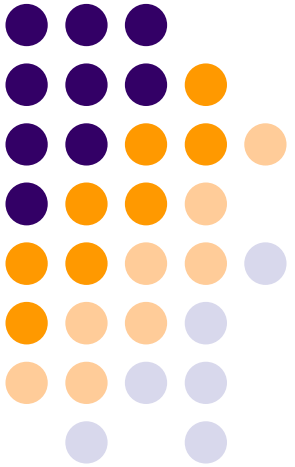
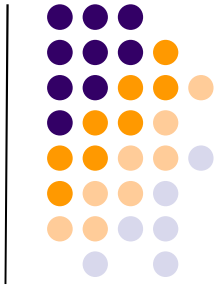
Unidad 4

Gestión de recursos compartidos en Active Directory

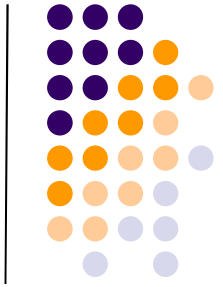


UNIDAD 4
Gestión de recursos compartidos en Active Directory



1. Carpetas compartidas
2. Permisos
3. Perfiles móviles

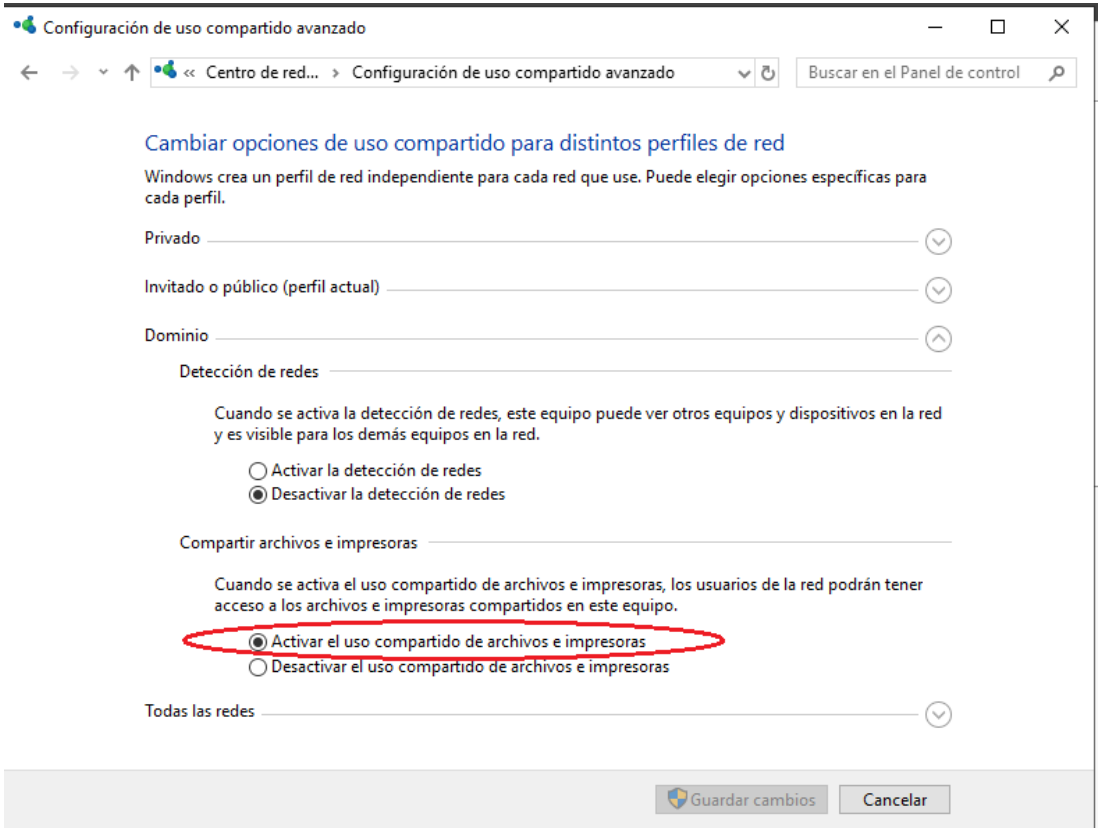
1. Carpetas compartidas



- Recursos compartidos
  - Los recursos compartidos son objetos que pueden utilizarse desde otras máquinas de la red
  - En un equipo se puede compartir:
    - **Capacidad de procesamiento** ➔ equipos que ofrecen sus recursos de procesamiento (CPU y memoria) a otros.
    - **Archivos y directorios** ➔ para almacenar y ofrecer información a otros usuarios.
    - **Periféricos** ➔ impresoras, escáneres, plóteres, etc.
  - Los principales recursos que se comparten en Windows son carpetas e impresoras, usando el protocolo **CIFS** (*Common Internet File System*), antiguo SMB (*Server Message Block*)

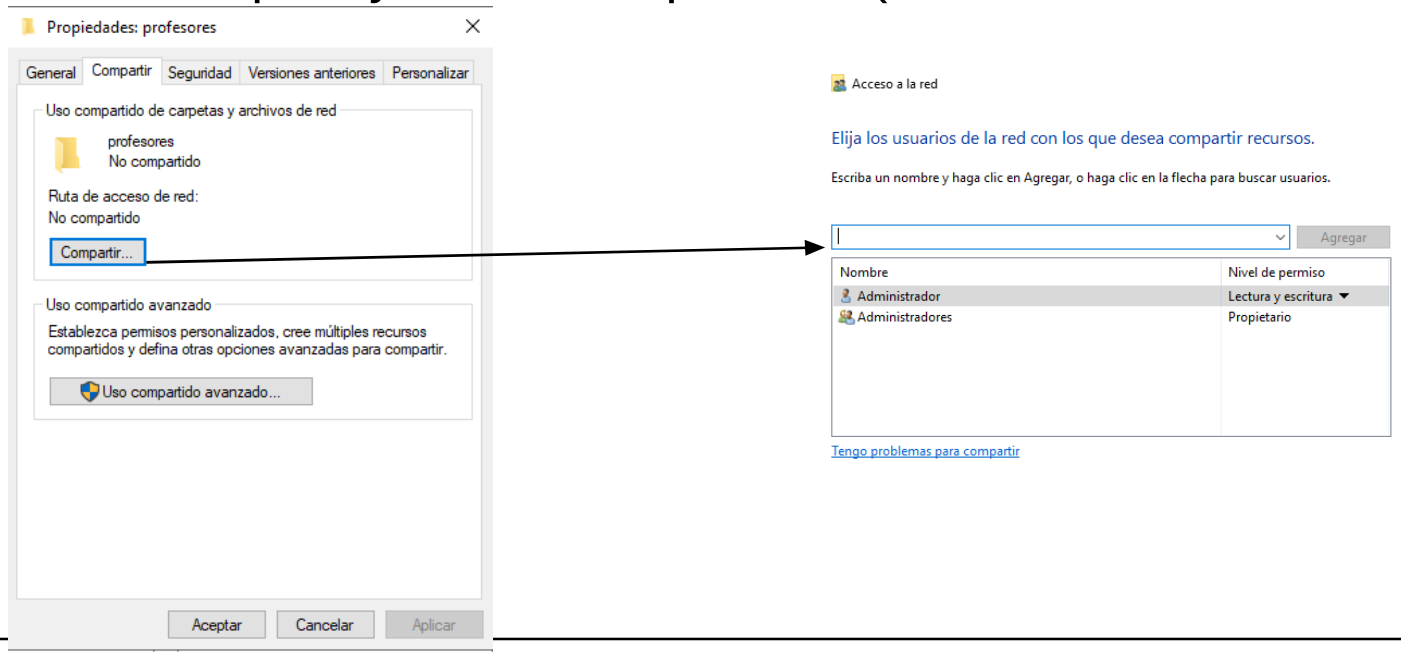
1. Carpetas compartidas

- Compartir carpetas
  - Previamente activar el *Uso compartido de archivos e impresoras* en el *Centro de redes y recursos compartidos*



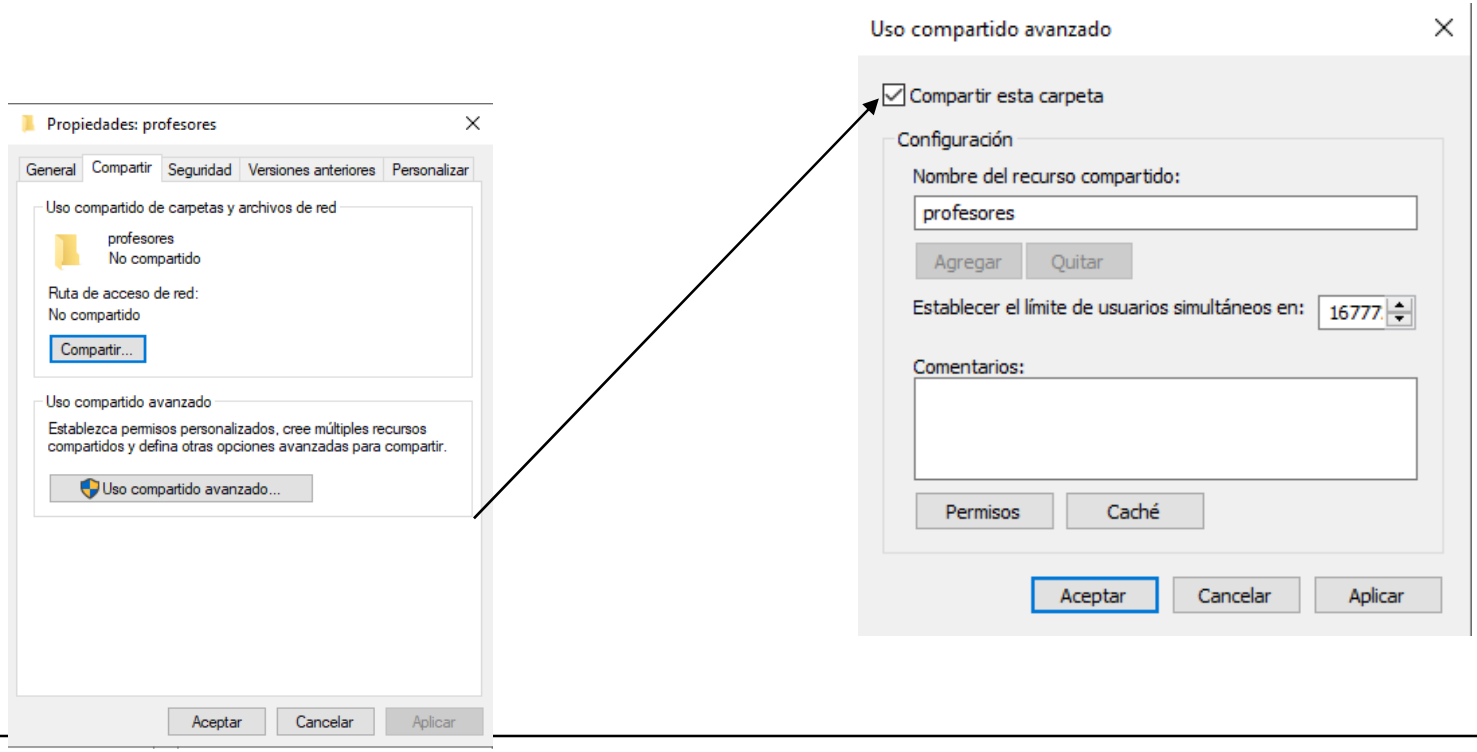
1. Carpetas compartidas

- Compartir carpetas
  - Forma simple
    - Seleccionaremos las *Propiedades* de la carpeta, pestaña *Compartir* y pulsamos en *Compartir.*
    - Seleccionaremos los usuarios y/o grupos con los que compartir la carpeta y el nivel de permiso (*Lectura* o *Lectura-Escritura*).

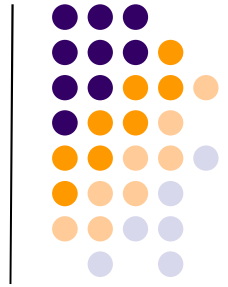


1. Carpetas compartidas

- Compartir carpetas
  - Uso compartido avanzado
    - Para tener más control a la hora de compartir una carpeta podemos seleccionar el ***Uso compartido avanzado***.

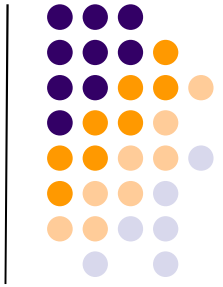


1. Carpetas compartidas



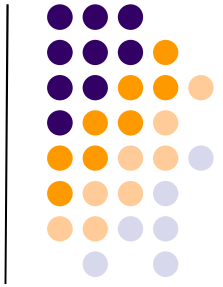
- Compartir carpetas
  - Uso compartido avanzado
    - Es posible establecer un nombre diferente para cuando el recurso compartido se visualice a través de la red.
    - Se pueden *Agregar* varios nombres diferentes y personalizar el acceso a cada recurso (todos apuntan a la misma carpeta).
    - El número de usuarios que pueden usar la carpeta de forma concurrente (a la vez).
    - Agregar o eliminar **permisos** a usuarios y grupos (por defecto otorga permiso de *Lectura* sobre la carpeta a *Todos* los usuarios del dominio).
    - Establecer el uso de memoria caché (para equipos sin conexión de red).

1. Carpetas compartidas



- Acceso a los recursos compartidos
  - Desde el entorno gráfico a través del explorador de archivos o a través de su **UNC** (Universal Naming Convention): **\\nombre_equipo\nombre_recurso**
- Ocultar carpeta en la red
  - Si queremos que una carpeta compartida no sea visible en la red le asignamos un nombre y al final le añadimos **$**
  - Para acceder a ella debemos conocer su ruta
    - Inicio, Ejecutar ➔ \\nombre_equipo\nombre_recurso$

1. Carpetas compartidas



- Control de los recursos compartidos
  - Las carpetas que Windows Server comparte tras su instalación se gestionan desde ***Administración de equipos*** > *Carpetas compartidas*
    - Opciones
      - Recursos compartidos
        - Carpetas compartidas en el servidor. Haciendo doble clic se accede a sus propiedades
      - Sesiones
        - Muestra las sesiones abiertas (visualiza los usuarios que están conectados actualmente)
      - Archivos abiertos
        - Para ver los usuarios que están accediendo a algún recurso en este momento

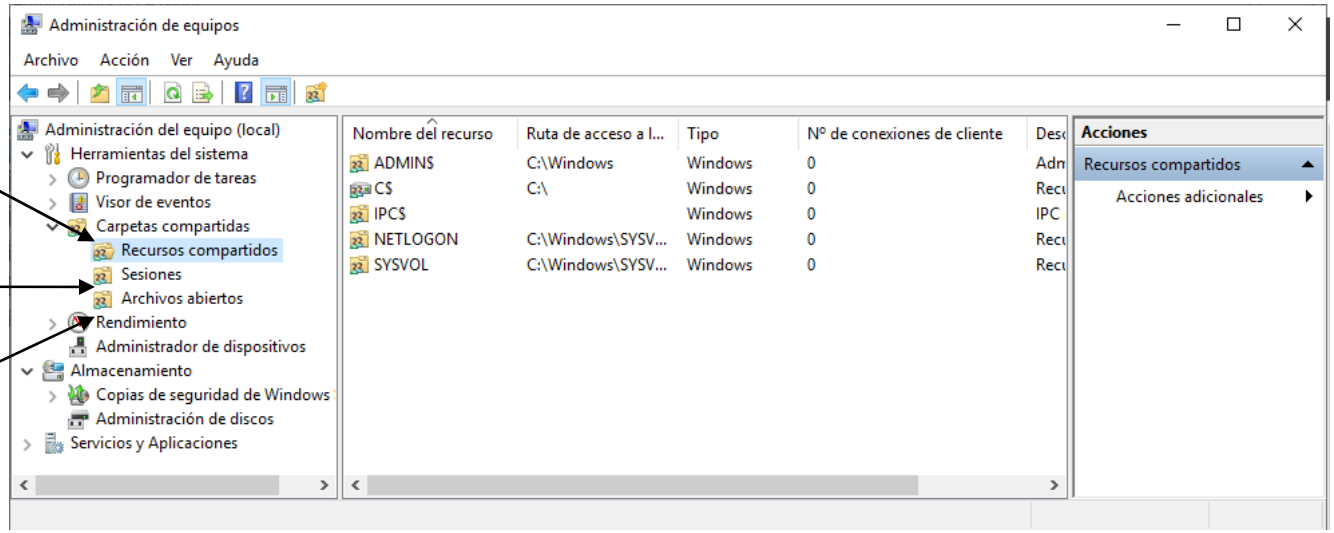
1. Carpetas compartidas

- Control de los recursos compartidos

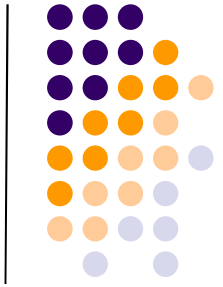
Carpetas compartidas en el servidor

Sesiones abiertas

Usuarios que están accediendo a algún recurso



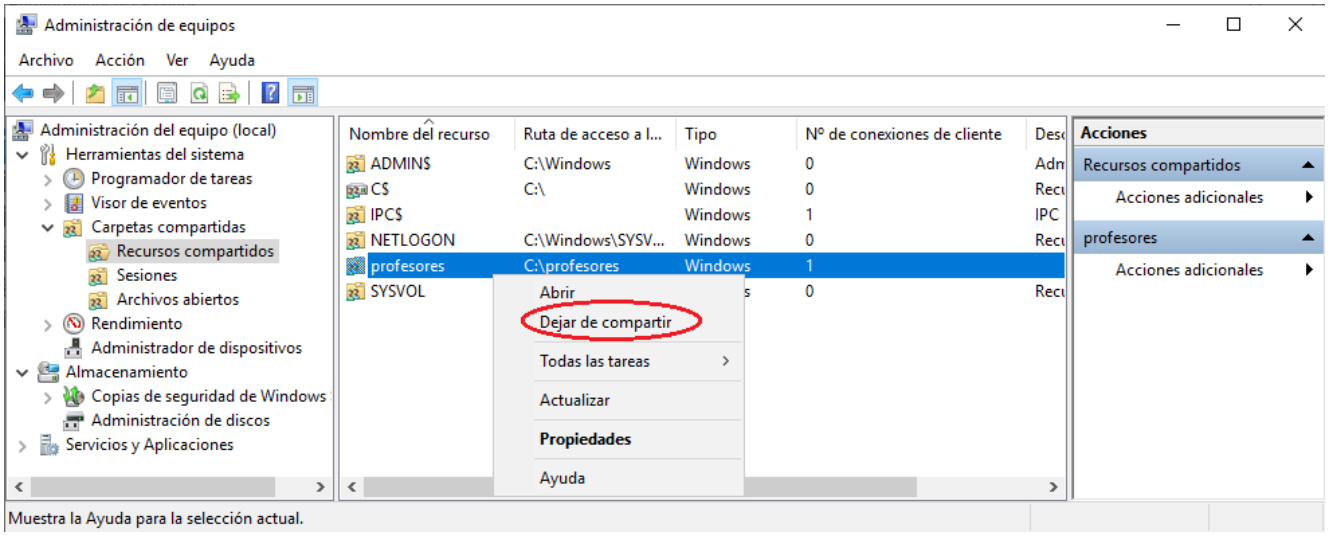
1. Carpetas compartidas



- Recursos compartidos administrativos
  - Son recursos especiales creados automáticamente por el SO para tareas administrativas (no recomendable su modificación)
    - ADMIN$ ➔ se usa para administrar una estación de trabajo remota
    - IPC$ ➔ sirve para la comunicación entre procesos. Se usa para consultar un recurso compartido
    - NETLOGON ➔ contiene programas que se ejecutarán en ordenadores remotos
    - PRINT$ ➔ utilizado para la administración remota de impresoras
    - FAX$ ➔ utilizado para la administración remota de fax
    - Unidad_logica_$ ➔ para acceder en modo remoto a una partición raíz
    - SYSVOL ➔ almacena los archivos públicos de un dominio, que se replican en cada controlador de dominio.

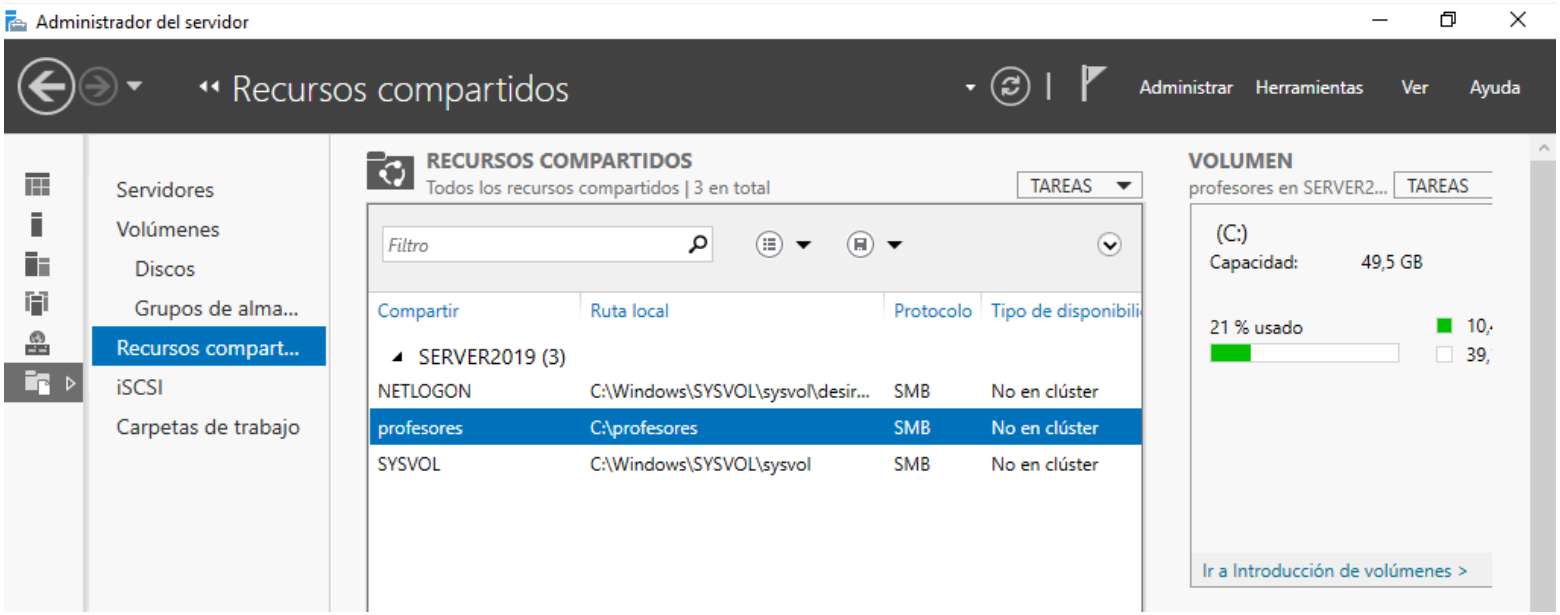
1. Carpetas compartidas

- Eliminar recursos compartidos
  - Para dejar de compartir una carpeta seleccionamos sus *Propiedades* y en la pestaña *Compartir seleccionamos Uso compartido avanzado* y desmarcamos la casilla *Compartir esta carpeta*
  - O desde *Administración de equipos*:

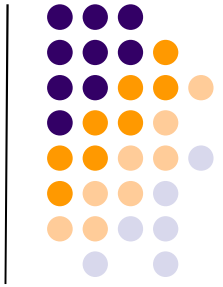


1. Carpetas compartidas

- Servicios de archivo y de almacenamiento
  - Otra forma de administrar carpetas compartidas en Windows Server es desde la opción *Recursos compartidos* del complemento *Servicios de archivo y de almacenamiento*

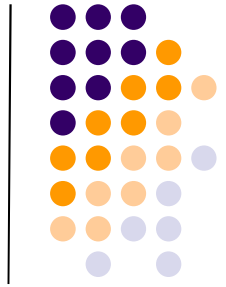


1. Carpetas compartidas



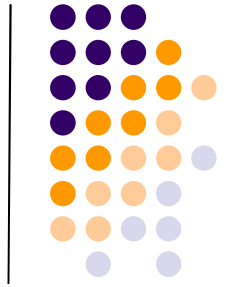
- Compartir carpetas en los clientes del dominio
  - También es posible compartir recursos locales de un equipo cliente que esté integrado en el dominio.
  - La diferencia es que este recurso no será controlado directamente por el *Administrador del dominio* de forma centralizada.
  - Podremos compartir la carpeta con otros usuarios o grupos locales del dominio al que pertenecemos o de otro dominio con el que haya establecidas relaciones de confianza.

2. Permisos



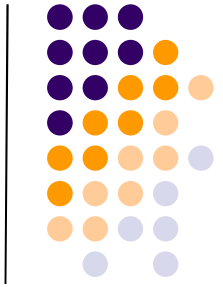
- Permisos en Windows
  - Windows diferencia entre **permisos de archivo** y **permisos de carpeta compartida.**
  - Los permisos de archivo se aplican siempre que se accede a un archivo o a una carpeta.
  - Los permisos de carpeta compartida solo se aplican cuando se accede a la carpeta a través de la red ➔ no afectan a los usuarios que inician sesión de forma local o mediante *Escritorio remoto.*
  - Estos dos tipos de permisos son independientes (uno no modifica al otro).

2. Permisos



- Permisos en Windows
  - Los permisos de archivo y de carpeta compartida son acumulativos.
  - En caso de conflicto, prevalece el permiso más restrictivo.
  - Los permisos sobre un objeto se pueden *Permitir* o *Denegar.*
  - El conjunto de todos los permisos establecidos sobre un recurso se denomina **permiso efectivo.**
  - Cuando un usuario pertenece a varios grupos se le aplica la suma de todos los permisos *Permitir* de esos grupos.
  - Si en algún caso tiene un permiso *Denegar* sobre un objeto, este prevalece sobre el resto.

2. Permisos

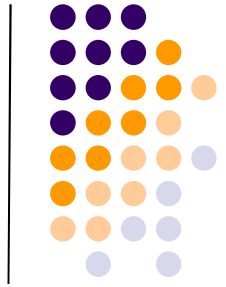


- Permisos en Windows
  - Windows Server utiliza listas de control de acceso (ACL) para controlar los permisos de un objeto.
    - Todos los objetos tienen una ACL, las cuales controlan lo que los usuarios pueden hacer o no con ellos
    - Una ACL contiene varias entradas de control de acceso (ACE), que indican qué permisos tendrá cada usuario o grupo
    - Cada ACE contiene un par (usuario-grupo/permiso) que indica el tipo de acceso determinado para el usuario o grupo
      - Ejemplo: ACL del archivo *base_datos.mdb*

alumnos/lectura, *profesores/escritura*, *administrador/control total*

ACE ACE ACE

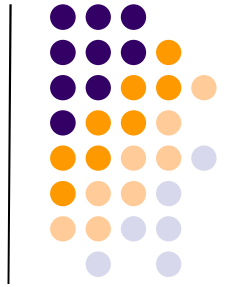
2. Permisos



- Permisos de carpeta compartida

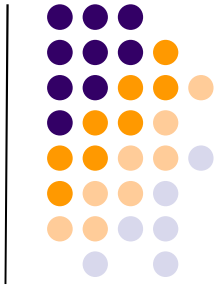
Tipo permiso	Descripción
Leer	Los usuarios pueden ver el contenido de una carpeta y abrir archivos y carpetas
Cambiar	Otorga todos los privilegios del permiso de *Lectura* y además permite a los usuarios cambiar el contenido de archivos y carpetas existentes así como eliminar y crear archivos y subcarpetas
Control total	Otorga todos los privilegios de *Cambiar* además de la capacidad de obtener la propiedad y modificar los permisos. Este permiso se le otorga automáticamente al creador o al propietario del archivo y a los miembros del grupo Administradores

2. Permisos



- Permisos de carpeta compartida
  - Por defecto, todos los archivos y subcarpetas heredan los permisos que tiene la carpeta en la que se encuentran.
  - Una **copia** de una carpeta compartida **no** conserva su estado de compartida.
  - El estado de carpeta compartida también se **cancela** al **mover** la carpeta o al **renombrarla.**

2. Permisos

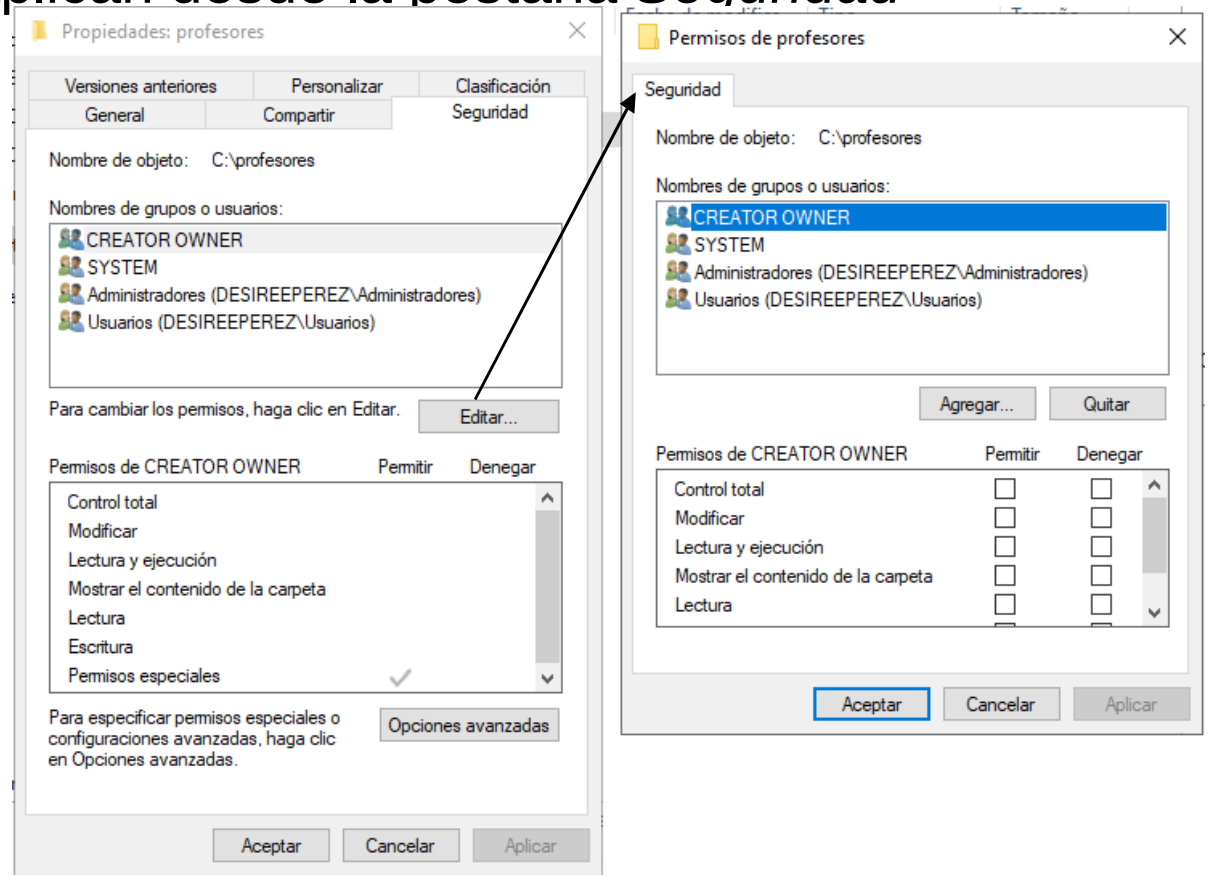


- Permisos de archivo estándar

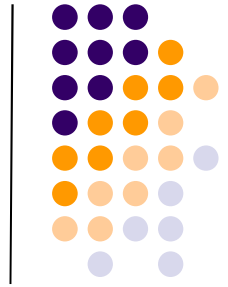
Tipo permiso	Descripción
Mostrar el contenido de la carpeta	Permite mostrar los archivos y subcarpetas que contiene una carpeta
Lectura	Permite mostrar los archivos y subcarpetas que contiene la carpeta junto con sus atributos, propietario y permisos; visualizar el contenido y ver los atributos en caso de archivo
Escritura	Permite crear nuevos archivos y subcarpetas; sobreescribir y cambiar los atributos en caso de archivo
Lectura y ejecución	Permite entrar en la carpeta y sus subcarpetas, además de lo permitido en *Lectura*; leer los archivos y ejecutarlos en caso de archivos ejecutables
Modificar	Permite borrar la carpeta además de todo lo concedido por *Lectura*, *Escritura* y *Mostrar contenido*; modificar y borrar en caso de archivos
Control total	Permite realizar cualquier operación sobre el archivo o carpeta, incluso cambiar sus permisos y propietario

2. Permisos

- Permisos de archivo estándar
  - Se aplican desde la pestaña *Seguridad*



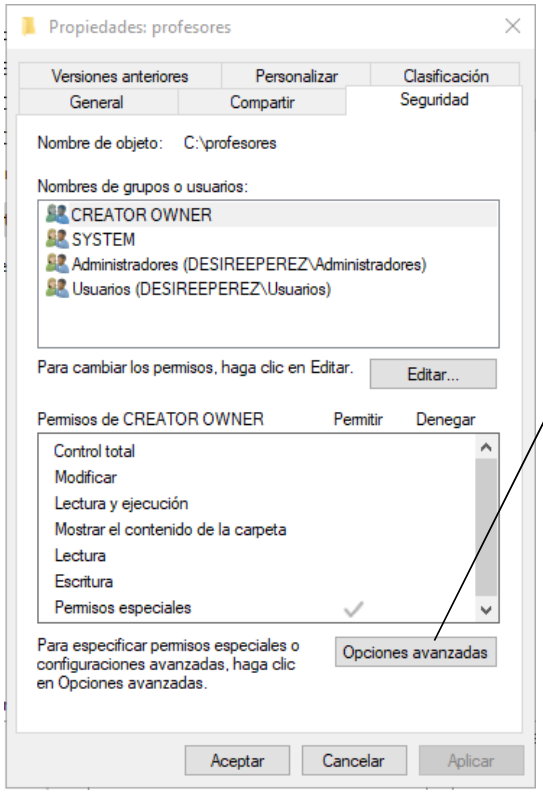
2. Permisos

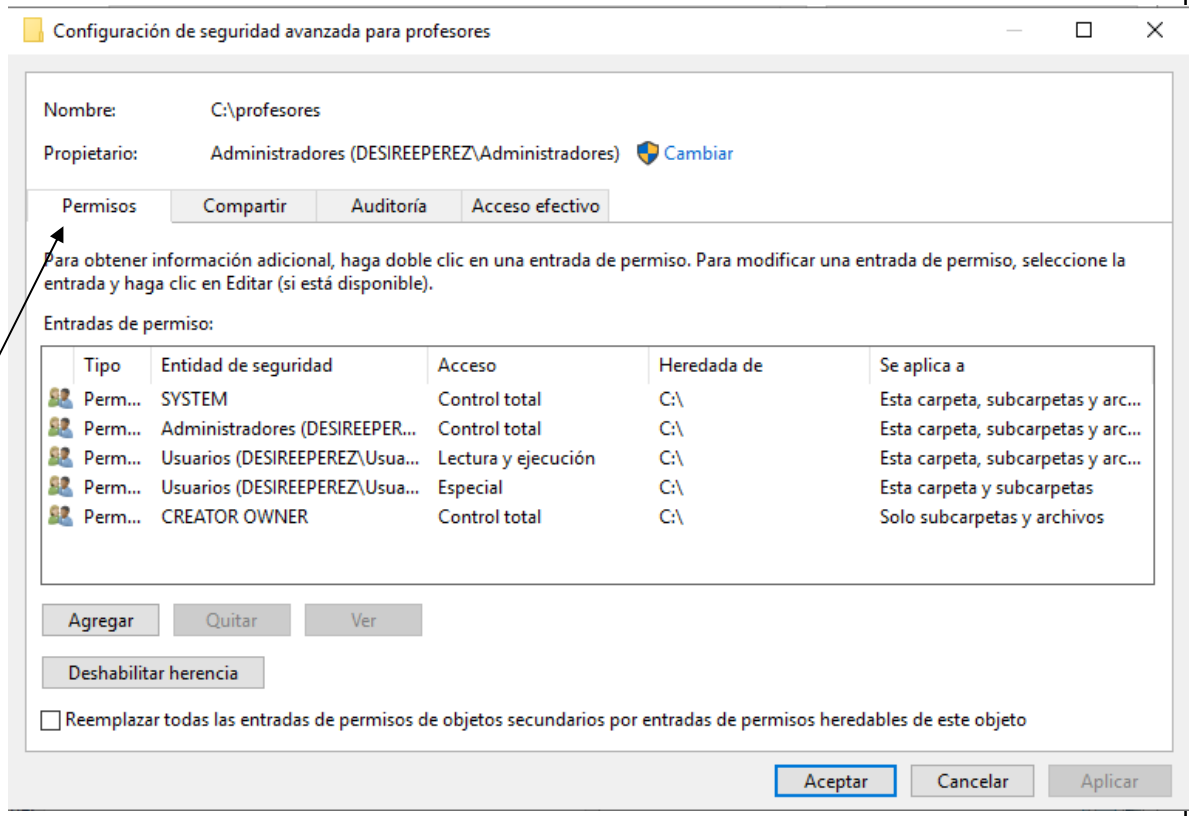


- Permisos especiales
  - En ocasiones, los permisos de archivo estándar pueden no ser suficientes cuando trabajamos en redes grandes
  - Los **permisos especiales** permiten concretar aún más lo que puede o no hacer un usuario o un grupo sobre un recurso
  - Se accede a ellos desde la pestaña *Seguridad*, *Opciones avanzadas*, de las propiedades del recurso
  - Existen 14 permisos especiales
  - Cada uno de los permisos de archivo estándar está asociado a un subconjunto de los 14 permisos especiales

2. Permisos

- Permisos especiales
  - Configuración de seguridad avanzada



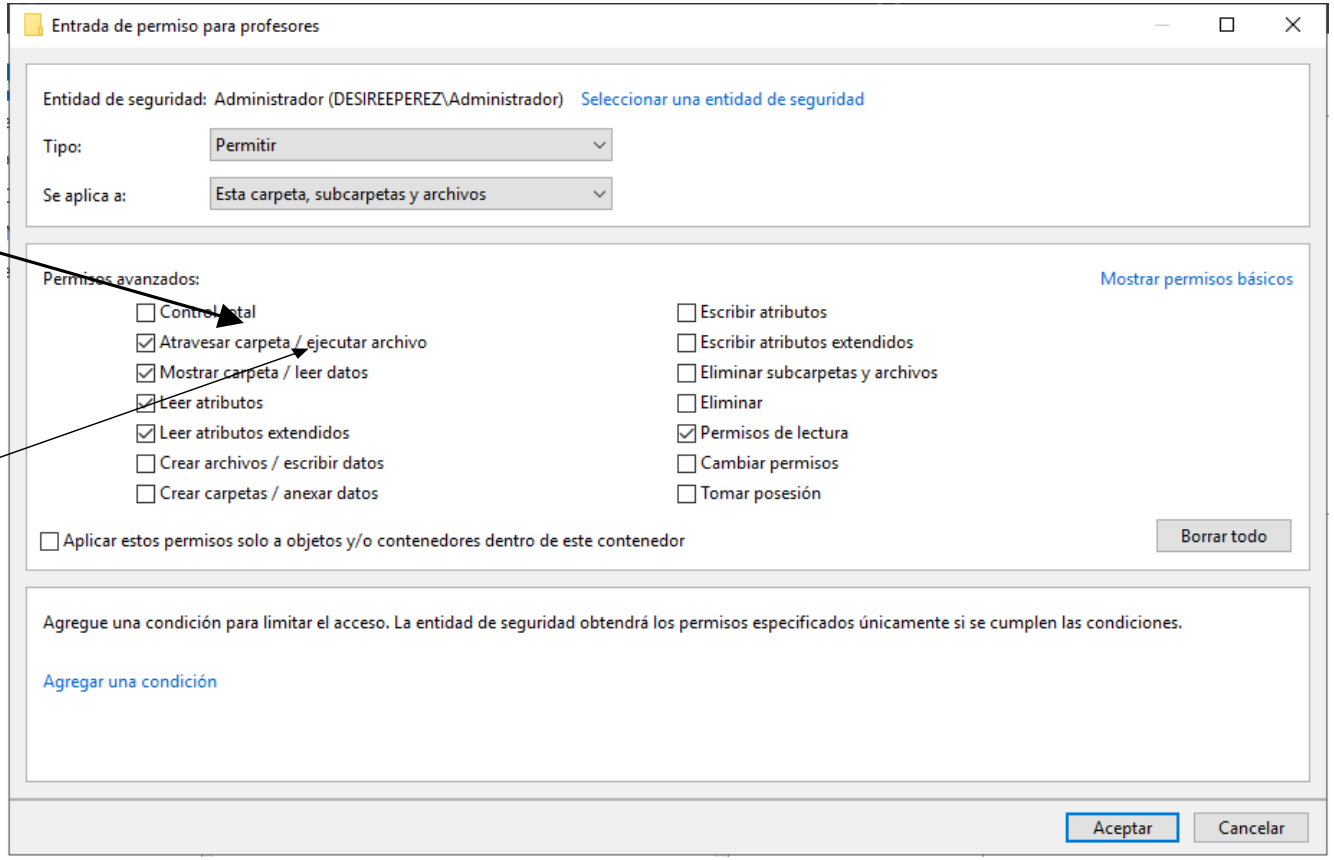


2. Permisos

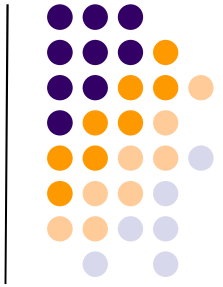
- Permisos especiales

Afectan a carpetas

Afectan a archivos



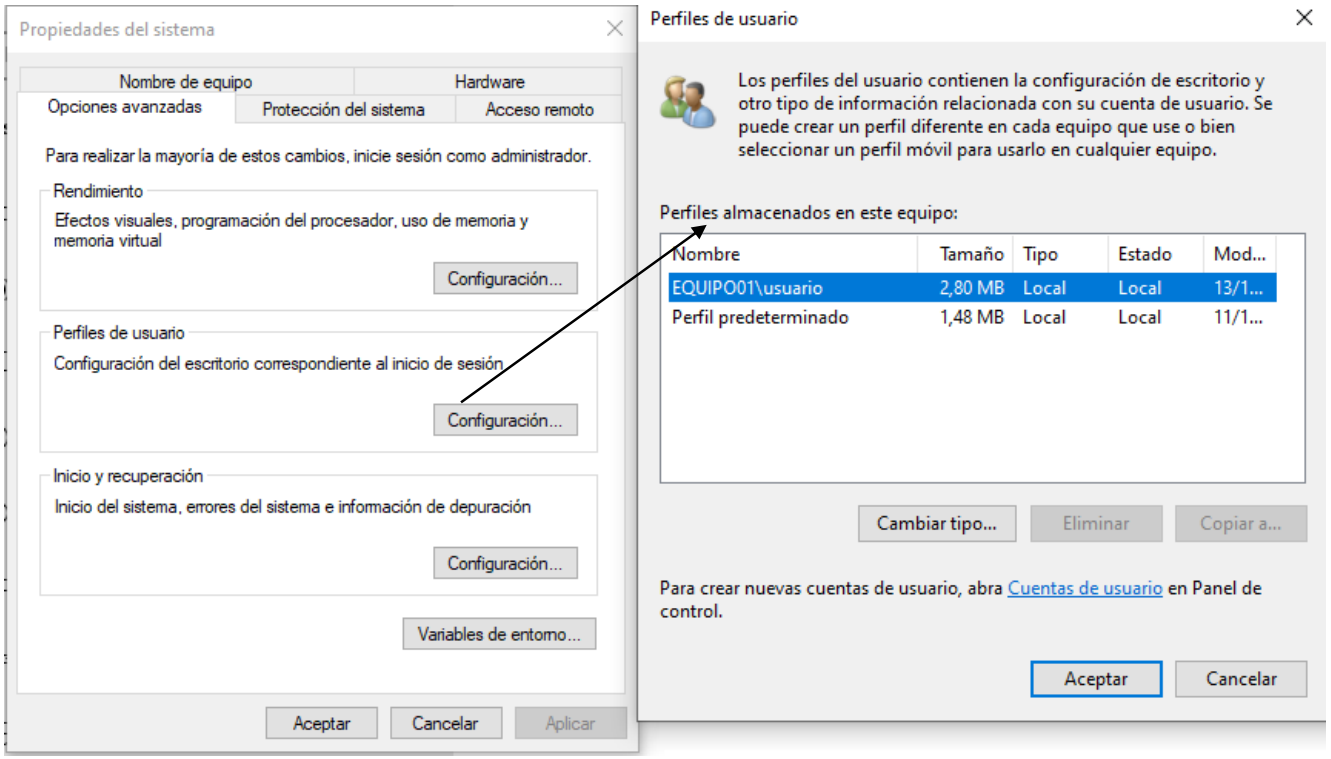
3. Perfiles móviles



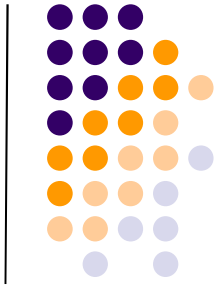
- Perfiles locales de usuario
  - Cada vez que se da de alta a un usuario local en un ordenador cliente e inicia sesión al menos una vez, el sistema crea una configuración personal específica para dicho usuario
  - Esta configuración se guarda en la carpeta ***Usuarios***
  - Dentro de *Usuarios* se generará una subcarpeta por cada usuario del equipo. Cada una contiene a su vez una serie de subcarpetas con opciones de inicio de sesión personalizadas para cada usuario: configuración del escritorio, favoritos del explorador, carpeta *Mis documentos*, etc.
  - Todo lo que el usuario modifique mientras trabaja no afectará al resto de usuarios del equipo
  - La carpeta ***Default*** contiene el perfil del usuario que se conecta por primera vez o aquel usuario que no tiene un perfil asignado.

3. Perfiles móviles

- Perfiles locales de usuario
  - En Windows 10, los perfiles de usuario se gestionan desde *Panel de Control* >Sistema y Seguridad >*Sistema*, *Configuración avanzada del sistema*, *Perfiles de usuario*, *Configuración*

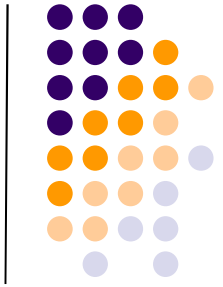


3. Perfiles móviles



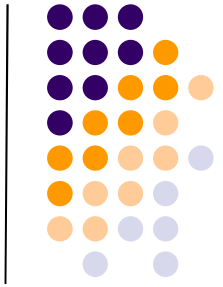
- Perfiles móviles de usuario
  - Cuando iniciemos sesión con un usuario global del dominio también se creará un perfil de usuario dentro del equipo local, generándose una carpeta con un nombre tipo: *nombre_usuario_dominio.nombre_NetBios_dominio*
  - Todos estos perfiles siempre serán perfiles locales del equipo en el que estamos trabajando
  - Otra forma de gestionar los perfiles de usuario es desde el controlador de dominio ➔ en este caso tendremos **perfiles móviles de usuario**
    - Permiten a los usuarios desplazarse de un equipo a otro dentro de la red y mantener sus opciones de configuración personalizadas en todos esos equipos

3. Perfiles móviles



- Perfiles móviles de usuario
  - Con un perfil móvil, el usuario podrá iniciar sesión en un equipo, trabajar en él y cerrar la sesión cuando haya finalizado su tarea ⇨ en ese momento, las modificaciones que haya hecho sobre su perfil se copiarán al servidor
  - Cuando vuelva a iniciar sesión en otro equipo, la información del perfil se copiará en dicho equipo
  - De esta forma, podrá trabajar desde cualquier equipo teniendo siempre la misma configuración de escritorio, programas, opciones personalizadas, etc.
  - Los cambios se guardan en el archivo **ntuser.dat**

3. Perfiles móviles



- Perfiles obligatorios
  - Similar al perfil móvil, pero obliga a que los usuarios trabajen siempre en un entorno que no se modifica.
  - Aunque el usuario puede modificar su perfil durante el tiempo que está trabajando en el cliente, una vez que cierra sesión los cambios no se guardan en el servidor. Cuando inicie sesión de nuevo, volverá al entorno configurado como obligatorio.
  - Estos perfiles solo pueden ser modificados por los administradores,
  - Para crearlo, tan solo hay que renombrar el archivo **ntuser.dat** (se encuentra dentro del subdirectorio del usuario donde se han creado los perfiles móviles) por **ntuser.man**