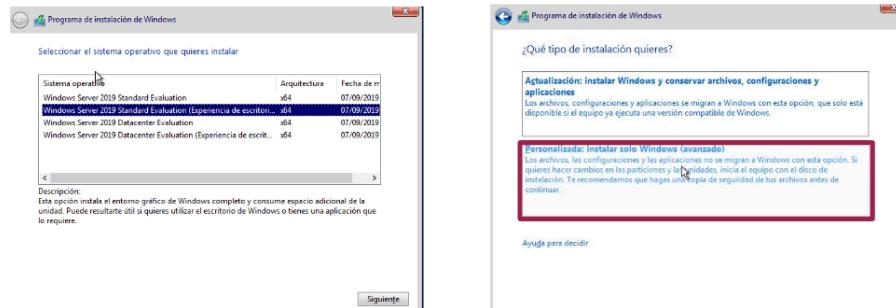
2. Instalación de Active Directory

Existen 3 métodos de instalación:

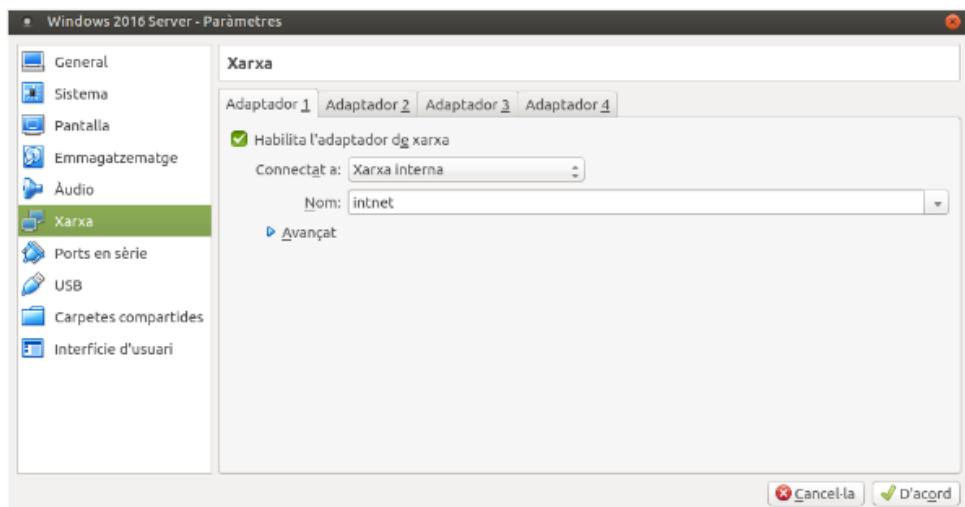
- Mediante PowerShell
- - Install-WindowsFeature AD-Domain-Services
 - Install-ADDSDomainController
- Mediante el administrador del servidor
- Mediante dcpromo /unattend:

2.1 Instalación de Active Directory mediante el Administrador del Servidor

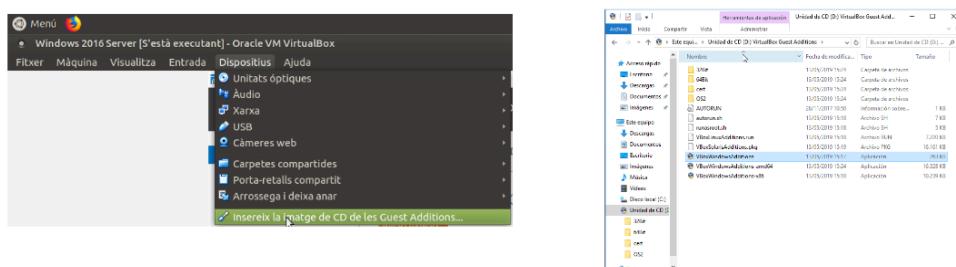
- Realizamos una instalación limpia de Windows Server 2019 con interfaz gráfica (GUI) en VirtualBox.



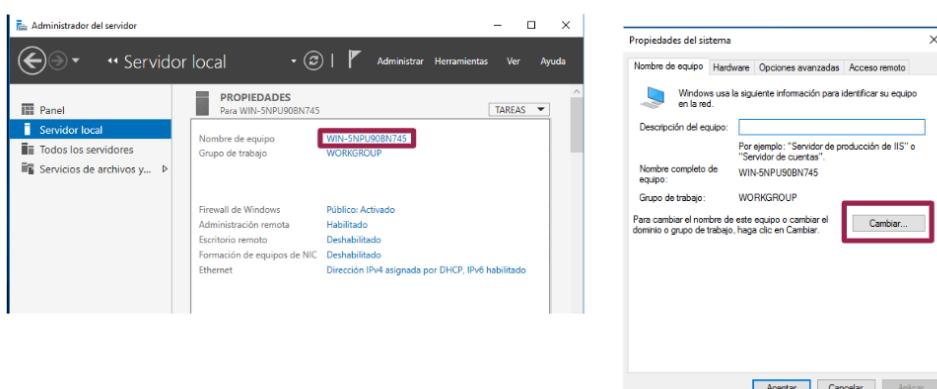
- El adaptador de red en VirtualBox lo cambiamos a **Red Interna**.



- Instalamos VirtualBox Guest Additions



- Renombramos el nombre del equipo a **empresa-DC1**



- Abrimos el **Administrador del Servidor**

- Seleccionamos **Servidor Local**

Nombre de equipo	EMPRESA-DC1
Grupo de trabajo	WORKGROUP
Firewall de Windows	Público: Activado
Administración remota	Habilitado
Escritorio remoto	Deshabilitado
Formación de equipos de NIC	Deshabilitado
Ethernet	Dirección IPv4 asignada por DHCP, IPv6 habilitado

- Un controlador de dominio (DC) no puede tener una IP dinámica, así que la cambiamos por la siguiente estática:

Usar la siguiente dirección IP:

Dirección IP:	172 . 16 . 0 . 10
Máscara de subred:	255 . 255 . 0 . 0
Puerta de enlace predeterminada:	· · ·

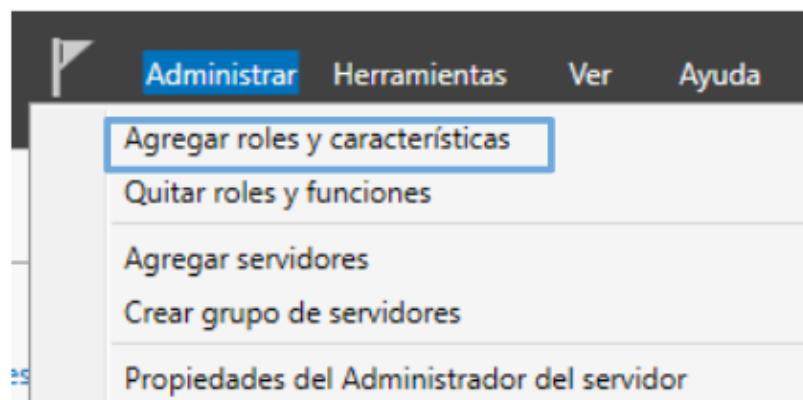
Obtener la dirección del servidor DNS automáticamente

Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido:	172 . 16 . 0 . 10
Servidor DNS alternativo:	· · ·

IMPORTANTE:
Una vez cambiada la IP actualizamos el Servidor Local para que muestre los cambios.

- A continuación hacemos click en **Administrar -> Agregar roles y características** (Parte superior derecha del Administrador del Servidor)



Seleccionar tipo de instalación

SERVIDOR DE DESTINO
EMPRESA-DC1

Antes de comenzar

- Tipo de instalación**
- Selección de servidor
- Roles de servidor
- Características
- Confirmación
- Resultados

Seleccione el tipo de instalación. Puede instalar roles y características en un equipo físico, en una máquina virtual o en un disco duro virtual (VHD) sin conexión.

Instalación basada en características o en roles

Para configurar un solo servidor, agregue roles, servicios de rol y características.

Instalación de Servicios de Escritorio remoto

Instale los servicios de rol necesarios para que la Infraestructura de escritorio virtual (VDI) cree una implementación de escritorio basada en máquinas o en sesiones.

Seleccionar servidor de destino

SERVIDOR DE DESTINO
EMPRESA-DC1

Antes de comenzar
Tipo de instalación
Selección de servidor
Roles de servidor
Características
Confirmación
Resultados

Seleccione un servidor o un disco duro virtual en el que se instalarán roles y características.

- Seleccionar un servidor del grupo de servidores
 Seleccionar un disco duro virtual

Grupo de servidores

Filtro:		
Nombre	Dirección IP	Sistema operativo
EMPRESA-DC1	172.16.0.10	Microsoft Windows Server 2016 Standard Evaluation

1 equipo(s) encontrado(s)

1 Seleccionar roles de servidor

Antes de comenzar
Tipo de instalación
Selección de servidor
Roles de servidor
Características
Confirmación
Resultados

- Seleccione uno o varios roles para instalarlos en el servidor seleccionado.
- Roles**
- Atestación de mantenimiento del dispositivo
 - Experiencia con Windows Server Essentials
 - Hyper-V
 - MultiPoint Services
 - Servicio de protección de host
 - Servicios de acceso y directivas de redes
 - Servicios de archivos y almacenamiento (1 de 12 instalados)
 - Servicios de certificados de Active Directory
 - Servicios de dominio de Active Directory
 - Servicios de Escritorio remoto
 - Servicios de federación de Active Directory
 - Servicios de implementación de Windows
 - Servicios de impresión y documentos
 - Servidor de fax
 - Servidor DHCP
 - Servidor DNS
 - Servidor web (IIS)
 - Volume Activation Services
 - Windows Server Update Services

2 Asistente para agregar roles y características

¿Desea agregar las características requeridas para Servicios de dominio de Active Directory?

No se puede instalar Servicios de dominio de Active Directory si no se instalan también los servicios de rol o las características siguientes.

[Herramientas] Administración de directivas de grupo
▪ Herramientas de administración remota del servidor
▫ Herramientas de administración de roles
▫ Herramientas de AD DS y AD LDS
▫ Módulo de Active Directory para Windows PowerShell
▫ Herramientas de AD DS
[Herramientas] Centro de administración de Active
[Herramientas] Complementos y herramientas de l...

Incluir herramientas de administración (si es aplicable)

Agregar características **Cancelar**

- En las siguientes pantallas hacemos clic en Siguiente y dejamos las opciones por defecto. Finalmente presionamos el botón de **Instalar**

Progreso de la instalación

SERVIDOR DE DESTINO
EMPRESA-DC1

Antes de comenzar
Tipo de instalación
Selección de servidor
Roles de servidor
Características
AD DS
Confirmación
Resultados

Ver progreso de la instalación

Instalación de característica

Requiere configuración. Instalación correcta en EMPRESA-DC1.

Servicios de dominio de Active Directory

Se requieren pasos adicionales para que esta máquina sea un controlador de dominio.

Promover este servidor a controlador de dominio

Administración de directivas de grupo

Herramientas de administración remota del servidor

Herramientas de administración de roles

Herramientas de AD DS y AD LDS

Módulo de Active Directory para Windows PowerShell

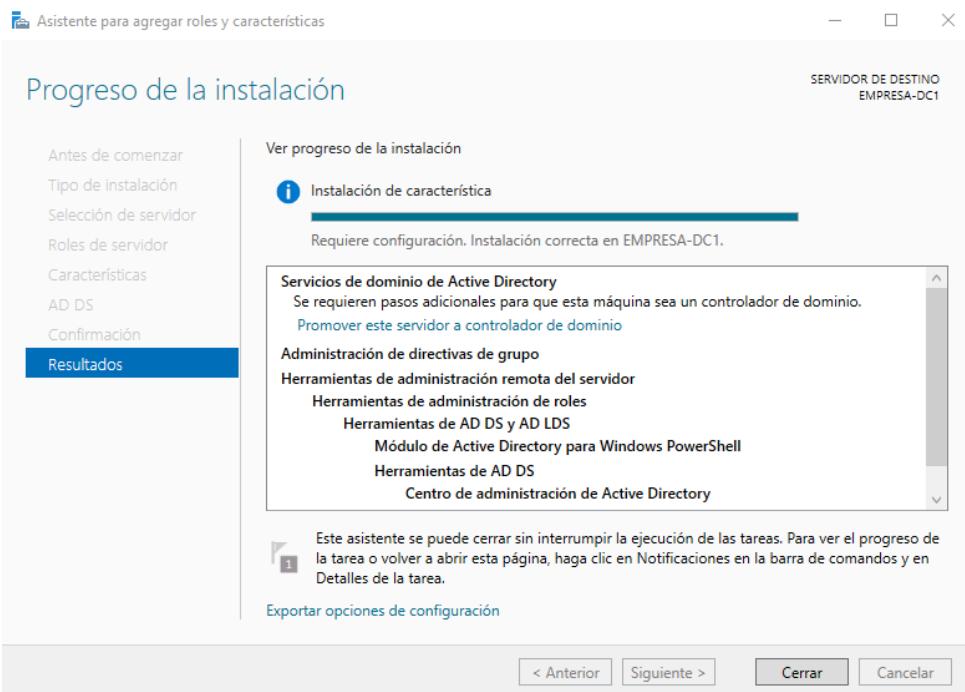
Herramientas de AD DS

Centro de administración de Active Directory

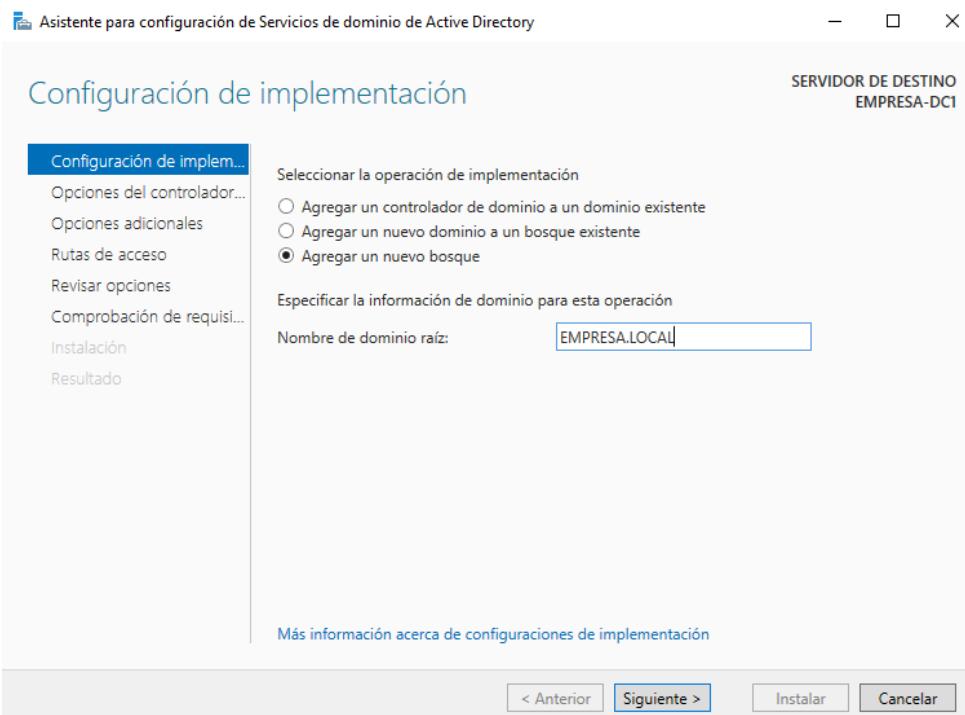
Este asistente se puede cerrar sin interrumpir la ejecución de las tareas. Para ver el progreso de la tarea o volver a abrir esta página, haga clic en Notificaciones en la barra de comandos y en Detalles de la tarea.

[Exportar opciones de configuración](#)

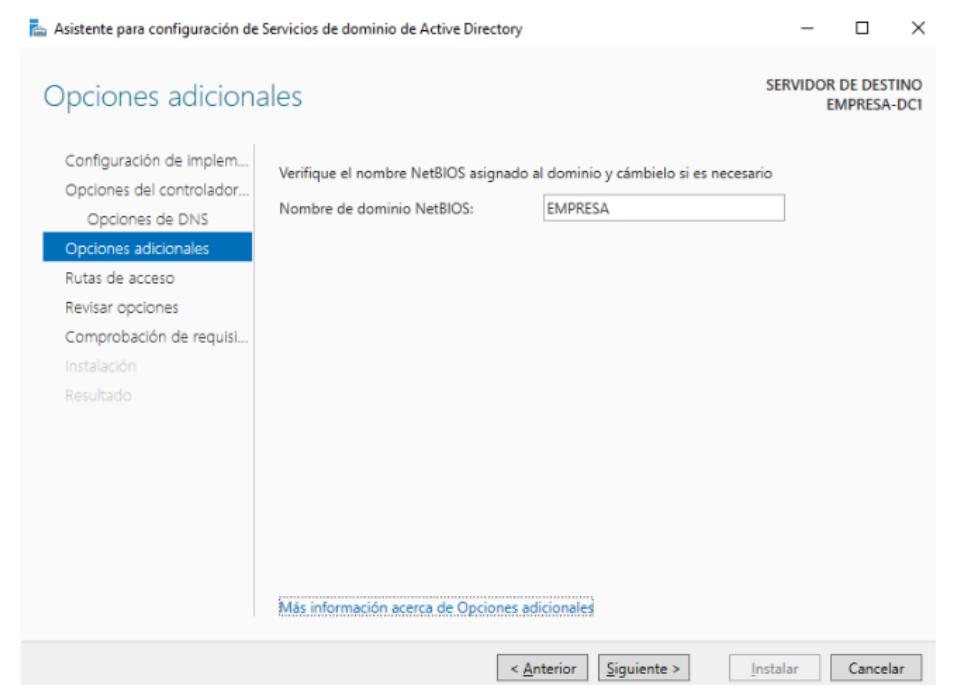
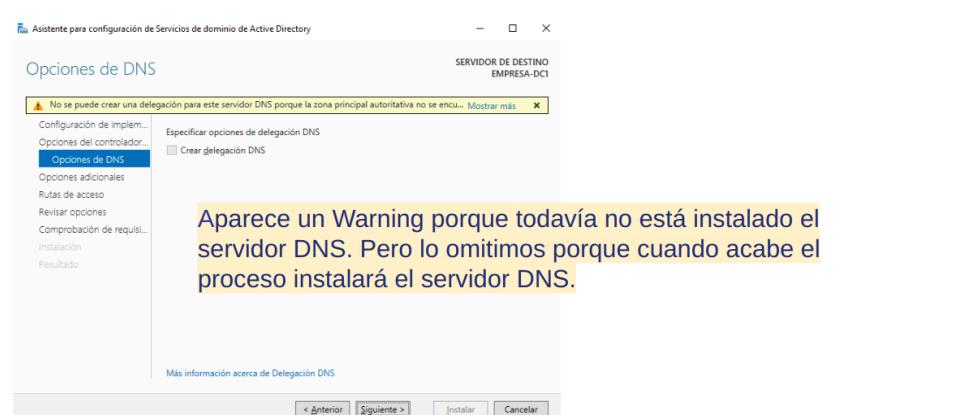
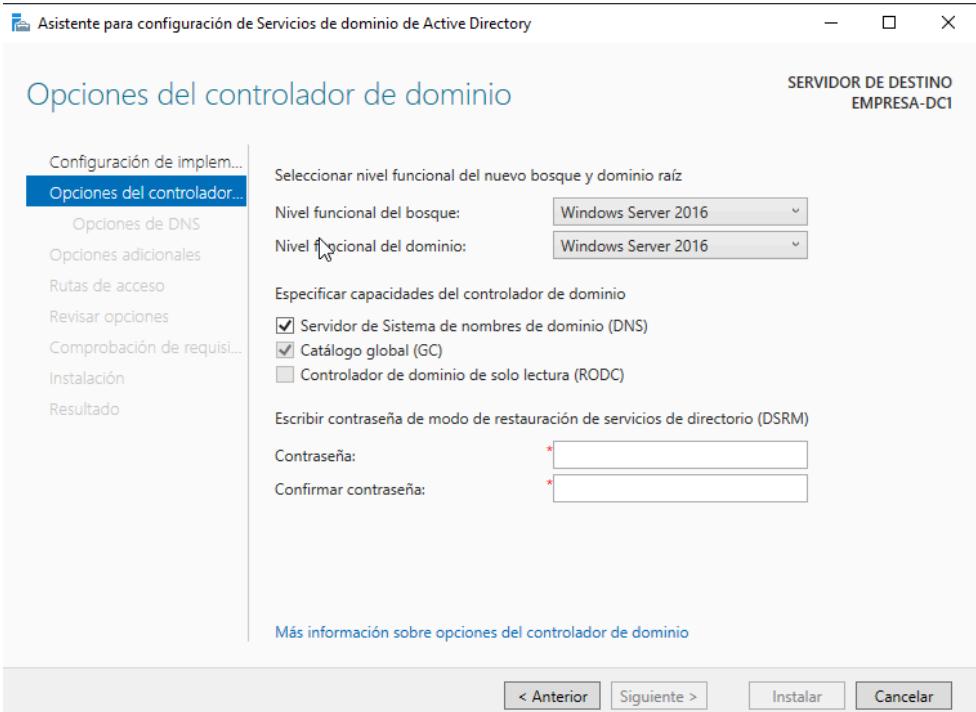
< Anterior **Siguiente >** Cerrar Cancelar

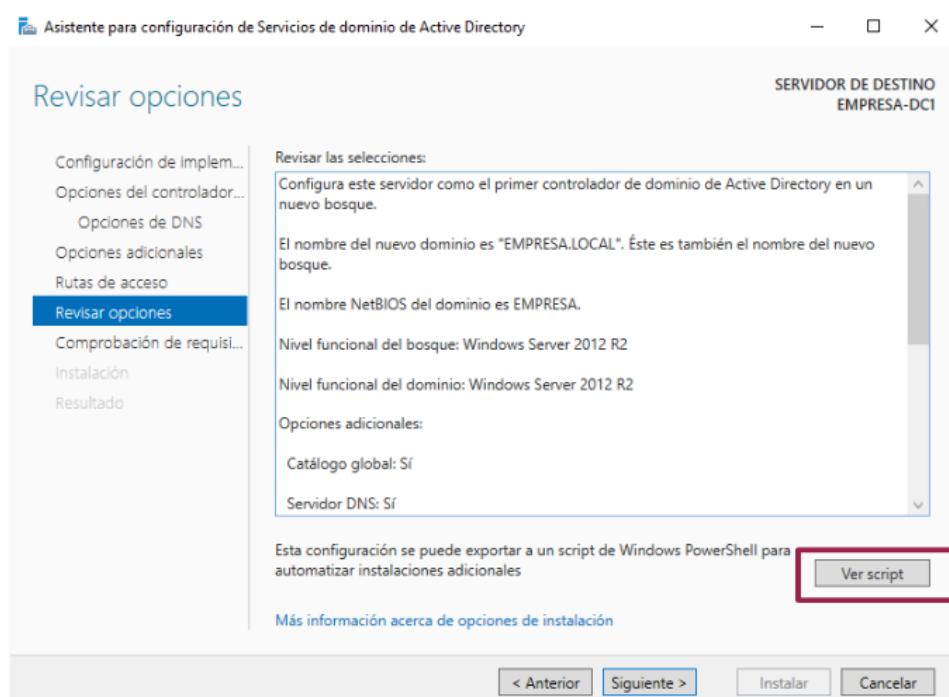
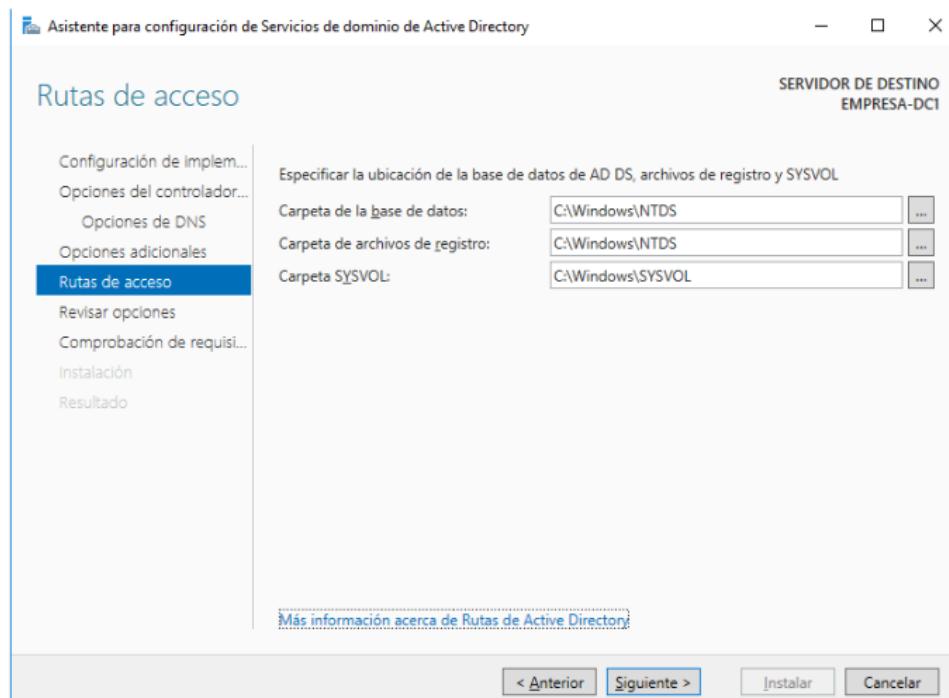


En esta pantalla debemos indicar el tipo de operación que queremos realizar. En este caso, como no disponemos de infraestructura previa, seleccionamos la opción de **Agregar un nuevo bosque**.



En el siguiente paso (*Opciones del controlador de dominio*) indicamos el nivel de funcionalidad del controlador.



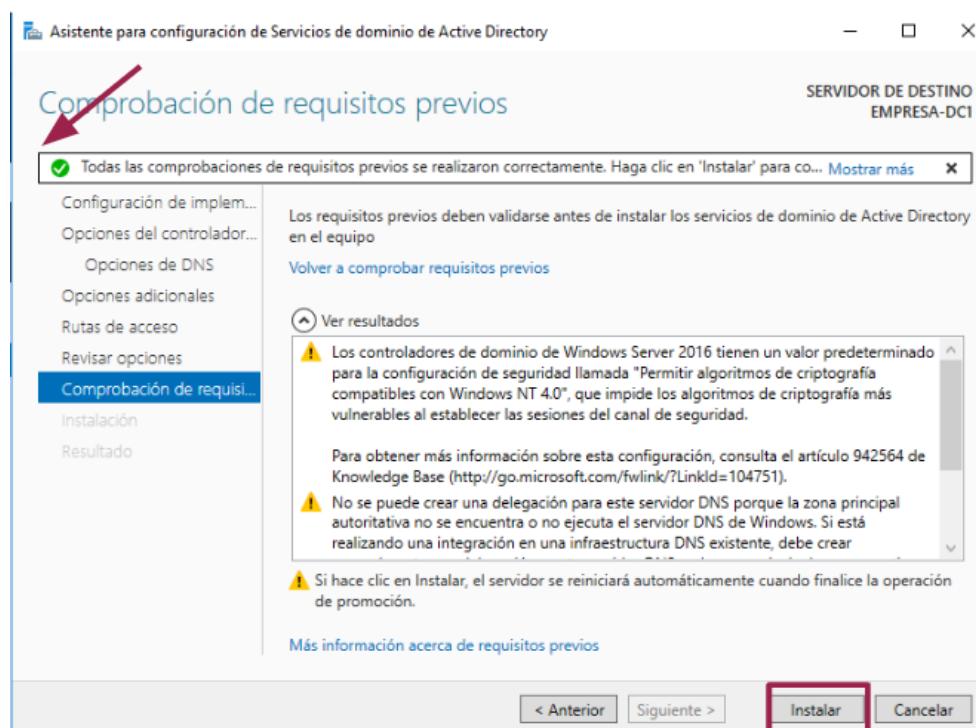


Ver script nos permite obtener un script en PowerShell para automatizar la instalación sin tener que volver a introducir de nuevo todos los datos.

```
tmp7DBD.tmp: Bloc de notas
Archivo Edición Formato Ver Ayuda
#
# Script de Windows PowerShell para implementación de AD DS
#
Import-Module ADDSDeployment
Install-ADDSForest `-
    -CreateDnsDelegation:$false `-
    -DatabasePath "C:\Windows\NTDS" `-
    -DomainName "EMPRESA.LOCAL" `-
    -DomainNetbiosName "EMPRESA" `-
    -ForestMode "WinThreshold" `-
    -InstallDns:$true `-
    -LogPath "C:\Windows\NTDS" `-
    -NoRebootOnCompletion:$false `-
    -SysvolPath "C:\Windows\SYSVOL" `-
    -Force:$true
```

Guardamos el script para poder instalar el active directory en un entorno de producción a través de **PowerShell**
Después pulsamos Siguiente en la ventana

En la pantalla de **Comprobación de requisitos**, se verifica que el sistema cumple todos los requisitos para convertirse en controlador de dominio.



2.2 Verificación de la instalación

- Accedemos a Windows Server con la cuenta del Administrador.



- Accedemos al "Administrador del Servidor" => Herramientas => Usuarios y equipos de Active Directory.



- Observamos como muestra el dominio EMPRESA.LOCAL que ha sido creado.

Usuarios y equipos de Active Directory

Archivo Acción Ver Ayuda



Nombre	Tipo	Descripción
Builtin	builtinDomain	
Computers	Contenedor	Default container for up...
Domain Controllers	Unidad organi...	Default container for do...
ForeignSecurityPrinci...	Contenedor	Default container for sec...
Managed Service Acc...	Contenedor	Default container for ma...
Users	Contenedor	Default container for up...

Administrador del servidor

Administrador del servidor > Servidor local

Panel

Servidor local

Todos los servidores

AD DS

DNS

Servicios de archivos y...

PROPIEDADES

Para EMPRESA-DC1

Nombre de equipo	EMPRESA-DC1	Últimas actualizaciones
Dominio	EMPRESA.LOCAL	Windows Update
Firewall de Windows	Público: Activado	Windows Defender
Administración remota	Habilitado	Comentarios y diagr...
Escrivano remoto	Deshabilitado	Configuración de se...
Formación de equipos de NIC	Deshabilitado	Zona horaria
Ethernet	172.16.0.10, IPv6 habilitado	Id. del producto
Versión del sistema operativo	Microsoft Windows Server 2016 Standard Evaluation	Procesadores
Información de hardware	innotek GmbH VirtualBox	Memoria instalada (...
		Espacio total en disc...

Administración de directivas de grupo

Administración de equipos

Administración de impresión

Centro de administración de Active Directory

Configuración del sistema

Copias de seguridad de Windows Server

Desfragmentar y optimizar unidades

Diagnóstico de memoria de Windows

Directiva de seguridad local

DNS

Dominios y confianzas de Active Directory

Editor ADSI

Firewall de Windows con seguridad avanzada

Información del sistema

Iniciador iSCSI

Liberador de espacio en disco

Módulo de Active Directory para Windows PowerShell

Monitor de recursos

Monitor de rendimiento

Orígenes de datos ODBC (32 bits)

Administrador de DNS

Archivo Acción Ver Ayuda

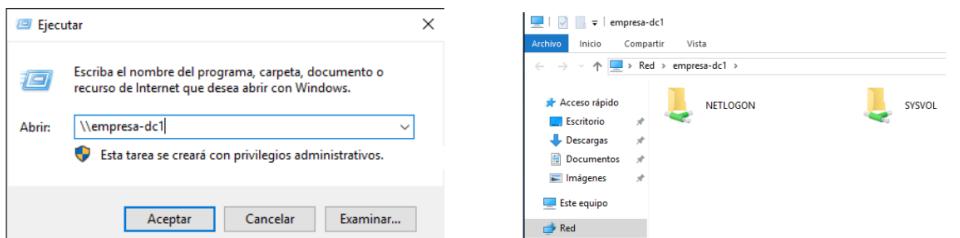


DNS

EMPRESA-DC1
Zonas de búsqueda directa
_msdcs.EMPRESA.LOCAL
dc
_sites
_tcp
domains
gc
pdc
EMPRESA.LOCAL
Zonas de búsqueda inversa
Puntos de confianza
Reenviadores condicionales

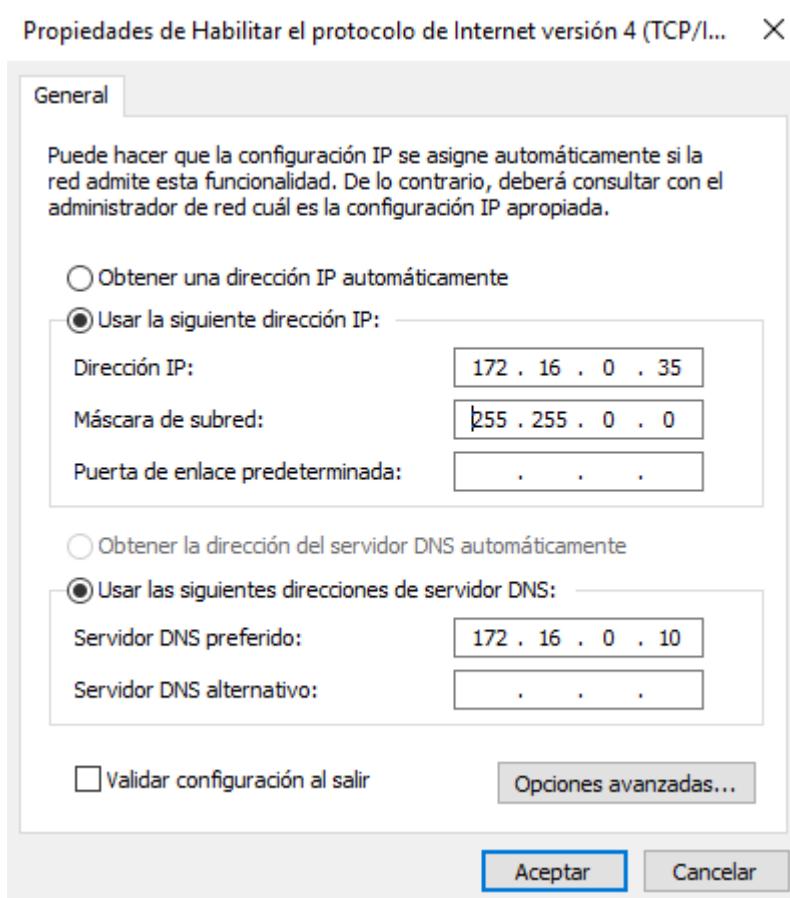
Nombre

Nombre	Tipo	Datos	Marca de
_kerberos	Registro de servicio (SRV)	[0][100][88] EMPRESA-DC...	19/07/201...
_ldap	Registro de servicio (SRV)	[0][100][389] EMPRESA-D...	19/07/201...

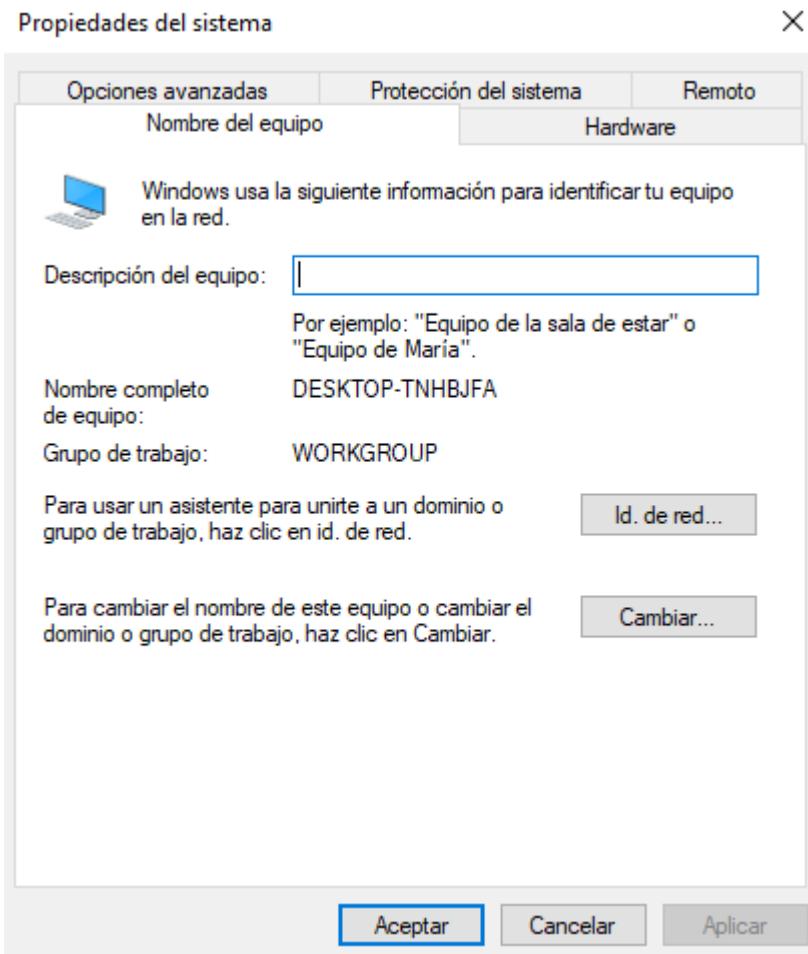


2.3 Unir un cliente Windows a un dominio

- Importamos en VirtualBox la máquina virtual de Windows 10 o Windows 11. No olvides marcar la opción de resetear MAC Address de las tarjetas de red.
- El adaptador de red en VirtualBox lo cambiamos a **Red Interna**.
- Arrancamos la máquina y accedemos a la configuración de red y cambiamos la dirección IP y la dirección de servidor DNS:



- Accedemos a las propiedades del equipo para unir al dominio EMPRESA.LOCAL



Cambios en el dominio o el nombre del equipo X

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

Nombre del equipo:

DESKTOP-TNHBJFA

Nombre completo de equipo:

DESKTOP-TNHBJFA

[Más...](#)

Miembro del

Dominio:

EMPRESA.LOCAL

Grupo de trabajo:

WORKGROUP

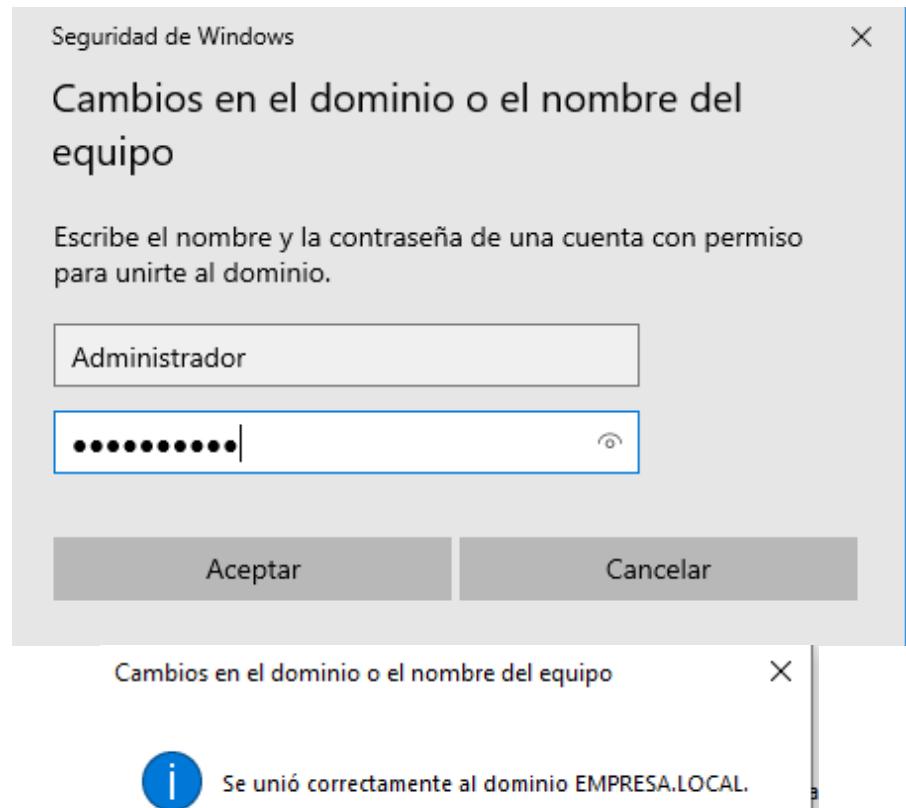
[Aceptar](#)

[Cancelar](#)



En caso de error:

- Verificar la dirección IP del cliente y del servidor que se encuentren en la misma red
 - Realizar ping del cliente a la dirección IP del servidor: **ping 172.16.0.10**
- Verificar el servidor DNS
 - Realizar **ping empresa.local**
- En caso de estar todo bien configurado nos pedirá las credenciales de Administrador del servidor para poder unir el cliente al dominio.



Cambios en el dominio o el nombre del equipo

Aceptar

Cancelar

Se unió correctamente al dominio EMPRESA.LOCAL.

Aceptar

3. Degradar un controlador de dominio desde la interfaz gráfica

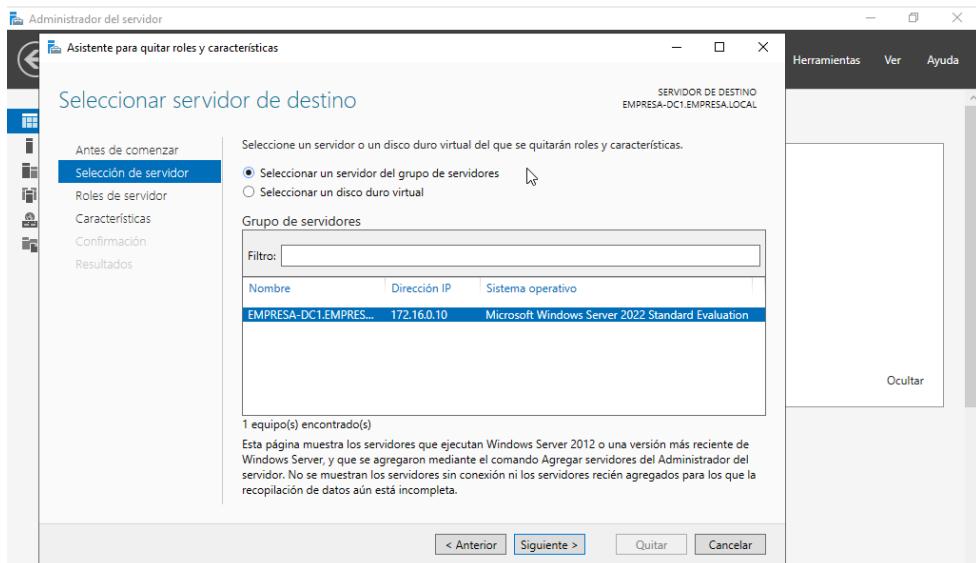
La degradación del controlador de dominio se divide en dos pasos:

- En primer lugar procederemos a la degradación del controlador de dominio. Al final de este paso, el servidor dejará de actuar como controlador de dominio.
- A continuación, desinstalaremos los roles *Servicios de dominio de Active Directory y DNS*.

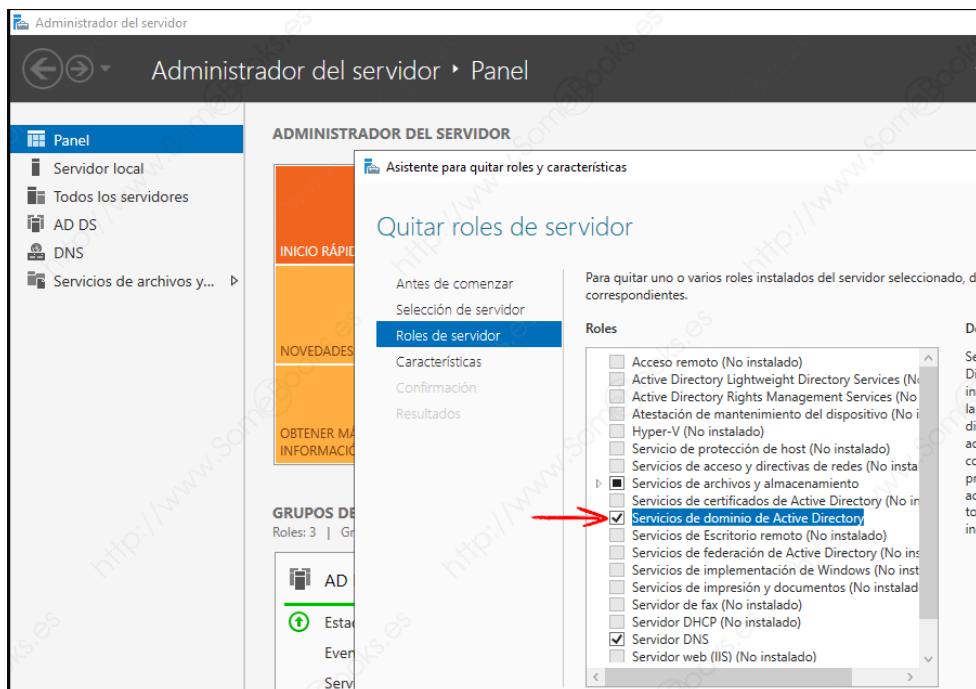
En el **Administrador del servidor**, desplegaremos el menú **Administrar** y elegiremos la opción **Quitar roles y funciones**.



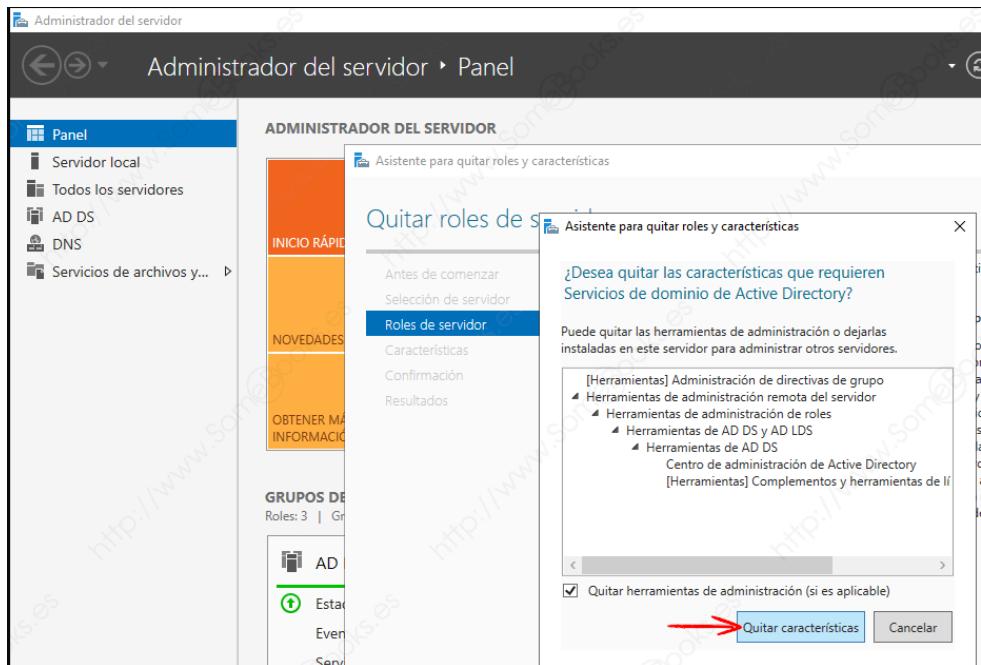
A continuación elegimos la opción “**Seleccionar un servidor del grupo de servidores**”.



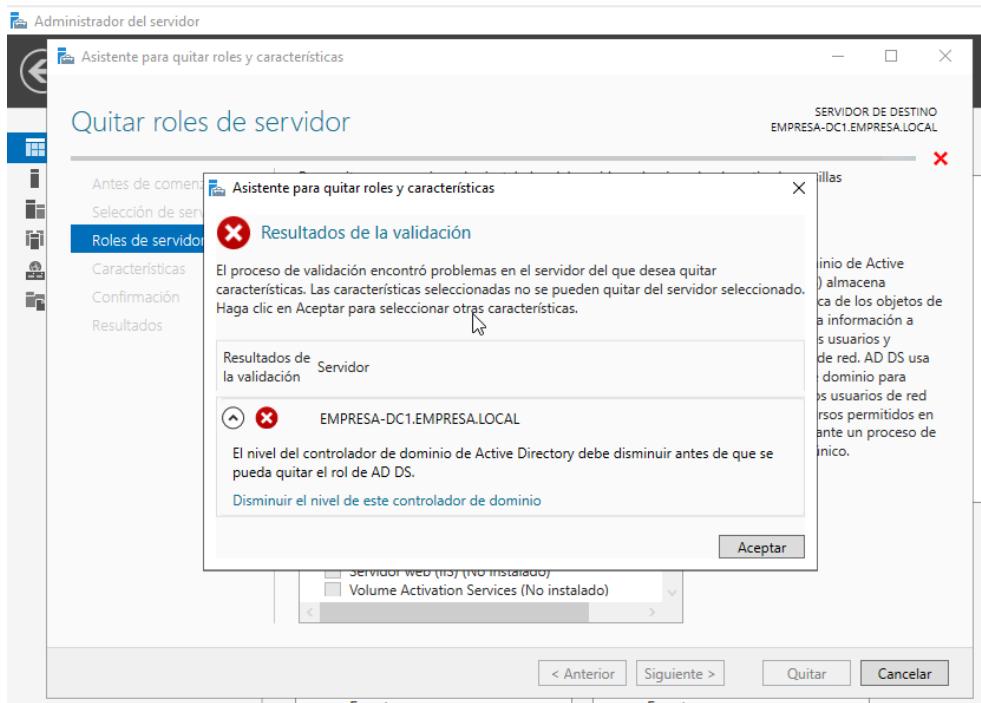
En la página Quitar roles de servidor, buscamos en la lista la entrada Servicios de dominio de Active Directory y hacemos clic para desmarcarla.



Después nos aparece un diálogo que nos indica que para eliminar los Servicios de dominio, también tendremos que eliminar las características.

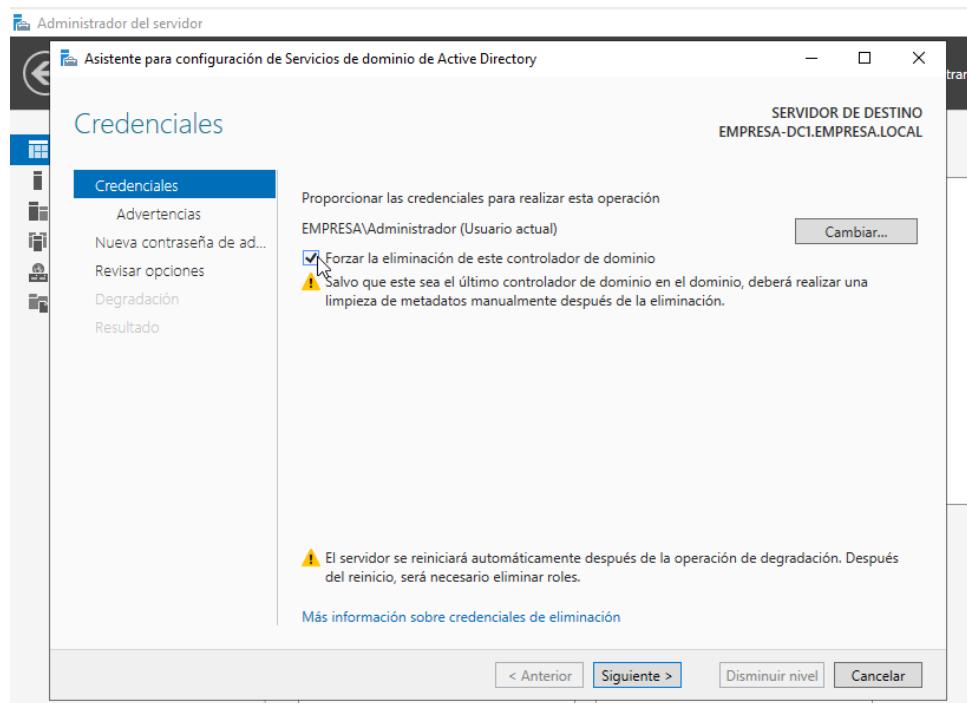


Se realiza una validación para ver si se cumplen todos los requerimientos que permitan desinstalar el rol y muestra un error.

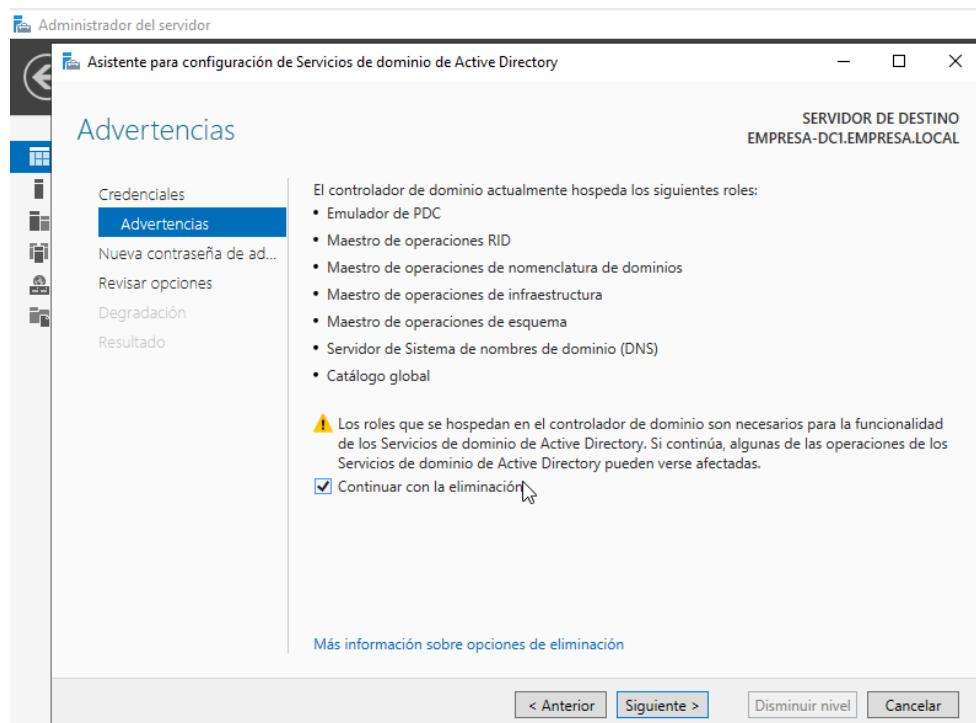


Hacemos clic en **disminuir el nivel del controlador de dominio** para poder proceder con la desinstalación.

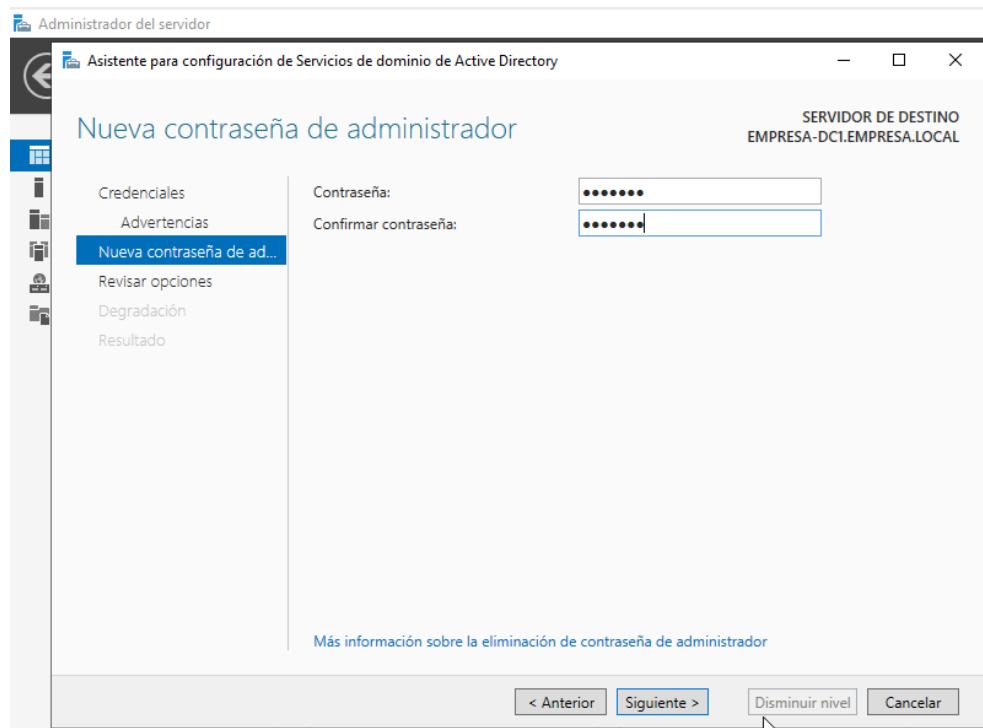
Hacemos clic sobre **Forzar la eliminación de este controlador de dominio.**



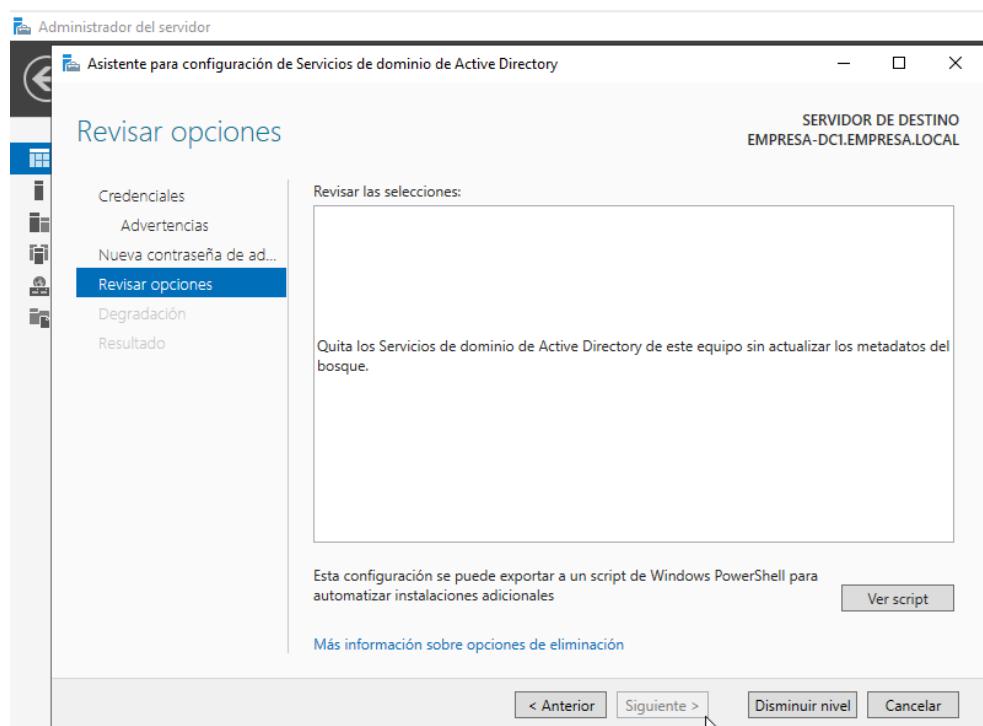
Para continuar, debemos marcar la opción *Continuar con la eliminación*.



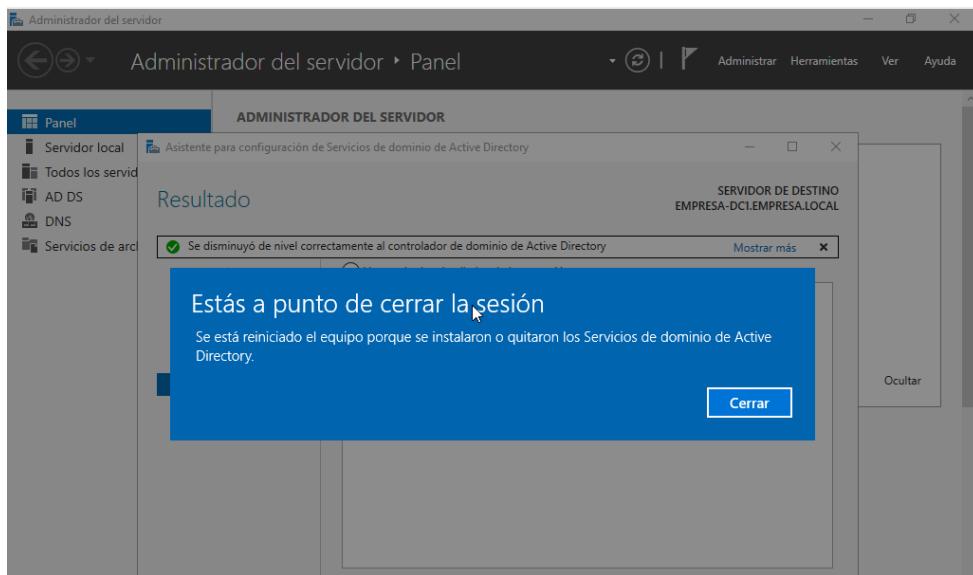
Escribimos la contraseña para la cuenta de Administrador.



Hacemos clic en **Disminuir nivel**



Después, el sistema comenzará a reiniciarse.

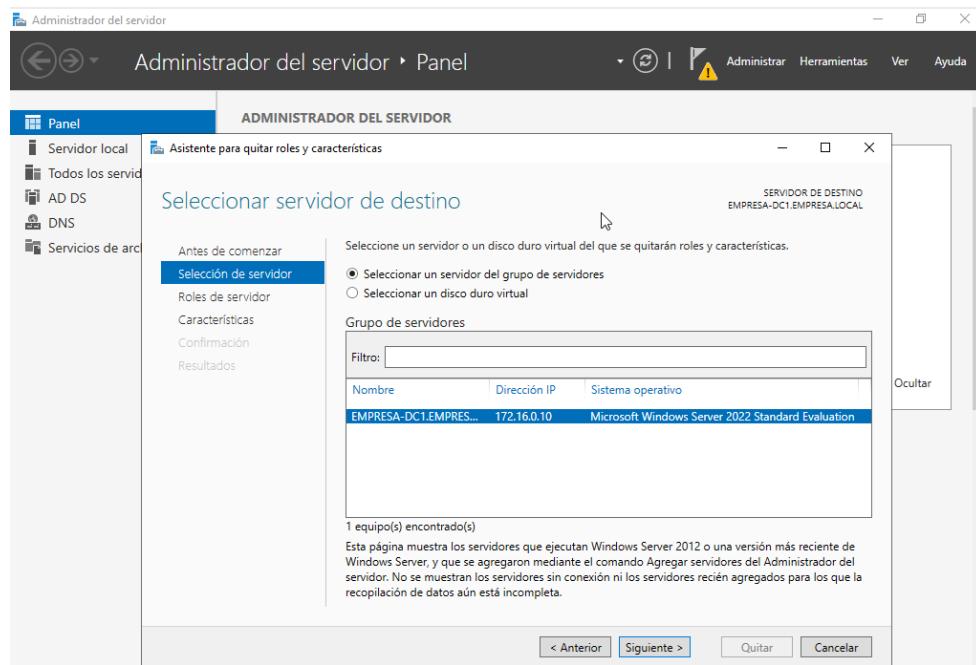


Una vez terminado el proceso de Disminuir nivel, debemos desinstalar los roles *Servicios de dominio de Active Directory* y *DNS*.

En el *Administrador del servidor*, desplegaremos el menú *Administrar*. Y elegimos la opción *Quitar roles y funciones*.



Seleccionar un servidor del grupo de servidores



Y desmarcamos la opción de “Servicios de dominio de Active Directory”

4. Gestión del directorio activo a través de la interfaz gráfica

4.1 Cuentas de usuario y equipo

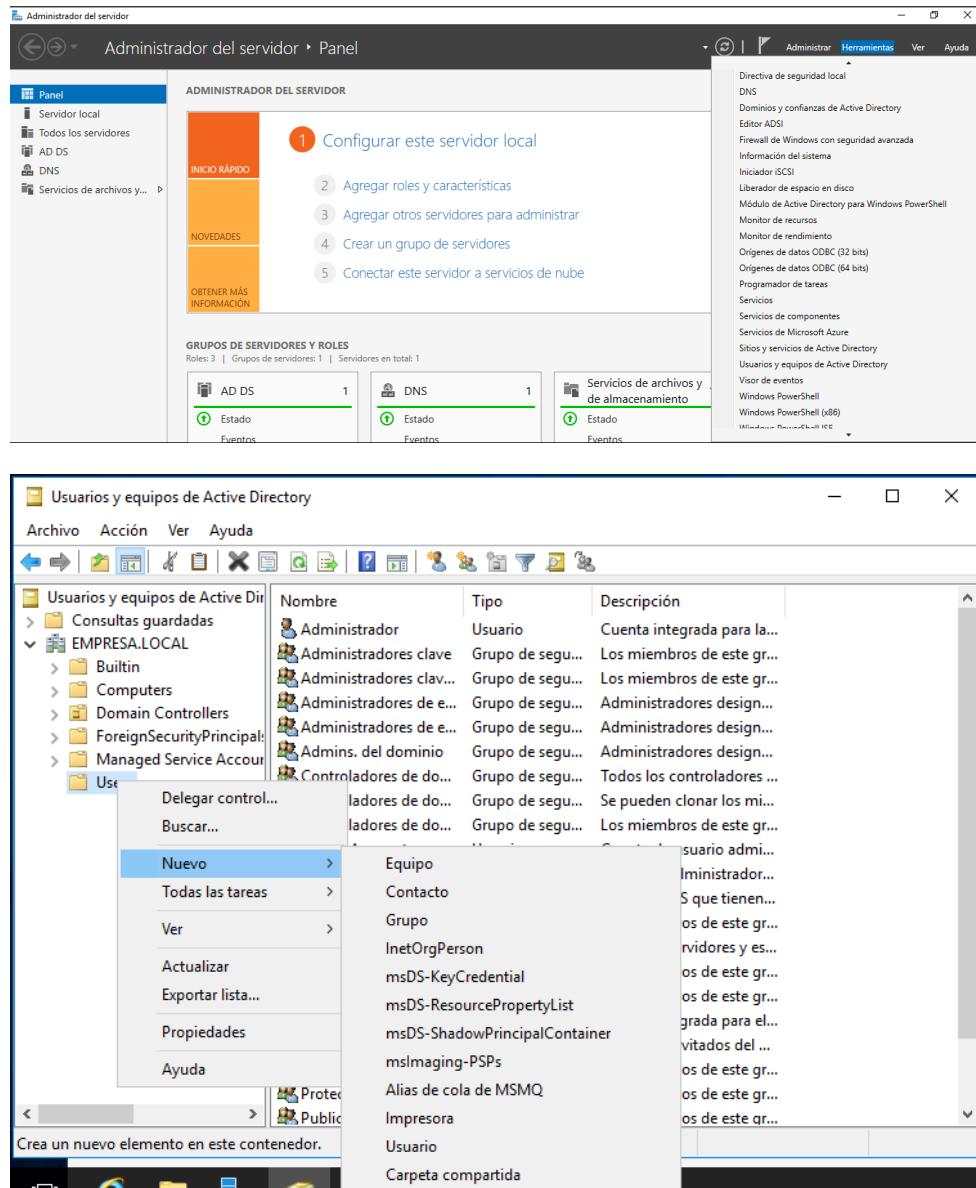
- Una **cuenta de usuario** es un objeto que posibilita el acceso a los recursos del dominio. No siempre representan a personas concretas, sino que también pueden ser utilizadas como mecanismos de acceso para determinados servicios o aplicaciones de la máquina local o, incluso, de un equipo remoto.



Cada cuenta de usuario dispone de un identificador de seguridad (**SID, Security Identifier**) que es único en el dominio.

- Una **cuenta de equipo** sirve para autenticar a los diferentes equipos que se conectan al dominio, permitiendo o denegando su acceso a los diferentes recursos del dominio. Aunque una cuenta de equipo se puede crear de forma manual (como veremos más adelante), también se puede crear en el momento en el que el equipo se une al dominio.

Para crear una cuenta de usuario acceder al menú **Herramientas del Administrador del Servidor**



- Creación de un nuevo Usuario

Nuevo objeto: Usuario



Crear en: EMPRESA.LOCAL/Users

Nombre de pila:	<input type="text"/>	Iniciales:	<input type="text"/>
Apellidos:	<input type="text"/>		
Nombre completo:	<input type="text"/>		
Nombre de inicio de sesión de usuario:	<input type="text"/>	@EMPRESA.LOCAL	<input type="button" value="▼"/>
Nombre de inicio de sesión de usuario (anterior a Windows 2000):	EMPRESA	<input type="text"/>	

[< Atrás](#) [Siguiente >](#) [Cancelar](#)

Una vez creado un usuario, podemos cambiar sus propiedades.

Usuarios y equipos de Active Directory

Archivo Acción Ver Ayuda

Usuarios y equipos de Active Dir

- > Consultas guardadas
- > EMPRESA.LOCAL
 - > BuiltIn
 - > Computers
 - > Domain Controllers
 - > ForeignSecurityPrincipal
 - > Managed Service Account
 - Users

Nombre	Tipo	Descripción
Administrador	Usuario	Cuenta integrada para la...
Administradores clave	Grupo de segu...	Los miembros de este gr...
Administradores clav...	Grupo de segu...	Los miembros de este gr...
Administradores de e...	Grupo de segu...	Administradores design...
Administradores de e...	Grupo de segu...	Administradores design...
Admins. del dominio	Grupo de segu...	Administradores design...
Angela B.	Copiar...	
Controlad...	Agregar a un grupo...	los controladores ...
Controlad...	Deshabilitar cuenta	den clonar los mi...
Controlad...	Restablecer contraseña...	embros de este gr...
DefaultAc...	Mover...	a de usuario admi...
DnsAdmin...	Abrir la página principal	de administrador...
DnsUpda...	Enviar correo	s DNS que tienen...
Enterprise...	Todas las tareas	embros de este gr...
Equipos c...	Cortar	embros de este gr...
Grupo de ...	Eliminar	s integrada para el...
Invitado	Cambiar nombre	los invitados del ...
Invitados		embros de este gr...
Propietar		embros de este gr...

Abre el cuadro de diálogo de propiedades de la selección

Propiedades: Angela Bañuls Serrano

Marcado	Entorno	Sesiones	Control remoto
Perfil de Servicios de Escritorio remoto		COM+	
General	Dirección	Cuenta	Perfil
		Telefonos	Organización
			Miembro de
 Angela Bañuls Serrano			
Nombre de pila: <input type="text" value="Angela"/> Iniciales: <input type="text"/> Apellidos: <input type="text" value="Bañuls Serrano"/> Nombre para mostrar: <input type="text" value="Angela Bañuls Serrano"/> Descripción: <input type="text"/> Oficina: <input type="text"/> Número de teléfono: <input type="text"/> Otros... Correo electrónico: <input type="text"/> Página web: <input type="text"/> Otros...			
<input type="button" value="Aceptar"/> <input type="button" value="Cancelar"/> <input type="button" value="Aplicar"/> <input type="button" value="Ayuda"/>			

Pestaña: Cuenta

Establecer horas de inicio de sesión

Propiedades: Angela Bañuls Serrano

Marcado	Entorno	Sesiones	Control remoto
Perfil de Servicios de Escritorio remoto		COM+	
General	Dirección	Cuenta	Perfil
		Telefonos	Organización
			Miembro de
Nombre de inicio de sesión de usuario: <input type="text" value="angela"/> @EMPRESA LOCAL Nombre de inicio de sesión de usuario (anterior a Windows 2000): <input type="text" value="EMPRESA"/> <input type="text" value="angela"/> <input type="button" value="Horas de inicio de sesión..."/> <input type="button" value="Iniciar sesión en..."/> <input type="checkbox"/> Desbloquear cuenta Opciones de cuenta: <input checked="" type="checkbox"/> El usuario debe cambiar la contraseña en el siguiente inicio de sesión <input type="checkbox"/> El usuario no puede cambiar la contraseña <input type="checkbox"/> La contraseña nunca expira <input type="checkbox"/> Almacenar contraseña utilizando cifrado reversible La cuenta expira: <input checked="" type="radio"/> Nunca <input type="radio"/> Fin de: <input type="text" value="lunes , 14 de octubre de 2019"/>			
<input type="button" value="Aceptar"/> <input type="button" value="Cancelar"/> <input type="button" value="Aplicar"/> <input type="button" value="Ayuda"/>			

Horas de inicio de sesión para Angela Bañuls Serrano

0	2	4	6	8	10	12	14	16	18	20	22	0
●												●
Todo												
lunes												
martes												
miércoles												
jueves												
viernes												
sábado												
domingo												

● Inicio de sesión permitido ○ Inicio de sesión denegado

De sábado a domingo de 0:00 a 0:00 horas

Pestaña: Cuenta

Limitar los equipos desde los que un usuario puede acceder

Propiedades: Angela Bañuls Serrano

Marcado	Entorno	Sesiones	Control remoto
Perfil de Servicios de Escritorio remoto		COM+	
General	Dirección	Cuenta	Perfil
		Telefonos	Organización
			Miembro de
Nombre de inicio de sesión de usuario: <input type="text" value="angela"/> @EMPRESA LOCAL Nombre de inicio de sesión de usuario (anterior a Windows 2000): <input type="text" value="EMPRESA"/> <input type="text" value="angela"/> <input type="button" value="Horas de inicio de sesión..."/> <input type="button" value="Iniciar sesión en..."/> <input type="checkbox"/> Desbloquear cuenta Opciones de cuenta: <input checked="" type="checkbox"/> El usuario debe cambiar la contraseña en el siguiente inicio de sesión <input type="checkbox"/> El usuario no puede cambiar la contraseña <input type="checkbox"/> La contraseña nunca expira <input type="checkbox"/> Almacenar contraseña utilizando cifrado reversible La cuenta expira: <input checked="" type="radio"/> Nunca <input type="radio"/> Fin de: <input type="text" value="lunes , 14 de octubre de 2019"/>			
<input type="button" value="Aceptar"/> <input type="button" value="Cancelar"/> <input type="button" value="Aplicar"/> <input type="button" value="Ayuda"/>			

Estaciones de trabajo de inicio de sesión

En Nombre de equipo, escriba el nombre NetBIOS o DNS (Sistema de nombres de dominio) del equipo.

Este usuario puede iniciar sesión en:

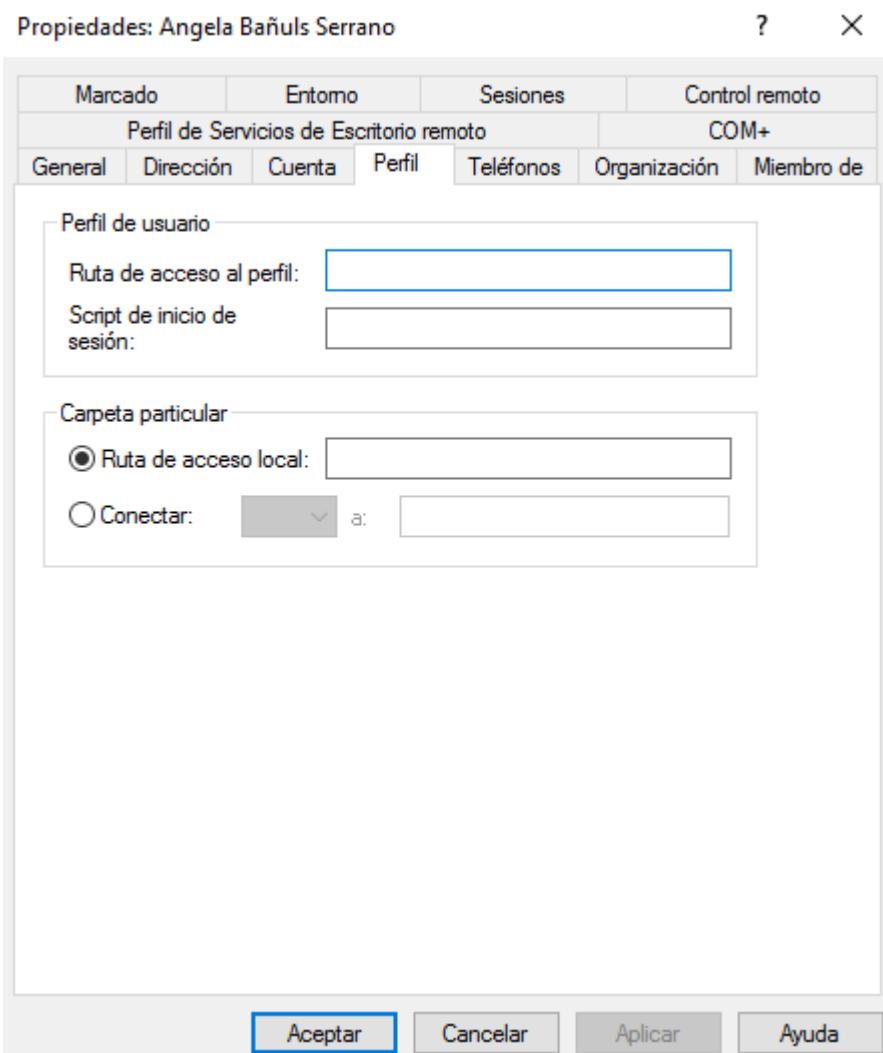
Todos los equipos Los siguientes equipos

Nombre de equipo:

El **perfil de un usuario** consiste en la personalización del entorno. Por defecto, se crea una carpeta en el equipo en el que se inicia sesión, pero esto puede modificarse.

- **Perfil móvil:** El usuario dispondrá de su personalización en todos los equipos del bosque en los que se autentique.
- **Perfil obligatorio:** El usuario no podrá personalizar su entorno. Podrá hacer modificaciones pero al iniciar sesión de nuevo se habrán perdido los cambios.

Pestaña: Perfil



Ruta de acceso al perfil: Indica donde se guardará el perfil. Si ponemos una ruta de red tendremos un perfil móvil.

Script de inicio de sesión: Se puede asociar un script para que se ejecute cada vez que el usuario inicie sesión.

Pestaña: Miembro de

Agregar / quitar grupos a los que pertenece un usuario

Propiedades: Angela Bañuls Serrano

?

X

Marcado	Entorno	Sesiones	Control remoto
Perfil de Servicios de Escritorio remoto			COM+
General	Dirección	Cuenta	Perfil
Teléfonos	Organización	Miembro de	

Miembro de:

Nombre	Carpeta de los Servicios de dominio de Active D
Usuarios del dominio	EMPRESA.LOCAL/Users

< >

Agregar... **Quitar**

Grupo principal: Usuarios del dominio

Establecer grupo principal No es necesario cambiar Grupo principal si no tiene clientes de Macintosh o aplicaciones compatibles con POSIX.

Aceptar **Cancelar** **Aplicar** **Ayuda**

Seleccionar Grupos

X

Seleccionar este tipo de objeto:

Grupos o Entidades de seguridad integradas

Tipos de objeto...

Desde esta ubicación:

EMPRESA.LOCAL

Ubicaciones...

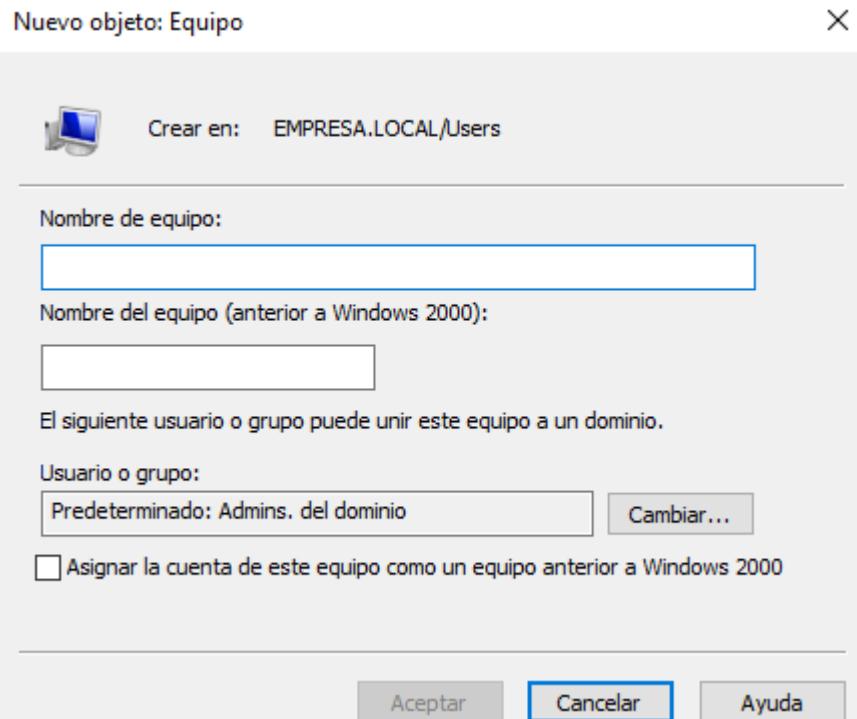
Escriba los nombres de objeto que desea seleccionar ([ejemplos](#)):

Profesores

Comprobar nombres

Opciones avanzadas...**Aceptar****Cancelar**

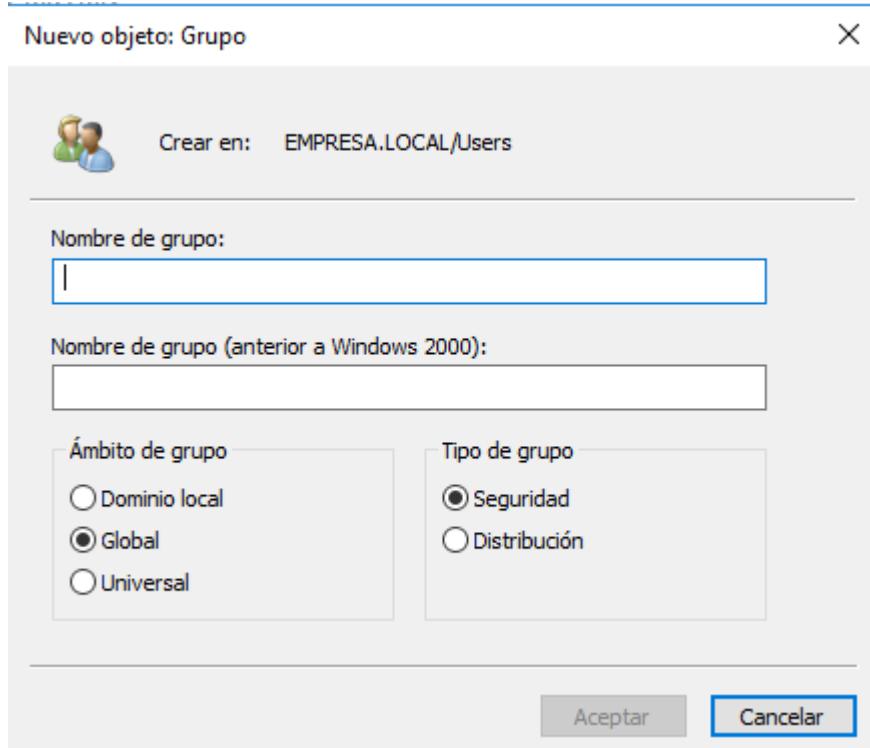
- Creación de un nuevo equipo



4.2 Cuentas de grupo

Una cuenta de grupo es una colección de cuentas de usuario que se puede utilizar para asignar un conjunto de permisos y derechos a varios usuarios al mismo tiempo. Un grupo también puede contener contactos, equipos y otros grupos.

Para crear una cuenta de grupo acceder al menú **Herramientas** del **Administrador del Servidor => Usuarios y equipos de AD**



4.2.1 Tipos de grupos

Existen dos tipos de grupos:

- **Distribución:** Para crear listas de distribución de correo electrónico.
- **Seguridad:** Para asignar permisos a los recursos compartidos

4.2.2 Ámbitos de un grupo

El ámbito de un grupo establece su alcance, es decir, en qué partes de la red puede utilizarse, y el tipo de cuentas que pueden formar parte de él.

Ámbito de grupo	El grupo puede incluir como miembros ...	Al grupo se le pueden asignar permisos en ...
Universal	- Cuentas de cualquier dominio del bosque - Grupos globales de cualquier dominio del bosque - Grupos universales de cualquier dominio del bosque	Cualquier dominio del bosque
Global	- Cuentas del mismo dominio del grupo - Grupos globales del mismo dominio del grupo	Cualquier dominio del bosque
Dominio local	- Cuentas de cualquier dominio - Grupos globales de cualquier dominio - Grupos universales de cualquier dominio - Grupos locales de su dominio	Su dominio



Los grupos universales se replican en los controladores de dominio que albergan el **catálogo global**. Cada vez que se deben comprobar los permisos se debe consultar el catálogo global.



GC (Global Catalogue): Catálogo global

4.3 Unidades organizativas

Una **Unidad Organizativa** es un contenedor de objetos que permite organizarlos en subconjuntos, dentro del dominio, siguiendo una jerarquía. De este modo, podremos establecer una estructura lógica que represente de forma adecuada nuestra organización y simplifique la administración. Me permiten delegar permisos y asignar políticas de seguridad para uno o varios objetos.

Las unidades organizativas que vienen creadas por defecto son:

- **Builtin**: Grupos creados por defecto del sistema.
- **Computers**: Cuentas de equipo incorporadas al dominio.
- **DomainControllers**: Equipos que son controladores.
- **Users**: Usuarios del dominio que se crean
- **ForeignSecurityPrincipals**: Contenedor para entidades principales de seguridad de dominios externos de confianza. No se debe modificar manualmente.

4.4 Directivas de grupo

Las directivas de grupo son un **conjunto de reglas** que controlan el entorno de trabajo de **cuentas de usuario** y **cuentas de equipo**. Las directivas de grupo proporcionan la gestión centralizada y configuración de sistemas operativos, aplicaciones y configuración de los usuarios en un entorno de Active Directory.

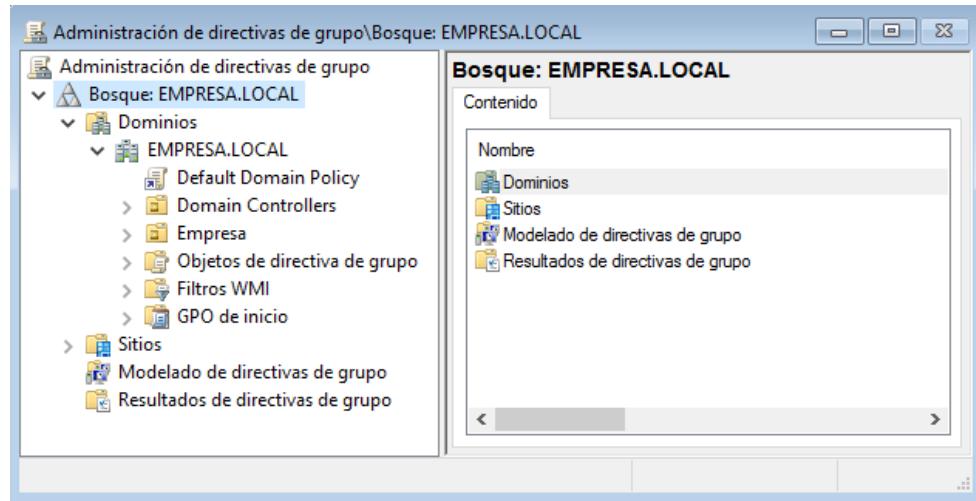
Para gestionar las directivas de grupo:

Herramientas->Administración de directivas de grupo

Las configuraciones de las directivas de grupo se encuentran en los objetos de directiva de grupo (**GPO**), que se vinculan con los siguientes contenedores de servicio de directorio de Active Directory: **sitios, dominios o unidades organizativas**.

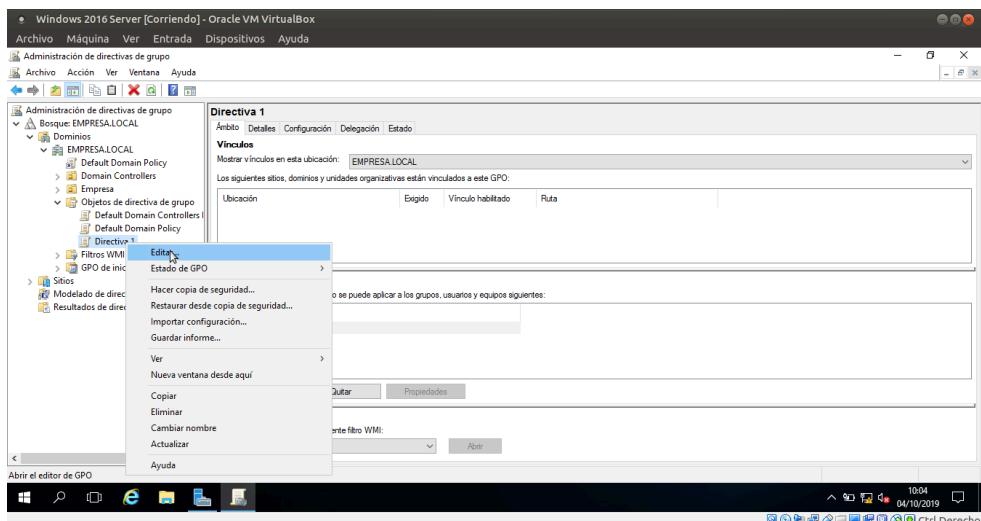
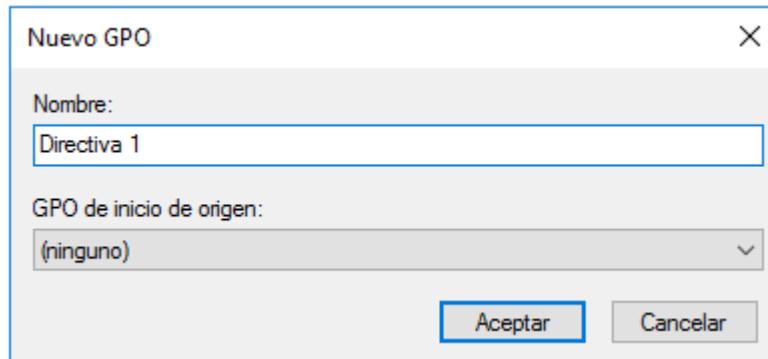
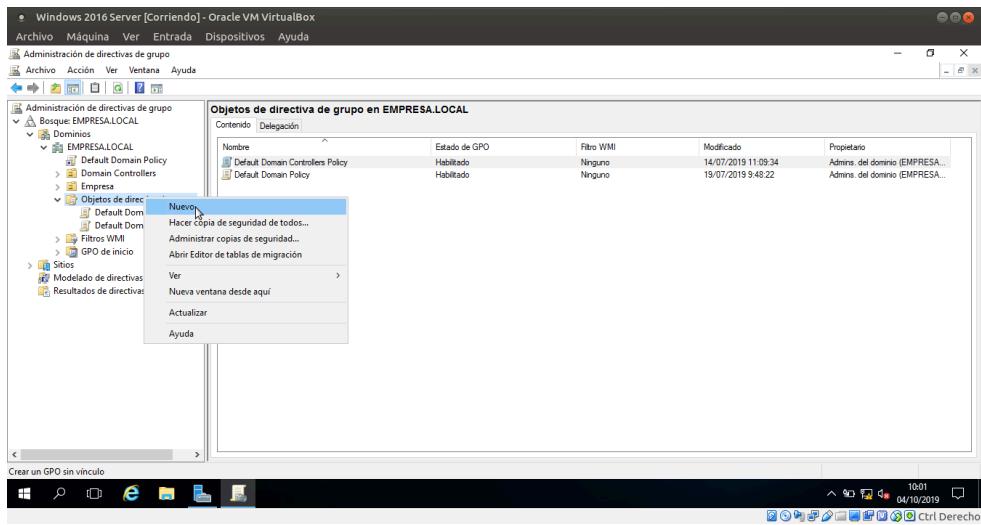


No pueden aplicarse a grupos. Si se desea aplicar una GPO a un grupo debemos crear una UO y dentro de esta un nuevo grupo e incorporar a este los grupos y/o usuarios a los que queremos aplicar dicha política.



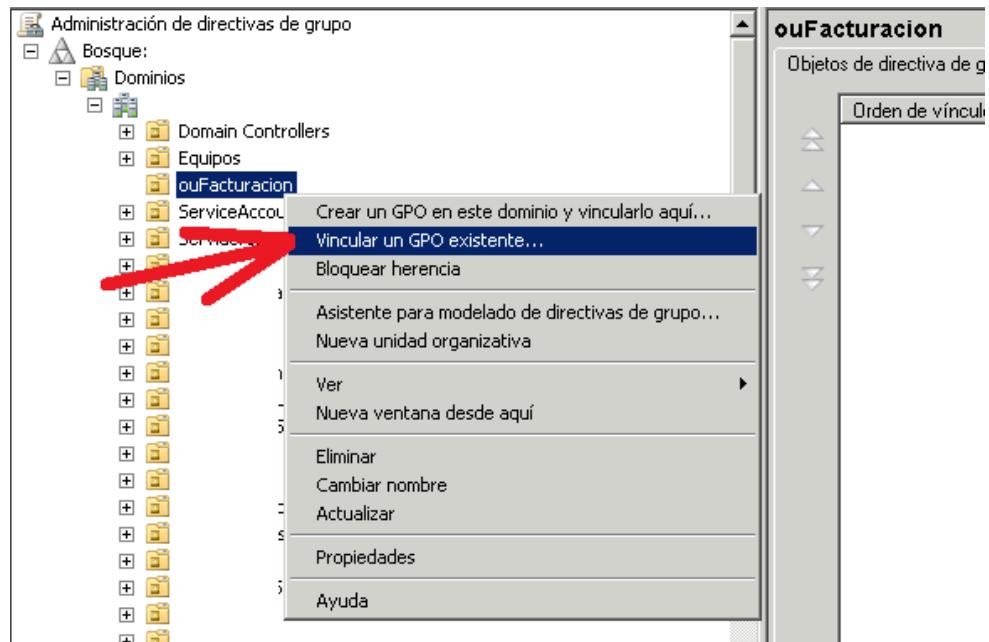
Default domain policy: Es la política que se aplica a todo el dominio empresa.local, es decir, a todos sus usuarios y equipos.

4.4.1 Creación de una nueva directiva

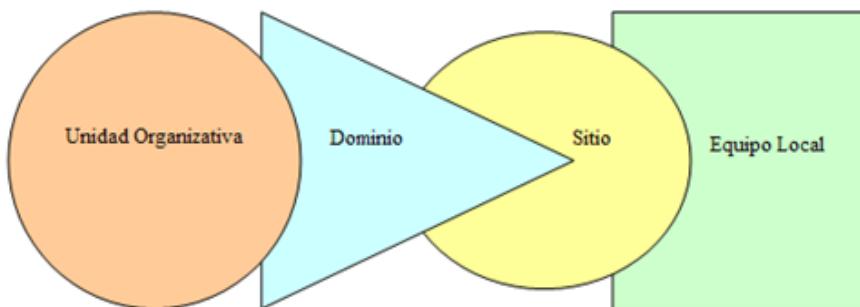


4.4.2 Vinculación de una directiva a una Unidad Organizativa

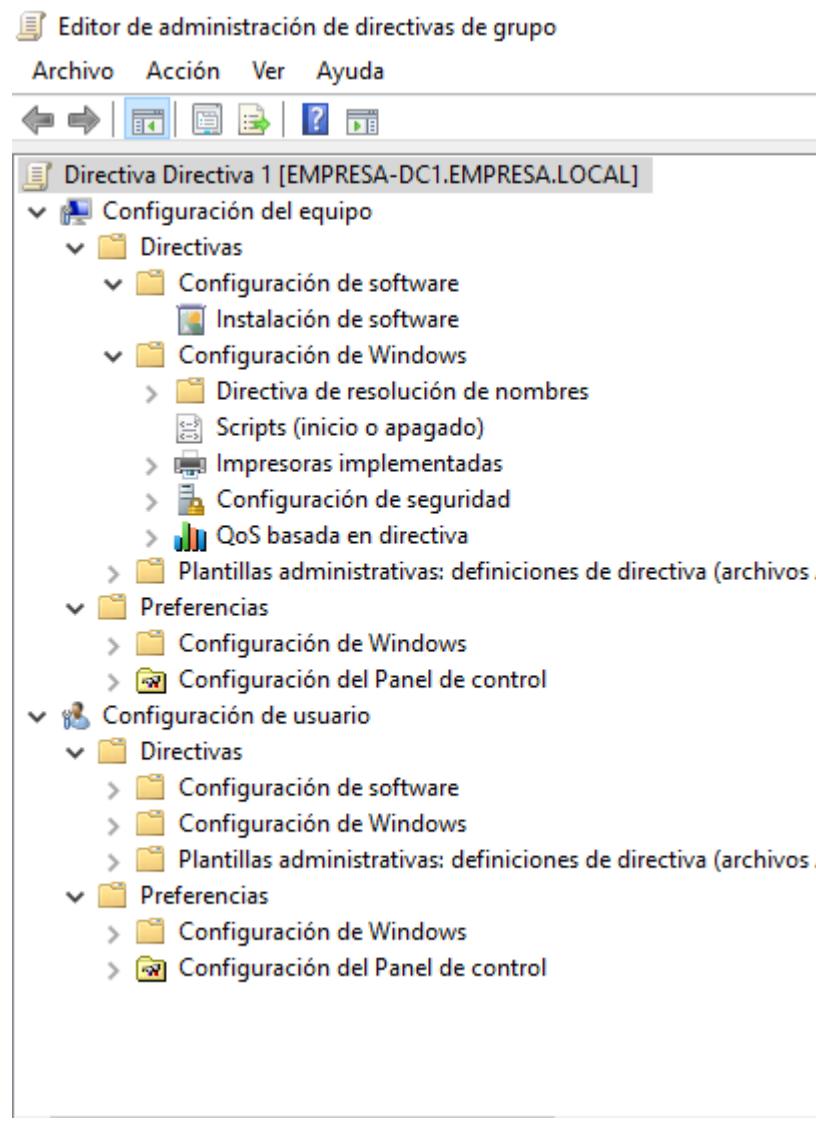
Para ello, desde el Administrador de directivas de grupo (**gpmc.msc**), pulsaremos con el botón derecho sobre la unidad organizativa a la que queramos asignarle la directiva creada.



4.4.3 Orden de prioridad de las directivas de grupo



Las GPO's de una OU prevalecen sobre las del dominio, que a su vez prevalecen sobre las de sitio, las cuales a su vez prevalecen sobre las del equipo local.

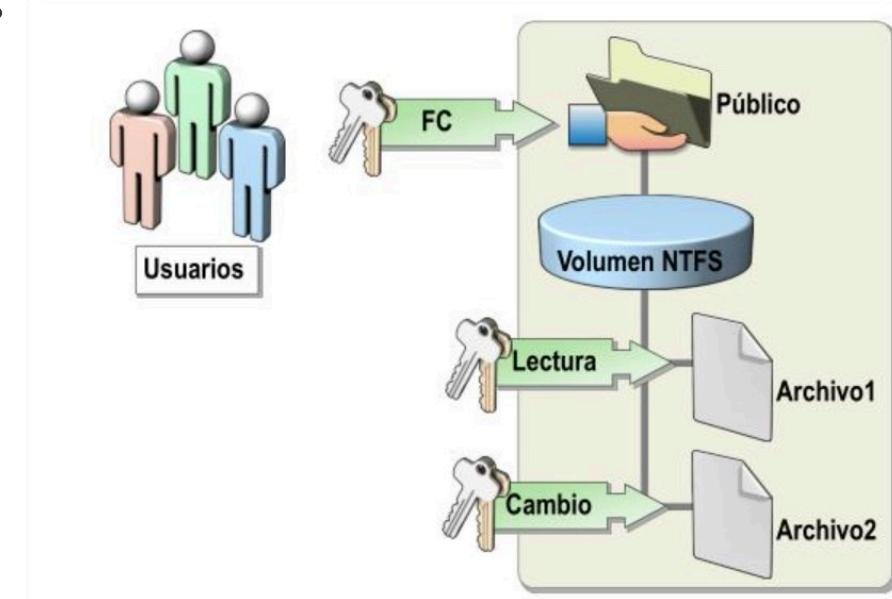


4.5 Permisos

Los sistemas operativos de la familia Windows poseen dos niveles de permisos para los recursos compartidos:

- **Permisos para carpetas compartidas:** se aplican cada vez que un usuario quiere acceder a un archivo o carpeta de la red.
- **Permisos para archivos y carpetas (NTFS):** se aplican sobre dispositivos con formato NTFS para definir en mayor detalle las acciones permitidas.
- Si accedemos en modo **local** a los archivos o carpetas sólo intervienen los **permisos NTFS**
- Si se accede a través de la red se aplican los **dos niveles de permisos:**
 - 1º Permisos de carpetas compartidas

- 2º Permisos NTFS



4.5.1 Permisos de recursos compartidos

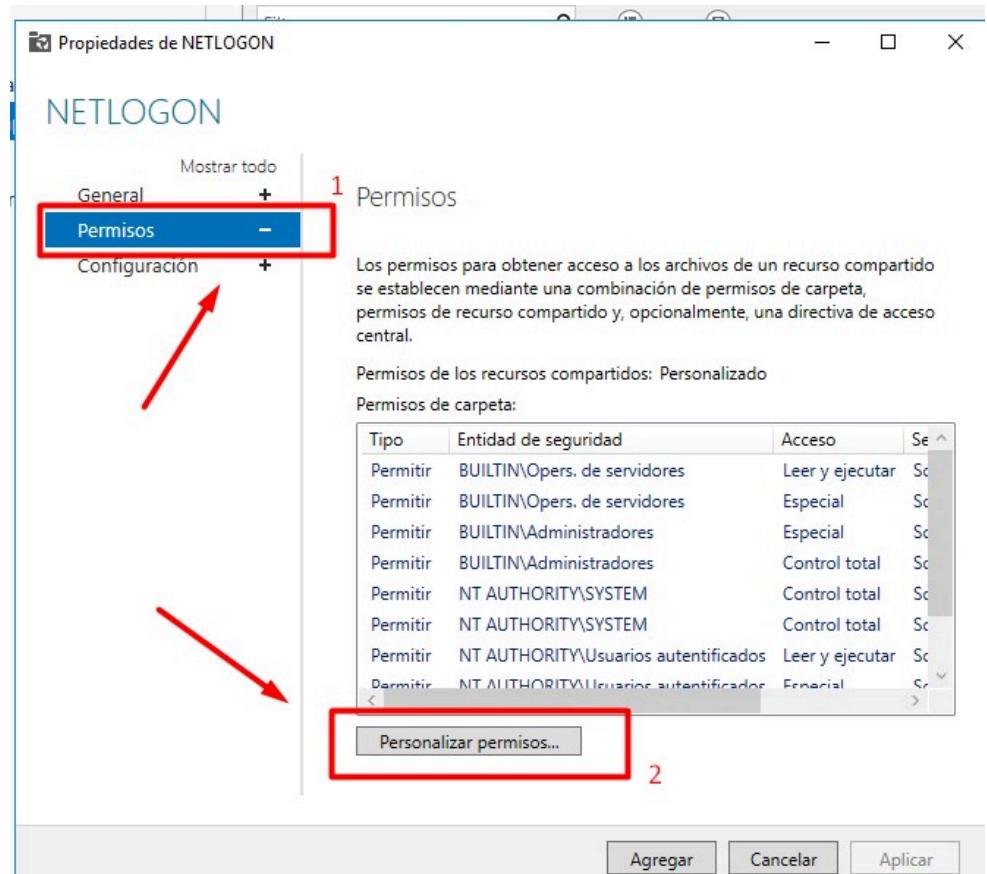
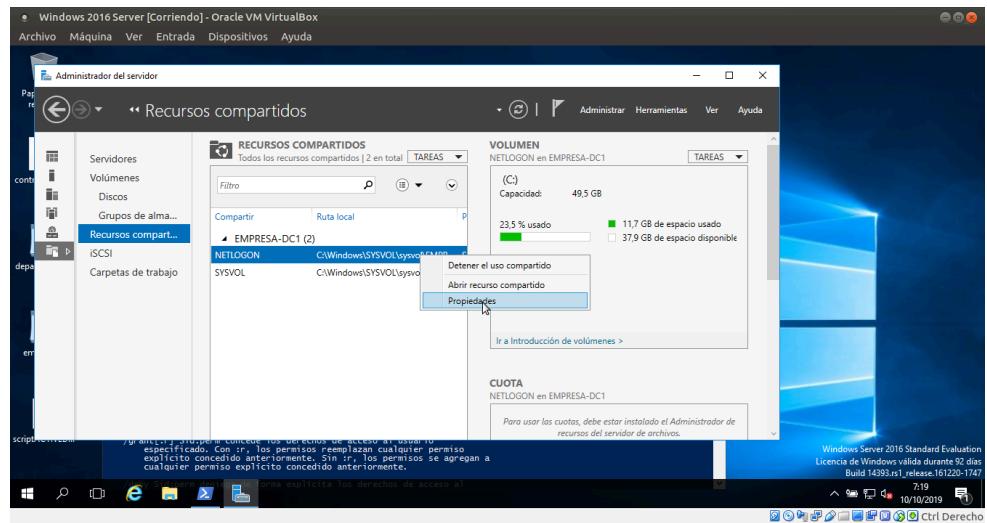
ADMINISTRADOR DEL SERVIDOR

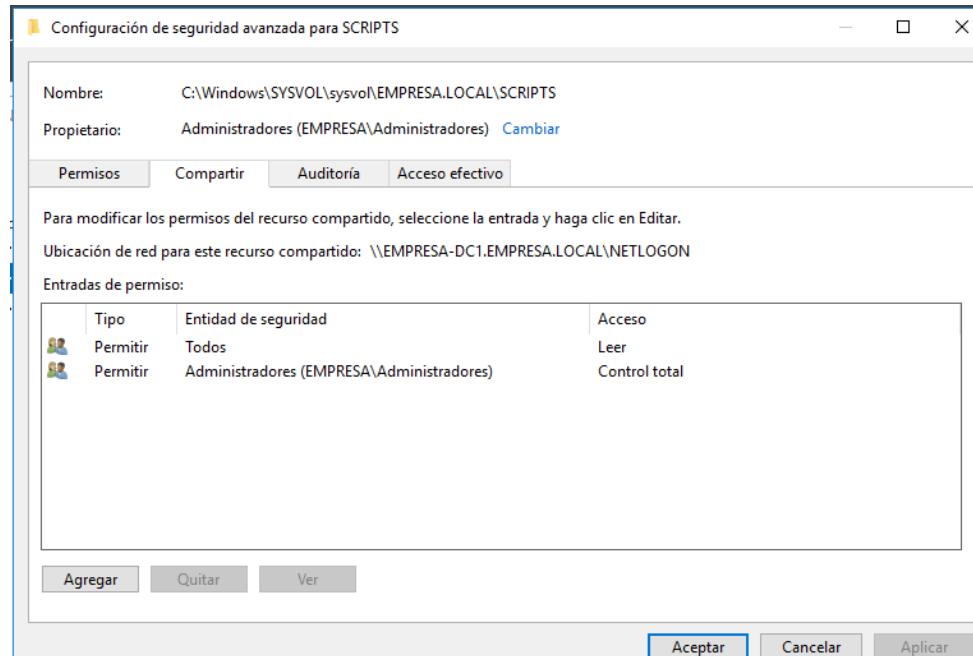
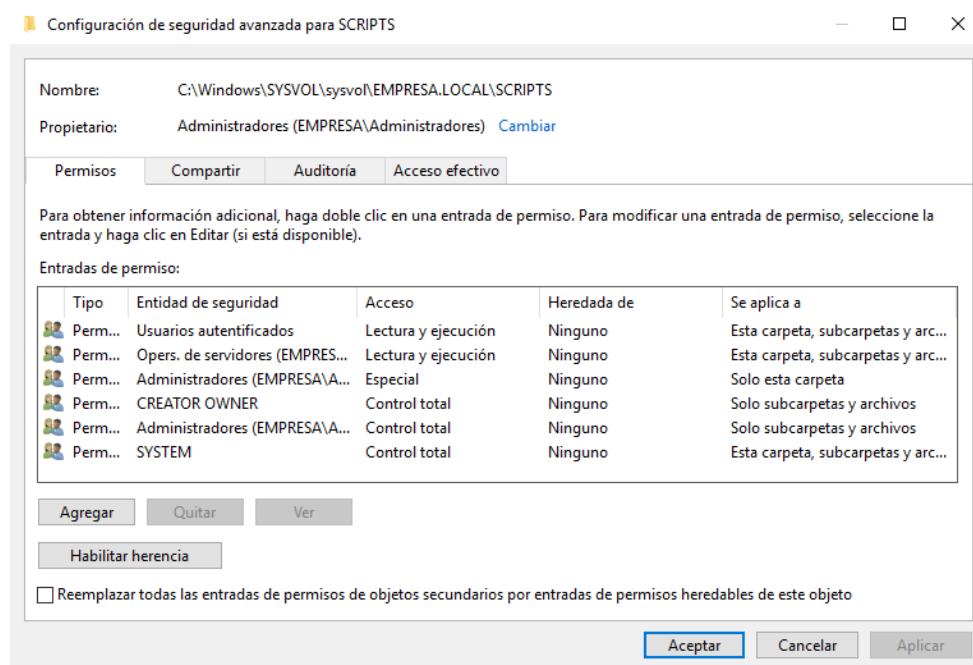
- 1 Configurar este servidor local
- 2 Agregar roles y características
- 3 Agregar otros servidores para administrar
- 4 Crear un grupo de servidores
- 5 Conectar este servidor a servicios de nube

GRUPOS DE SERVIDORES Y ROLES
Roles: 6 | Grupos de servidores: 1 | Servidores en total: 1

RECURSOS COMPARTIDOS
Todos los recursos compartidos | 2 en total | TAREAS ▾

Compartir	Ruta local
EMPRESA-DC1 (2)	
NETLOGON	C:\Windows\SYSVOL\sysvol\EMPR...
SYSVOL	C:\Windows\SYSVOL\sysvol\





Tipos de permisos:

Control Total: Todas las operaciones y cambio de permisos.

Cambiar: permite crear, modificar y borrar carpetas y archivos.,

Lectura: sólo permite la lectura y ejecución de archivos.

Entrada de permiso para NETLOGON

Entidad de seguridad: Todos [Seleccionar una entidad de seguridad](#)

Tipo:	<input type="button" value="Permitir"/>
	<input type="button" value="Denegar"/>
	<input type="button" value="Permitir"/>

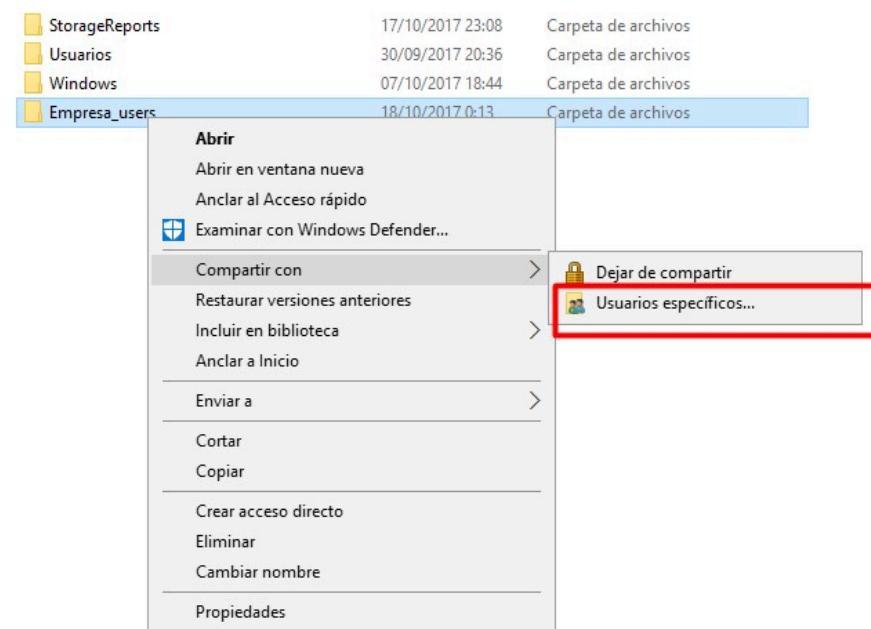
Permisos:

- Control total
- Cambiar
- Leer
- Permisos especiales

Establecer permisos de recursos compartidos

1º Compartir con usuarios específicos

Seleccionar el recurso y hacer clic con el botón secundario 'Compartir con' y usuarios específicos.



2º Compartir mediante el uso de Compartido avanzado

Propiedades: Empresa_users

General Compartir Seguridad Versiones anteriores Personalizar

Uso compartido de carpetas y archivos de red

Empresa_users Compartido

Buena de acceso de red: \\MASTER200\Empresa_users

[Compartir...](#)

Uso compartido avanzado

Establezca permisos personalizados, cree múltiples recursos compartidos y defina otras opciones avanzadas para compartir.

[Uso compartido avanzado...](#)

Propiedades: Empresa_users

Uso compartido avanzado

Nombre del recurso compartido: Empresa_users

Buena de acceso de red: \\MASTER200\Empresa_users

Configuración

Nombre del recurso compartido: Empresa_users

Buena de acceso de red: \\MASTER200\Empresa_users

Uso compartido avanzado

Establezca permisos personalizados, cree múltiples recursos compartidos y defina otras opciones avanzadas para compartir.

[Uso compartido avanzado...](#)

Permisos de Empresa_users

Permisos de los recursos compartidos

Nombre de grupo o usuario: Todos Administradores (CEIRE2017/Administradores)

Permisos de Todos

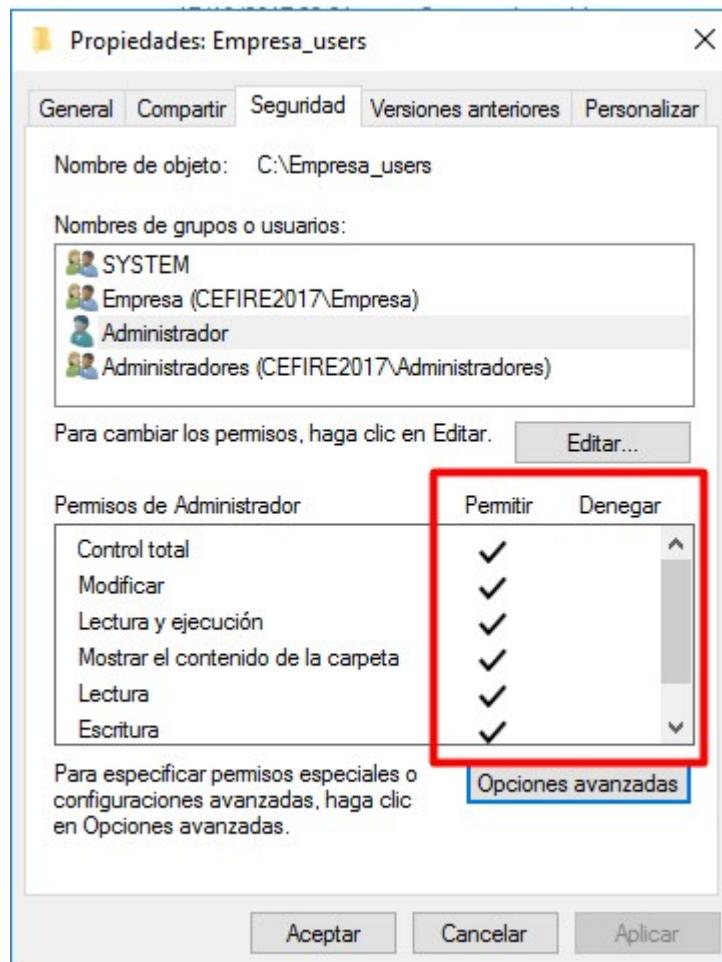
Control total Cambiar Leer

Permitir Denegar

4.5.2 Permisos NTFS

Los Permisos NTFS permiten controlar qué usuarios y grupos puede tener acceso a archivos y carpetas en un volumen NTFS.

Podemos asignar los siguientes permisos:



- **Control total.** Otorga todos los permisos posibles, incluido el control total sobre los permisos NTFS y los permisos de compartir.
- **Modificar.** Permite leer, escribir, modificar y eliminar archivos y subcarpetas, así como ejecutar archivos.
- **Lectura y ejecución.** Permite ver el contenido de un archivo o carpeta y ejecutar archivos ejecutables, pero no permite modificarlos.
- **Mostrar el contenido de la carpeta.** Permite ver el contenido de una carpeta, pero no permite acceder a los archivos dentro de ella ni ejecutarlos.
- **Lectura.** Permite únicamente la lectura de archivos y carpetas, sin posibilidad de modificar o eliminar.
- **Escritura.** Permite crear nuevos archivos y carpetas, así como modificar o eliminar los existentes, pero no permite

ver el contenido de la carpeta.

	Control total	Cambiar	Leer y ejecutar	Mostrar el contenido de la carpeta	Leer	Escribir
Recorrer por carpeta/ejecutar archivo	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Mostrar carpeta/leer datos	<input checked="" type="checkbox"/>					
Atributos de lectura	<input checked="" type="checkbox"/>					
Atributos extendidos de lectura	<input checked="" type="checkbox"/>					
Crear archivos/escribir datos	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>
Crear carpetas/agregar datos	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>
Atributos de escritura	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>
Atributos extendidos de escritura	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>
Eliminar subcarpetas y archivos	<input checked="" type="checkbox"/>					
Eliminar	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
Permisos de lectura	<input checked="" type="checkbox"/>					
Cambiar permisos	<input checked="" type="checkbox"/>					
Tomar posesión	<input checked="" type="checkbox"/>					

Permisos NTFS avanzados

Propiedades: Empresa_users

General Compartir Seguridad Versiones anteriores Personalizar

Nombre de objeto: C:\Empresa_users

Nombres de grupos o usuarios:

- SYSTEM
- Empresa (CEFIRE2017\Empresa)
- Administrador
- Administradores (CEFIRE2017\Administradores)

Para cambiar los permisos, haga clic en Editar...

Permisos de Administrador Permitir Denegar

Control total	✓
Modificar	✓
Lectura y ejecución	✓
Mostrar el contenido de la carpeta	✓
Lectura	✓
Escritura	✓

Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas.

Opciones avanzadas

Configuración de seguridad avanzada para Empresa_users

Nombre: C:\Empresa_users
Propietario: Administradores (CEFIRE2017\Administradores)

Permisos Compartir Auditoría Acceso efectivo

Para obtener información adicional, haga doble clic en una entrada de permiso. Para modificar una entrada de permiso, seleccione la entrada y haga clic en Editar (si está disponible).

Entradas de permiso:

Tipo	Entidad de seguridad	Acceso	Heredada de	Se aplica a
Perm.	Administrador (CEFIRE2017\A...	Control total	Ninguno	Esta carpeta, subcarpetas y arc...
Perm.	Administradores (CEFIRE2017\...	Control total	Ninguno	Esta carpeta, subcarpetas y arc...
Perm.	SYSTEM	Control total	Ninguno	Esta carpeta, subcarpetas y arc...
Perm.	Empresa (CEFIRE2017\Empresa)	Control total	Ninguno	Esta carpeta, subcarpetas y arc...

Editar

Reemplazar todas las entradas de permisos de objetos secundarios por entradas de permisos heredados de este objeto

Entrada de permiso para Empresa_users

Entidad de seguridad: Administrador (CEFIRE2017\Administrador) [Seleccionar una entidad de seguridad](#)

Tipo: ▼

Se aplica a: ▼

Permisos básicos:

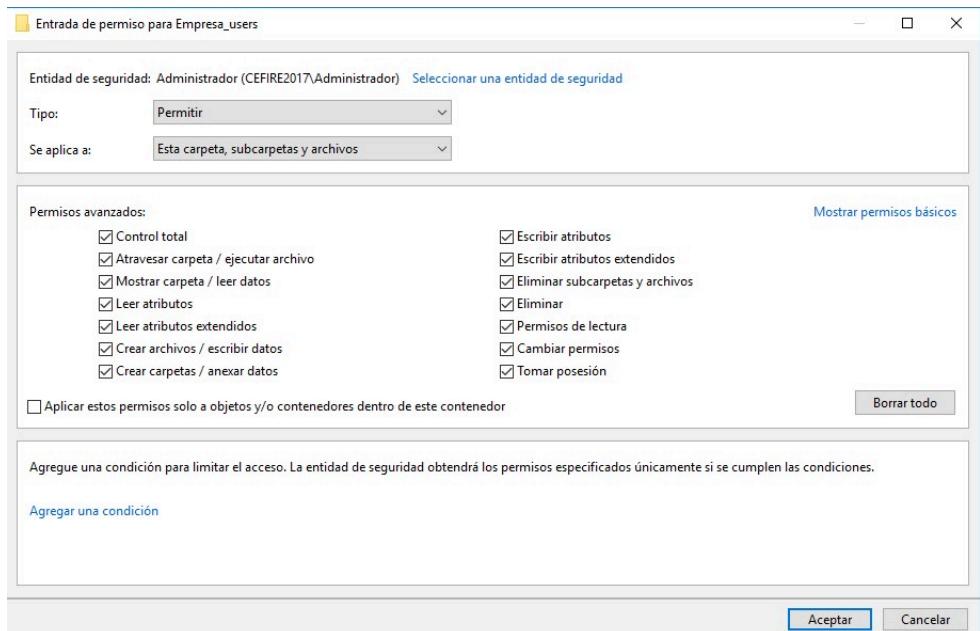
- Control total
- Modificar
- Lectura y ejecución
- Mostrar el contenido de la carpeta
- Lectura
- Escritura
- Permisos especiales

Mostrar permisos avanzados

Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor

Agregue una condición para limitar el acceso. La entidad de seguridad obtendrá los permisos especificados únicamente si se cumplen las condiciones.

[Agregar una condición](#)



Herencia de permisos

Al crear un archivo o una carpeta en un volumen NTFS, ese objeto hereda automáticamente los permisos de su carpeta padre, y a la inversa.

En ocasiones, puede interesarnos eliminar esa herencia de permisos. Podemos eliminarla de tres formas:

- Eliminar la herencia a nivel de la carpeta de nivel superior. Los objetos contenidos en ella dejan de heredar los permisos.
- Eliminar la herencia a nivel de subcarpeta o archivo contenido dentro del recurso principal.
- Permitir o denegar explícitamente un permiso de manera diferente a como está definido en el recurso contenedor.

Para *eliminar la herencia* seguimos los siguientes pasos:

1 - Se selecciona el recurso con el botón derecho y se pulsa **Propiedades**

2 - A través de la pestaña **Seguridad** accedemos a **Opciones avanzadas**

3 - En el cuadro que aparece, en la pestaña **Permisos**, se pulsa el botón **Deshabilitar herencia**.

4 - Al pulsar en **Deshabilitar herencia** hay dos opciones:

- Convertir los permisos heredados en permisos explícitos: mantiene los permisos de todos los archivos y subcarpetas, pero no están vinculados a los de nivel superior.
- Quitar todos los permisos: elimina todos los permisos heredados.

Como norma general se marcará la primera opción, convertir los permisos en permisos explícitos.

4.6 Perfiles

Podemos definir un perfil como aquellos aspectos de configuración del equipo y del entorno de trabajo propios del usuario y que además son exportables a otras máquinas de manera transparente al mismo. mediante los perfiles conseguimos que el usuario independientemente del equipo en el que inicie la sesión disponga de un entorno de trabajo similar.

Existen tres tipos de perfiles:

- **Perfiles locales**: se almacenan en el equipo
- **Perfiles móviles**: se almacenan en el servidor
- **Perfiles obligatorios**: son perfiles móviles de solo lectura. Sólo el administrador puede modificarlos.

Hay que tener en cuenta de que cuando un usuario con perfil móvil inicia la sesión, la información del servidor se copia al cliente. Cuando cierra la sesión se realiza la operación inversa. Un alto número de usuarios con perfil móvil puede **sobrecargar la red** demasiado.

[« Scripting en Windows. PowerShell](#)

[Administracion del servicio de directorio en Windows con PowerShell »](#)



Esta obra está bajo una [licencia de Creative Commons Reconocimiento-CompartirIgual 4.0 Internacional](#).