

ADMINISTRACIÓN DE RECURSOS COMPARTIDOS.



Contenido

1. Introducción
 - 1.1. Recursos compartidos
2. Carpetas compartidas administrativas
 - 2.1. Carpetas ocultas
3. Compartir carpetas
 - 3.1. Crear carpetas compartidas
 - Compartir carpetas con el administrador de equipos
 - Compartir una carpeta desde el explorador de archivos
 - Compartir una carpeta desde la línea de comandos
4. Carpetas compartidas publicadas
 - 4.1. Publicar una carpeta compartida en una unidad organizativa
5. Permisos en carpetas compartidas
 - 5.1. Establecer permisos
6. Conectarse a las carpetas compartidas
 - 6.1. Mediante conectar a unidad de red (todas las versiones de Windows):
 - 6.2. Mediante la opción ejecutar
 - 6.3. Con comando de consola
7. Administrar el acceso mediante NTFS
 - 7.1. Herencia de permisos NTFS
 - 7.2. Limpiar permisos
 - 7.3. Permisos efectivos
 - 7.4. Posesión de archivos o carpetas
 - 7.5. Ver los permisos efectivos
8. Administración de recursos del servidor
9. Trabajar con cuotas
 - 9.1. Plantillas de cuota
 - 9.2. Crear una cuota. Crear una plantilla de cuota
10. Filtrar archivos
- 10.1. Trabajar con grupos de archivos

Para crear un grupo de archivos: Crear un filtro de archivos

1. Introducción

Una vez que tenemos nuestro directorio activo configurado con nuestros objetos: usuarios, equipos, grupos y unidades organizativas, ya podemos empezar a compartir y administrar recursos.

1.1. Recursos compartidos

Los permisos definen el tipo de acceso concedido a un usuario, grupo o equipo para un objeto.

Por ejemplo, podemos permitir a un usuario leer el contenido de un archivo, dejar que otro usuario realice cambios en el archivo e impedir a los demás usuarios el acceso al archivo. Podemos también establecer permisos en impresoras para que determinados usuarios puedan configurar y administrar una impresora y otros usuarios sólo puedan imprimir en ella.

Los permisos se aplican a cualquier objeto protegido, como archivos, objetos de nuestro directorio activo y objetos del registro. Los permisos se pueden conceder a cualquier usuario, grupo o equipo. Podemos conceder permisos para objetos a:

- Grupos, usuarios e identidades especiales del dominio.
- Grupos y usuarios de cualquier dominio de confianza.
- Grupos y usuarios locales del equipo en el que reside el objeto.

Al establecer permisos, se especifica el nivel de acceso de los grupos y usuarios. Los permisos adjuntos a un objeto dependen del tipo de objeto. Por ejemplo, los permisos que se adjuntan a un archivo son diferentes de los que se adjuntan a una clave de registro. Sin embargo, algunos permisos, son comunes a la mayoría de los tipos de objeto.

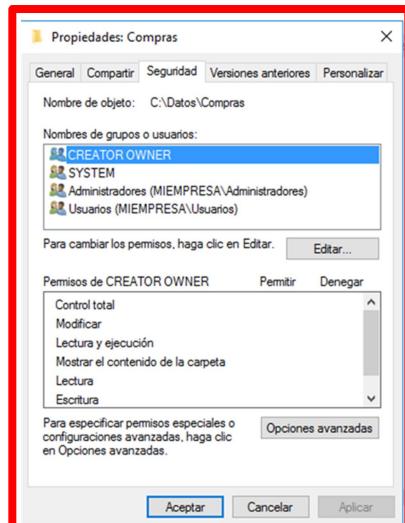
Los permisos siguientes son permisos comunes:

- Permisos de lectura
- Permisos de escritura
- Permisos de eliminación

Permisos estándar y especiales

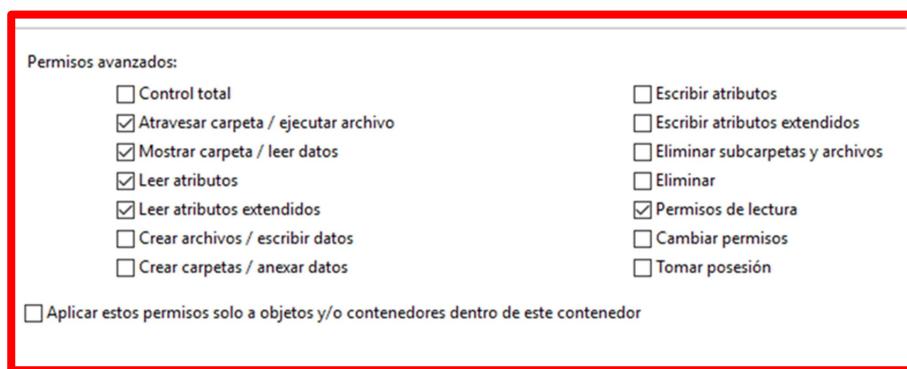
Podemos conceder permisos estándar y especiales para objetos. Los permisos estándar son los que utilizaremos la mayoría de las veces ya que implican a las operaciones más sencillas. Los permisos especiales ofrecen un grado de control más preciso para asignar acceso a objetos, cuando queramos afinar mucho seguramente no nos valga con la pantalla de permisos estándar y tengamos que acudir a ésta. Veamos las pantallas de estos dos tipos de permisos:

Permisos estándar:



El sistema tiene un nivel de configuración de seguridad predeterminado para cada tipo de objeto. Esta configuración constituye el conjunto de permisos más habituales que solemos utilizar como administradores de sistema. La lista de permisos estándar disponibles varía en función del tipo de objeto para el que se está modificando la seguridad.

Permisos especiales:



Los permisos siempre se aplican sobre particiones formateadas con el sistema de archivos NTFS. Si intentamos aplicar estos permisos en un disco o partición con FAT32 no tendríamos prácticamente opciones de seguridad, ya que no las permite. Por regla general debemos evitar siempre la utilización de FAT32 en el formato de nuestros discos.

Los permisos especiales nos permiten, además:

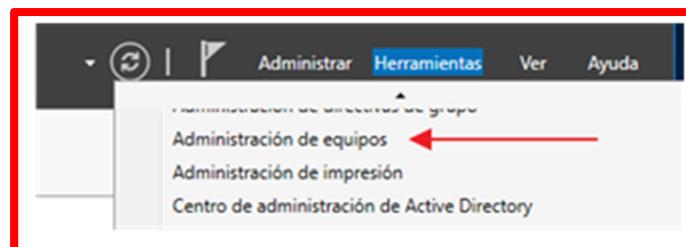
- Mostrar lista de carpetas/leer datos
- Leer atributos
- Leer atributos extendidos
- Leer permisos

Si el administrador del sistema elimina un permiso especial relacionado con un permiso estándar, la casilla de verificación del permiso estándar deja de estar activada. En su lugar, se activa la casilla de verificación del permiso especial incluido en la lista de permisos estándar.

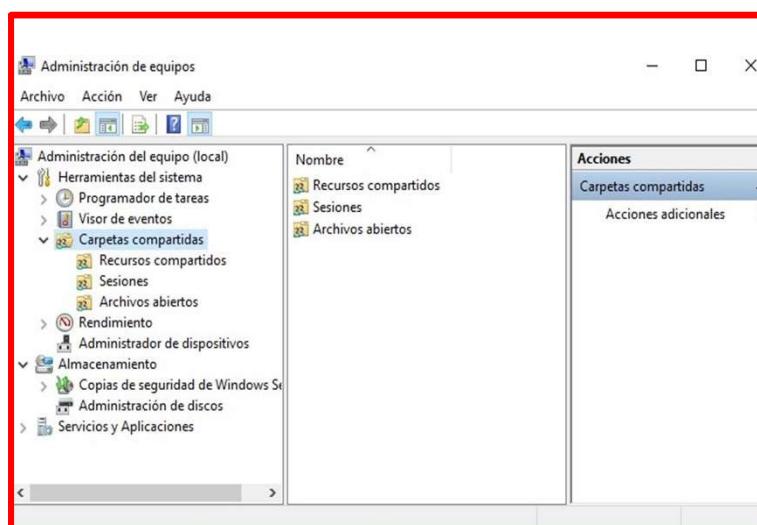
2. Carpetas compartidas administrativas

Existen una serie de carpetas que todos los equipos tienen ya compartidas y que se utilizan para labores administrativas. Para verlas, debemos abrir la consola del administrador de equipos.

Por ejemplo, en nuestro servidor lo haremos desde la consola de administración del servidor:



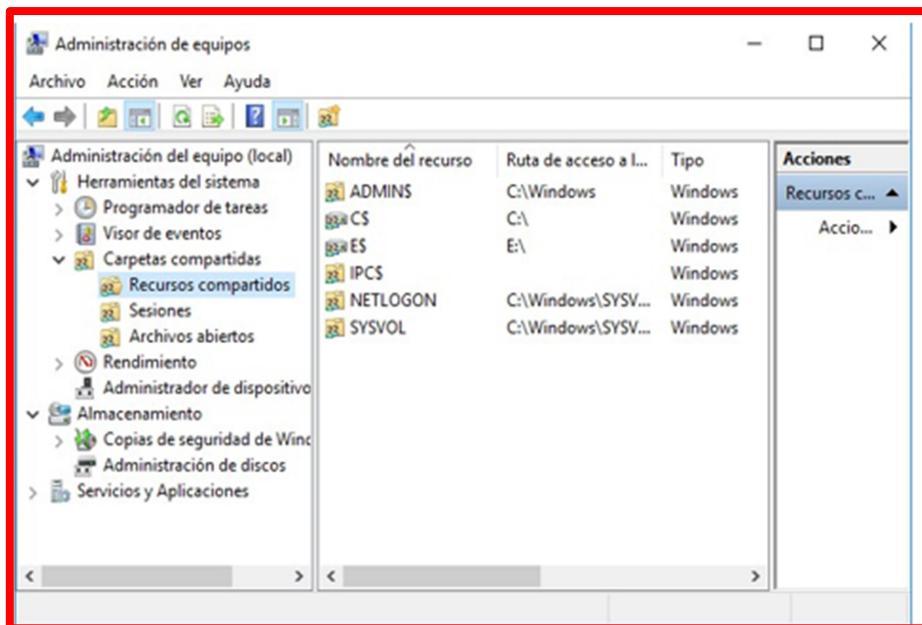
Nos muestra la consola que ya conocemos y de la que sabemos que podemos conectarnos a otros equipos remotos para administrarlos (desde la consola de administración del directorio activo o desde el menú "Archivo" de la consola):



Esta consola administrativa del equipo nos proporciona mucha ayuda y va ser imprescindible en nuestras tareas de administrador de la red.

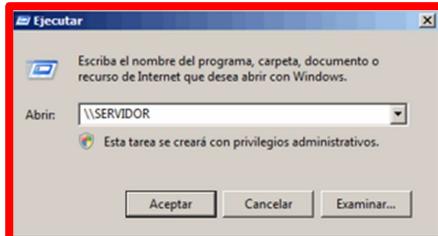
La primera vez que se accede a esta consola sorprende ver que ya hay carpetas o recursos compartidos. Si nos fijamos en algunos de ellos tienen al final un símbolo "\$". Los recursos que queramos que estén ocultos para los usuarios terminar con este carácter "\$".

Ahora expandimos la carpeta que pone "Carpetas compartidas" y hacemos clic en "recursos compartidos":

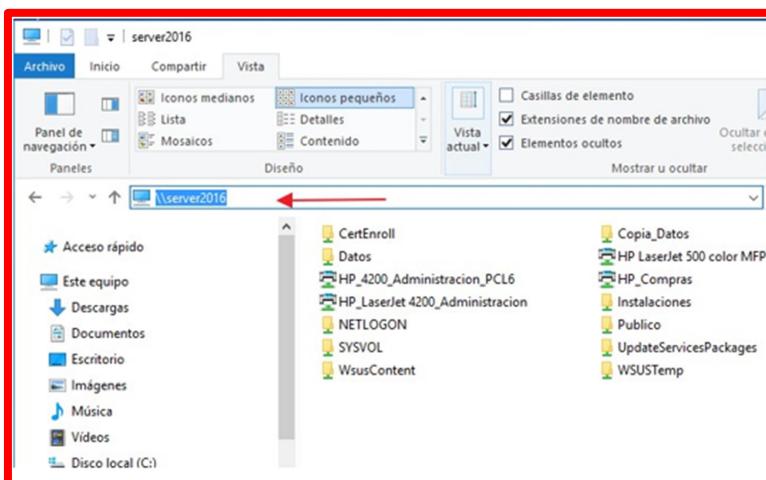


Esto lo podemos hacer desde el propio servidor o desde cualquier equipo de nuestro dominio y además contra cualquier equipo.

Vamos a hacer una pequeña comprobación antes de continuar. Aunque lo veremos después comprobaremos que es cierto esto de los recursos... hay una forma rápida y sencilla de acceder a los recursos compartidos de todos los equipos y es la de ir al menú "Inicio" luego damos a "Ejecutar" y escribir el nombre del equipo así (con su notación UNC) "\servidor":



Si el nombre es correcto se mostrará una pantalla con todos sus recursos compartidos, como vemos en la parte derecha.



Las carpetas "Netlogon" y "Sysvol", coinciden con las que hemos visto arriba y que lógicamente no terminan con el símbolo "\$" ya que este símbolo hace que no se muestren al estar ocultas.

2.1. Carpetas ocultas

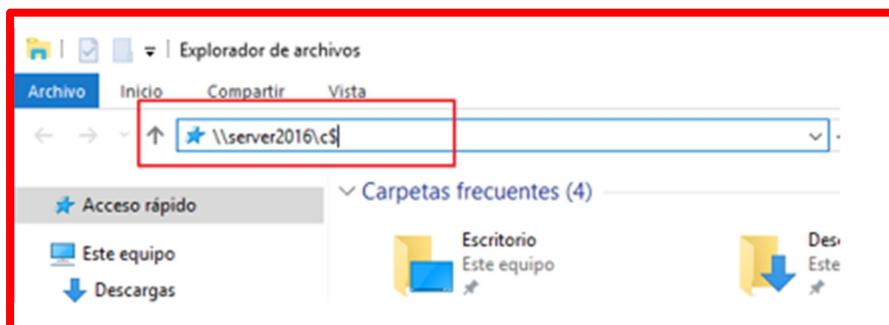
Veamos la definición de las carpetas ocultas. Windows Server comparte automáticamente carpetas que permiten realizar tareas administrativas. Se caracterizan por incluir un signo de dólar (\$) al final del nombre de carpeta. El signo de dólar permite ocultar la carpeta compartida a los usuarios que examinan el equipo en "Mis sitios de red". Podemos administrar de forma rápida archivos y carpetas en servidores y equipos remotos utilizando estas carpetas compartidas ocultas.

Los miembros del grupo "Administradores" tienen, de manera predeterminada, compartidas permiso de control total en las carpetas compartidas administrativas. No se pueden modificar los permisos de las carpetas compartidas administrativas. La siguiente tabla describe la finalidad de las carpetas compartidas administrativas que ofrece automáticamente Windows Server:

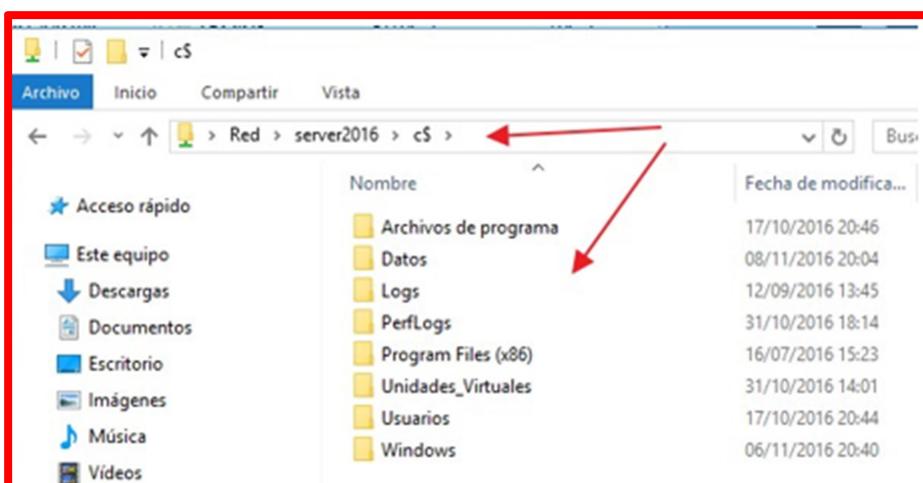
- C\$, D\$, E\$ Utilizaremos estas carpetas compartidas para conectarnos de forma remota a un equipo y realizar tareas administrativas. La raíz de cada partición (que tenga una letra de unidad asignada) del disco duro se comparte automáticamente. Al conectarse a esta carpeta, tenemos acceso a toda la partición.
- Admin\$ Esta es la carpeta raíz del sistema, que se encuentra de forma predeterminada en C:\WINDOWS. Podemos obtener acceso a esta carpeta compartida para administrar Windows Server sin necesidad de conocer en qué carpeta está instalada esta aplicación.
- Print\$ Esta carpeta ofrece acceso a los archivos de controladores de impresora de los equipos clientes. Al instalar la primera impresora compartida, la carpeta ubicada en Systemroot\System32\Spool\Drivers se comparte con el nombre Print\$. Sólo los miembros de los grupos "Administradores", "Operadores de servidor" y "Operadores de impresión" tienen permiso de control total para esta carpeta. El grupo "Todos" tiene permiso de lectura para esta carpeta.
- IPC\$ Se utiliza durante la administración remota de un equipo y al ver sus recursos compartidos.
- FAX\$ Esta carpeta compartida se utiliza para almacenar temporalmente archivos en caché y para obtener acceso a las portadas del servidor.

Ya sabemos cómo ver todos los recursos compartidos de un equipo (\\\nombre_servidor). También sabemos que, para que un recurso compartido esté oculto y no se muestre en esa lista debemos ponerle un "\$" al final, y por último sabemos que, por defecto, y para uso administrativo, todas las unidades de todos los equipos están compartidas para los administradores.

Es decir, si queremos acceder al recurso compartido "c\$" del equipo llamado "server2016".



No es necesario que sea un recurso local, también podemos hacerlo de equipos remotos.

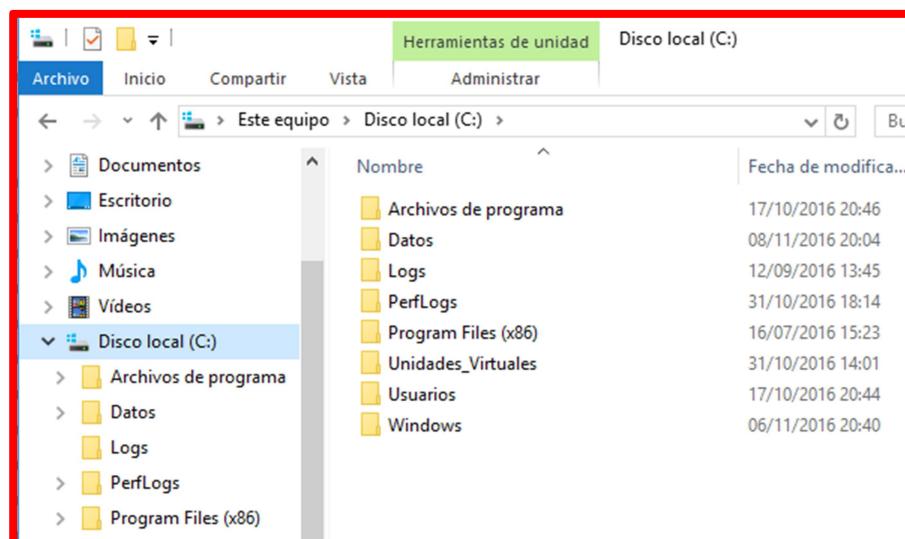


Obviamente para que esto funcione debemos pertenecer al grupo de usuarios de "**Administradores del dominio**". Se trata de una poderosa ayuda porque podemos acceder a todas las unidades de todos los ordenadores de nuestra red con sólo un comando.

En este punto y dada la "peligrosidad" de este comando entra en juego los acuerdos de confidencialidad y protección de datos de la empresa. Con este comando podemos entrar en todos los ordenadores y ver, sin que se entere el usuario, todos sus archivos y documentación confidencial. Así que es un punto crítico en cuanto a la obligada confidencialidad y prudencia que deben mantener los administradores de la red. En cualquier caso, las auditorias de los equipos podrían descubrir que se está accediendo por este sistema a los equipos, así que no es completamente anónimo.

3. Compartir carpetas

La familia Windows Server organiza los archivos en directorios, representados gráficamente como carpetas. Estas carpetas contienen todo tipo de archivos y más niveles de subcarpetas. Algunas de estas carpetas se reservan para los archivos del sistema operativo y los archivos de programa:



Los usuarios no deberían introducir datos en las carpetas del sistema operativo o de los archivos de programa. Esta es una de las grandes equivocaciones y mejorable diseño histórico de Windows. Estas carpetas tan críticas deberían ser incluso inaccesible para los usuarios, y, además, deberían tener un control de versiones más potente. Cada vez que instalamos programas se van instalando en estas carpetas haciéndolas crecer y "ensuciando" lo que era el sistema operativo.

Comentábamos que las carpetas compartidas proporcionan acceso a archivos y carpetas a través de una red. Los usuarios pueden conectarse a la carpeta compartida a través de la red para obtener acceso a los archivos y las carpetas que contiene.

Estas carpetas compartidas pueden contener aplicaciones, datos públicos o datos personales del usuario. Mediante la utilización de carpetas de aplicaciones compartidas, se centraliza la administración, permitiendo así la instalación y mantenimiento de las aplicaciones en un servidor en lugar de utilizar equipos clientes. La utilización de carpetas de datos compartidas ofrece una ubicación central desde la que los usuarios pueden obtener acceso a los archivos comunes. De este modo, se simplifica el almacenamiento de seguridad de los datos que contienen estos archivos.

Una de las primeras funciones que se aplican es la de "servidor de ficheros", realizando esta tarea mediante la compartición de recursos.

Al tener todos los ficheros de trabajo de los usuarios en un sólo sitio obtenemos muchos beneficios:

- Se ubican en un potente servidor especialmente diseñado para este fin. (discos de alto rendimiento)
- Centralizamos la administración al estar todo en un recurso del servidor
- Facilitamos la copia de seguridad de los datos
- Los usuarios no tienen versiones diferentes de los documentos en distintos equipos compartidos.

Una carpeta compartida es aquella a la que pueden obtener acceso varios usuarios a través de la red. Una vez que se comparte una carpeta, los usuarios pueden obtener acceso a todos sus archivos y subcarpetas, siempre que se les hayan concedido permisos.

Entre las características de las carpetas compartidas tenemos:

- Sólo se pueden compartir carpetas, no archivos individuales. Si varios usuarios necesitan obtener acceso al mismo archivo, debemos introducirlo en una carpeta y luego compartir ésta.
- Cuando compartimos una carpeta, se concede un permiso de lectura al grupo "Todos" de forma predeterminada. Debemos eliminar este permiso predeterminado y estableceremos los permisos de cambio o de lectura a los grupos según necesitemos.
- Cuando se agregan usuarios o grupos a una carpeta compartida, el permiso predeterminado es el de lectura.
- Al copiar una carpeta compartida, se sigue compartiendo la carpeta compartida original, pero no así su copia. Cuando una carpeta compartida se mueve a otra ubicación, deja de estar compartida.
- Podemos ocultar una carpeta compartida si ponemos un signo de dólar (\$) al final del nombre de la carpeta. El usuario no puede ver la carpeta compartida en la interfaz de usuario, pero puede obtener acceso a ella escribiendo el nombre UNC (Universal Naming Convention, Convención de nomenclatura Universal). Por ejemplo [\\servidor\\secretos\\$](\\servidor\\secretos$).

3.1. Crear carpetas compartidas

Tenemos tres formas de compartir carpetas:

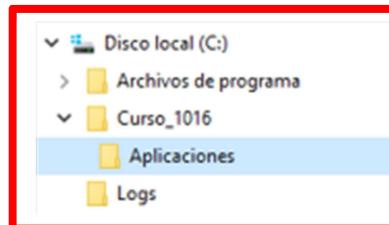
- Mediante la administración de equipos
- Directamente desde el explorador de archivos del equipo
- Con un comando de consola

Cada una de ellas tiene su momento. Por ejemplo, el primer caso es más laborioso porque se realiza con un asistente y cuesta algo más tiempo, pero gracias a esto podemos administrarlas de una forma más segura y con más información.

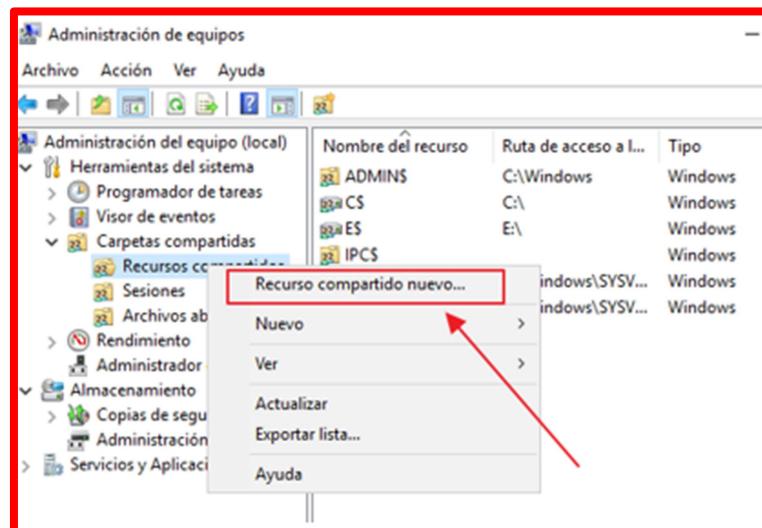
El segundo método es el más sencillo y habitual cuando estamos en un equipo en local. El tercer sistema es muy cómodo cuando estamos acostumbrados a escribir comandos en consolas o cuando queremos hacer una compartición automática desde un fichero de comandos BAT o de PowerShell.

- **Compartir carpetas con el administrador de equipos**

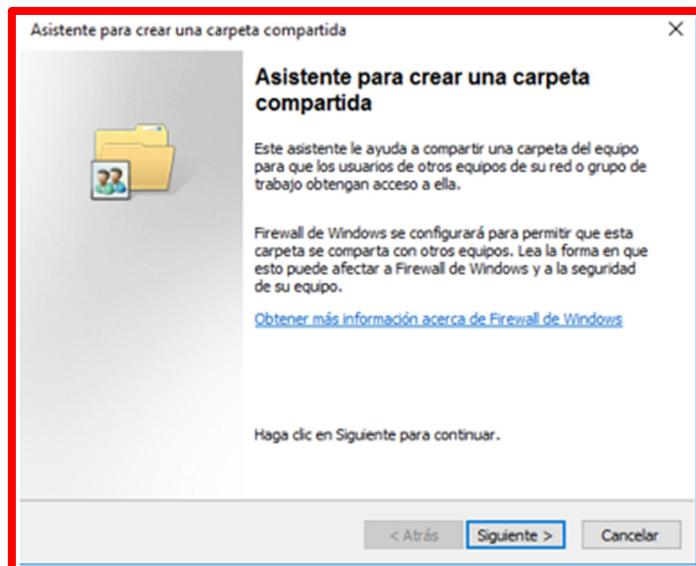
1. Primero vamos a crear una carpeta en la unidad "c:" que se llame "curso_2016" y luego otra dentro que se llame "aplicaciones":



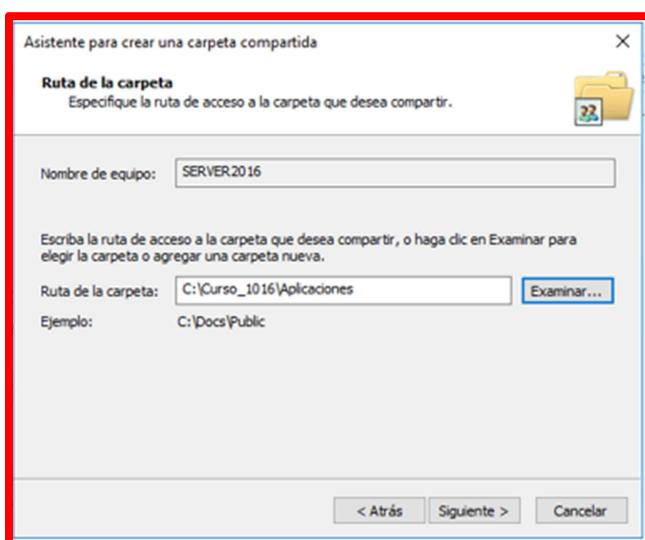
2. Para crear el recurso compartido vamos a la pantalla de administración del equipo:



3. Hacemos clic con el botón derecho en la carpeta de la izquierda "Recursos compartidos" para seleccionar la opción de crear un nuevo recurso compartido:

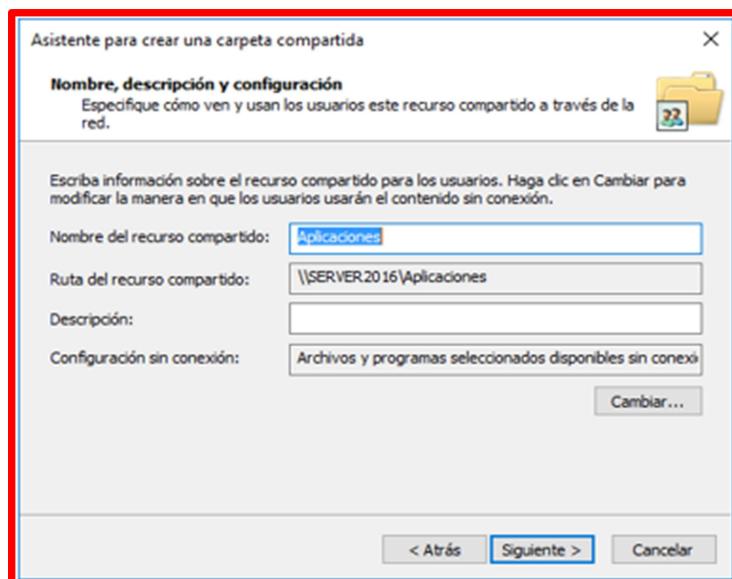


4. Pulsamos en siguiente y seleccionamos la carpeta a compartir:



Vemos primero el equipo donde estamos compartiendo el recurso, y luego la carpeta a compartir, que obviamente ya debe existir.

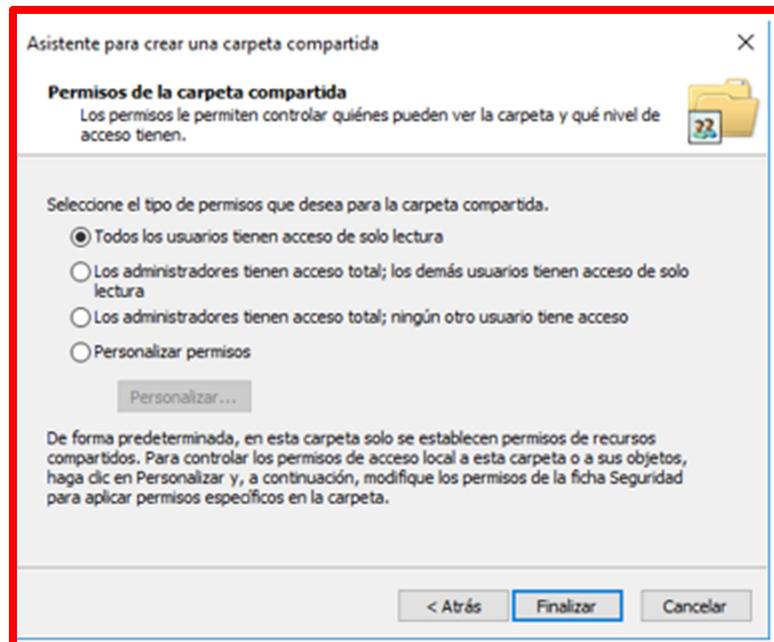
5. Pulsaremos en "Examinar" para encontrarla. La seleccionamos y pulsamos en "Siguiente":



Ya tenemos en nombre de la carpeta a compartir y la ruta completa que será: \\server2016\aplicaciones. En la nomenclatura, se escribe primero "\\", luego el equipo que queremos ver o compartir algo y por último una carpeta: "\\servidor\aplicaciones".

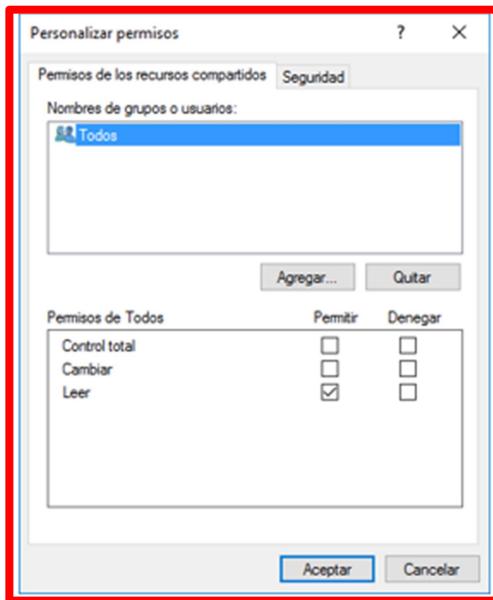
El asistente nos muestra un cuadro de texto para poner una descripción y, por último, la configuración para cuando se trabaje sin conexión, concepto que no veremos de momento.

6. Pulsemos en "Siguiente":



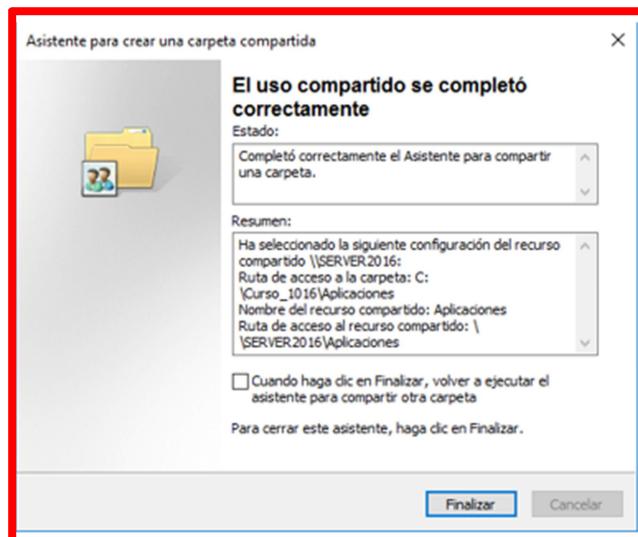
Ahora nos pide los permisos que debemos poner en este recurso compartido. Los habituales son el segundo y tercero, es decir, que los administradores siempre tengan permiso completo y que los demás tengan de lectura o de escritura.

7. Si queremos podemos personalizar por grupos de usuarios lo haremos con la última opción:



Podemos ir seleccionando los grupos de usuarios y cada uno de ellos con su propio tipo de permiso. Vemos que en los recursos compartidos sólo existen tres tipos de permisos: "Control total", "Cambiar" (escritura) y "Leer". No los confundamos con los permisos del sistema de ficheros NTFS que son mucho más amplios.

8. Pulsamos en "siguiente"



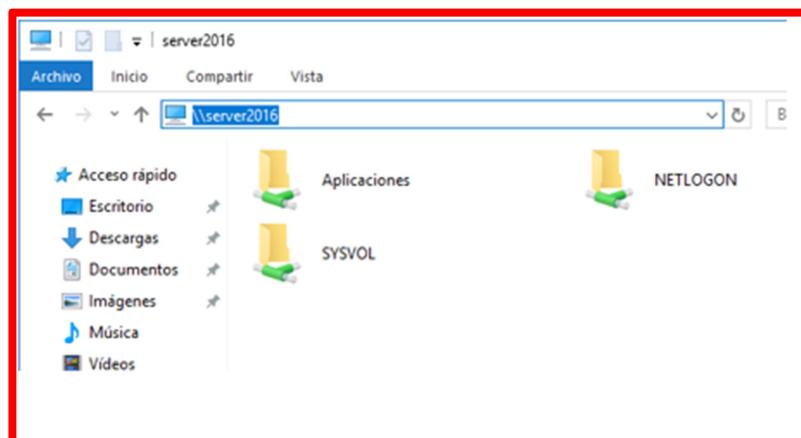
Nos informa de que ya tiene toda la información necesaria para crear el recurso compartido.

9. Pulsamos en "Finalizar" y vamos a la pantalla de los recursos para ver si todo es correcto:

Nombre del recurso	Ruta de acceso a la carpeta	Tipo
ADMIN\$	C:\Windows	Windows
Aplicaciones	C:\Curso_1016\Aplicaciones	Windows
CS	C:\	Windows
ES	E:\	Windows
IPCS		Windows
NETLOGON	C:\Windows\SYSVOL\sysvol\...	Windows
SYSVOL	C:\Windows\SYSVOL\sysvol	Windows

Efectivamente, en nuestra lista de recursos aparece ahora también "Aplicaciones".

10. Veamos ahora preguntando por los recursos compartidos desde otro equipo de la red con "\\server2016". Por ejemplo, desde un Windows 10:

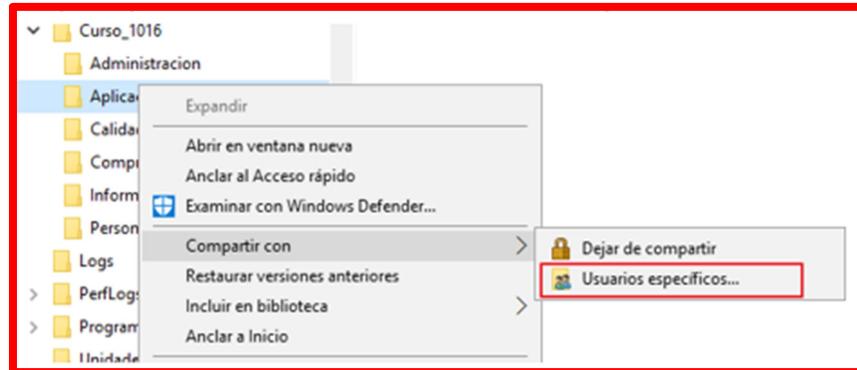


Comprobado, también aparece nuestra carpeta compartida.

- **Compartir una carpeta desde el explorador de archivos**

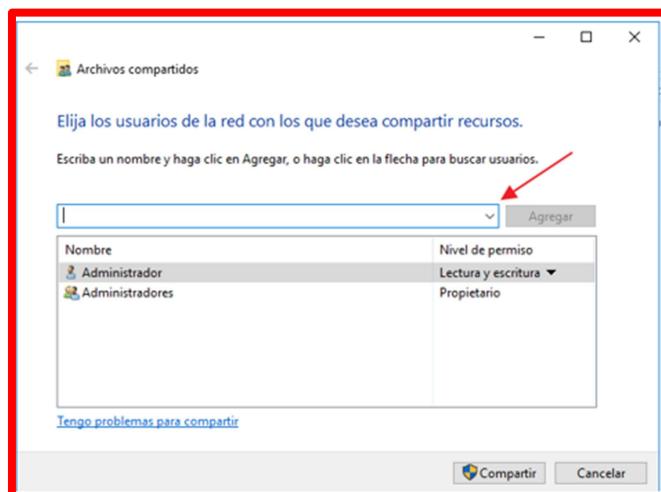
Es la forma más rápida cuando estamos en el mismo equipo del recurso que queremos compartir.

1. Simplemente nos vamos con el explorador de archivos, seleccionamos la carpeta que queremos compartir y con el botón derecho seleccionamos "Compartir":



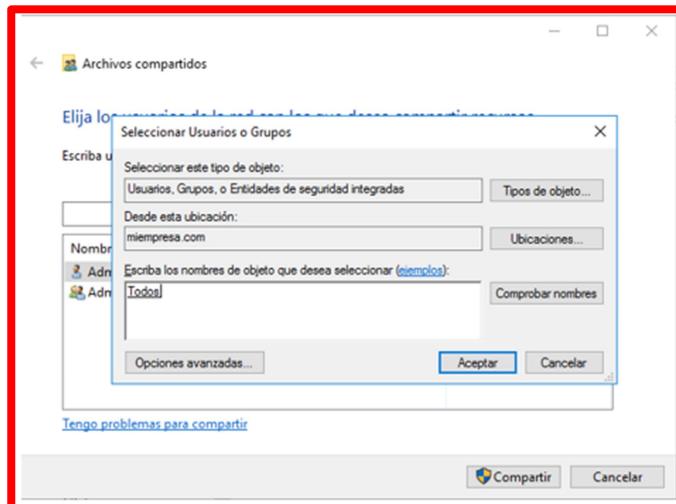
Antes de continuar vamos a crear unas cuantas carpetas para las pruebas de este tema:

2. Nos mostrará esta pantalla:

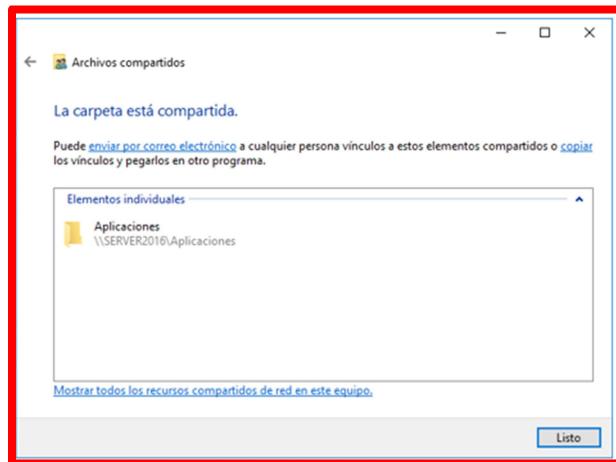


El aspecto es algo distinto a las versiones anteriores de Windows, pero ofrece las mismas funciones.

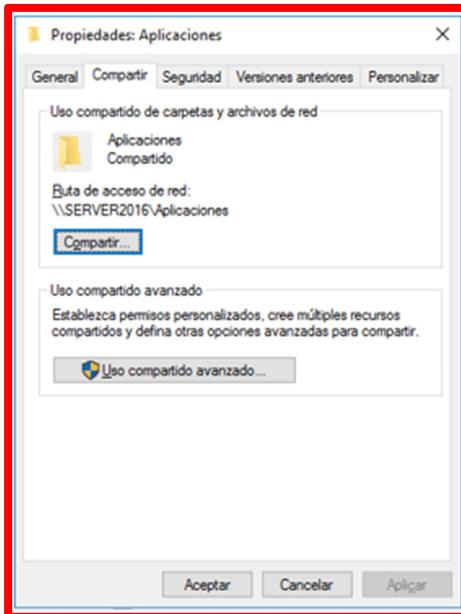
3. Pulsaremos en la flecha para indicar más usuarios, y elegimos "Buscar":



4. Para añadir "todos", quedando la carpeta compartida:

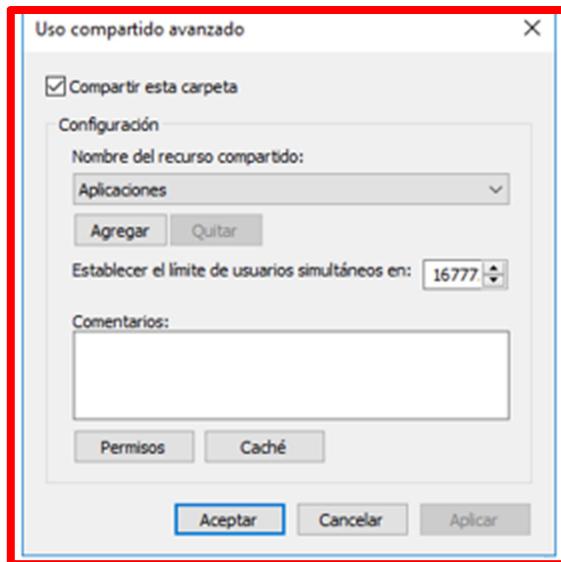


5. Si seleccionamos la carpeta desde el administrador de archivos y pulsamos en las propiedades sobre esta misma carpeta podemos ver algunos detalles más:



Si seleccionamos el botón "Compartir", podríamos dejar de compartir la carpeta o modificar los usuarios con permisos.

6. Si pulsamos en la opción "Uso compartido avanzado":



Podemos igualmente dejar de compartir o añadir otro nombre para el recurso compartido. Por ejemplo, podemos añadir "info\$" para que quede oculto y quitar el anterior, con lo que pasa a tener un solo nombre y además oculto para los usuarios.

- **Compartir una carpeta desde la línea de comandos**

La compartición de recursos puede realizarse también en una consola utilizando el comando **net share**. La sintaxis es la siguiente:

Mandato **net share**: Crea, elimina o muestra recursos compartidos.

```
net share net share recurso_compartido
net share recurso_compartido=unidad:ruta_de_acceso [/users:número | /unlimited] [/remark:"texto"]
net share recurso_compartido [/users:número | unlimited] [/remark:"texto"]
net share {recurso_compartido | unidad:ruta_de_acceso} /delete
```

4. Carpetas compartidas publicadas

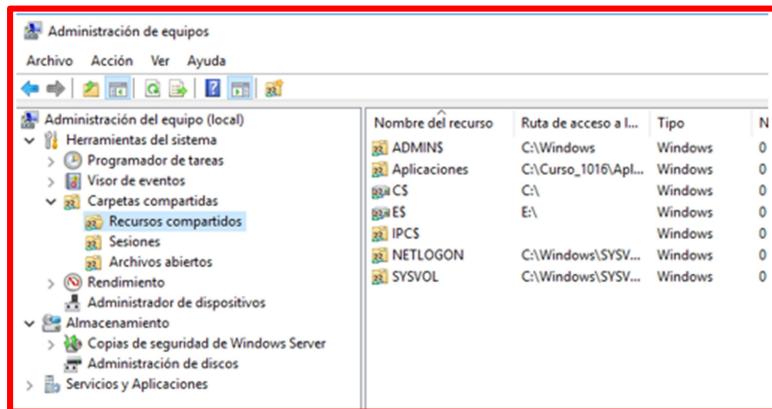
Las carpetas compartidas van a permitir a los usuarios buscar recursos de la red, incluso aunque cambie la ubicación física de los recursos. Por ejemplo, si se mueve una carpeta publicada a otro equipo, todos los accesos directos que señalan al objeto del directorio activo que representa a la carpeta compartida publicada siguen funcionando, siempre que se actualice la referencia a la ubicación física. No es necesario que los usuarios actualicen las conexiones.

Es muy interesante ya que si en algún momento hacemos una reorganización de recursos compartidos todos los accesos directos y referencias a estas ubicaciones fallarán. Por ejemplo, hojas vinculadas dentro de Excel. Otro ejemplo: supongamos que nuestro servidor de datos se empieza a agotar su espacio de almacenamiento. Para solucionarlo, adquirimos uno nuevo o una cabina de discos externa. Sólo debemos copiar los datos al nuevo dispositivo de almacenamiento y actualizar la carpeta compartida publicada.

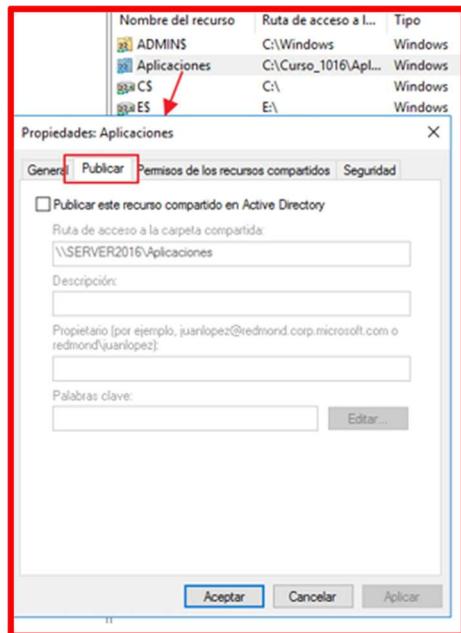
Podemos publicar una carpeta compartida a la que se pueda obtener acceso mediante un nombre UNC (del tipo `\servidor\recurso`). Una vez publicada una carpeta compartida, el usuario puede utilizar el directorio activo para buscar el objeto que representa a la carpeta compartida y conectarse a ésta. Tenemos dos formas de publicar una carpeta: desde la administración de equipos o desde una unidad organizativa, veamos los dos métodos y luego los comentaremos.

Para publicar una carpeta compartida como objeto del servidor haremos estos pasos.

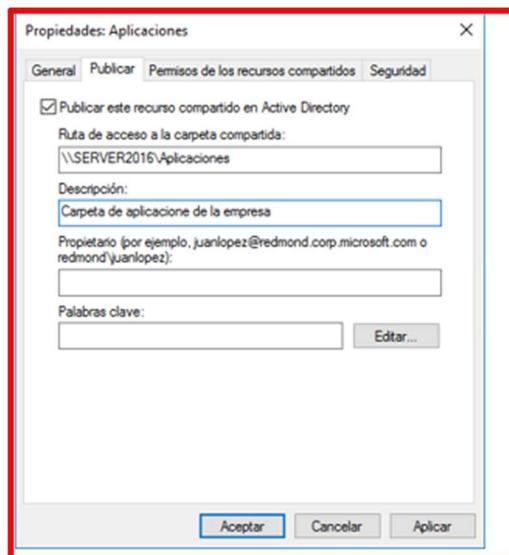
1. Primero en el "Administración de equipos" y en el árbol de la consola expandimos "Carpetas compartidas" y hacemos clic en Recursos compartidos.



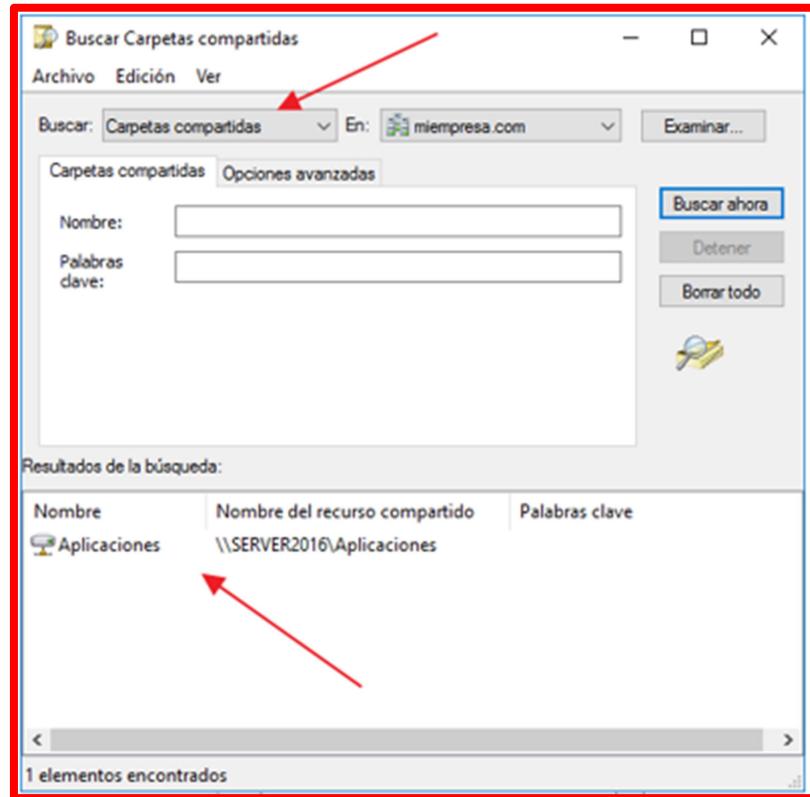
2. Ahora hacemos clic con el botón derecho en una carpeta compartida y luego seleccionamos "Publicar" de las "Propiedades":



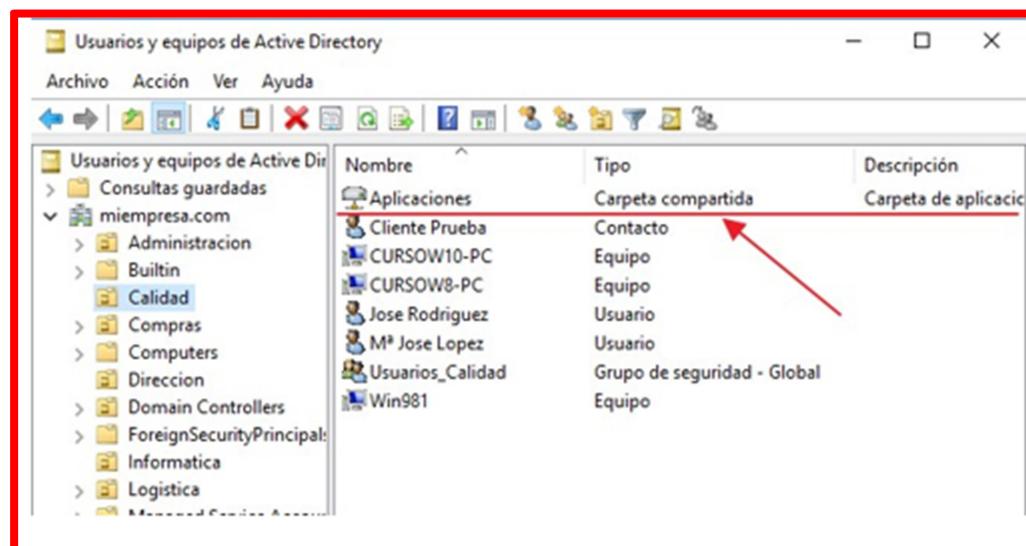
3. Queremos publicar la carpeta "aplicaciones" así que la marcamos y ponemos algún dato más como una descripción:



4. Ahora vamos a la consola de usuarios y equipos y en "buscar" indicamos las carpetas compartidas:



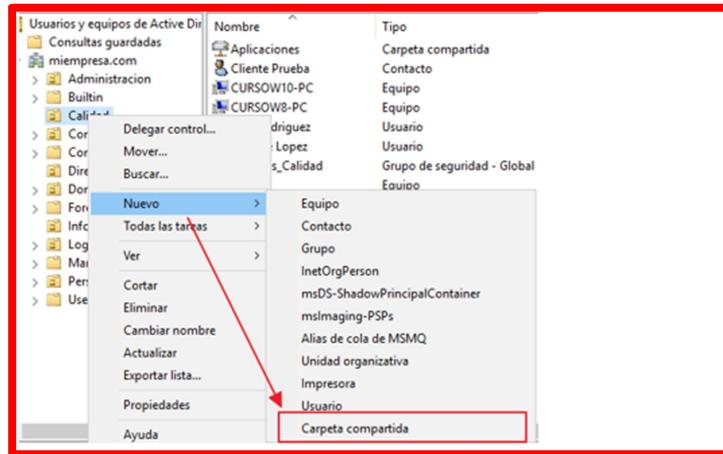
5. Con el botón derecho del ratón podemos decirle "Mover" e indicarle una unidad organizativa concreta, con lo que quedaría:



4.1. Publicar una carpeta compartida en una unidad organizativa

Para publicar una carpeta con este sistema abrimos la consola de "administración de usuarios y equipos del directorio activo" y luego seleccionamos la unidad organizativa en la que queremos publicar.

- Con el botón derecho seleccionamos la opción de "nuevo" y luego "carpeta compartida":



- Escribimos el nombre con el que queremos compartir y el nombre UNC del recurso que queremos compartir:

The left screenshot shows the 'Nuevo objeto: Carpeta compartida' (New Object: Shared Folder) dialog. It has a 'Nombre:' field containing 'datos_calidad' and a 'Ruta de red (\servidor\recurso compartido):' field containing '\\servidor\calidad'. The 'Aceptar' (Accept) button is visible at the bottom. The right screenshot shows the 'Usuarios y equipos de Active Dir' (Active Directory Users and Computers) list. A new entry 'datos_calidad' is visible under the 'Calidad' organizational unit, highlighted with a red box. The 'Nombre' column lists various objects like 'Aplicaciones', 'CURSOW10-PC', etc., and the 'Tipo' column indicates they are 'Carpeta compartida' (Shared Folder).

Al publicar una carpeta de esta forma debemos tener cuidado, ya que no se valida. Es decir, podemos escribir una ubicación que no existe y nos lo permitirá. Por esta razón es aconsejable utilizar el primer método, donde partimos de una ubicación correcta ya existente.

5. Permisos en carpetas compartidas

Los permisos de las carpetas compartidas sólo se aplican a los usuarios que se conectan a la carpeta a través de la red. No restringen el acceso de los usuarios a la carpeta del equipo en el que está almacenada. Podemos conceder permisos de carpeta compartida a cuentas de usuario, grupos y cuentas de equipo.

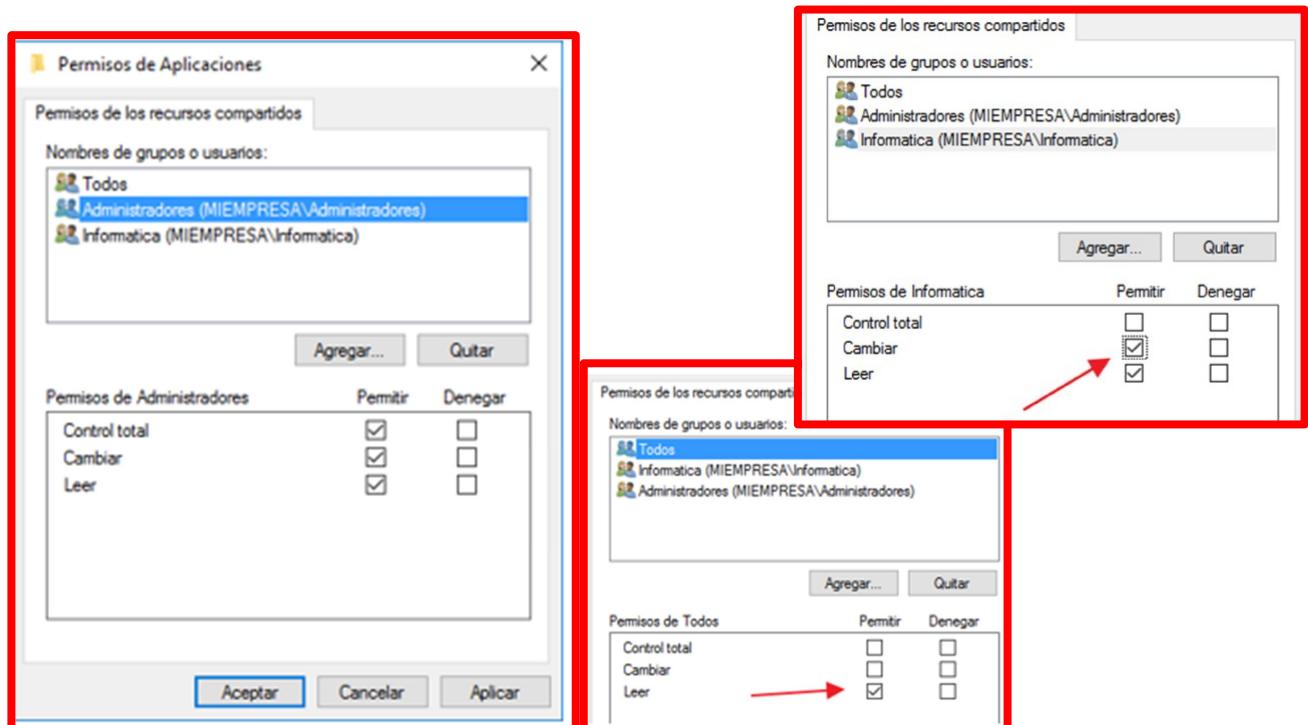
Los permisos que tenemos son:

- **Lectura.** El permiso de lectura es el permiso de carpeta compartida predeterminado y se aplica al grupo "Todos", permite:
 - Ver datos de archivos y atributos.
 - Ver los nombres de archivos y subcarpetas.
 - Ejecutar archivos de programa.
- **Cambio.** Incluye todos los permisos de lectura y también permite:
 - Agregar archivos y subcarpetas.
 - Cambiar datos en archivos.
 - Eliminar subcarpetas y archivos.
- **Control total.** Incluye todos los permisos de lectura y cambio. Además, permite cambiar los permisos de los archivos y las carpetas NTFS.

5.1. Establecer permisos

Para establecer permisos, utilizaremos las dos pantallas ya conocidas: la de la administración de equipos y la del explorador de archivo de Windows.

Por ejemplo, podemos dar a un recurso compartido estos permisos:



Tres grupos de permisos donde uno de ellos es a los administradores para que tengan siempre "Control total" sobre el recurso. Al resto de los usuarios les dejamos como sólo lectura. Los permisos siempre se deben dar sobre grupos de usuarios nunca sobre usuarios individuales.

6. Conectarse a las carpetas compartidas

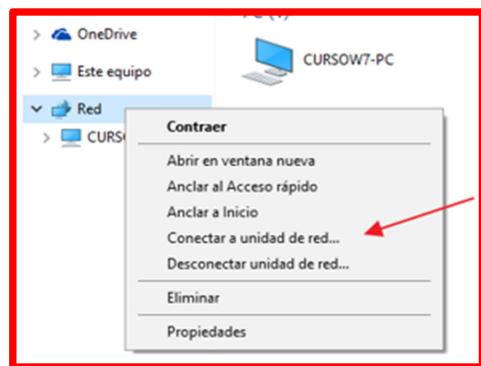
Una vez creada una carpeta compartida, los usuarios pueden obtener acceso a ella a través de la red. Pueden hacerlo desde "Mis sitios de red", la función "Conectar a unidad de red", el comando "Ejecutar" del menú Inicio o con un comando en modo consola. Veamos cómo conectarnos.

6.1. Mediante conectar a unidad de red (todas las versiones de Windows):

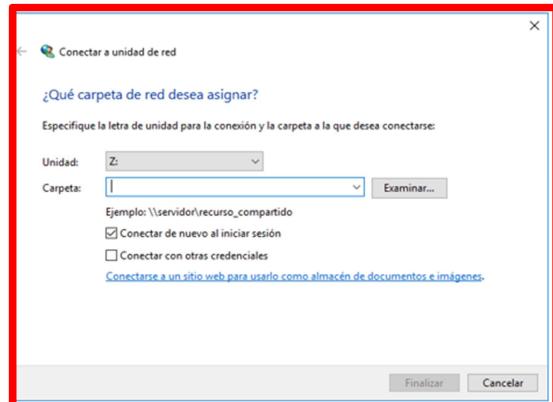
Si lo que queremos es asociar una letra e ícono de unidad a una carpeta compartida específica, debemos asignar una unidad de red. De esto modo, es más fácil reflejar la ubicación de un archivo de una carpeta compartida. Es la forma más cómoda y utilizada donde comúnmente se dice que "mapeamos" una unidad local con un recurso de red.

También puede utilizar letras de unidad para obtener acceso a las carpetas compartidas en las que no se puede utilizar una ruta UNC, como la carpeta de una aplicación antigua.

- Para conectarnos a una carpeta compartida mediante haremos clic con el botón derecho del ratón en "red" y a continuación en "Conectar a unidad de red".

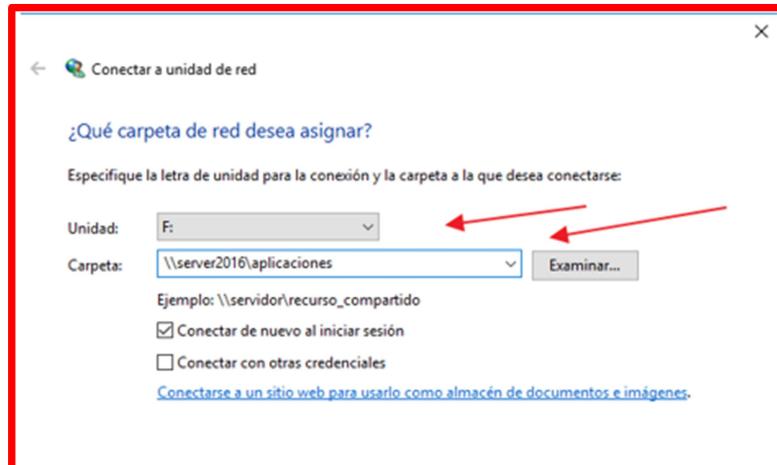


- Tanto en Windows 7, como en 8 y en Windows 10 se solicitan estos datos:

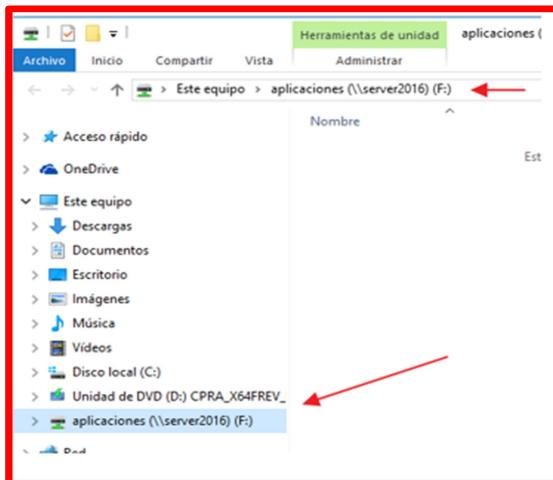


Por defecto nos pone la unidad "Z", vamos a cambiarlo por otra, por ejemplo, la "F:" y examinamos para localizar el recurso al que nos queremos conectar.

- Finalmente dejamos marcada la casilla de verificación "Conectar de nuevo" porque queremos que para la próxima vez que inicie el equipo aparezca esta conexión:



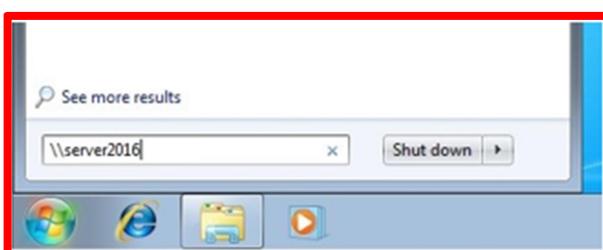
4. Ahora podemos comprobar en el explorador de archivos que ahora la unidad "F:" está mapeada a un recurso remoto:



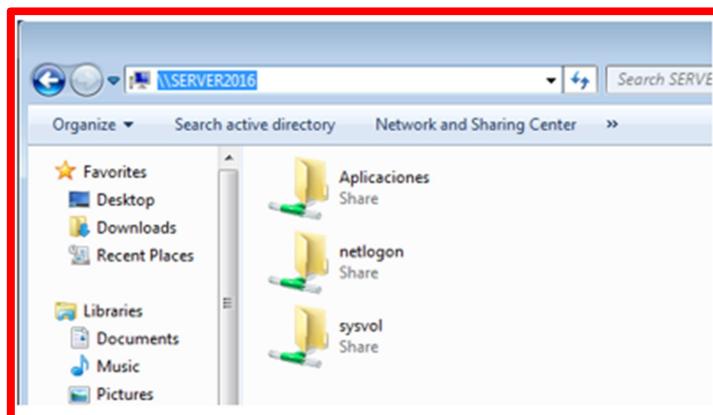
6.2. Mediante la opción ejecutar

Si no queremos mapear una unidad y sólo acceder de una forma rápida a un recurso compartido lo tenemos más fácil todavía.

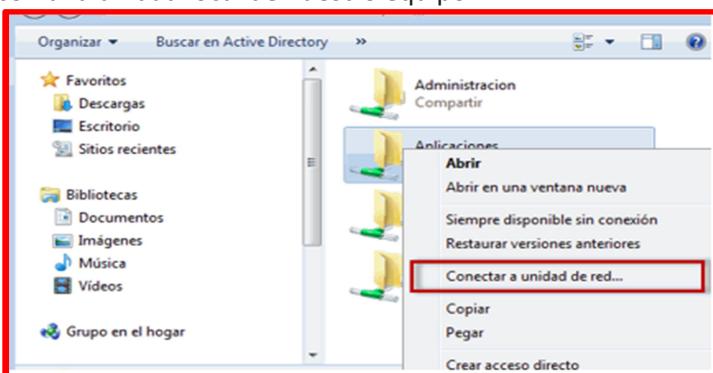
1. Si tenemos Windows 7, haremos clic en Inicio y a continuación en "Ejecutar". Luego en este cuadro de diálogo, escribiremos la ruta UNC del servidor y finalmente hacemos clic en "Aceptar":



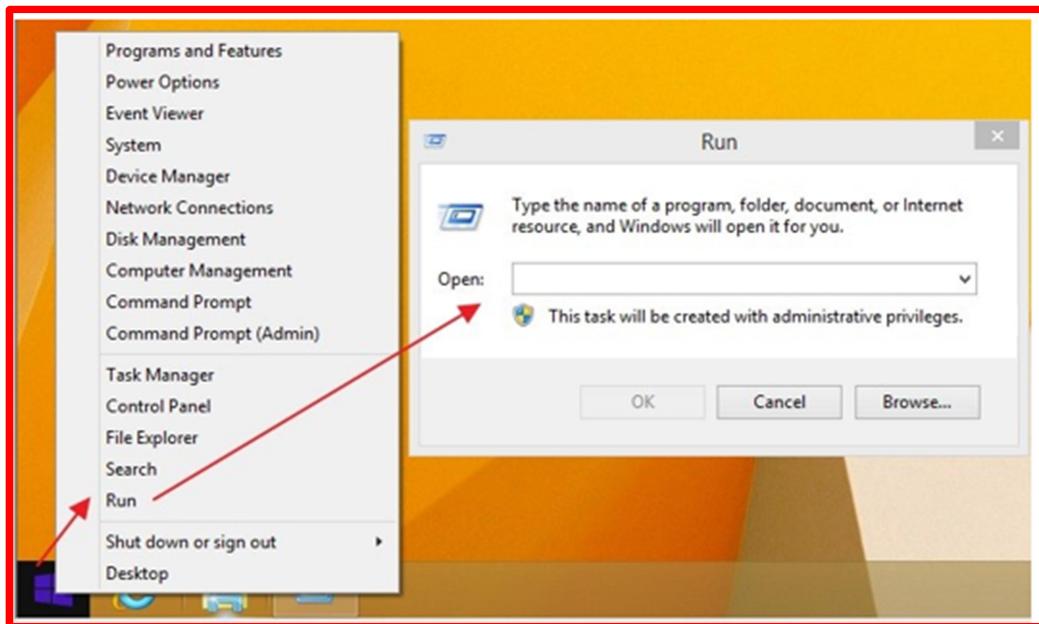
2. Al introducir el nombre de servidor, aparece una lista de las carpetas compartidas disponibles:



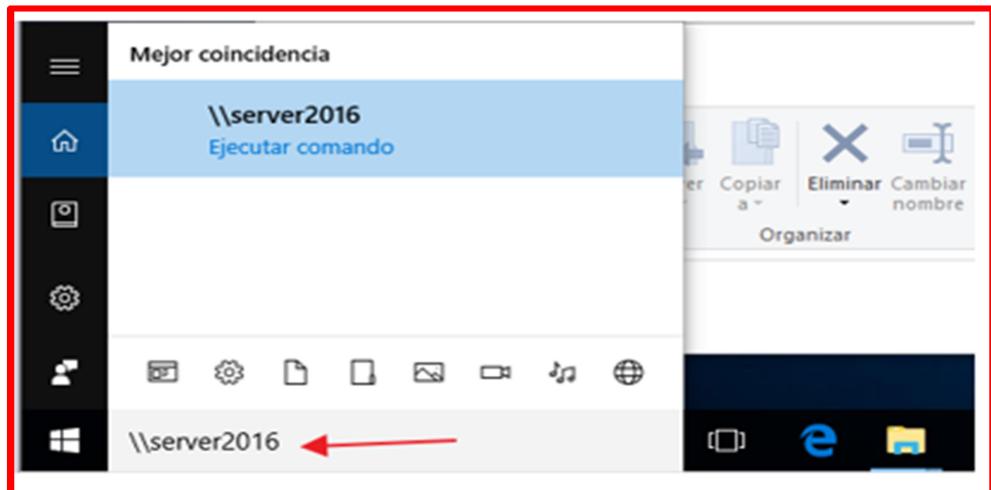
3. Seleccionamos el recurso y ya podemos acceder a sus datos. Además, con el botón derecho podemos hacer el "mapeo" de esa ruta con una unidad local de nuestro equipo:



4. En Windows 8 la ejecución de comandos sería con el botón derecho en el menú inicio y luego "ejecutar":



Y en Windows 10 igual que en 8 ó desde la misma línea de Cortana:



6.3. Con comando de consola

Comando "net use"

Conecta o desconecta un equipo de un recurso compartido o muestra información acerca de las conexiones del equipo. También controla las conexiones de red persistentes.

```
net use [nombre_dispositivo]
[\\nombre_equipo\recurso_compartido[\volumen]] [contraseña | *]
[/user:[nombreDominio\]nombre_usuario] [[/delete] | [/persistent:{yes | no}]] net use nombre_dispositivo
[/home[contraseña | *]]
[/delete:{yes | no}] net use [/persistent:{yes | no}]
```

Por ejemplo:

- net use f: \\servidor\carpeta Asigna a la unidad F: la carpeta compartida "carpeta" del servidor "servidor"
- net use f: /delete Elimina un recurso compartido
- net use f: \\servidor\carpeta /persistent:yes Hace que este recurso esté disponible la próxima vez que iniciemos el equipo, equivale a la casilla de verificación que vimos antes.

Ejercicio: Entra con el usuario José Rodríguez en el equipo de Windows 10 y utiliza el comando net use para asignar la unidad de disco N: a la carpeta compartida DocumentosPCXX en el servidor. Haz que este recurso esté disponible la próxima vez que iniciemos el equipo.

7. Administrar el acceso mediante NTFS

Windows guarda una completa lista de permisos para cada fichero o carpeta. Esta lista se llama ACL o lista de control de accesos y es la parte que vamos a ver ahora. NTFS es un sistema de archivos mucho más avanzado que el antiguo FAT32 utilizado en las versiones antiguas del sistema operativo Windows y por tanto nos ofrece muchas e importantes ventajas, como...

- **Fiabilidad.** NTFS utiliza el archivo de registro y la información de punto de comprobación para restaurar la integridad del sistema de archivos al reiniciar el equipo. Si se produce un error de sector defectuoso, NTFS vuelve a asignar de forma dinámica el clúster que contiene este sector defectuoso y asigna un nuevo clúster para los datos. NTFS también marca el clúster como inservible.
- **Seguridad a nivel de archivos y de carpetas.** Los archivos NTFS utilizan el Sistema de archivos de cifrado (EFS, Encrypting File System) para proteger los archivos y las carpetas. Si EFS está activado, pueden cifrarse los archivos y las carpetas para uno o varios usuarios. Este cifrado ofrece como ventaja la confidencialidad e integridad de los datos. En otras palabras, los datos están protegidos frente a una modificación accidental o no autorizada. También permite establecer permisos de acceso a un archivo o una carpeta. Se pueden establecer permisos de lectura, de lectura y escritura, o permisos para denegar el acceso. NTFS también almacena una lista de control de acceso (ACL, access control list) con todos los archivos y carpetas de una partición NTFS. Esta ACL contiene una lista de todas las cuentas de usuarios, grupos y equipos a los que se les concede acceso al archivo o carpeta y el tipo de acceso concedido. Para un usuario que desea obtener acceso a un archivo o carpeta, la ACL debe contener una entrada, denominada ACE, para la cuenta de usuario, grupo o equipo a la que está asociado el usuario. ACE debe permitir de forma específica el tipo de acceso que solicita el usuario para poder obtener acceso al archivo o carpeta. Si no existe una entrada ACE en la ACL, Windows Server deniega el acceso del usuario al recurso.
- **Administración mejorada del aumento de almacenamiento.** NTFS admite cuotas de disco, que permiten especificar la cantidad de espacio en disco disponible para un usuario. Mediante las cuotas de disco, se puede realizar un seguimiento y controlar el uso del espacio en disco y establecer si se permite a los usuarios superar un nivel de advertencia o el límite de cuota de almacenamiento. NTFS admite archivos de mayor tamaño y número de archivos por volumen que FAT o FAT32.
- **Permisos a varios usuarios.** Si se conceden permisos NTFS a una cuenta de usuario individual y a un grupo al que pertenezca el usuario, se le conceden también varios permisos al usuario. Existen reglas para determinar cómo NTFS puede combinar estos permisos múltiples con el fin de producir los permisos efectivos del usuario.
- **Permisos de archivo y de carpetas.** Los permisos NTFS se utilizan para especificar los usuarios, grupos y equipos pueden obtener acceso a los archivos y las carpetas. También permiten establecer las acciones que pueden realizar los usuarios, grupos y equipos con el contenido de los archivos o carpetas.

Estos son los permisos que se pueden establecer en las carpetas y en los ficheros:

	Permisos de archivo	Permisos de carpeta
Control total	Permite cambiar permisos, tomar posesión de objetos y realizar en general todas las opciones disponibles en NTFS.	Permite cambiar permisos, tomar posesión de objetos, eliminar archivos y subcarpetas y realizar en general todas las opciones disponibles en NTFS.
Modificar	Permite modificar y eliminar archivos y realizar operaciones autorizadas por el permiso de escritura y de lectura y ejecución.	Modificar Permite eliminar carpetas y realizar las operaciones autorizadas por el permiso de escritura y el de lectura y ejecución.
Leer y ejecutar	Permite ejecutar aplicaciones y las acciones autorizadas por el permiso de lectura.	Permite recorrer carpetas y realizar las acciones autorizadas por el permiso de lectura y el de mostrar el contenido de la carpeta.
Escritura	Permite sobrescribir el fichero, cambiar sus atributos y ver sus permisos y posesión.	Permite crear nuevos archivos y subcarpetas, cambiar los atributos de la carpeta y ver sus permisos y posesión.
Lectura	Permite leer los archivos y ver sus atributos, permisos y posesión.	Permite ver los archivos y subcarpetas y sus atributos, permisos y posesión.
Mostrar el contenido de la carpeta		Permite ver los nombres de los archivos y subcarpetas.

Como vemos en la tabla, la diferencia entre ambos está en que en las carpetas hay además "mostrar el contenido de la carpeta". Éste no permite leer ningún fichero, sino que simplemente ver el contenido de una carpeta. ¿utilidad? Pues sí, y muy importante... imaginemos que tenemos una carpeta dentro de otra y que en esa segunda queremos dar permisos a algunas personas. Para esto debemos otorgar permisos en el nivel anterior de "mostrar el contenido de la carpeta" para que pueda acceder al siguiente nivel.

- **Mover ficheros o carpetas con permisos.** Sabemos los permisos que se pueden asignar a los ficheros o carpetas. ¿Qué pasa con los permisos cuando movemos objetos entre carpetas?
- **Al copiar o mover un archivo o una carpeta,** los permisos pueden cambiar en función de la ubicación a la que se mueva. Al copiar archivos o carpetas de una carpeta a otra, o de una partición a otra, los permisos de los archivos o carpetas pueden cambiar. Al copiar un archivo o carpeta, se producen los siguientes efectos en los permisos NTFS:
 - Al copiar una carpeta o archivo en una única partición NTFS, la copia de la carpeta o archivo hereda los permisos de la carpeta de destino.
 - Al copiar una carpeta o archivo a una partición NTFS diferente, la copia de la carpeta o archivo hereda los permisos de la carpeta de destino.
 - Al copiar una carpeta o archivo a una partición no NTFS, como, por ejemplo, una partición FAT, la copia de la carpeta o archivo pierde los permisos NTFS debido a que las particiones no NTFS no admiten este tipo de permisos.
- **En el caso de mover archivos o carpetas...**
 - Al mover una carpeta o archivo en una partición NTFS, la carpeta o archivo conserva sus permisos originales.
 - Al mover una carpeta o archivo a una partición NTFS diferente, la carpeta o archivo hereda los permisos de la carpeta de destino. Al mover una carpeta o archivo entre particiones, Windows Server copia la carpeta o archivo a la nueva ubicación y, a continuación, la elimina de la antigua ubicación.
 - Al mover una carpeta o archivo a una partición no NTFS, la carpeta o archivo pierde los permisos NTFS debido a que las particiones no NTFS no admiten este tipo de permisos.
 - Para mover archivos y carpetas en una única partición NTFS o entre particiones NTFS, debemos tener permiso de escritura para la carpeta de destino y permiso de modificación para la carpeta o archivo de origen. Es necesario tener permiso de modificación para mover un archivo o carpeta debido a que Windows Server elimina la carpeta o archivo de la carpeta de origen tras copiarla en la carpeta de destino.

7.1. Herencia de permisos NTFS

Hasta Windows 2000 el tratamiento de los permisos era un poco caótico ya que si, por ejemplo, teníamos una carpeta y copiábamos un archivo le teníamos que poner los permisos a mano en lugar de adquirir los permisos de la carpeta destino. Además, si en la raíz de una carpeta queríamos poner un permiso este se propagaba inmediatamente a las carpetas inferiores con el consiguiente destrozo de la lista ACL.

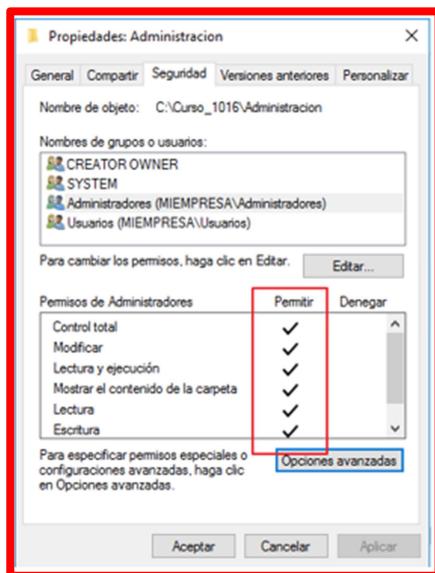
Todas las antiguas deficiencias se resolvieron a partir de Windows 2000 Server gracias a la herencia de permisos. Ventaja que podemos activar o desactivar según nuestro criterio. Veamos en qué consiste esto de la herencia.

Los permisos que se conceden a una carpeta principal son heredados de forma predeterminada por las subcarpetas y los archivos incluidos en ella. Al crear archivos y carpetas y al formatear una partición con NTFS, Windows Server asigna automáticamente permisos NTFS predeterminados.

Podemos evitar que los archivos y las subcarpetas hereden los permisos asignados a la carpeta principal. Al impedir esta herencia de permisos, podemos hacer dos cosas:

- Copiar los permisos heredados de la carpeta principal
- Eliminar los permisos heredados y mantener sólo aquéllos que se hayan asignado explícitamente.

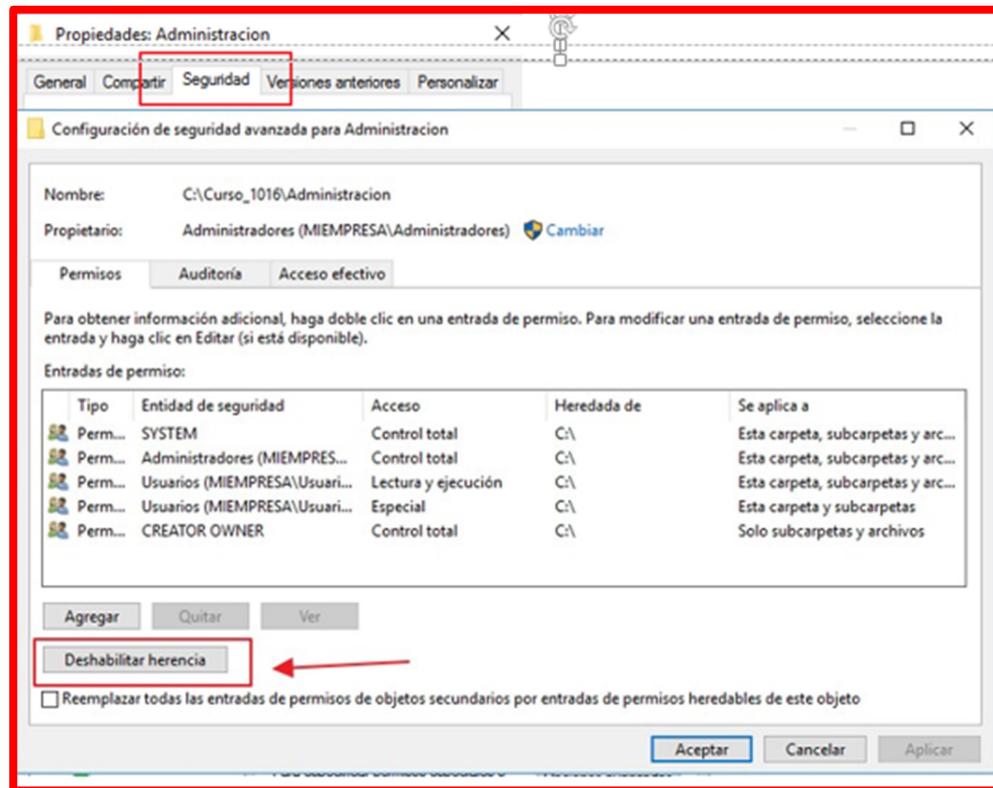
La carpeta en la que impide la herencia de permisos se convierte en la nueva carpeta principal. De esta forma, las subcarpetas y los archivos incluidos en ella heredan los permisos que se le asignaron.



Veamos los permisos de una carpeta:

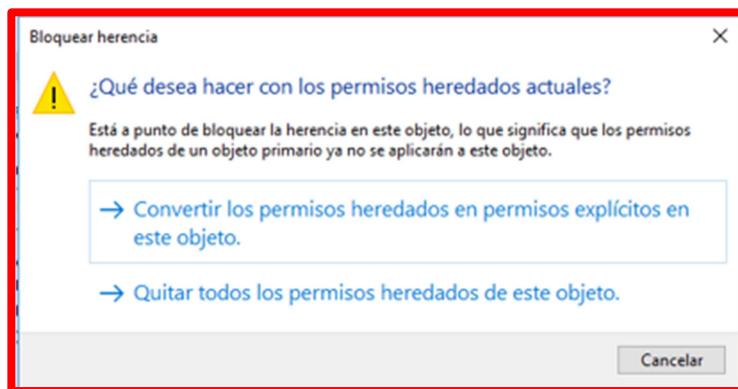
Nos fijaremos ahora en la pestaña de "Seguridad" que es la que se encarga de los permisos NTFS. Aparecen una serie de grupos con unos permisos y debajo los permisos que tienen. Si intentamos modificar estos permisos, el sistema operativo no nos lo permite.

Esto es porque esta carpeta tiene activada la herencia de permisos y sólo admite los que tenga la carpeta de su nivel superior. Hacemos clic en el botón de "Opciones avanzadas":



Además de algunas opciones que ya veremos, nos encontramos debajo con que está activada la herencia porque nos aparece la opción de desactivarla con "Deshabilitar herencia". Es decir, esta carpeta hereda los permisos de la carpeta padre y por eso no nos deja modificar los permisos.

Esto lo veremos después, pero si queremos eliminar la herencia de permisos de esta carpeta para ponerles unos distintos la desactivaremos pulsando en el botón "Deshabilitar herencia":



Son las dos opciones que comentábamos al principio de esta sección de herencia. Esta carpeta tenía ya unos permisos establecidos por herencia. Si los quitamos nos pregunta qué queremos hacer con los que ya existen. Los podemos copiar, y de esta forma sólo tengo que hacer una pequeña modificación, o los podemos quitar porque queremos ponerlos nuevos. Sólo se trata de una ayuda para ver qué hacemos con los permisos que ya existen. Veamos qué sucede al indicar que queremos que los copie, es decir "convertir los permisos heredados en permisos explícitos en este objeto".

Los permisos siguen estando porque los hemos copiado de su carpeta padre de donde estaba heredando. Además, como hemos roto esa herencia, permite ponerle permisos distintos ya que están activas las casillas de verificación de abajo.

Apenas se aprecia la diferencia visualmente pero funcionalmente es muy distinta. Antes no podíamos modificar permisos porque estaba activada la opción que tuviera los de la carpeta inmediatamente principal. Ahora en cambio, son totalmente editables ya que le hemos indicado que tenga sus propios permisos rompiendo la herencia.

Recomendaciones

Después de este ejemplo sigamos viendo las recomendaciones necesarias para asignar correctamente los permisos.

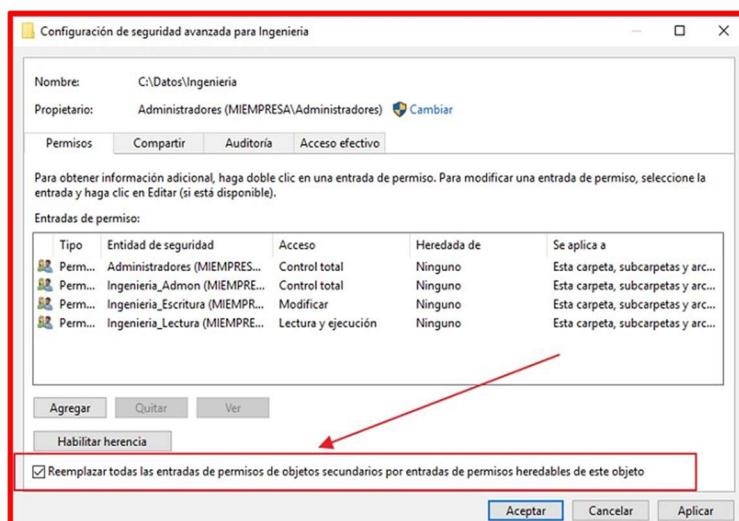
- Se deben conceder permisos a grupos en lugar de a usuarios. Como no es eficaz mantener cuentas de usuario directamente, evita conceder permisos a usuarios individuales.
- Utilizar permisos Denegar en las siguientes situaciones:
 - Para excluir a un subconjunto de un grupo que tiene permisos Permitir.
 - Para excluir un permiso cuando ya se han concedido permisos de control total a un usuario o grupo.
- Si es posible, no cambiaremos las entradas de permisos predeterminadas de los objetos del sistema de archivos. Sobre todo, en las carpetas del sistema y las carpetas raíz. Si se cambian los permisos predeterminados, pueden producirse problemas de acceso inesperados o se puede reducir la velocidad.
- No denegaremos nunca el acceso del grupo "Todos" a un objeto. Si lo hacemos, también se deniega a los administradores. En su lugar, es recomendable que se eliminemos el grupo "Todos", siempre y cuando se concedan permisos para el objeto a otros usuarios, grupos o equipos. (como hemos hecho antes)
- Conceder permisos a un objeto ubicado en el nivel más alto posible del árbol para que la configuración de seguridad se propague por todo éste. Podemos conceder de forma rápida y eficaz permisos a todos los objetos secundarios o a un subárbol de un objeto principal. Mediante esta acción, podemos conceder permisos a la mayor parte de los objetos con el menor esfuerzo. Para simplificar la administración, agruparemos los archivos según su función. Por ejemplo:
 - Agrupar archivos de programa en las carpetas en las que residen las aplicaciones utilizadas habitualmente.
 - Agrupar en una carpeta las carpetas de datos que contienen carpetas principales.
 - Agrupar en una carpeta los archivos de datos compartidos por varios usuarios.
- Sólo autorizaremos a los usuarios el nivel de acceso que necesiten. Por ejemplo, si un usuario necesita leer un archivo, concederemos al grupo al que pertenece un permiso de lectura para ese archivo.
- Concederemos permisos de escritura y permisos de lectura y ejecución al grupo "Usuarios" o permisos de modificación al grupo "Creador Propietario" para las carpetas de datos. Esto permite a los usuarios leer y modificar documentos que crean otros usuarios y leer, modificar y eliminar los archivos y las carpetas que crean ellos mismos.

Aunque estas son normas estándar, podemos mejorarlitas un poco más evitando la utilización de la opción de "denegar" permisos. Si algún usuario no debe tener permiso es mejor crear un grupo donde no se encuentre que poner a todos y luego una excepción a ese usuario.

7.2. Limpiar permisos

Hay una forma de aplicar unos permisos en la raíz de ingeniería y que aplique todo esto a su interior de forma que modifique la ACL completa de todas las carpetas y directorios estableciendo la que pongamos en la raíz. Haremos lo siguiente...

Ponemos los permisos que queramos aplicar hacia adentro, es decir a las carpetas inferiores, nos vamos a las propiedades avanzadas y:



Queremos que haga lo que pone en la casilla de verificación: "Reemplazar todas las entradas...". Esto hace que quite todos los permisos y establece los que pone en esta lista.

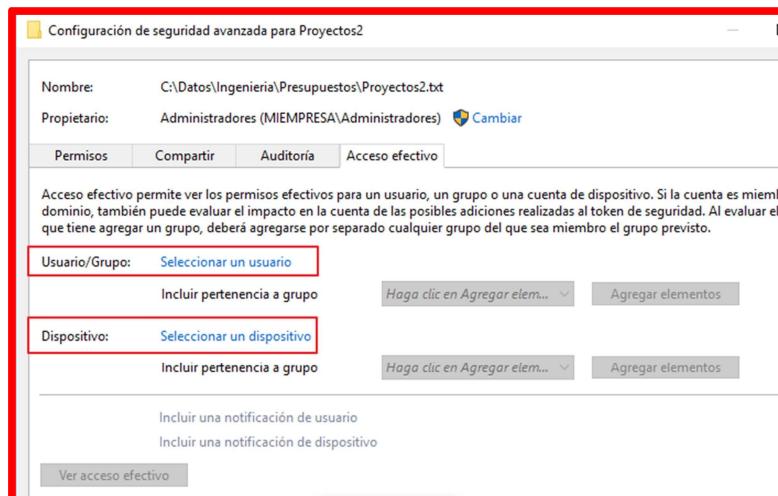
Con esto conseguimos limpiar completamente todo nuestro árbol y así poder comenzar a poner los permisos de los usuarios, pero con grupos.

7.3. Permisos efectivos

Con todas estas opciones de permisos, hay ocasiones en las que puede que algún usuario no tenga acceso a algún fichero o carpeta. Nos gustaría saber de alguna forma qué permisos efectivos tiene una carpeta o fichero. Entre las herencias de permisos y otras manipulaciones puede que hayamos creado una incongruencia en los permisos. Para ver el resultado de todos los permisos aplicados tenemos una pequeña ayuda que nos va a indicar los permisos que tiene ese fichero o carpeta.

Disponemos de una herramienta que nos muestra los permisos acumulados basados en la pertenencia a un grupo. La información se calcula a partir de las entradas de permisos existentes y se muestra en formato de sólo lectura. Los permisos efectivos tienen las siguientes características:

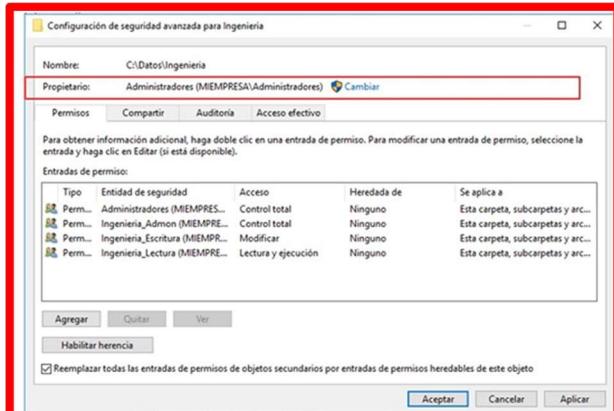
- Los permisos acumulados son la combinación de los permisos NTFS de más alto nivel concedidos al usuario y todos los grupos de los que el usuario es miembro.
- Los permisos de archivo NTFS tienen prioridad sobre los permisos de carpeta.
- Cada objeto, ya sea de un volumen NTFS o de Active Directory, tiene un propietario. El propietario controla el modo en que se establecen los permisos del objeto y a quién se conceden.
- También tiene en cuenta todos los permisos heredados del objeto principal. Durante ese análisis se examinan todos los grupos de dominios y locales de los que el usuario o el grupo es miembro.



7.4. Posesión de archivos o carpetas

Si un administrador necesita arreglar o cambiar los permisos de un archivo, debe tomar posesión del archivo. Así que antes de ver los permisos veamos qué es ser el propietario de un fichero o carpeta y cómo se toma posesión.

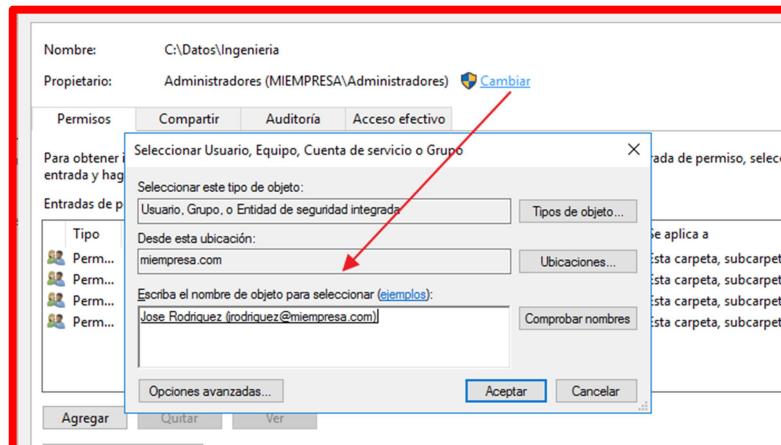
En la familia Windows Server, el propietario es de manera predeterminada el grupo "Administradores". El propietario puede cambiar en todo momento los permisos de un objeto, incluso aunque se le haya denegado el acceso a este objeto. Además de este grupo también lo será el usuario que lo ha creado. En este ejemplo lo hicimos con el usuario administrador, pero podía ser tranquilamente "jose_rodriguez". Los propietarios deben, además del que ha creado el objeto, ser los administradores del sistema para poder corregir situaciones de falta de acceso o errores en los permisos.



La posesión puede ser tomada por:

- Un administrador. De manera predeterminada, al grupo Administradores se le concede el derecho de usuario "Tomar posesión de archivos y otros objetos".
- Cualquier usuario o grupo que tenga el permiso "Tomar posesión" en el objeto en cuestión. Un usuario que tenga el privilegio "Restaurar archivos y directorios".

La posesión se puede transferir de muchas formas, pero las más fáciles es indicando esta acción desde:



7.5. Ver los permisos efectivos

Ya sabemos quién es el propietario de un archivo o carpeta. Ahora veremos cómo podemos saber los permisos efectivos de un fichero.

Una vez seleccionado, pulsamos en el botón de "Ver acceso efectivo":

Acceso efectivo	Permiso	Acceso limitado por
X	Control total	Permisos de archivo
X	Acceder carpetas / ejecutar archivo	Permisos de archivo
X	Mostrar carpeta / leer datos	Permisos de archivo
X	Leer atributos	Permisos de archivo
X	Leer atributos extendidos	Permisos de archivo
X	Crear archivos / escribir datos	Permisos de archivo
X	Crear carpetas / anexar datos	Permisos de archivo
X	Escribir atributos	Permisos de archivo
X	Escribir atributos extendidos	Permisos de archivo
X	Eliminar	Permisos de archivo
X	Permisos de lectura	Permisos de archivo

8. Administración de recursos del servidor

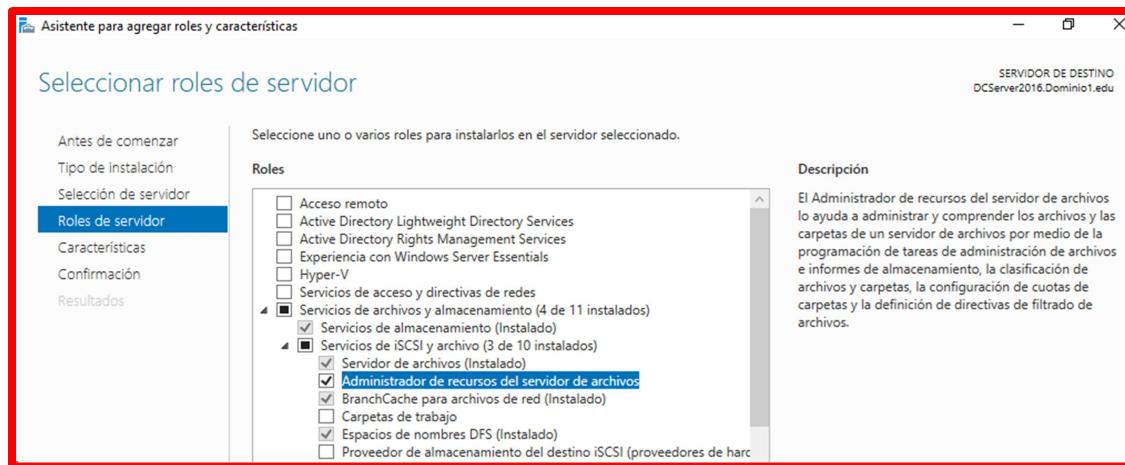
El **Administrador de recursos del servidor de archivos** es un conjunto de herramientas que permite a los administradores controlar y administrar la cantidad y el tipo de datos almacenados en los servidores. Los administradores pueden usarlo para asignar cuotas a volúmenes, realizar un filtrado activo de los archivos y carpetas, generar informes de almacenamiento exhaustivos, controlar la infraestructura de clasificación de archivos y usar las tareas de administración de archivos para llevar a cabo acciones programadas en conjuntos de archivos. Este conjunto de instrumentos avanzados ayuda a los administradores no solo a supervisar los recursos de almacenamiento existentes eficazmente, sino también a planear e implementar futuros cambios de directivas.

Mediante el **Administrador de recursos del servidor de archivos** se pueden acometer las siguientes tareas:

- Crear cuotas para limitar el espacio asignado a un volumen o carpeta y generar notificaciones de correo electrónico o de otro tipo cuando se esté a punto de alcanzar o superar el límite de dichas cuotas.
- Generar y aplicar cuotas automáticamente a las subcarpetas nuevas y existentes de un volumen o carpeta.
- Crear filtros de archivos para controlar el tipo de archivos que los usuarios pueden guardar, así como enviar notificaciones cuando los usuarios intenten guardar archivos bloqueados.
- Definir plantillas de filtrado de archivo y de cuota que puedan aplicarse fácilmente a nuevos volúmenes o carpetas y que se puedan usar en toda una organización.

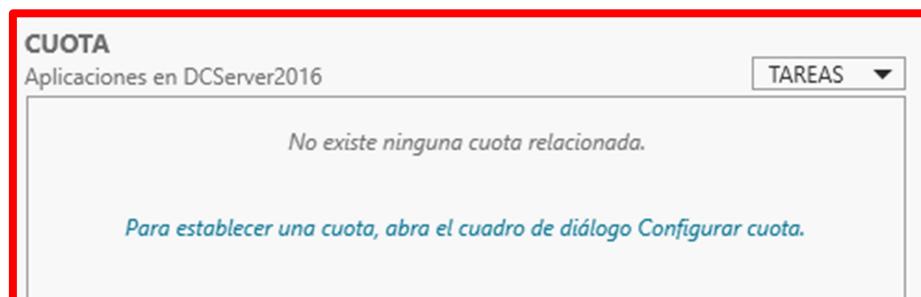
El **Administrador de recursos del servidor de archivos** es un servicio del rol **Servicios de archivo** en Windows Server 2016. Puede instalarse como parte de este rol mediante el **Administrador de servidores**. El requisito mínimo para utilizar el **Administrador de recursos del servidor de archivos** es pertenecer al grupo local **Administradores** o grupo equivalente.

Para su instalación vamos a **Agregar roles de servidor > Servicios de archivos y almacenamiento > Servicios de iSCSI y archivo > Administrador de recursos del servidor de archivos** (marcar opción)

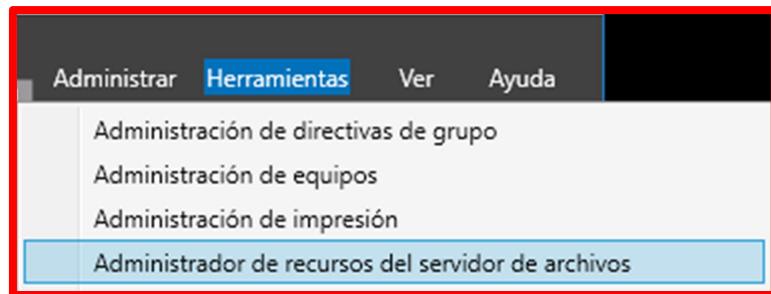


En las siguientes opciones los limitaremos a marcar la opción **Siguiente** hasta que nos ofrezca la opción **Instalar**.

Si volvemos a **Administrador del servidor > Servicios de archivos y de almacenamiento (panel de la izquierda) > Recursos compartidos**, veremos a la derecha que ahora sí nos permite crear **cuotas**.



Una vez instalado abriremos la consola *Administrador de recursos del servidor de archivos* desde *las Herramientas administrativas*.



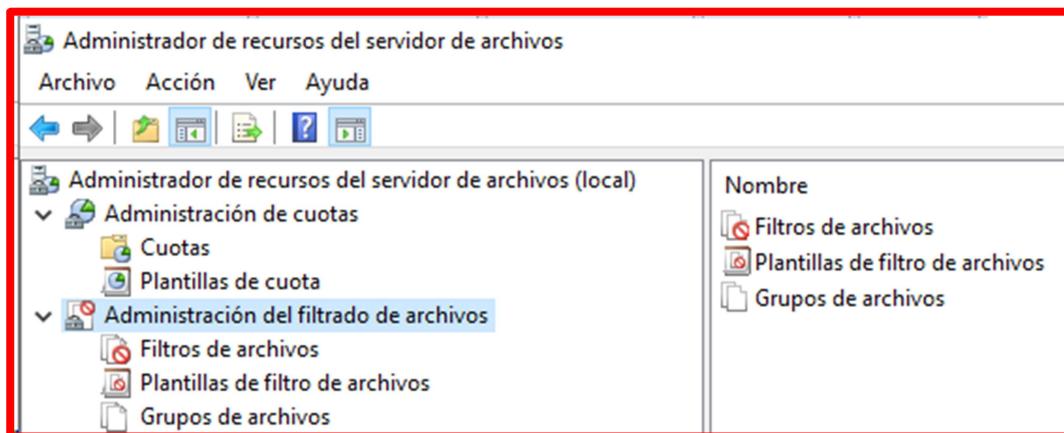
A continuación, aparece una lista de las tareas que puede realizar desde los nodos principales en el complemento del *Administrador de recursos del servidor de archivos*. Sólo veremos las siguientes:

Administración de cuotas:

- Para crear, administrar y obtener información acerca de las cuotas, las cuales se utilizan para establecer un límite de espacio en una carpeta o volumen. Al definir los umbrales de notificación, podemos enviar notificaciones por correo electrónico, registrar un evento, ejecutar un comando o un script o generar informes cuando los usuarios se acercan a la cuota o la superan.
- Para crear y administrar plantillas de cuotas para simplificar la administración de las cuotas.

Administración del filtrado de archivos:

- Para crear, administrar y obtener información acerca de los filtros de archivos, los cuales se utilizan para bloquear tipos de archivos seleccionados de una carpeta o volumen. Cuando los usuarios intenten guardar archivos no autorizados, se podrá enviar un correo electrónico a los administradores.
- Para crear excepciones de filtro de archivos para invalidar determinadas reglas de filtrado de archivos.
- Para crear y administrar plantillas de filtro de archivo para simplificar la administración del filtrado de archivos.
- Para crear y administrar grupos de archivos. Cuando se utilizan con filtros de archivos y excepciones de filtros de archivos, los grupos de archivos determinan qué archivos se bloquearán y cuáles se permitirán.



9. Trabajar con cuotas

Podemos utilizar el *Administrador de recursos del servidor de archivos* para crear una cuota para un volumen o carpeta y limitar así el espacio en disco que se le asigna. El límite de la cuota se aplica a todo el subárbol de carpetas.

Podemos crear una cuota máxima o una cuota de advertencia:

- Una **cuota máxima** impide a los usuarios guardar archivos una vez alcanzado el límite de espacio y genera notificaciones cuando el volumen de datos llega al umbral configurado.
- La **cuota de advertencia** no impone un límite de cuota, pero genera todas las notificaciones configuradas.

Para determinar qué sucede cuando la cuota se acerca al límite, podemos configurar **umbrales de notificación**. Para cada umbral que definamos, podemos enviar notificaciones por correo electrónico, registrar un evento, ejecutar un comando o script, o generar informes de almacenamiento. Por ejemplo, es posible que deseemos enviar una notificación al administrador y al usuario que guardó el archivo cuando una carpeta alcance el 85% del límite de su cuota, y enviar otra notificación cuando se alcance el límite de la cuota. En algunos casos, podríamos desear ejecutar un script que aumente el límite de la cuota automáticamente cuando se alcance un umbral.

Al crear una *cuota en un volumen o una carpeta*, podemos basar la cuota en una plantilla de cuota o usar propiedades personalizadas. Es recomendable que, siempre que sea posible, basemos una cuota en una plantilla de cuota. Una plantilla de cuota se puede volver a usar para crear cuotas adicionales y simplifica el mantenimiento continuo de la cuota.

El *Administrador de recursos del servidor de archivos* también puede generar *cuotas automáticamente*. Al configurar una cuota automática, podemos aplicar una plantilla de cuota a un volumen o una carpeta principal. Se crea una cuota basada en la plantilla para cada una de las subcarpetas existentes y se genera una cuota automáticamente para cada subcarpeta nueva que se cree.

9.1. Plantillas de cuota

El *Administrador de recursos del servidor de archivos* proporciona flexibilidad para crear, utilizar y administrar plantillas, tanto para cuotas como para filtros de archivos.

Una *plantilla de cuota* define un límite de espacio, el tipo de cuota (máxima o de advertencia) y un conjunto de notificaciones que se generarán cuando se acerque o supere el límite de la cuota.

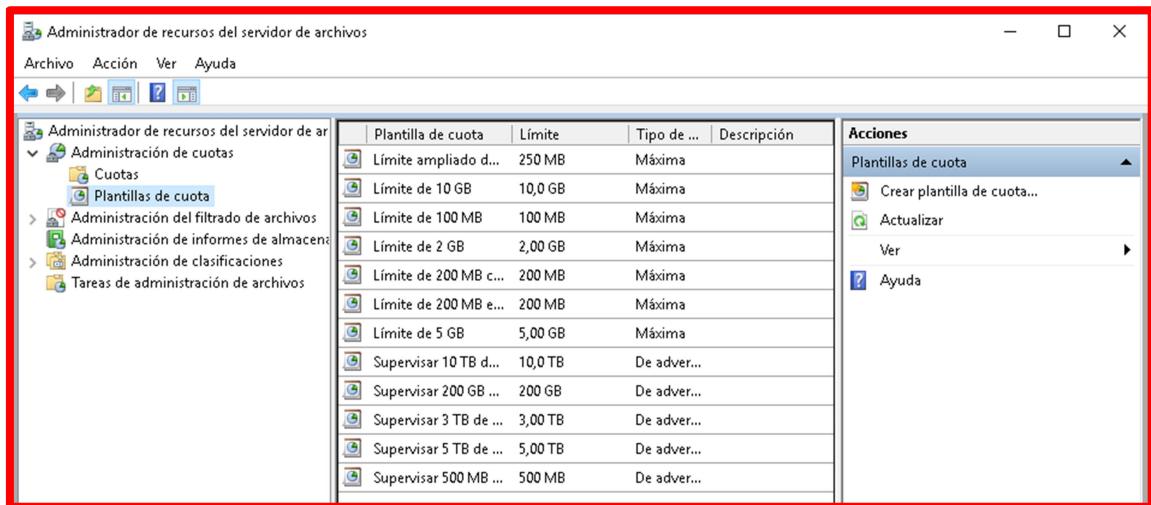
Las plantillas de cuota simplifican la creación y el mantenimiento de cuotas:

- Si usamos una plantilla de cuota, podemos aplicar un límite de almacenamiento estándar y un conjunto estándar de umbrales de notificación para muchos volúmenes y carpetas en los servidores de la organización.
- Si basamos las cuotas en una plantilla, podemos actualizar automáticamente todas las cuotas basadas en una plantilla determinada mediante la edición de dicha plantilla. Esta característica simplifica el proceso de actualización de las propiedades de las cuotas.

El *Administrador de recursos del servidor de archivos* proporciona varias plantillas de cuota. Por ejemplo:

- Podemos usar la plantilla **Límite de 200 MB** en informes a usuario para aplicar un límite máximo de 200 MB a la carpeta personal de cada usuario.
- Para algunas carpetas, es posible que deseemos usar la **plantilla Límite de 200 MB con extensión de 50 MB** para aumentar automáticamente el límite de la cuota cuando se alcance un límite de cuota de 200 MB.
- Otras plantillas predeterminadas están diseñadas para supervisar el uso del disco mediante cuotas de advertencia (por ejemplo, la plantilla **Supervisar 200 GB de uso de volumen** y la plantilla **Supervisar 500 MB de recursos compartidos**). Al usar estas plantillas, los usuarios pueden superar el límite de la cuota, pero cuando lo hacen se generan notificaciones de correo electrónico y del registro de eventos.

Para ver las plantillas predeterminadas, hacemos clic en el nodo Plantillas de cuota en el árbol de consola del Administrador de recursos del servidor de archivos:



Ejercicio: ¿Qué es una cuota? ¿Qué diferencia hay entre una cuota máxima y una cuota de advertencia? Muestra las plantillas de cuota predeterminadas.

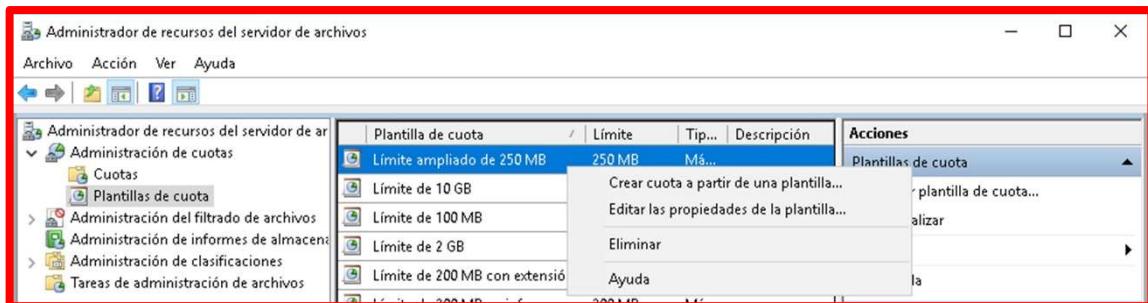
9.2. Crear una cuota

El siguiente procedimiento nos dirigirá en el proceso de crear una **cuota basada en una plantilla** (éste es el procedimiento recomendado).

Ejercicio: Crea una cuota basada en una plantilla tal y como se muestra en el siguiente apartado.

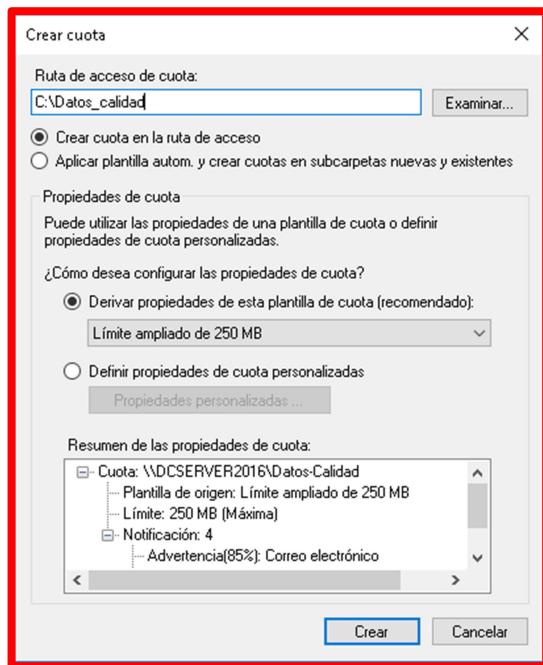
Para crear una cuota basada en una plantilla:

1. En **Administración de cuotas**, hacemos clic en el **nodo Plantillas de cuota**.
2. En el panel de resultados, seleccionamos la plantilla sobre la que basaremos la cuota, por *ejemplo Límite ampliado de 250 MB*.
3. Hacemos clic con el botón secundario en la plantilla y seleccionamos **Crear cuota a partir de una plantilla ...** (o seleccionamos **Crear cuota a partir de una plantilla ...** en el panel **Acciones**).



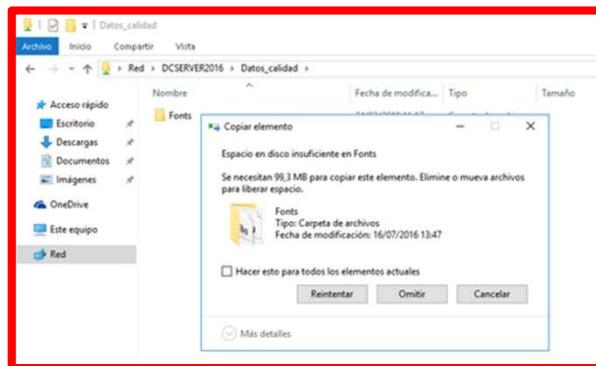
4. Se abrirá el cuadro de diálogo **Crear cuota** con las propiedades resumidas de la plantilla de cuota mostrada.
5. En **Ruta de acceso de cuota**, escribiremos el nombre del volumen o carpeta al que se aplicará la cuota o lo buscamos.

6. Haremos clic en la opción **Crear cuota en la ruta de acceso**. Tengamos en cuenta que las propiedades de la cuota se aplicarán a todo el volumen o carpeta.



7. En **Derivar propiedades** desde esta plantilla de cuota, aparecerá preseleccióna la plantilla usada en el paso 2 para crear la nueva cuota (o podemos seleccionar otra plantilla en la lista). Tengamos en cuenta que las propiedades de la plantilla se mostrarán en el **Resumen de las propiedades de cuota**.
8. Finalmente hacemos clic en **Crear**.

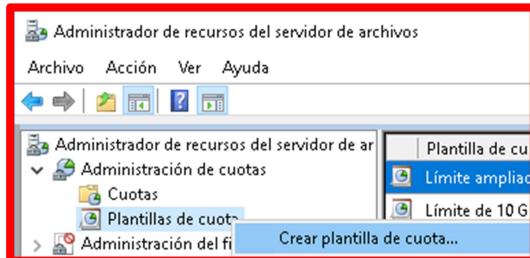
Si no deseamos basar la cuota en una plantilla, o si queremos editar las propiedades que se copiaron desde una plantilla, en el cuadro de diálogo **Crear cuota** elegimos **Definir propiedades de cuota personalizadas** y, a continuación, hacemos clic en **Propiedades personalizadas**. Tengamos en cuenta que, si creamos una cuota con propiedades personalizadas, tendremos la opción de guardar una plantilla de cuota con la configuración de cuota personalizada. Si elegimos esa opción, se guardará una plantilla nueva y se aplicará dicha plantilla a la nueva cuota, de forma que se mantenga un vínculo entre la cuota y la plantilla.



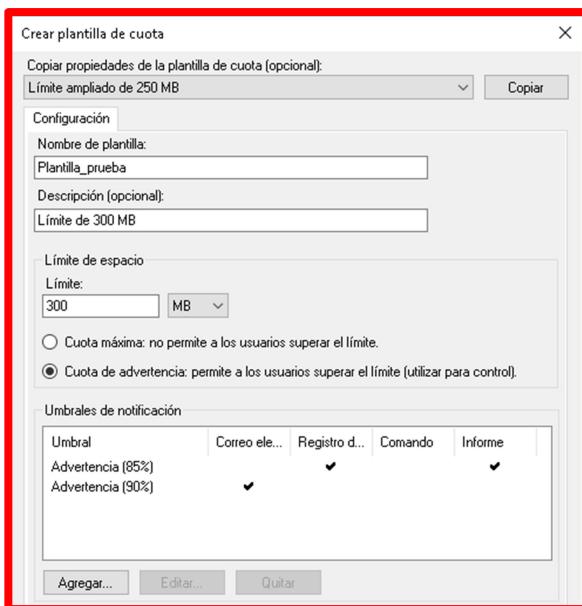
Crear una plantilla de cuota

Para ello seguiremos los siguientes pasos:

1. En **Administración de cuotas**, hacemos clic en el nodo **Plantillas de cuota**.
2. Hacemos clic con el botón secundario en **Plantillas de cuota** y, a continuación, pulsamos en **Crear plantilla de cuota** (o seleccionamos **Crear plantilla de cuota** en el panel Acciones).



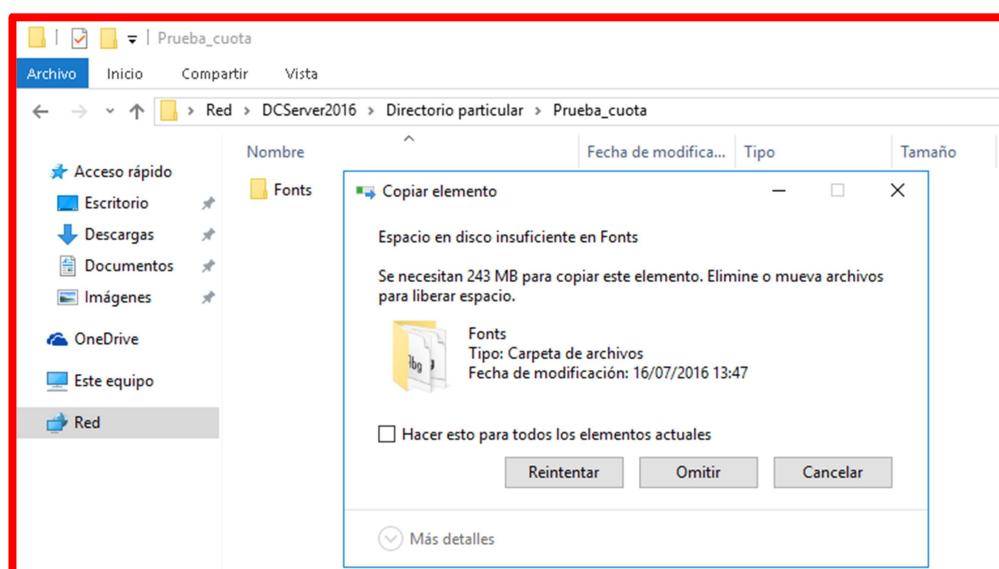
3. Si deseamos copiar las propiedades de una plantilla existente para usarla como base de la nueva plantilla, seleccionamos una plantilla en la lista desplegable **Copiar propiedades de la plantilla de cuota**. A continuación, hacemos clic en **Copiar**.
4. En el cuadro de texto **Nombre de plantilla**, escribimos el nombre de la nueva plantilla, por ejemplo *Plantilla_prueba*.
5. En el cuadro de texto **Descripción**, escribiremos una etiqueta descriptiva opcional que aparecerá junto a las cuotas derivadas de la plantilla, por ejemplo *Límite de 300 MB*.
6. En **Límite de espacio**:
 - a. En el cuadro de texto **Límite**, escribiremos un número y elegiremos una unidad (KB, MB, GB o TB) para especificar el límite de espacio de la cuota, por ejemplo 300 MB.
 - b. Hacemos clic en la **opción Cuota máxima o Cuota de advertencia**. La cuota máxima impide a los usuarios guardar archivos una vez alcanzado el límite de espacio y genera notificaciones cuando el volumen de datos llega al umbral configurado. La cuota de advertencia no impone un límite de cuota, pero genera todas las notificaciones configuradas.
7. Podemos configurar uno o varios umbrales de notificación opcionales para la plantilla de cuota. Después de seleccionar todas las propiedades de la plantilla de cuota que deseemos usar, hacemos clic en **Aceptar** para guardar la plantilla.



Y ya tendremos creada nuestra **plantilla de cuota** personalizada:

Plantilla de cuota	Límite	Tip...	Descripción
Límite ampliado de 250 MB	250 MB	Má...	
Límite de 10 GB	10,0 GB	Má...	
Límite de 100 MB	100 MB	Má...	
Límite de 2 GB	2,00 GB	Má...	
Límite de 200 MB con extensi... on	200 MB	Má...	
Límite de 200 MB en informes ...	200 MB	Má...	
Límite de 5 GB	5,00 GB	Má...	
Plantilla_prueba	300 MB	De ...	Límite de 30...
Supervisar 10 TB de uso de vol...	10,0 TB	De ...	
Supervisar 200 GB de uso de v...	200 GB	De ...	
Supervisar 3 TB de uso de volu...	3,00 TB	De ...	
Supervisar 5 TB de uso de volu...	5,00 TB	De ...	
Supervisar 500 MB de recursos ...	500 MB	De ...	

Ahora podríamos crear cuotas sobre volúmenes o carpetas tal y como hemos hecho en el apartado anterior.



A continuación, podemos ver las cuotas que tenemos definidas hasta el momento:

Ruta de acceso de cuota	% usado	Límite	Tipo de cuota	Plantilla de origen	Coincide con plantilla	Descripción
C:\Directorio particular	0%	100 MB	Máxima	Ejercicio2	Sí	Límite 100 MB
C:\Datos_calidad	96%	250 MB	Máxima	Límite ampliado de 250 MB	Sí	

10. Filtrar archivos

Crear *filtros de archivos* sirve para bloquear archivos que pertenezcan a *grupos de archivos* particulares para evitar que se guarden en un volumen o en un árbol de carpetas. El filtro de archivos afecta a todas las carpetas de la ruta de acceso designada. Por ejemplo, podríamos crear un filtro de archivos para impedir que los usuarios almacenen archivos de audio y vídeo en sus carpetas personales en el servidor.

Podemos configurar el *Administrador de recursos del servidor de archivos* para que genere correo electrónico u otro tipo de notificaciones cuando se produzca un evento de filtrado de archivos.

Un filtro de archivos puede ser activo o pasivo:

- Un **filtrado activo** impide que los usuarios guarden tipos de archivos no autorizados en el servidor y genera notificaciones configuradas cuando intentan hacerlo.
- El **filtrado pasivo** envía notificaciones configuradas a los usuarios que guardan tipos de archivos específicos, pero no impide que los guarden.

Un filtro de archivos no impide que los usuarios y aplicaciones accedan a los archivos que se guardaron en la ruta de acceso antes de que se creara dicho filtro, aunque los archivos sean miembros de grupos de archivos bloqueados.

Para simplificar la administración de los filtros de archivos, recomendamos basar los filtros en *plantillas de filtro de archivos*. Una plantilla de filtro de archivos define un tipo de filtrado (activo o pasivo), un conjunto de grupos de archivos que se debe bloquear y un conjunto de notificaciones que se generará cuando un usuario intente guardar un archivo no autorizado. El *Administrador de recursos del servidor de archivos* proporciona varias plantillas de filtro de archivos predeterminadas, que se pueden utilizar para bloquear archivos de audio y vídeo, archivos ejecutables, archivos de imágenes y archivos de correo electrónico, etc. Para ver las plantillas predeterminadas, seleccionamos el nodo **Plantillas de filtro de archivos** en el árbol de consola del *Administrador de recursos del servidor de archivos*.



Para mayor flexibilidad, podemos configurar una *excepción al filtro de archivos* en una subcarpeta en una ruta de acceso donde hayamos creado un filtro de archivos. Cuando coloquemos una excepción al filtro de archivos en una subcarpeta, permitiremos que los usuarios guarden tipos de archivos que, de lo contrario, serían bloqueados por el filtro de archivos que se aplicó a la carpeta principal.

10.1. Trabajar con grupos de archivos

Antes de comenzar a trabajar con filtros de archivos, debemos entender la función que tienen los grupos de archivos en la determinación de qué archivos se van a filtrar. Un *grupo de archivos* se utiliza para definir un espacio de nombres para un filtro de archivos o una excepción al filtro de archivos, o bien para generar un informe de almacenamiento de archivos por grupo de archivos.

Un grupo de archivos consta de un conjunto de patrones de nombre de archivo, que se agrupan en archivos incluidos y archivos excluidos:

- **Archivos incluidos:** archivos que pertenecen al grupo.
- **Archivos excluidos:** archivos que no pertenecen al grupo.

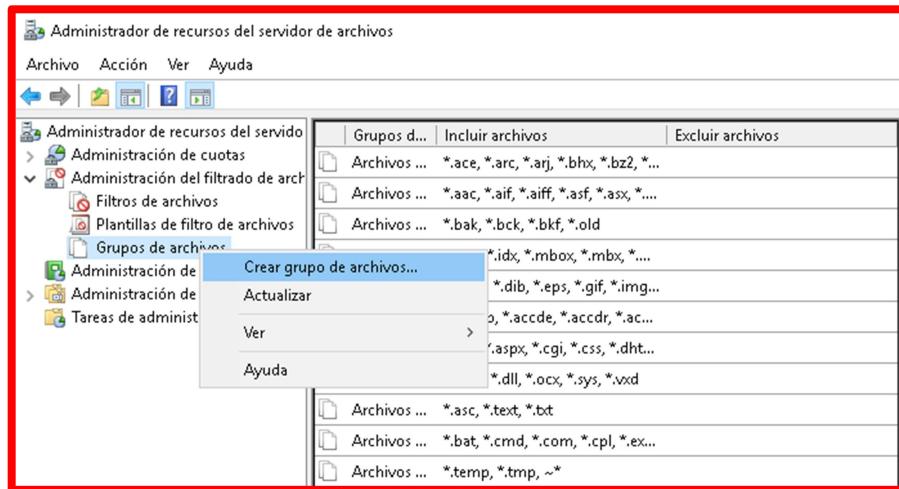
Por ejemplo, un grupo de archivos *Archivos de audio* podría incluir los siguientes patrones de nombre de archivo:

- **Archivos incluidos:** **.mp**: incluye todos los archivos de audio que se crean en formatos MPEG actuales y futuros MPEG (MP2, MP3, MP4, MP5, etc.).
- **Archivos excluidos:** **.mpp*: excluye los archivos creados en Microsoft Project (archivos .mpp), que de lo contrario serían incluidos por la regla de inclusión **.mp**.

El *Administrador de recursos del servidor de archivos* proporciona varios grupos de archivos predeterminados que podemos ver en **Administración del filtrado de archivos** haciendo clic en el nodo **Grupos de archivos**. Podemos definir grupos de archivos adicionales, o bien cambiar los archivos incluidos y excluidos. Cualquier cambio que hagamos a un grupo de archivos afecta a todos los filtros, plantillas e informes existentes a los cuales se ha agregado el grupo de archivos.

Para crear un grupo de archivos:

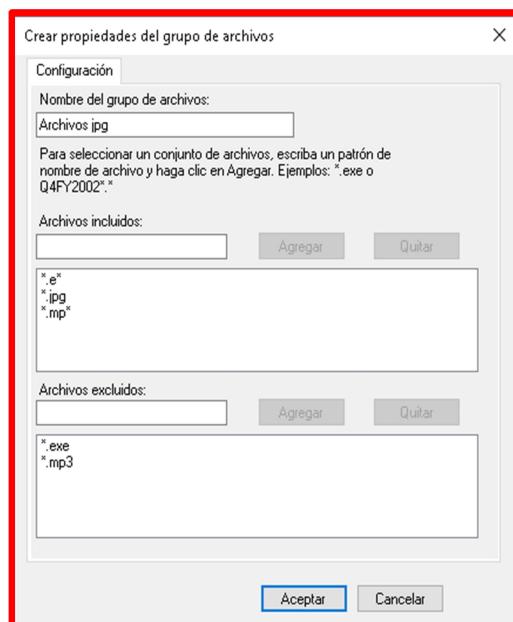
1. En **Administración del filtrado de archivos**, hacemos clic en **Grupos de archivos**.
2. Pulsamos con el botón derecho del ratón en **Crear grupo de archivos**. Se abrirá el cuadro de diálogo **Crear propiedades del grupo de archivos**.



3. En el cuadro de diálogo **Crear propiedades del grupo de archivos**, escribimos un nombre para el grupo de archivos, por ejemplo, *Archivos jpg*.

4. Agregamos los archivos que se van a incluir y los que se van a excluir:

- Para cada conjunto de archivos que deseemos **incluir** en el grupo de archivos, en **Archivos incluidos**, escribiremos un patrón de nombre de archivo y luego pulsamos en **Agregar**. Se aplican reglas estándares para caracteres comodines. Por ejemplo, ***.jpg** selecciona todos los archivos con este formato para imágenes. También bloquearemos ***.e*** y ***.mp***.
- Para cada conjunto de archivos que deseemos **excluir** del grupo de archivos, en **Archivos excluidos**, escribiremos un patrón de nombre de archivo y luego pulsaremos en **Agregar**. Tengamos en cuenta que se aplican reglas estándares para caracteres comodines, por ejemplo, ***.exe** selecciona todos los archivos ejecutables y ***.mp3** selecciona los archivos con este formato de audio.



5. Finalmente pulsamos en **Aceptar**.

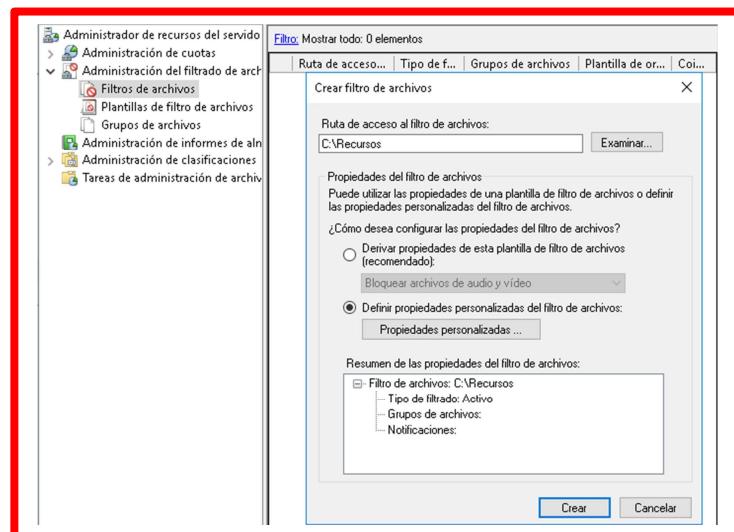
Crear un filtro de archivos

En el siguiente procedimiento, crearemos un nuevo filtro de archivos y en el proceso guardaremos una plantilla de filtro de archivos que se basa en las propiedades personalizadas del filtro de archivos que definimos anteriormente. La nueva plantilla se aplica al filtro de archivos de manera que se mantiene un vínculo entre el filtro de archivos y la plantilla.

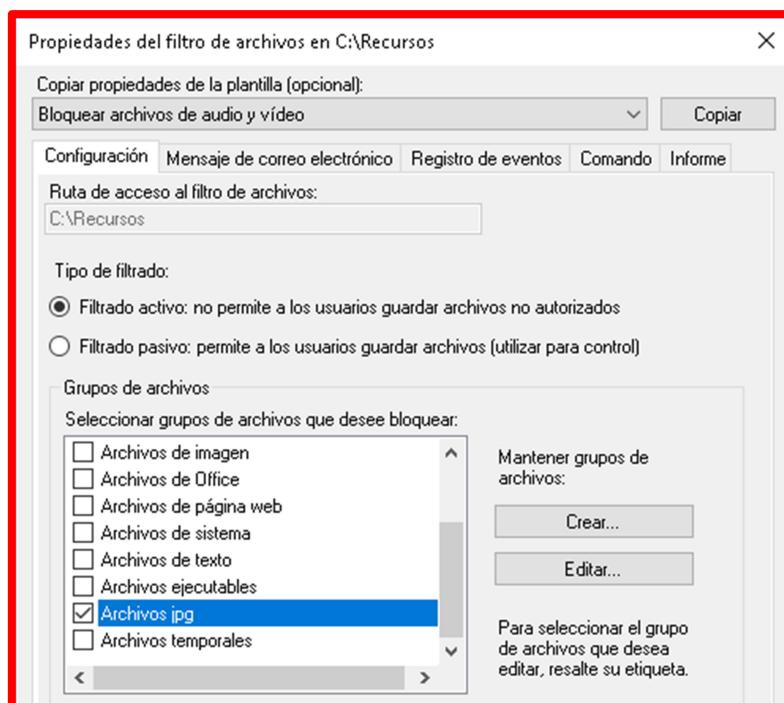
De manera similar, podemos crear una nueva *plantilla de filtro de archivos* que se base en las propiedades de un *filtro de archivos* que creamos.

Para crear un **filtro de archivos**:

1. En **Administración del filtrado de archivos**, hacemos clic en el nodo **Filtros de archivos**.
2. Hacemos clic con el botón secundario del mouse en **Filtros de archivos** y pulsamos en **Crear filtro de archivos** (o en **Crear filtro de archivos** en el panel **Acciones**). Se abrirá el cuadro de diálogo **Crear filtro de archivos**.
3. En **Ruta de acceso al filtro de archivos**, escribiremos el nombre de la carpeta a la que se aplicará el filtro de archivos. El filtro de archivos se aplicará a la carpeta seleccionada y a todas sus subcarpetas. Por ejemplo crearemos una carpeta vacía llamada **Recursos**.
4. En **¿Cómo desea configurar las propiedades del filtro de archivos?**, hacemos clic en **Definir propiedades personalizadas del filtro de archivos** y, a continuación, clic en **Propiedades personalizadas**. Se abrirá el cuadro de diálogo **Propiedades del filtro de archivos**.

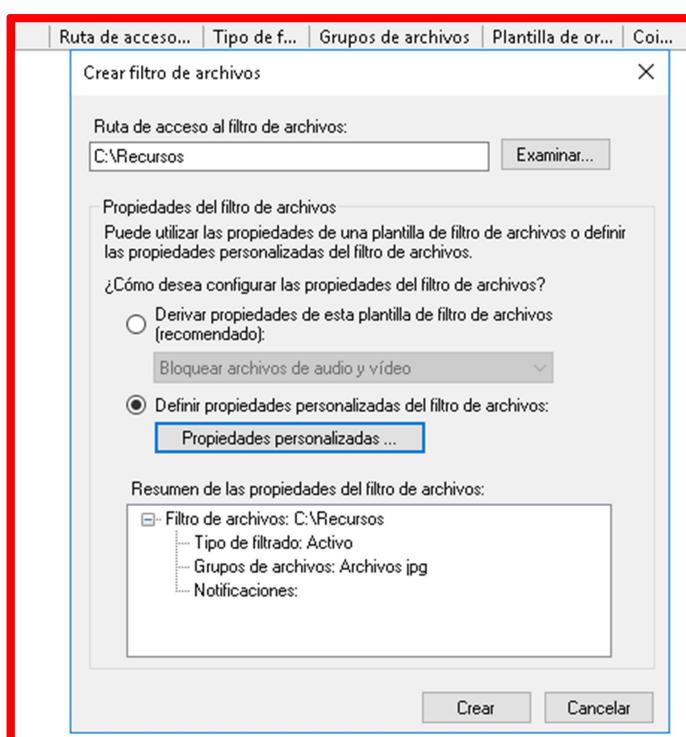


5. Si deseamos copiar las propiedades de una plantilla existente para usarla como base de su nuevo filtro de archivos, seleccionamos una plantilla de la lista desplegable **Copiar propiedades de la plantilla**. A continuación hacemos clic en **Copiar**. En nuestro caso no lo basaremos en ninguna plantilla por lo que no pulsaremos este botón.
6. En **Grupos de archivos**, seleccionamos cada grupo de archivos que deseamos incluir en el filtro de archivos. Elegiremos el creado anteriormente **Archivos jpg**.



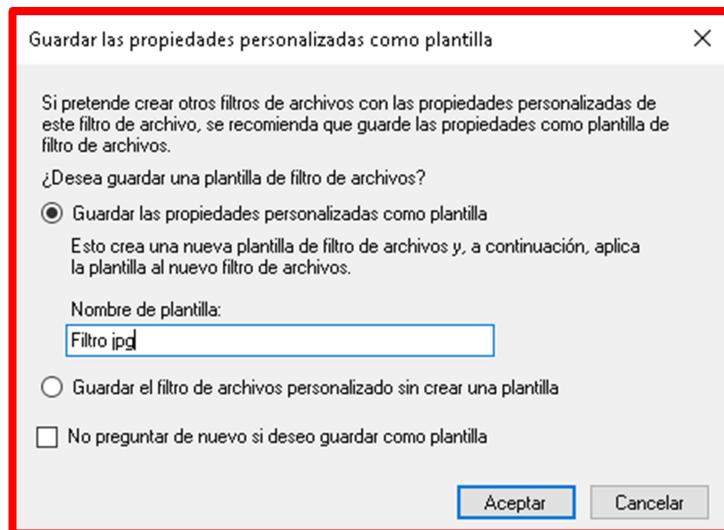
7. En **Tipo de filtrado**, hacemos clic en la opción **Filtrado activo** o **Filtrado pasivo**. Elegiremos, en nuestro ejemplo, **Filtrado activo para que no permita a los usuarios guardar archivos ejecutables en la carpeta Recursos**.
8. Si deseamos generar notificaciones de correo electrónico, en la ficha **Mensaje de correo electrónico**, configuraremos las siguientes opciones (no lo haremos en nuestro caso):
 - Para notificar a los administradores cuándo un usuario o una aplicación intente guardar un archivo no autorizado, activamos la casilla **Enviar correo electrónico a los siguientes administradores** y especificamos los nombres de las cuentas administrativas que van a recibir notificaciones. Usaremos el formato cuenta@dominio y separaremos las distintas cuentas con punto y coma.
 - Para enviar una notificación por correo electrónico al usuario que intentaba guardar el archivo, activaremos la casilla **Enviar correo electrónico al usuario que ha intentado guardar un archivo no autorizado**.
 - Para configurar el mensaje, editaremos la línea de asunto y el cuerpo de mensaje predeterminados que se proporcionan. El texto entre paréntesis inserta información de variables sobre el evento de filtro de archivos que causó la notificación. Por ejemplo, la variable **[Source Is Owner]** inserta el nombre del usuario que intentamos guardar el archivo no autorizado. Para insertar variables adicionales en el texto, haremos clic en **Insertar variable**.
 - Para configurar encabezados de correo electrónico adicionales (incluidos De, CC, CCO y Responder a), hacemos clic en **Encabezados de correo electrónico adicionales**.
 - Si deseamos registrar un error en el registro de eventos cuando un usuario intenta guardar un archivo no autorizado, en la ficha **Registro de eventos**, activaremos la casilla **Enviar advertencia al registro de eventos**. De manera opcional, editaremos la entrada de registro predeterminada.

9. Despu  s de seleccionar todas las propiedades del filtro de archivos que deseamos usar, haremos clic en **Aceptar** para cerrar el cuadro de di  logo **Propiedades del filtro de archivos**.



10. En el cuadro de di  logo **Crear filtro de archivos**, haremos clic en **Crear** para guardar el filtro de archivos. De este modo se abre el cuadro de di  logo **Guardar las propiedades personalizadas como plantilla**.

11. Para guardar una plantilla que se basa en estas propiedades personalizadas, haremos clic en **Guardar las propiedades personalizadas como plantilla** y escribiremos un nombre para la plantilla, por ejemplo **Filtro jpg**. Esta opción se aplica a la plantilla para el nuevo filtro de archivos, y se puede usar dicha plantilla para crear filtros de archivos adicionales en el futuro.

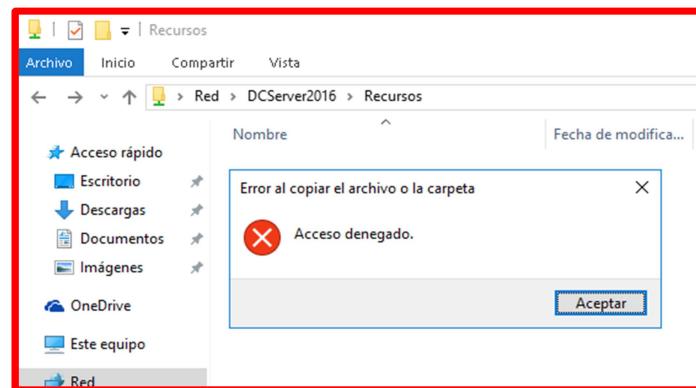


12. Acabamos pulsando en **Aceptar**.

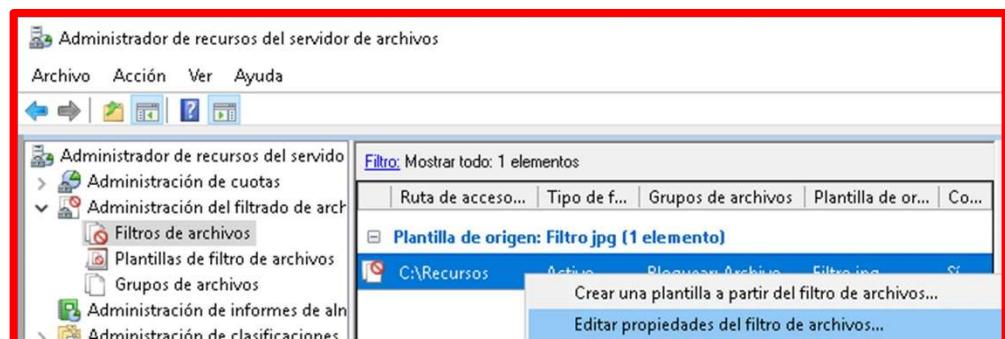
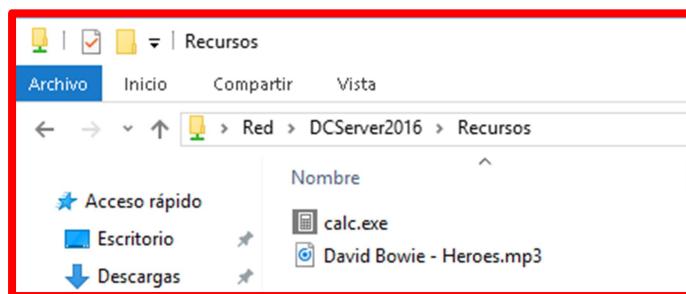
Plantilla de origen:	Filtro jpg (1 elemento)
C:\Recursos	Activo Bloquear: Archivo... Sí

Plantilla de filtro ...	Tipo de fil...	Grupos de archivos
Bloquear archivos ...	Activo	Bloquear: Archivos de audio y vídeo
Bloquear archivos ...	Activo	Bloquear: Archivos de correo electrónico
Bloquear archivos ...	Activo	Bloquear: Archivos de imagen
Bloquear archivos ...	Activo	Bloquear: Archivos ejecutables
Filtro jpg	Activo	Bloquear: Archivos jpg
Supervisar archivo...	Pasivo	Advertir: Archivos ejecutables, Archivos ...

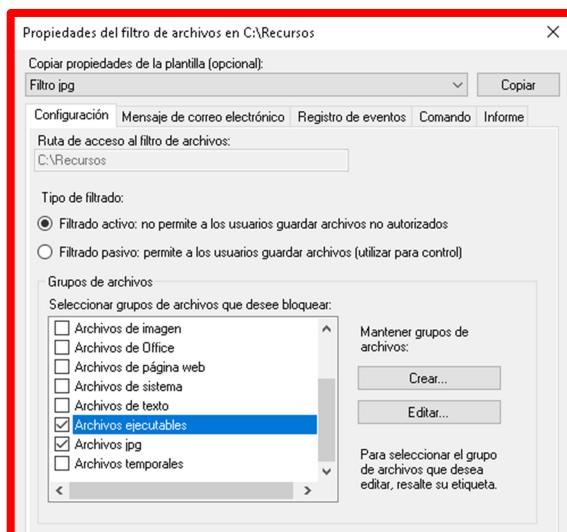
Nos aparecerá el siguiente aviso ya que existen archivos que no se pueden copiar en **Recursos** por las restricciones que hemos impuesto. **Omitimos para todos los elementos actuales:**



Finalmente, sólo copiará aquellos archivos cuya extensión hemos permitido como los .mp3 o .exe:



Marcamos, en sus propiedades, *Archivos ejecutables*, para que los bloquee y no puedan, ahora, copiarse archivos de este tipo en la carpeta **Recursos**:



Evidentemente, no nos lo permitirá, al estar bloqueados este tipo de archivos:

