**UD**

**ACTIVE DIRECTORY**

[**1.- Introducción** 2](#_Toc153310461)

[**2.- Active Directory** 2](#_Toc153310462)

[**2.1.- Kerberos** 3](#_Toc153310463)

[**3.- El dominio** 4](#_Toc153310464)

[**Pasos previos**: 4](#_Toc153310465)

[**1.- Poner nombre al equipo.** 4](#_Toc153310466)

[**2.- Poner una IP que sea fácilmente reconocible dentro de la red local**. 5](#_Toc153310467)

[**3.- Creación del dominio** 7](#_Toc153310468)

[**4.- El bosque** 12](#_Toc153310469)

[**5.- Árbol** 12](#_Toc153310470)

[**6.- Unidad Organizativa** 13](#_Toc153310471)

[**6.1.- Creación de Unidades Organizativas** 13](#_Toc153310472)

[**7.- Los objetos** 15](#_Toc153310473)

[**8.- El catálogo global** 16](#_Toc153310474)

[**9.- Los sitios AD** 16](#_Toc153310475)

[**10.- Nivel funcional del dominio y del bosque** 17](#_Toc153310476)

[**11.- Creación de usuarios** 18](#_Toc153310477)

[**12.- Unir equipos al dominio** 23](#_Toc153310478)

# **1.- Introducción**

Uno de los recursos más importantes en las empresas enfocadas al trabajo mediante terminales informáticos, **es el uso de usuarios y permisos.**

Para ello, lo que realmente necesitamos es un ordenador **o servidor** que se dedique a estas funciones de creación de usuarios y asignación de permisos. Es precisamente aquí en donde entra en juego **Active Directory**.

# **2.- Active Directory**

Active Directory es un directorio implementado en los sistemas operativos desde Windows 2000 Server. Son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos, principalmente LDAP, DNS, DHCP y Kerberos. ¿Qué es Active Directory y para qué sirve**?**<https://www.youtube.com/watch?v=n_DTMgjvxJg>

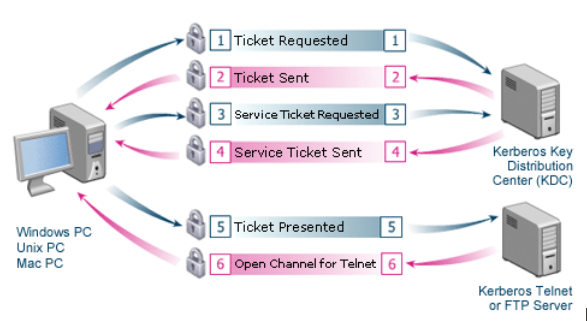
## **2.1.- Kerberos**

Este protocolo hace un servicio de **autenticación en las redes** de ordenadores.

Fue creado por el MIT (Instituto Tecnológico de Massachusetts), permite a **dos ordenadores** en una red insegura **demostrar su identidad** mutuamente de manera segura.

Esta es la base principal de un **servicio de directorios**, tener la autenticación y la autenticación se asegura de que exista una **relación de confianza entre los equipos y el dominio**.

Sus diseñadores se concentraron primeramente en un **modelo de cliente servidor** y brinda autenticación mutua.



Su funcionamiento es el siguiente:

* El **cliente** envía un **token** (un *Token* en la cabecera. Este Token no es más que una **firma** cifrada que **permite identificar al usuario**) a el servidor de autenticación
* Este responde al cliente y **una vez que ha respondido** se establece la **comunicación** entre ambos.
* Se **crea un ticket en el equipo cliente** hacia el Servicio del Servidor y este responde al cliente.

# **3.- El dominio**

**Un dominio en Active Directory** es un **conjunto de ordenadores** conectados a una red los cuales cuentan con un **equipo servidor** para **administrar** las cuentas de usuario y credenciales de la red. Hasta aquí es todo igual, lo que ocurre es que en una red no solamente podremos **tener un dominio, sino varios de ellos**

Para crear un dominio tenemos que realizar unas configuraciones previas en el equipo que será el **DC (Controlador de dominio)**:

Instalar y configurar Active Directory en Windows Server 2019 <https://www.youtube.com/watch?v=3uAKa4OQGuc>

<https://www.youtube.com/watch?v=321C85DLc7I>

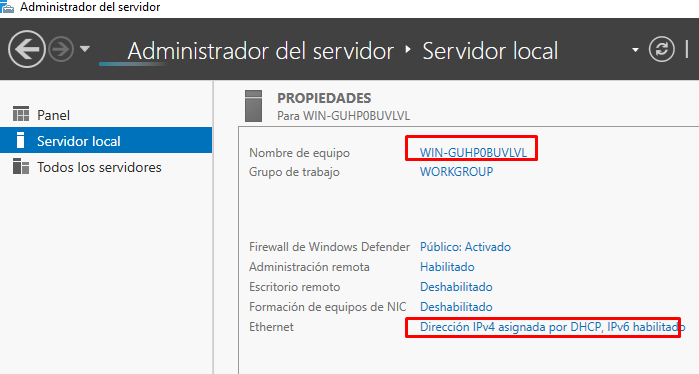
Crear Usuarios: <https://www.youtube.com/watch?v=dKD-dv5ugtE>

Y grupos locales: <https://www.youtube.com/watch?v=ruzEuNY6Vjo>

## **Pasos previos**:

## **1.- Poner nombre al equipo.**

Es importante que el **DC** tenga un **nombre** que pueda ser **reconocido** desde la **red local**, para poder **acceder** **a él** con facilidad. Después reiniciar la máquina.



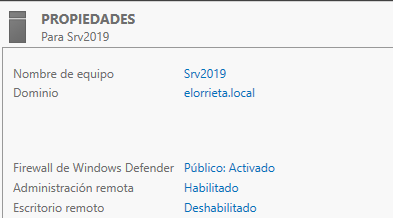
Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamenteInterfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

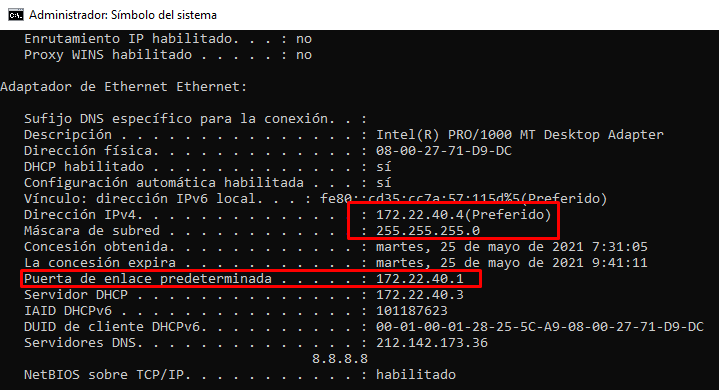
administrar, - > agregar roles y características

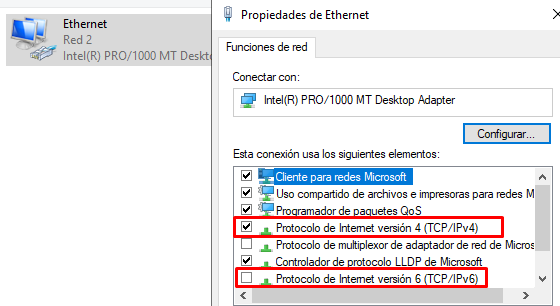
<https://blogdesistemas.com/crear-dominio-windows-server-2019/>



## **2.- Poner una IP que sea fácilmente reconocible dentro de la red local**.

Para ello primero comprobamos cual es la IP que nos da el DHCP del router. Es **aconsejable** **deshabilitar el protocolo IPv6**, ya que suele dar problemas con la resolución de nombres de dominio (DNS).

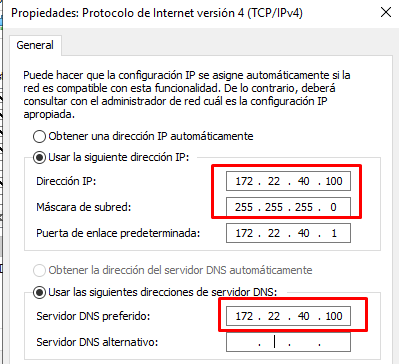


.

Como este **servidor va a ser un DC**, la **dirección** del **servidor DNS**, será la suya **es decir se** **apunta a sí mismo** y el será el que resuelva las peticiones de los clientes hacia los dominios. En el momento en que la guardemos y hallamos creado el Dominio veremos que se cambia automáticamente y aparece la dirección 127.0.0.1 que se llama **dirección IP de loopback (**es una **dirección** especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos**)**

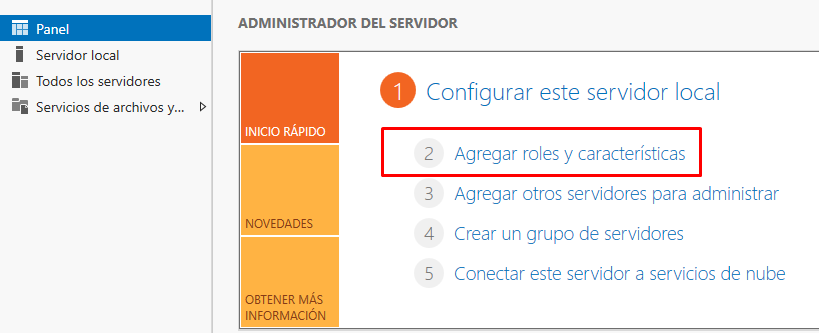
En este caso como nuestra red es **172.22.40.0/24** quiere decir que la máscara es **255.255.255.0** (Podemos tener 28 = 256-2 = 254 equipos)

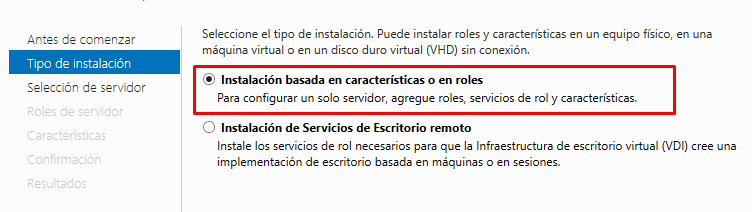
Ver propiedades de red: **Windows + R: ncpa.cpl**

****

## **3.- Creación del dominio**

Una vez que hemos realizado los pasos previos, es hora de **agregar el rol**

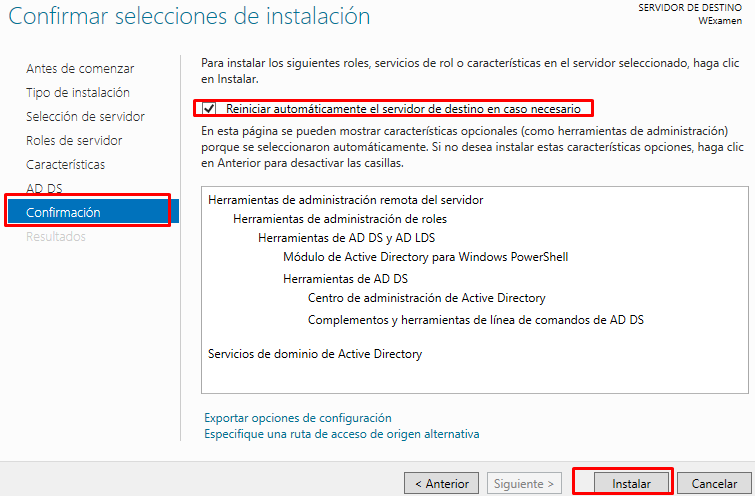
****

****

Seleccionar Servicios de dominio de Active directory:

****

Seleccionar Reiniciar automáticamente en caso necesario:

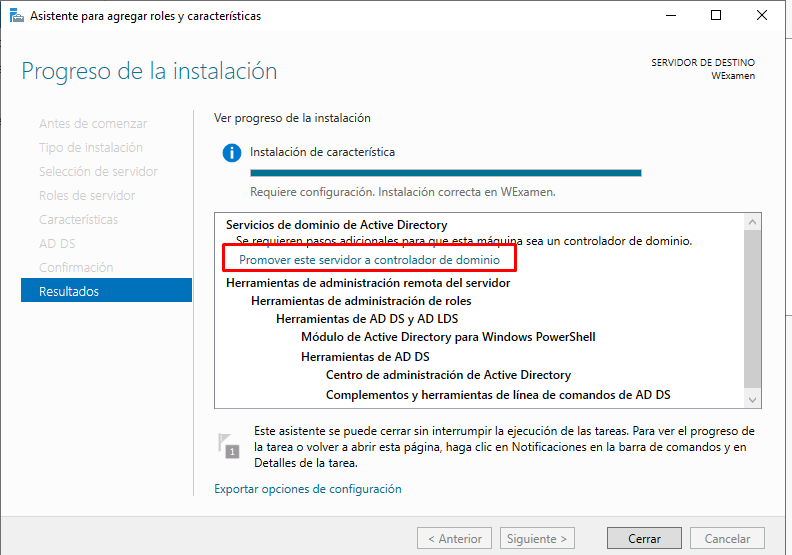
****

Instalar.

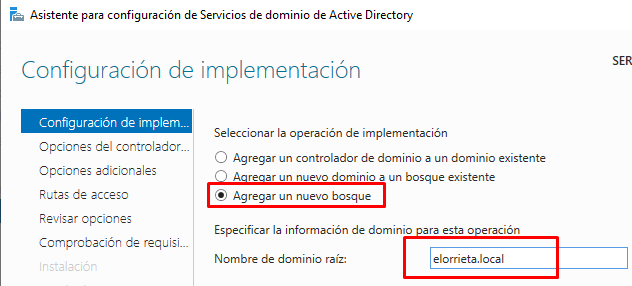
Una vez que se ha instalado el rol **promovemos** el servidor a **controlador de dominio,** desde el Server Manager, pulsaremos en Promocionar controlador de dominio.

[Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente](https://blogdesistemas.com/wp-content/uploads/2019/05/Ashampoo_Snap_04-December-2018_19h48m45s_046_.png)

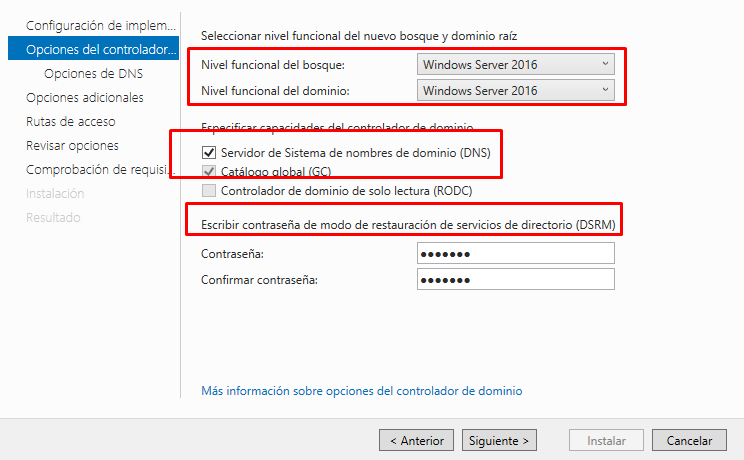
****

Creamos un **nuevo bosque** en el cual iremos **añadiendo los dominios** que vayamos **creando**

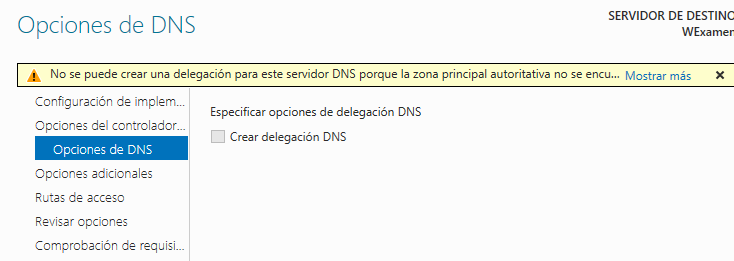
****

Un **nivel funcional** permite la activación de una o varias características para un dominio o un bosque. Hay disponibles varios niveles, sin embargo, cualquier modificación de nivel es irreversible (a continuación, es imposible disminuir un nivel).

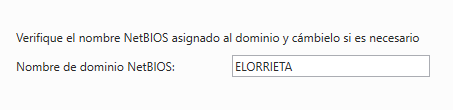
Esto tiene un impacto en el dominio o en el bosque, y principalmente en los controladores de dominio. Es preciso que **todos los controladores de dominio** ejecuten el **sistema operativo correspondiente al del nivel funcional** seleccionado. Si el nivel elegido es Windows Server 2016, los controladores de dominio deben ejecutar, **como mínimo**, Windows Server 2016

****

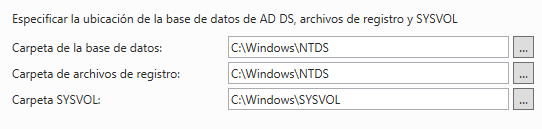
El siguiente paso **no lo tocamos** ya que **más adelante** configuraremos el Servicio **DNS:**



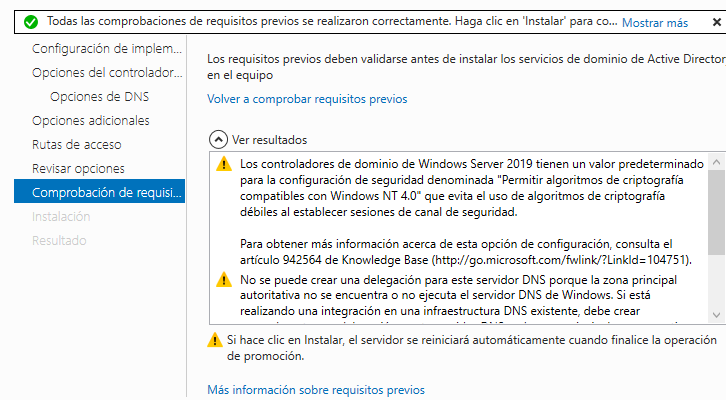
El nombre **NetBIOS** nos tiene que aparecer de forma **automática**. (**Nombre** de dominio **NetBIOS**: normalmente, el **nombre** de dominio **NetBIOS** es el subdominio del **nombre** de dominio DNS. Por ejemplo, si el **nombre** de dominio es **contoso**.com, el **nombre** de dominio **NetBIOS** es **contoso**.)



Nos muestra en que carpetas se guardarán las bases de datos, los scripts, etc.



Nos muestra el resultado con las **advertencias** de lo que **va a realizar** y pulsamos sobre **instalar**.

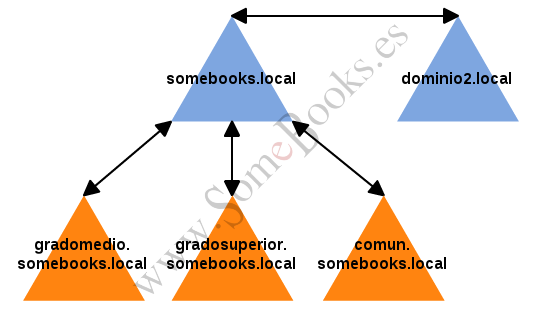


Como hemos marcado anteriormente que se reinicie en caso necesario, se reiniciará y nos mostrará el dominio creado



# **4.- El bosque**

Un bosque es una **colección de uno o varios dominios** de Active Directory, el **primero** **instalado** se denomina dominio **raíz**. Su nombre DNS (por ejemplo: **mcgrawhill.es**) se asignará también al bosque. Ejemplo **bosque**: **somebooks.local + dominio2.local** (Bosque contenedor lógico: abarca todos los dominios dentro de su ámbito.)



# **5.- Árbol**

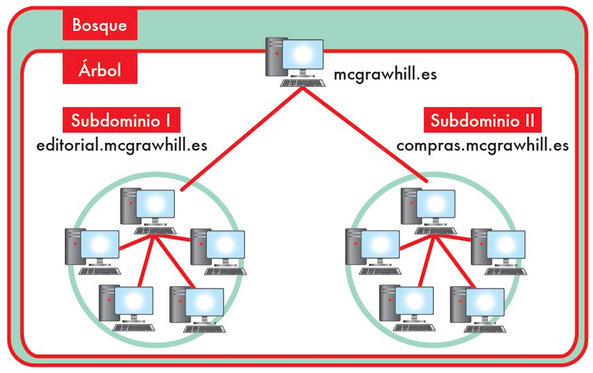
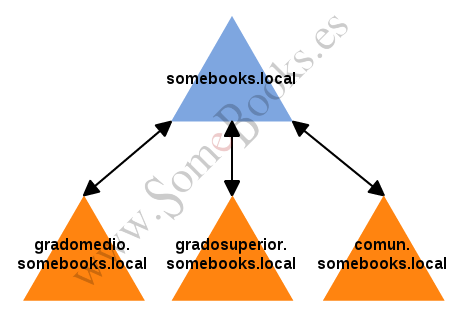
Un **árbol** es un conjunto de **dominios**, los cuales **dependen de una raíz común** y están organizados en una determinada jerarquía, también llamada **DNS común**.

El **dominio** representa un **límite de seguridad** donde se definen los usuarios.

Un **dominio** contiene, **al menos,** un **controlador de dominio**.

Un servidor con el rol de controlador de dominio tiene la responsabilidad de realizar entre otras tareas, la autentificación de las cuentas de usuario y de equipo. <http://somebooks.es/3-2-conceptos-basicos-en-una-estructura-de-directorio-activo/>

Ejemplo Árbol: editorial + compras



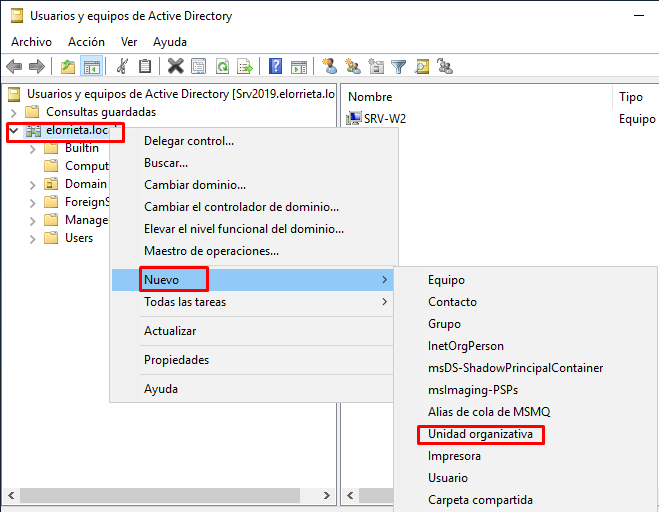
# **6.- Unidad Organizativa**

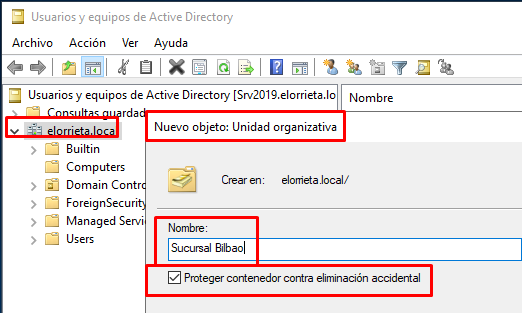
Una **unidad organizativa** (**OU**, ***Organizational Unit***) es un objeto de tipo **contenedor**. Permite construir una **jerarquía** en el directorio Active Directory. Los **objetos** (usuarios, equipos) se agrupan, de este modo, mediante la aplicación de **GPO** (*Group Policy Object* - **directiva de grupo**), facilitando su administración.

**Desde** Windows Server **2008** es posible **protegerse** contra el **borrado accidental de una OU**. Esta protección se activa por defecto tras la creación de una unidad organizativa. Es preciso **desmarcar** la opción **Proteger objeto contra eliminación accidental** en la pestaña **Objeto** de las propiedades para poder suprimir una OU.

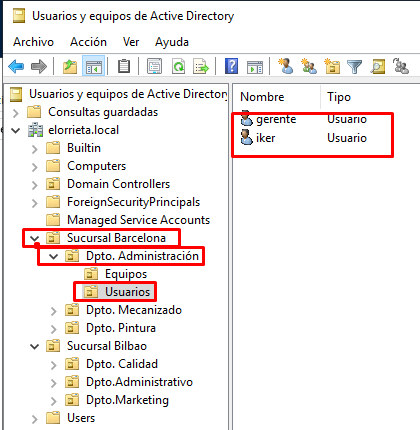
## **6.1.- Creación de Unidades Organizativas**

Vamos a Herramientas 🡪 Usuarios y equipos en AD:

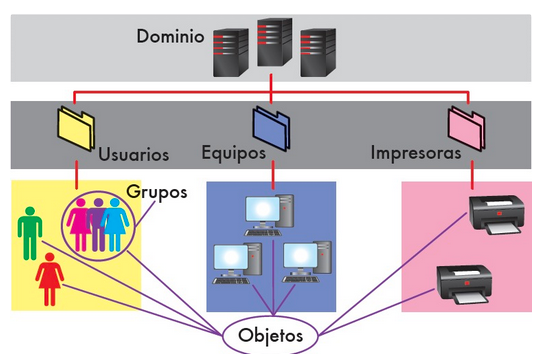
****

****

Dentro de cada sucursal, vamos creando los diferentes departamentos (otra nueva UO), y dentro de ellos la UO de equipos y usuarios:

****

# **7.- Los objetos**



Es posible encontrar distintos tipos de objeto en Active Directory:

* **Usuario**: permite autentificar los usuarios físicos que abren una sesión en el dominio. Se le asocia derechos y permisos a la cuenta con el objetivo de permitir el acceso a un recurso (carpeta compartida, buzón de correo electrónico, impresora…).
* **Grupo**: permite agrupar distintos objetos (usuarios, equipos) que deben tener un **acceso idéntico** (lectura, modificación, etc.) sobre un recurso (directorio compartido, etc.). La **administración** de permisos resulta mucho **más sencilla** utilizando grupos.
* **Equipo**: permite autentificar los **puestos físicos o virtuales** conectados al dominio. Es posible configurar la cuenta de equipo en una ACL (Lista Control Acceso), lo que permite el acceso a un recurso. Si la autentificación no puede llevarse a cabo, el inicio de sesión en el dominio es imposible.
* **Unidad organizativa**: **contenedor** que permite **organizar objetos** de manera jerárquica. Es posible **aplicarle** una o varias **directivas de grupo**. Además, este objeto ofrece la posibilidad de configurar una **delegación**.
* **Impresora**: es posible publicar una impresora compartida en Active Directory. Esta acción simplifica las etapas de búsqueda e instalación para el usuario.

# **8.- El catálogo global**

Un **servidor de catálogo global** es un controlador de dominio que posee una **copia** de los **atributos de todos los objetos de Active Directory** de su dominio. Por defecto, **solo ciertos atributos** se replican; sin embargo, puede incluir otros atributos en función de su versión.

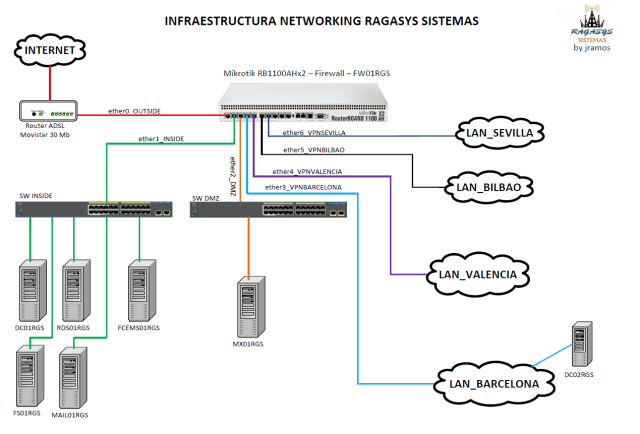
La consola **Esquema Active Directory** permite seleccionar los atributos que se deben replicar.

Tras la autentificación del usuario se consulta al servidor catálogo global con el objetivo de recuperar la lista de grupos universales a los que pertenece el usuario.

# **9.- Los sitios AD**

Para reducir el uso de líneas que vinculen las distintas entidades físicas (sede central y sedes remotas), los **dominios** se **dividen** en **sitios AD**. Estos representan generalmente la **topología física** de la empresa. (Sitio: normalmente los asociamos a sitios físicos, como pueden ser oficinas, sucursales, **delegaciones**… ubicadas en una ciudad.)

<https://blog.ragasys.es/organizacion-sitios-y-servicios-de-active-directory-sobre-ms-windows-server-2016>

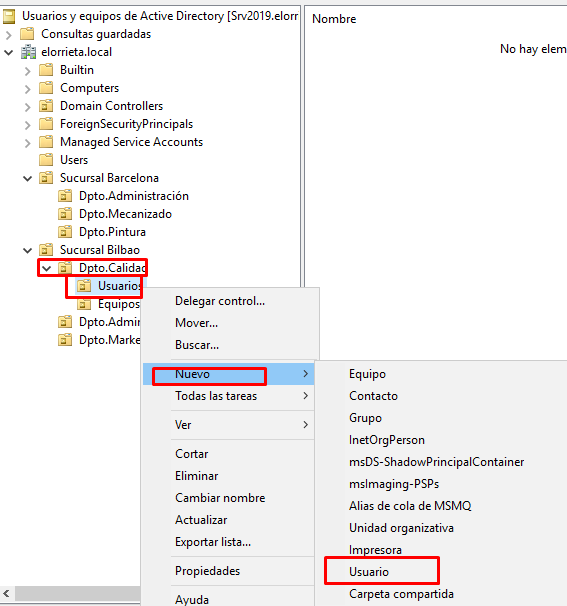


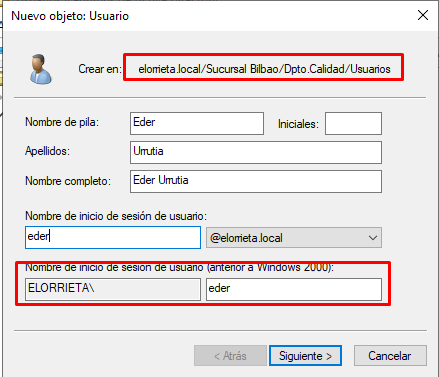
# **10.- Nivel funcional del dominio y del bosque**

Un **nivel funcional** permite la **activación** de una o **varias características para un dominio** o un bosque. Hay disponibles varios niveles, sin embargo, cualquier modificación de nivel es irreversible (a continuación, es imposible disminuir un nivel).

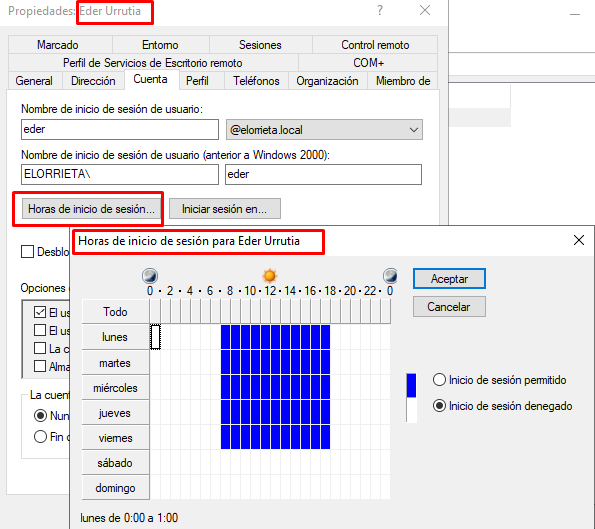
Esto tiene un impacto en el dominio o en el bosque, y principalmente en los controladores de dominio. Es preciso que **todos los controladores de dominio** ejecuten el **sistema operativo correspondiente al del nivel funcional** seleccionado. Si el nivel elegido es Windows Server 2016, los controladores de dominio deben ejecutar, **como mínimo**, Windows Server 2016.

# **11.- Creación de usuarios**

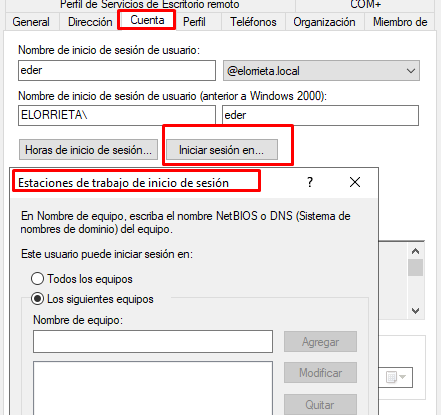




Una vez creado el usuario podemos **limitar** el **acceso** con su cuenta de usuario al dominio **solamente en el horario laboral** de la empresa: **Horas de inicio de sesión**



Podemos también **limitar el acceso a un equipo o a varios** del dominio

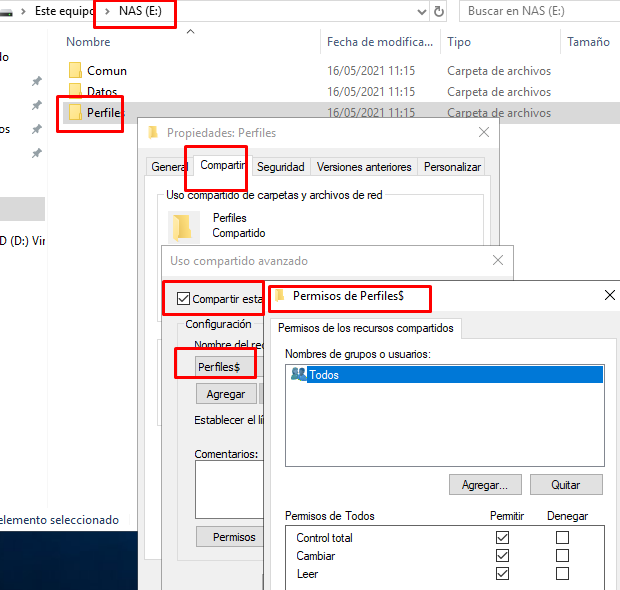


Dentro de la pestaña **perfiles** añadimos las rutas a la **carpeta perfiles**, al **script de inicio** de sesión y a la **carpeta particular** de datos. En **C:** creamos 3 carpetas: Comun, Datos y Perfiles

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente





Sobre **Perfiles**, botón derecho **Propiedades**: pestaña **Compartir**

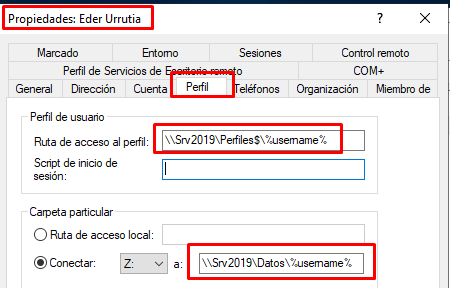
**Uso compartido avanzado**

Marcar: compartir esta carpeta

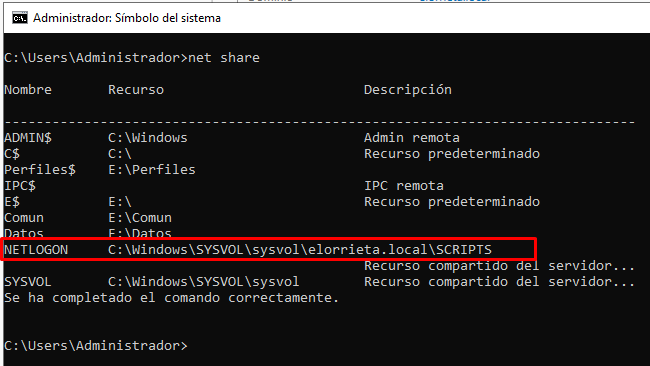
Permisos: Dar a Todos, todos los permisos

Los **perfiles de usuarios móviles** redireccionan los perfiles de usuarios a un recurso compartido de archivos para que los **usuarios** reciban la **misma configuración del sistema operativo y la aplicación** en **varios equipos**. Es decir, el usuario dispondrá de su **perfil** (documentos, favoritos de Internet, fondo de escritorio, etc.) con **independencia del equipo cliente que esté utilizando** en cada momento.

Desde Usuarios y equipos de AD ir al usuario, propiedades, pestaña Perfil:



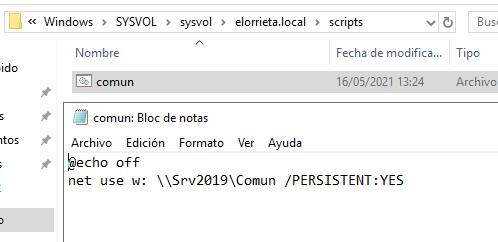
El **script** de **inicio de sesión** lo tenemos que colocar **en su ruta dentro del DC** que es el elemento compartido NETLOGON. Ejecutas desde CMD el comando: **net share**, y así ves la **carpeta** donde debes meter el **script**



**Dentro de esa ruta** creamos el fichero **.bat** (script) que se encargará de **crear** las **unidades de red** que necesitemos <https://www.pantallazos.es/2019/04/windows-cmd-conectar-unidades-red-NET-USE.html>

**Vamos a la carpeta: C:\Windows\SYSVOL\sysvol\elorrieta.local\scripts 🡪 creas un bloc de notas con este código le das a guardar como, Tipo: todos los archivos**

**Comando: NET USE** y, seguidamente la **letra de unidad** que queremos asignar a la **carpeta compartida**.  
  
A continuación, definiremos la **ruta y el nombre de la carpeta de red** y podemos usar el modificador **/PERSISTENT** : Eligiendo el valor **YES**, conseguiremos restaurar automáticamente las conexiones creadas en el siguiente inicio de sesión (es decir, una vez creada se mantiene), si definimos el modificador  **PERSISTENT**con el valor **NO** limitaremos la vida de la nueva conexión de red a la sesión actual.  
  
**NET USE f: \\SRVDC\Datos /PERSISTENT:YES**



<https://somebooks.es/crear-carpetas-compartidas-para-un-grupo-de-usuarios-en-windows-server-2019/>

# **12.- Unir equipos al dominio**

Arrancamos otra MV, en este caso Windows 10, en configuración de red, la misma que el servidor (Puente o RED NAT). Para **unir un equipo al dominio** debemos tener en **cuenta el que el DNS del equipo que vamos a unir** al dominio **tiene que ser el del controlador del dominio (DC)**.

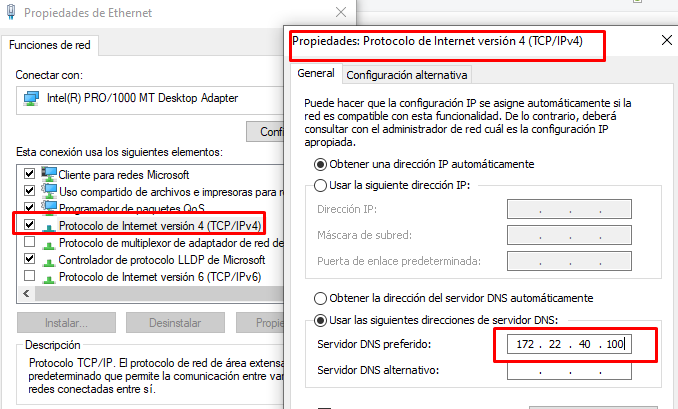
Si el equipo cliente está recibiendo la IP por DHCP y este servicio lo está dando el DC, no hará falta modificar los DNS, porque por regla general, manda como DNS la IP del DC

Por el contrario, si el servicio DHCP lo estuviera recibiendo, por ejemplo, del router y este tiene configurado para el despliegue otro DNS que no sea el del DC, habría que poner de forma manual los DNS del DC para poder unir el equipo al dominio.

Para cambiar el DNS, ver las propiedades de la red, puedes:

1-Ejecutar: Windows+R: ncpa.cpl 🡪Protocolo Ipv4🡪 Propiedades

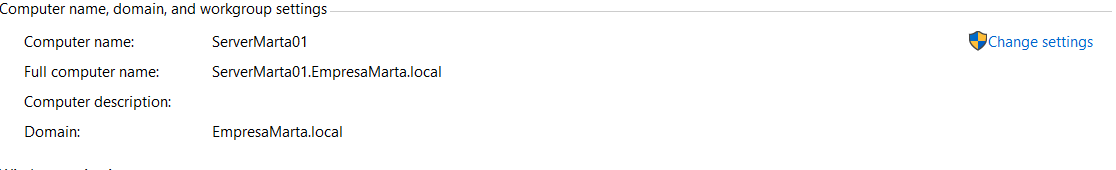
2-Panel de control: Control Panel\Network and Internet\Network and Sharing Center 🡪 conexión Ethernet

 Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

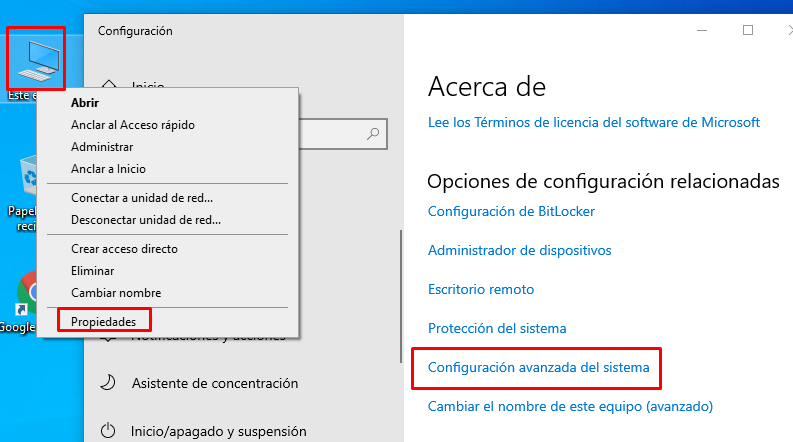
Cuando ya tenemos definidos los DNS, vamos a cambiar el dominio y meterlo en el dominio creado. Lo hacemos desde:

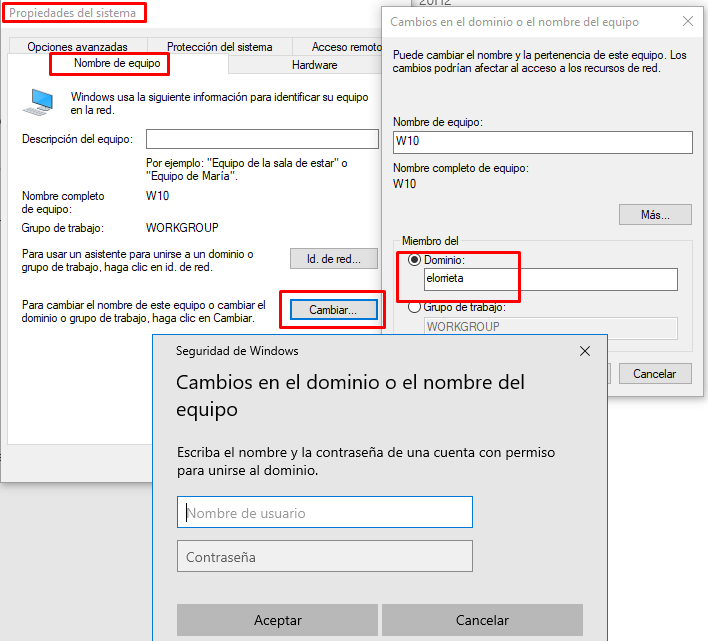
1-Explorador de carpetas: This PC: bton derecho propiedades 🡪 Change settings:



O

2-“**Este equipo** ……….”





Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Te pide reiniciar el equipo.

Cuidado con que equipos has permitido al usuario: Todos o solo 1 en concreto.

Nos valdría para unir al dominio, si está bien configurado el servicio DNS, poner únicamente el nombre **NETBIOS** del dominio. En caso de que **nos diera error**, pondríamos el **nombre completo del dominio** (en este caso elorrieta.local)

Una **vez unido el equipo al dominio**, entramos con el **usuario** que hemos creado y comprobamos que se le generan las unidades de red que hemos planificado en la pestaña de perfiles:

Interfaz de usuario gráfica, Sitio web

Descripción generada automáticamente

