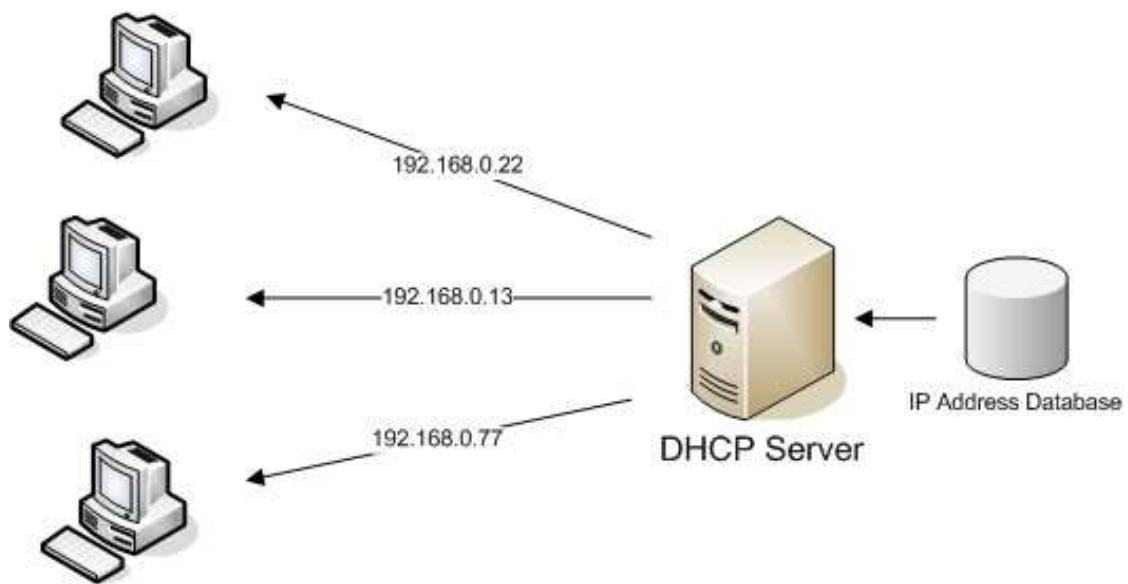


# UD8 Windows Server. Almacenamiento.

## Escritorio Remoto



## ÍNDICE

<b>1. Servidor DHCP .....</b>	<b>3</b>
<b>1.1. Definición de servidor DHCP .....</b>	<b>3</b>
<b>1.2. Instalación del servidor DHCP.....</b>	<b>4</b>
<b>1.3. Configuración del servidor DHCP.....</b>	<b>5</b>
<b>2. PERMISOS DE ARCHIVOS Y CARPETAS.....</b>	<b>11</b>
<b>2.1 Compartir archivos y carpetas.....</b>	<b>11</b>
<b>2.2 Permisos de carpetas y archivos .....</b>	<b>12</b>
<b>2.3 Definición de los permisos especiales .....</b>	<b>13</b>
<b>2.4 Establecimiento de permisos NTFS estándar para undirectorio o un archivo .....</b>	<b>17</b>
<b>2.5 Establecimiento de permisos NTFS especiales.....</b>	<b>18</b>
<b>2. 6 Ver permisos efectivos de archivos y carpetas .....</b>	<b>20</b>
<b>2. 7 Para ver permisos efectivos de archivos y carpetas .....</b>	<b>20</b>
<b>2.8 El propietario de un directorio o un archivo.....</b>	<b>20</b>
<b>2.9 Cómo establecer el permiso de toma de posesión .....</b>	<b>21</b>
<b>2.10 Cómo tomar posesión.....</b>	<b>21</b>
<b>3. Copia de seguridad del Directorio Activo .....</b>	<b>22</b>
<b>3.1 Proceso de copia de seguridad .....</b>	<b>23</b>
<b>3.2 Restauración .....</b>	<b>28</b>
<b>4. Almacenamiento en Windows Server .....</b>	<b>34</b>
<b>4.1. Sistemas RAID .....</b>	<b>35</b>
<b>4.3. Consola de administración de discos .....</b>	<b>38</b>
<b>4.4. Los discos en Windows Server.....</b>	<b>39</b>
<b>4.5. Administrar discos con Windows.....</b>	<b>43</b>
<b>5. Cuotas .....</b>	<b>53</b>
<b>5.1 Trabajar con cuotas .....</b>	<b>56</b>
<b>5.2 Acerca de las plantillas de cuota .....</b>	<b>56</b>
<b>5.3 Crear una cuota .....</b>	<b>57</b>
<b>5.3 Crear una plantilla de cuota .....</b>	<b>60</b>
<b>5.5 Filtrar archivos .....</b>	<b>62</b>

<b>5.6 Crear un filtro de archivos .....</b>	<b>62</b>
<b>5.7 Trabajar con grupos de archivos.....</b>	<b>66</b>
<b>5.7 Crear un filtro de archivos basado en un grupo de archivos personalizado .....</b>	<b>68</b>
<b>6. Definición de Escritorio remoto .....</b>	<b>76</b>
<b>6.1 Instalación de Servicios de Escritorio remoto .....</b>	<b>76</b>
<b>6.2 Habilitar el Escritorio remoto en el servidor .....</b>	<b>79</b>
<b>6.3 Ejecución del cliente de escritorio remoto .....</b>	<b>80</b>

# 1. Servidor DHCP.

---

## 1.1. Definición de servidor DHCP.

---

El protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) es un estándar TCP/IP diseñado para simplificar la administración de la configuración IP de los equipos de nuestra red. El estándar DHCP permite el uso de servidores DHCP para administrar la asignación dinámica, a los clientes DHCP de la red, de direcciones IP y otros detalles de configuración relacionados, siempre que los clientes estén configurados para utilizar un servidor DHCP (en lugar de estar configurados manualmente con una dirección IP, en las conexiones de red de las estaciones de trabajo, activaremos la "*configuración automática de IP*").

Cada equipo de una red TCP/IP debe tener un nombre y una dirección IP únicos. La dirección IP (junto con su máscara de subred relacionada) identifica al equipo host y a la subred a la que está conectado. Al mover un equipo a una subred diferente, se debe cambiar la dirección IP; DHCP permite asignar dinámicamente una dirección IP a un cliente, a partir de una base de datos de direcciones IP de servidor DHCP de la red local. En las redes TCP/IP, el servicio DHCP reduce la complejidad y cantidad de trabajo que debe realizar el administrador para reconfigurar los equipos.

DHCP es el protocolo de servicio TCP/IP que "alquila" o asigna dinámicamente direcciones IP durante un tiempo (duración del alquiler) a las estaciones de trabajo, distribuyendo además otros parámetros de configuración entre clientes de red autorizados, tales como la puerta de enlace o el servidor DNS. DHCP proporciona una configuración de red TCP/IP segura, confiable y sencilla, evita conflictos de direcciones y ayuda a conservar el uso de las direcciones IP de clientes en la red. Utiliza un modelo cliente-servidor en el que el servidor DHCP mantiene una administración centralizada de las direcciones IP utilizadas en la red. Los clientes compatibles con DHCP podrán solicitar a un servidor DHCP una dirección IP y obtener la concesión como parte del proceso de inicio de red.

Las estaciones de trabajo "piden" su dirección IP (y demás configuraciones para este protocolo) al servidor DHCP, y éste les va asignando direcciones del rango que sirve, de entre aquellas que le quedan libres; si deseamos que a determinados equipos el servidor les sirva siempre la misma, pero también podemos llegar a "forzar" la asignación de la dirección IP deseada a equipos concretos. Además, también pueden excluirse del rango de direcciones IP que va a servir nuestro servidor, aquellas que deseamos que estén asociadas de forma estática a determinados equipos o periféricos de red.

Si por error dejásemos algún equipo de la red configurado con un direccionamiento IP estático del rango gestionado por nuestro servidor DHCP, podría ocurrir que cuando nuestro servidor "alquilase" una IP a la estación de trabajo solicitante, dicha dirección IP fuera la que estuviera siendo utilizada por el equipo con direccionamiento estático, provocándose un conflicto de IP; en ese caso el cliente selecciona otra dirección IP y la prueba, hasta que obtenga una dirección IP que no esté asignada actualmente a

ningún otro equipo de nuestra red. Por cada conflicto de direcciones, el cliente volverá a intentar configurarse automáticamente hasta con 10 direcciones IP.

Antes de comenzar con los procesos de instalación y configuración de nuestro DHCP, vamos a definir algunos términos que utilizaremos a lo largo de dicho proceso.

- **Ámbito servidor DHCP.** Un ámbito es un agrupamiento administrativo de equipos clientes de una subred que utilizan el servicio DHCP.
- **Rango servidor DHCP.** Un rango de DHCP está definido por un grupo de direcciones IP en una subred determinada, como por ejemplo de 192.168.0.1 a 192.168.0.254, que el servidor DHCP puede conceder a los clientes.
- **Concesión o alquiler de direcciones.** Es un período de tiempo que los servidores DHCP especifican, durante el cual un equipo cliente puede utilizar una dirección IP asignada.
- **Autorización servidor DHCP.** Habilitación del servidor DHCP instalado para que sirva direcciones IP a los clientes pertenecientes al dominio gestionado por el Active Directory.
- **Servidor WINS.** Permite registrar nombres de recursos de red NetBIOS y resolver éstos a sus direcciones IP correspondientes; se suele utilizar en estaciones de trabajo que ejecutan versiones antiguas de sistemas operativos de Microsoft.

## 1.2. Instalación del servidor DHCP.

Desde el *Administrador del servidor* realiza la instalación del servidor DHCP en el equipo con Active Directory y DNS que ya tenemos en funcionamiento en el dominio. Vamos a suponer que se llama *Dominio1.edu*. Inicialmente habrá que añadir el rol *servidor DHCP*. En esta instalación no agregaremos ámbitos y tampoco autorizaremos al servidor DHCP.

Tras pulsar en *Instalar* y una vez que complete ésta, nos aparecerá:



### 1.3. Configuración del servidor DHCP.

---

En este apartado vamos a configurar el servidor DHCP del controlador de dominio *DCServer2016*, instalado en el apartado anterior. Incluir los pantallazos del proceso.

Al pulsar en el vínculo para *Completar la configuración de DHCP* confirmamos al *Administrador* del dominio (y sólo a él) para autorizar este servidor DHCP en el *Active Directory* para servir direcciones IP a los equipos del dominio correctamente. Una vez hecho, reiniciamos para que se actualicen los cambios.

Ahora desde el menú *Herramientas*, pulsamos sobre la consola *DHCP*. Ahora vamos a definir un nuevo **ámbito**, para lo cual pulsaremos con el botón derecho del ratón sobre nuestro servidor, sobre la entrada **IPv4** y seleccionamos la opción "**Ámbito nuevo...**".

La primera pantalla que se muestra es la del asistente de creación de nuevo ámbito; pulsaremos sobre el botón "**Siguiente**" para continuar con la definición del nuevo ámbito.

En la siguiente pantalla de instalación, debemos seleccionar el nombre del nuevo ámbito a definir; en nuestro caso como el servidor DHCP va a dar servicio a toda la red, vamos a definir un único ámbito cuyo nombre va a ser *Dominio1*; si bien podríamos crear distintos ámbitos, de forma que cada uno de ellos podría servir un rango de direcciones IP diferente, de modo que por ejemplo, aisláramos los equipos de la zona de dirección de los de alumnado sirviendo a cada uno de ellos un rango de direccionamiento IP diferente.

A continuación, debemos indicar el **rango de direcciones IP** que va a otorgar nuestro servidor DHCP; indicamos que las direcciones a servir están en el rango 192.168.1.1 a 192.168.1.254 con máscara de subred 255.255.255.0, de modo que pueda "alquilar" 254 direcciones IP a los clientes.

Asistente para ámbito nuevo

**Intervalo de direcciones IP**

Para definir el intervalo de direcciones del ámbito debe identificar un conjunto de direcciones IP consecutivas.



Opciones de configuración del servidor DHCP

Escriba el intervalo de direcciones que distribuye el ámbito.

Dirección IP inicial: 192 . 168 . 1 . 1

Dirección IP final: 192 . 168 . 1 . 254

Opciones de configuración que se propagan al cliente DHCP

Longitud: 24

Máscara de subred: 255 . 255 . 255 . 0

< Atrás

Siguiente >

Cancelar

En la siguiente pantalla de configuración, podremos indicar si alguna de las direcciones del rango que otorga nuestro servidor DHCP queremos que sea excluida, por ejemplo excluiremos la IP de nuestro servidor, la 192.168.1.1 y además otras 54 direcciones (de la 192.168.1.201 a la 192.168.1.254) para recursos de red que requieran de alguna dirección IP estática, tales como el router (puerta de enlace) en la 192.168.1.254 por ejemplo, o cualquier otro elemento tal como impresores de red, puntos de acceso inalámbrico, etc.

Asistente para ámbito nuevo

**Agregar exclusiones y retraso**

Exclusiones son direcciones o intervalos de direcciones que no son distribuidas por el servidor. Retraso es el tiempo que retrasará el servidor la transmisión de un mensaje DHCPoffer.



Escriba el intervalo de direcciones IP que desea excluir. Si desea excluir una sola dirección, escriba solo una dirección en Dirección IP inicial.

Dirección IP inicial: Dirección IP final:

Agregar

Intervalo de direcciones excluido:

Dirección 192.168.1.1  
192.168.1.200 a 192.168.1.254

Quitar

Retraso de subred en milisegundos:

0

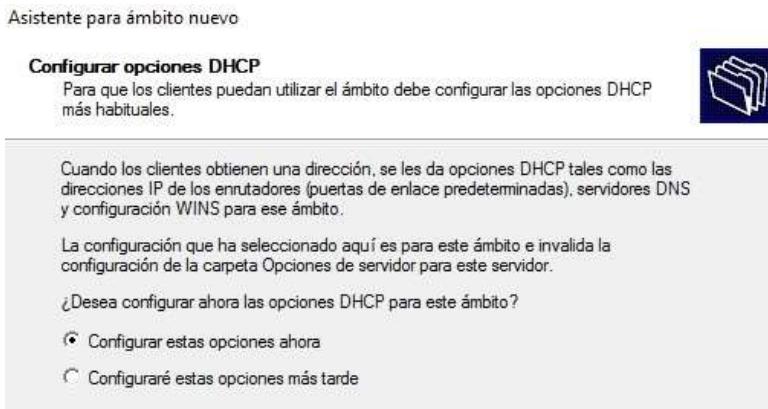
< Atrás

Siguiente >

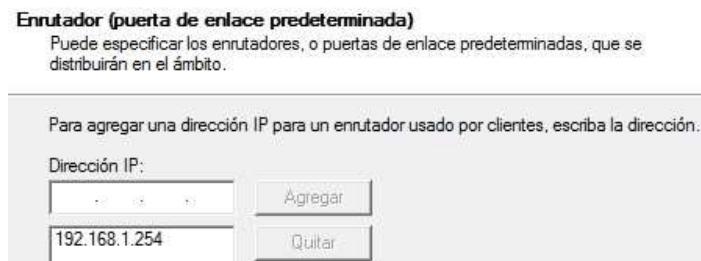
Cancelar

A continuación, debemos especificar la duración del **alquiler o concesión de las direcciones** a los equipos clientes; dejaremos la opción por defecto (8 días).

Hasta ahora hemos configurado todo lo relativo al direccionamiento IP que va a ser asignado a las estaciones de trabajo cuando el servidor DHCP les conceda el "alquiler" de su IP, pero aún quedan otra serie de parámetros que nuestro servidor debe asignar, y que configuraremos seleccionando la opción *Configurar estas opciones ahora* y pulsando sobre el botón *Siguiente*.

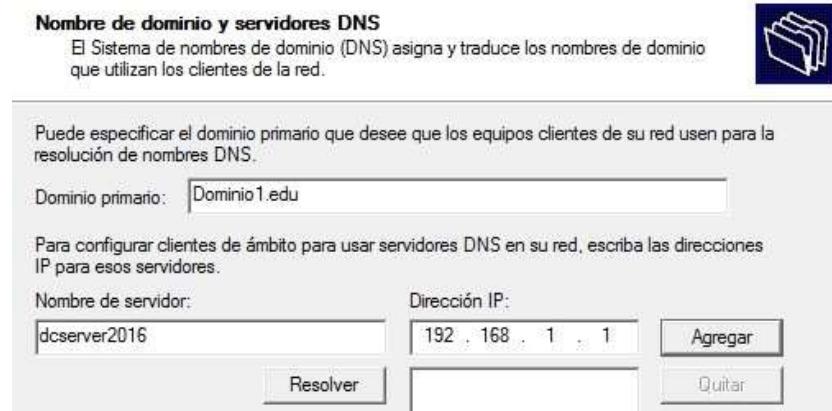


El primero de ellos son los **enrutadores o puertas de enlace** que nos servirán, junto con la dirección IP, nuestro servidor DHCP. Indicaremos como puerta de enlace la IP de nuestro router 192.168.1.254, tecleando dicha IP en la casilla *Dirección IP* y pulsando a continuación sobre el botón *Agregar*; esta puerta de enlace será la que se envíe a cada cliente que solicite una concesión a nuestro servidor DHCP.



**NOTA:** En este apartado, como ya sabemos la dirección IP de la puerta de enlace debe ser la dirección IP correspondiente al router del entorno de trabajo.

El siguiente parámetro por configurar es el servidor DNS que se asocia a nuestros clientes; especificaremos como nombre de dominio primario, el que gestiona nuestro controlador de dominio, es decir *Dominio1.com*; posteriormente indicaremos la dirección IP del servidor DNS que va a ser configurado en nuestros clientes, tecleándola directamente en la caja de texto *Dirección IP*. Otra opción sería teclear en la caja de texto *Nombre de servidor* el nombre de nuestro servidor, p.ej. supongamos que es *DCServer2016*, y luego pulsar sobre el botón *Resolver*, apareciendo escrita de forma automática la dirección IP de nuestro servidor en la casilla *Dirección IP*,



y finalmente pulsando sobre el botón *Agregar*. De este modo cualquier resolución que soliciten nuestros clientes de red, será resuelta por nuestro servidor DNS.

La siguiente opción permite definir la dirección IP de nuestro **servidor WINS**; como en nuestro caso no vamos a utilizar ningún servidor WINS, pulsaremos sobre el botón *Siguiente* sin introducir ningún dato en esta pantalla.

Una vez definidos todos los parámetros anteriores, tan sólo nos queda activar el ámbito definido para nuestro servidor DHCP; así pues, marcamos la opción *Activar este ámbito ahora*. Para completar la definición del nuevo ámbito, pulsaremos sobre el botón *Finalizar*.

Una vez terminado pulsaremos con el botón derecho del ratón sobre el nombre del controlador del dominio *dcserver2016.dominio1.edu* y elegiremos la opción *Actualizar*. Ahora tenemos en verde el ámbito creado y así que nuestro DHCP está ahora funcionando perfectamente, integrado en el *Directorio Activo*.

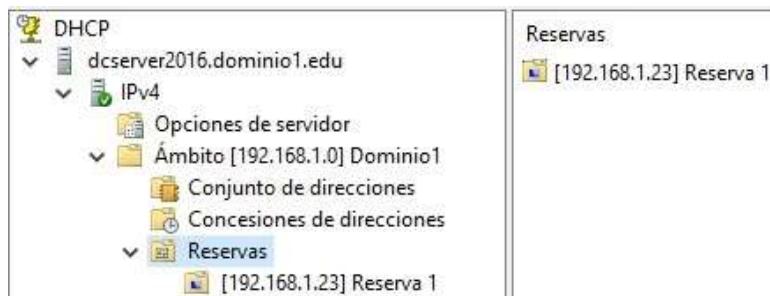


Una interesante opción que podemos configurar en nuestro servidor DHCP es la reserva de direcciones, que nos permitirá que el servidor DHCP conceda siempre la misma dirección IP a los clientes que deseemos; para ello nos situaremos sobre el ámbito definido, hacemos doble clic sobre él; tras ello pulsaremos con el botón derecho del ratón sobre la *Reservas* y seleccionaremos la opción "*Reserva nueva...*".

Una vez en esta ventana debemos indicar la dirección MAC de la tarjeta de red del cliente al cual vamos a asociar siempre la dirección IP deseada (en el ejemplo será, por ejemplo, la 192.168.1.23), de modo que esta dirección IP nunca será servida a otro equipo que no sea el que tenga la tarjeta de red con dicha dirección MAC.



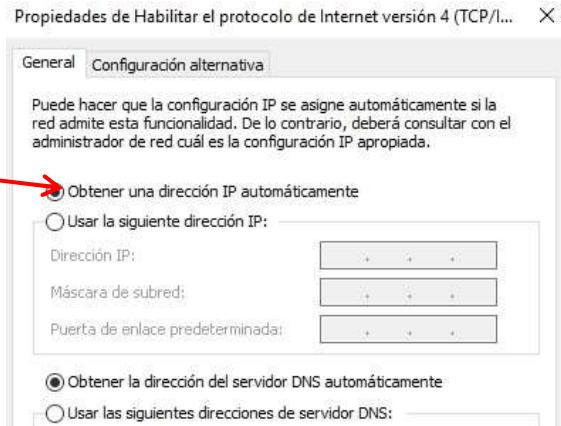
Una vez hecho esto, en *Reservas* de nuestro servidor DHCP encontraremos una entrada con la dirección IP reservada.



La reserva de direcciones tiene el inconveniente de que cuando un equipo que tenga una dirección IP reservada, cambie su tarjeta de red (por ejemplo por una avería en la misma), la dirección IP indicada no le volverá a ser servida hasta que cambiemos la antigua dirección MAC asociada a dicha IP, por la de la nueva tarjeta de red.

**NOTA:** El uso de reserva de direcciones permitirá identificar fácilmente al equipo que está solicitando un determinado servicio cuando llevemos a cabo análisis del tráfico de red.

En los equipos clientes debemos activar las opciones *Obtener la dirección IP y DNS automáticas* (dinámicas)



y a continuación ejecutar el comando `ipconfig /renew`

Con lo que ha concedido dinámicamente la IP 192.168.1.2 (la primera libre) al equipo cliente *CliTuNombreW10* (que antes tenía la IP 192.168.1.11). Además, si ejecutamos *ipconfig /all* veremos cómo ha concedido dinámicamente la dirección del servidor DNS:

Cuando nuestro servidor DHCP comience a servir direcciones IP a los clientes de nuestra red, en la carpeta *Concesión de direcciones* del servidor DHCP, por cada IP concedida encontraremos la dirección IP entregada, el equipo al que ha sido servida, y la fecha de caducidad de la concesión.

Dirección IP del cliente	Nombre	Expiración de cesión	Tipo
192.168.1.2	TuNombreW10.Dominio1.edu	08/01/2021 14:14:52	DHCP
192.168.1.23	Reserva 1	Reserva (inactiva)	Ninguno

## 2. PERMISOS DE ARCHIVOS Y CARPETAS.

En las particiones con formato FAT sólo se pueden restringir los permisos de los archivos en el nivel de carpetas y sólo si la carpeta está compartida. Sin embargo, en los volúmenes NTFS, se pueden utilizar los permisos de modo local y en red.

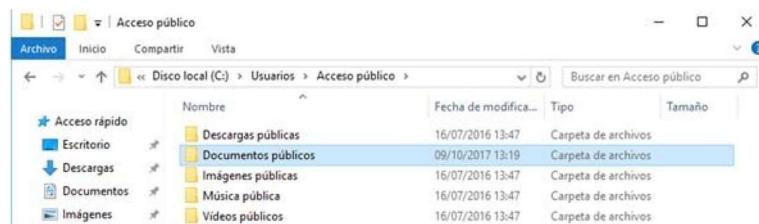
Si se configuran permisos de carpeta compartida y permisos NFTS para esa carpeta y su contenido, se aplicarán los más restrictivos.

Si un usuario tiene un permiso para una carpeta compartida y además forma parte de un grupo con permisos diferentes, entonces los permisos se combinan.

Ejemplo: el usuario tiene permiso solo de lectura mediante los permisos del recurso compartido, pero pertenece a un grupo con permiso de control total, entonces el usuario tendrá control total.

### 2.1 Compartir archivos y carpetas.

- Se pueden compartir archivos y carpetas almacenados en el equipo.
- Al compartir hay que tener especial cuidado en proteger los archivos y carpetas.
- Es necesario saber con quién y de qué modo se quieren compartir □ En función del tipo de usuarios se realizan diferentes actuaciones:
  - o Si ambos utilizan el mismo equipo: Se colocan los archivos o carpetas dentro de la carpeta Documentos públicos y así están disponibles para otros usuarios del equipo.



La carpeta de Acceso público tiene un comportamiento especial, que hace que pueda estar compartida, aunque tengamos desactivado el Uso compartido de archivos.

Podemos elegir entre activar o desactivar el uso compartido de las carpetas de Acceso público.

- o Si ambos equipos están en la misma red: Se puede compartir entre usuarios de la red y además se puede controlar si los archivos o carpetas pueden ser modificados por otros usuarios.
    - Se comparte la carpeta o unidad
    - Se establecen los controles de acceso. (Para establecer, ver, cambiar o quitar permisos de archivos y carpetas)
- Si el equipo está conectado a un grupo de trabajo y no quieres que nadie pueda tener acceso a tus carpetas hay que convertirlas en privadas:
- En Windows 10 es muy fácil hacer que una carpeta sea privada de tal forma que no sea accesible a otros usuarios, es decir a todos aquellos que no han iniciado sesión con nuestro usuario Windows. Basta con hacer clic derecho encima de la carpeta o archivo que nos interesa hacer privado y en el menú contextual que emerge usamos la opción: *Compartir con / Dejar de compartir*.

## 2.2 Permisos de carpetas y archivos

---

Cuando se establecen los permisos sobre un directorio, se define el acceso de un usuario o de un grupo a dicho directorio y sus archivos. Estos permisos solo puede establecerlos y cambiarlos el propietario o aquel usuario que haya recibido el permiso del propietario.

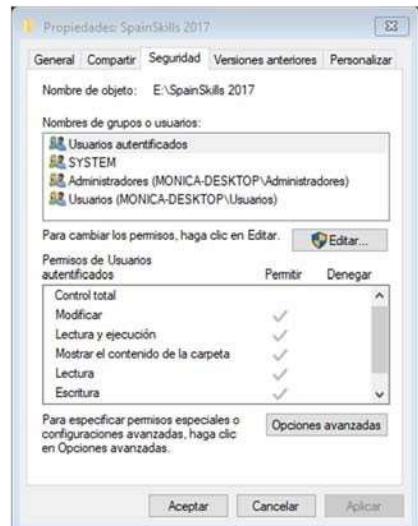
Una vez establecidos los permisos, afectarán a los archivos y subdirectorios que dependan de él, tanto los que se creen posteriormente como los que ya existían previamente (este hecho se denomina herencia). Si no se desea que se hereden, deberán indicarse expresamente cuando se indiquen los permisos.

Hay tres modos de realizar cambios en los permisos heredados:

- Realizar los cambios en la carpeta principal y la carpeta secundaria heredará estos permisos.
- Seleccionar el permiso contrario (Permitir o Denegar) para sustituir al permiso heredado.
- Desactivar la casilla de verificación Incluir todos los permisos heredables del objeto primario de este objeto (para Windows 10). De esta manera, se podrán realizar cambios en los permisos, ya que la carpeta no heredará los permisos de la carpeta principal.

Sólo es posible establecer permisos para directorios de unidades formateadas con el sistema NTFS. Los permisos estándar para directorios que se pueden conceder o denegar son:

- **Control total:** es el máximo nivel y comprende poder realizar todas las acciones tanto a nivel de archivos como de directorios.
- **Modificar:** comprende todos los permisos menos eliminar archivos y subdirectorios, cambiar permisos y tomar posesión.
- **Lectura y ejecución:** comprende ver los nombres de los archivos y subdirectorios, ver los datos de los archivos, ver los atributos y permisos y ejecutar programas.
- **Mostrar el contenido de la carpeta:** comprende los mismos permisos que lectura y ejecución, pero aplicables sólo a las carpetas.
- **Leer:** comprende ver los nombres de los archivos y directorios, ver los datos de los archivos, así como ver los atributos y permisos.
- **Escribir:** comprende crear archivos y subdirectorios, añadir datos a los archivos, modificar los atributos y leer los permisos.
- **Permisos especiales:** se activa cuando se indican permisos más concretos (se indicará cómo hacerlo posteriormente).



Estos permisos son acumulables, pero denegar el permiso Control total elimina todos los demás. Hay que tener mucho cuidado a la hora de denegar un permiso, ya que LA DENEGACIÓN PREVALECE SOBRE TODO.

Cada uno de estos permisos se compone de un grupo lógico de permisos especiales.

Los permisos NTFS para los archivos son muy parecidos a los de los directorios y la forma de establecerlos es similar.

### 2.3 Definición de los permisos especiales

---

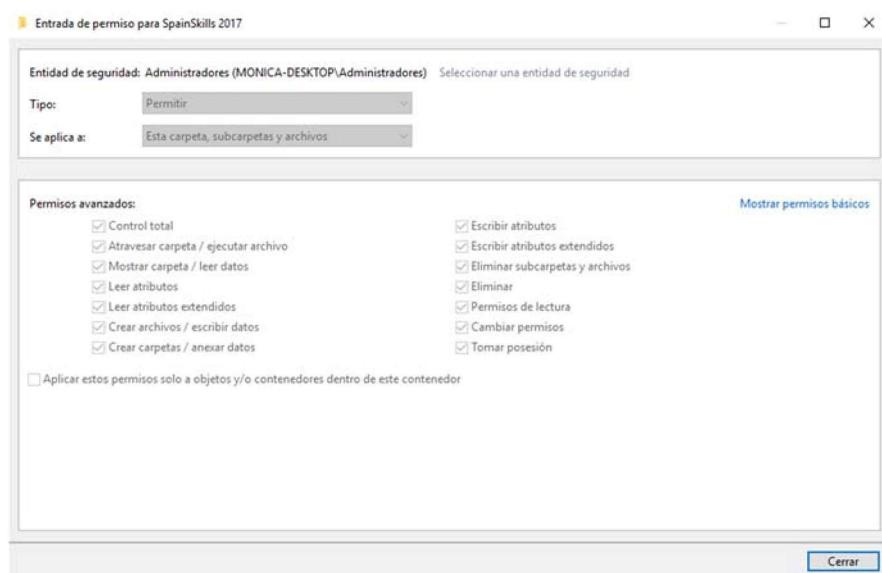
Puedes configurar cualquiera o todos los permisos especiales siguientes para archivos y carpetas:

- **Atravesar carpeta / ejecutar archivo**
  - Para carpetas: el permiso Atravesar carpeta permite o impide que el usuario pase de una carpeta a otra para llegar a otros archivos o carpetas, incluso aunque el usuario no tenga permisos para las carpetas atravesadas (sólo se aplica a carpetas).
  - Para archivos: el permiso Ejecutar archivos permite o deniega los archivos de programa.
  - Al configurar el permiso Atravesar carpeta en una carpeta no se configura automáticamente el permiso Ejecutar archivo en todos los archivos de dicha carpeta.

- **Mostrar carpeta / Leer datos**
  - Para carpetas: El permiso Mostrar carpeta permite o impide que el usuario vea los nombres de archivo y de subcarpeta en la carpeta.
  - Para archivos: El permiso Leer datos permite o impide ver datos de archivos.
- **Leer atributos**
  - Permite o impide que el usuario vea los atributos de un archivo o de una carpeta, de sólo lectura y oculto. Los atributos están definidos por el sistema de archivos NTFS.
- **Leer atributos extendidos**
  - Permite o deniega la vista de atributos extendidos de un archivo o carpeta. Los atributos extendidos se definen mediante programas y pueden variar según el programa.
- **Crear archivos / Escribir datos**
  - Para carpetas: El permiso Crear archivos permite o impide al usuario crear archivos en la carpeta
  - Para archivos: El permiso Escribir datos permite o impide que el usuario haga cambios en el archivo y sobrescriba contenido existente.
- **Crear carpetas / Anexar datos**
  - Para carpetas: El permiso Crear carpetas permite o impide al usuario crear carpetas en una carpeta.
  - Para archivos: El permiso Anexar datos permite o impide que el usuario haga cambios en el final del archivo pero que no cambie, elimine ni sobrescriba datos existentes.
- **Escribir atributos**
  - Permite o impide que el usuario cambie los atributos de un archivo o de una carpeta, de sólo lectura y oculto. Los atributos están definidos por el sistema de archivos NTFS.
  - No implica la creación o eliminación de archivos o carpetas; sólo incluye el permiso para hacer cambios en los atributos de un archivo o de una carpeta.
- **Escribir atributos extendidos**
  - Permite o deniega el cambio de los atributos extendidos de un archivo o carpeta. Los atributos extendidos se definen mediante programas y pueden variar según el programa.
  - Este permiso no implica la creación o eliminación de archivos o carpetas, sólo incluye el permiso para realizar cambios en los atributos de un archivo o una carpeta. Para permitir (o denegar) operaciones de creación o eliminación, vea Crear archivos / Escribir datos, Crear carpetas / Anexar datos, Eliminar subcarpetas y archivos y Eliminar.
- **Eliminar subcarpetas y archivos**
  - Este permiso permite o impide que el usuario elimine subcarpetas y archivos, incluso aunque no se haya concedido el permiso Eliminar para la subcarpeta o el archivo. Este permiso se aplica sólo a las carpetas.
- **Eliminar**
  - Permite o impide que el usuario elimine el archivo o la carpeta. Si no tienes el permiso Eliminar para un archivo o una carpeta, puedes eliminarlo si se te han concedido los permisos Eliminar subcarpetas y archivos en la carpeta principal.

- **Permisos de lectura**
  - Permite o impide que el usuario lea los permisos del archivo o de la carpeta, de Control total, Leer y Escribir.
- **Cambiar permisos**

El permiso Cambiar permisos permite o impide que el usuario cambie los permisos del archivo o de la carpeta, de Control total, Leer y Escribir.
- **Tomar posesión**
  - El permiso Tomar posesión permite o impide que el usuario tome posesión del archivo o de la carpeta. El propietario de un archivo o de una carpeta puede cambiar los permisos correspondientes, cualesquiera que sean los permisos existentes que protegen el archivo o la carpeta.



En la tabla siguiente se describen los permisos especiales de archivos y carpetas.

Permisos especiales	Control total	Modificar	Leer y ejecutar	Mostrar el contenido de la carpeta (sólo en carpetas)	Lectura	Escritura
Recorrer carpeta / Ejecutar archivo	x	x	x	x		
Listar carpeta / Leer datos Atributos de lectura	x	x	x	x	x	
Atributos extendidos de lectura	x	x	x	x	x	
Crear archivos / Escribir datos	x	x				x
Crear carpetas / Anexar datos	x	x				x
Atributos de escritura	x	x				x
Atributos extendidos de escritura	x	x				x
Eliminar subcarpetas y archivos	x	x				
Permisos de lectura	x	x	x	x	x	x
Cambiar permisos	x					
Tomar posesión	x					

**IMPORTANTE:** los grupos o los usuarios a los que se concede Control total para una carpeta pueden eliminar cualquier archivo de dicha carpeta, cualesquiera que sean los permisos que protegen al archivo.

**Nota:** Aunque parece que **Mostrar el contenido de la carpeta** y **Leer y ejecutar** tienen los mismos permisos especiales, estos permisos se heredan de manera diferente. Mostrar el contenido de la carpeta lo heredan las carpetas, pero no los archivos, y sólo aparece al ver los permisos de carpetas. Leer y ejecutar lo heredan tanto los archivos como las carpetas y siempre está presente cuando ve los permisos de archivos o de carpetas.

## 2.4 Establecimiento de permisos NTFS estándar para un directorio o un archivo.

---

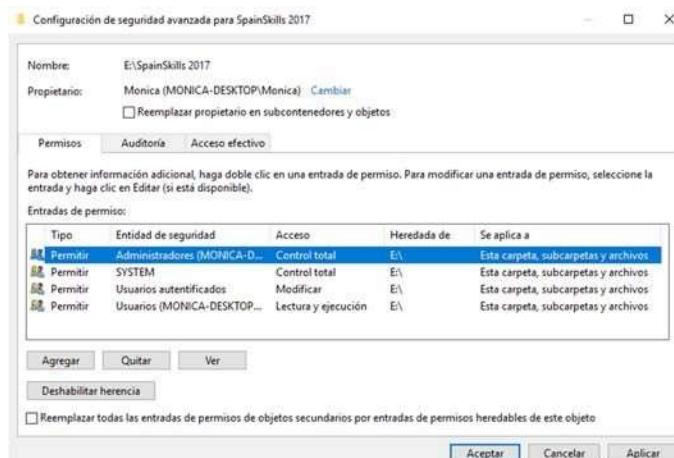
Sigue los siguientes pasos:

1. Desde Equipo del menú Inicio, selecciona el directorio o archivo que deseas, muestra su menú contextual, selecciona Propiedades y después la pestaña Seguridad.
2. En ella se encuentran los nombres de los usuarios, grupos e identidades especiales que tienen permisos sobre dicha carpeta y, debajo, los permisos estándar de directorio que posee cada uno de ellos.
3. Si deseas **consultar** los **permisos** de alguno de ellos, sitúate sobre él y verás que, en la parte inferior, se muestran los permisos que tiene establecidos. Si hay marcas grises, corresponden a permisos heredados.
4. Si deseas **modificar** los **permisos** de alguno de ellos, pulsa en Editar, sitúate sobre él y verás que, en la parte inferior, se muestran los permisos que tiene establecidos. Si hay casillas grises, corresponden a permisos heredados. Activa la casilla correspondiente al permiso deseado en la columna Permitir, se le concede el permiso, o Denegar, se le deniega el permiso.
5. Si deseas añadir otros usuarios o grupos a la lista de nombres, pulsa en Agregar, en Opciones Avanzadas y en Buscar ahora. Se abrirá una ventana con todos los posibles usuarios, grupos e identidades especiales a los que puedes otorgar o denegar permisos.
6. Si seleccionas elementos de la lista y pulsas en Aceptar dos veces, se añadirán a los grupos o usuarios que tienen permisos sobre la carpeta. Una vez que estén en la lista, indica los permisos que deseas conceder o denegar a cada uno de los usuarios que has añadido.
7. Si deseas **quitar** algún **usuario** o **grupo**, sitúate sobre él, pulsa en Quitar (no pedirá ninguna confirmación).
8. Pulsa en Aceptar hasta volver a la pantalla principal de la utilidad.
9. Cuando hayas finalizado, cierra la utilidad.

## 2.5 Establecimiento de permisos NTFS especiales

Para establecer los permisos NTFS especiales de archivo o directorio, sigue los siguientes pasos:

1. Desde Equipo del menú Inicio, selecciona el directorio o archivo que deseas, muestra su menú contextual, selecciona Propiedades y después la pestaña Seguridad.
2. Pulsa en Opciones avanzadas y verás una pantalla en donde se encuentran los nombres de los usuarios, grupos e identidades especiales que tienen permisos sobre dicho directorio o archivo junto con la descripción de los permisos y dónde se aplican. Si seleccionamos una Entidad de Seguridad y pulsamos Ver, se mostrarán los permisos básicos de dicho usuario o grupo, pero no nos permitirá cambiarlos, salvo que lo hallamos añadido
3. posteriormente o deshabilitemos la herencia.



4. Una vez hecho lo anterior, para poder modificar los permisos establecidos, selecciona un usuario y pulsa en Editar. Como puedes ver, muestra los permisos básicos que tiene establecidos el usuario o grupo
5. seleccionado. Para ver los permisos especiales, pulsar en la parte derecha de la ventana. Si hay casillas grises, corresponden a permisos heredados.
6. Puedes modificar los permisos que deseas. Para ello, elije en Tipo, permitir o denegar y activa la casilla correspondiente al permiso deseado.
7. Indica, en el apartado Aplicar a: el ámbito de los permisos que estás
8. indicando; puedes modificar el ámbito seleccionando una opción de la lista desplegable correspondiente.

Si activas la casilla *Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor*, evitarás que los archivos y subcarpetas secundarias hereden estos permisos.

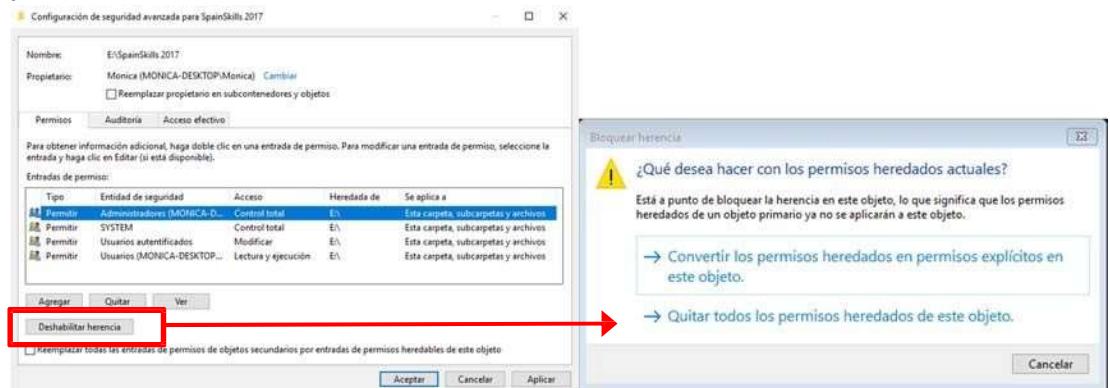


Cuando hayas finalizado, pulsa en Aceptar y volverás a la pantalla anterior.

- Si deseas añadir otros usuarios o grupos a la lista de nombres, pulsa en Agregar ""7 Seleccionar una entidad de seguridad ""7 en Opciones Avanzadas y en Buscar ahora. Se abrirá una ventana con todos los posibles usuarios, grupos e identidades especiales a los que puedes otorgar o denegar permisos.

Si seleccionas elementos de la lista y pulsas en Aceptar dos veces, pasarás a la pantalla donde deberás indicar los permisos y ámbito de aplicación deseados. Cuando hayas finalizado, pulsa en Aceptar.

- Si deseas quitar algún usuario o grupo, sitúate sobre él, pulsa en Quitar (no pedirá ninguna confirmación).
- Si deseas que los permisos de la carpeta principal no se hereden a una carpeta secundaria (fíjate que hay casillas de permisos que pueden estar en gris porque son permisos heredados), pulsa en *Deshabilitar herencia* y se mostrará una pantalla con varias opciones.



Si pulsas en *Convertir los permisos heredados en permisos explícitos en este objeto*, concederás al objeto los permisos que tenía el objeto principal y podrán ser modificados

Si pulsas en *Quitar todos los permisos heredados de este objeto*, el objeto no heredará los permisos del objeto principal y podrán añadirse nuevos permisos. **Pero cuidado con esta opción, que desaparecen**

**todos los usuarios y grupos y si, por equivocación aceptamos, ya no tendremos acceso al objeto.**

4. Si deseas que los permisos indicados para esta carpeta se hereden a todos los objetos secundarios, activa la casilla *Reemplazar todas las entradas de objetos secundarios por entradas de permisos heredables de este objeto*, pulsa en Aplicar y te mostrará una pantalla que te indica que se eliminarán los permisos explícitos indicados en los subdirectorios y archivos que cuelgan de este directorio y se reemplazarán por los de la carpeta en cuestión. Pulsa en Sí para continuar.
5. Cuando hayas finalizado, pulsa en Aceptar hasta volver a la pantalla de Propiedades del directorio.
6. Cuando hayas finalizado, pulsa en Aceptar para volver a la utilidad y ciérrala.

## 2. 6 Ver permisos efectivos de archivos y carpetas

---

Cuando se crea un archivo o carpeta, Windows asigna permisos predeterminados a ese objeto o el creador puede asignar permisos específicos. El permiso de **lectura** es el permiso mínimo requerido para ver permisos efectivos.

## 2. 7 Para ver permisos efectivos de archivos y carpetas

---

1. En objeto cuyos permisos deseas ver, haz clic con el botón secundario en **Propiedades** y, a continuación, en la ficha **Seguridad**.
2. Haz clic en Opciones avanzadas, haz clic en la pestaña *Acceso efectivo* y, a continuación, en *Seleccionar un usuario*.
3. En la ventana que aparece escribe el nombre de un usuario o grupo y, después, haz clic en Aceptar y a continuación pulsar *Ver acceso efectivo*. Aparecerá una lista indicando todos los permisos especiales con una cruz o un tick en verde, según si el usuario o grupo tienen o no esos permisos.

## 2.8 El propietario de un directorio o un archivo

---

Cuando un usuario crea un directorio, un archivo o cualquier objeto, se convierte automáticamente en su propietario (también durante el proceso de instalación se adjudicaron propietarios a todos los directorios y archivos que se crearon).

Un propietario puede asignar permisos a sus directorios, archivos u objetos, aunque no puede transferir su propiedad a otros usuarios. Puede conceder el permiso **Tomar posesión**, que permitirá, a los usuarios que se le conceda, tomar posesión en cualquier momento.

También pueden tomar posesión los administradores, pero no pueden transferirla a otros usuarios. De esta manera, un administrador que tome posesión y cambie los permisos podrá acceder a los archivos para los que no tiene concedido ningún permiso.

## 2.9 Cómo establecer el permiso de toma de posesión

---

Aunque es un permiso especial y se actúa como se ha indicado en el apartado anterior, como tiene consideraciones especiales, se indica expresamente cómo hacerlo. Para conceder el permiso de toma de posesión, sigue los pasos siguientes:

1. Selecciona el directorio o archivo al que deseas establecer el permiso de toma de posesión. Muestra su menú contextual, selecciona **Propiedades**, pulsa en la ficha **Seguridad** y, después, pulsa en **Opciones Avanzadas**.
2. Como vas a modificar los permisos que tiene este objeto, pulsa en **Cambiar permisos y Deshabilita la herencia**, te mostrará una pantalla con varias opciones. Si pulsas la primera opción, concederás al objeto los permisos que tenía el objeto principal y podrán ser modificados. Si pulsas la segunda, el objeto no heredará los permisos del objeto principal y podrán añadirse nuevos permisos.
3. Selecciona al usuario o grupo al que deseas dar el permiso **Tomar posesión**, pulsa en **Editar** "**7 Mostrar permisos avanzados**" y te mostrará los permisos que puedes permitir o denegar.
4. Desplázate hasta el último permiso, **Tomar posesión**, y actívalo para conceder la toma de posesión. Cuando lo hayas hecho, pulsa en **Aceptar** hasta salir.

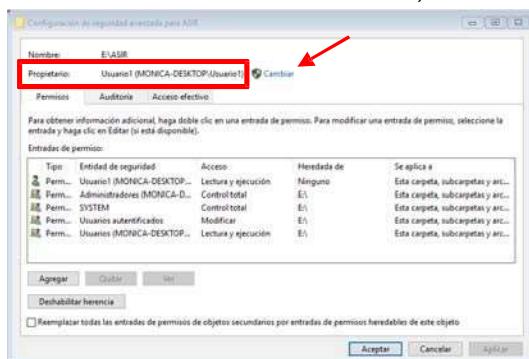
## 2.10 Cómo tomar posesión

---

Una vez que se ha establecido el permiso de tomar posesión, cualquier grupo o usuario que tenga concedido dicho permiso podrá tomar posesión de dicho directorio, archivo u objeto. Para ello, realiza los siguientes pasos:

5. Selecciona un archivo o directorio, muestra su menú contextual, selecciona Propiedades y pulsa, en la ficha Seguridad, en Opciones Avanzadas. En la ventana indicará el propietario del objeto y a su derecha, en azul "Cambiar".
6. Si deseas añadir algún otro usuario o grupo a la lista, pulsa en Cambiar, después, en Otros usuarios o grupos, pulsa en Opciones Avanzadas y, finalmente, en Buscar ahora. Se abrirá una ventana con todos los posibles usuarios, grupos e identidades especiales.
7. Si seleccionas elementos de la lista, pulsa en Aceptar y vuelve a pulsar en Aceptar, pasarás a la ventana Nuevo propietario.

8. Selecciona el usuario o grupo que deseas para que tome posesión del archivo o directorio y pulsa en Aplicar. Te mostrará un mensaje de aviso, pulsa en Aceptar y verás cómo cambia el nombre del propietario.
9. Si activas la casilla Reemplazar propietario en subcontenedores y objetos, reemplazará el propietario en todos los objetos y subcarpetas que cuelgan de esta carpeta.
10. Cuando hayas finalizado, pulsa en Aceptar hasta volver a la pantalla principal de la utilidad. Cuando lo deseas, cierra la utilidad.



### 3. Copia de seguridad del Directorio Activo

Hacer *backup* del controlador de dominio es fundamental para poder restaurar la base de datos del Directorio Activo en caso de avería. Podemos hacer esta copia de respaldo utilizando aplicaciones comerciales como *BackupExec* o *DataProtecto*, pero tenemos suficientes herramientas como para hacerlo también desde nuestro Windows.

Debemos copiar con relativa frecuencia el estado del sistema de los controladores de dominio para así recuperar ese punto cuando queramos. De esta forma, si esto lo hacemos todos los días perderíamos sólo un parte del día de trabajo. Para automatizarlo para estos periodos estableceremos una regla en el planificador de tareas.

**Nota:** La mejor opción es mantener un controlador de dominio con pocas funciones que no sean del propio Windows (software de otros fabricantes) y, por supuesto, tener un controlador de dominio de *backup*, así podremos tener siempre disponible el directorio activo completo.

El **estado del sistema de controlador de dominio** incluye los siguientes componentes:

- El *Directorio Activo*
- La *carpeta compartida SYSVOL*. Esta carpeta compartida contiene plantillas de políticas de grupo y secuencias de comando de inicios de sesión. La carpeta compartida SYSVOL está presente solamente en controladores de dominio.
- *Registro*. Esta base de datos contiene la información sobre la configuración del equipo.
- *Ficheros de inicio del sistema*. Windows Server requiere estos archivos durante su fase de inicio físico del equipo. Incluye el arranque y archivos de sistema

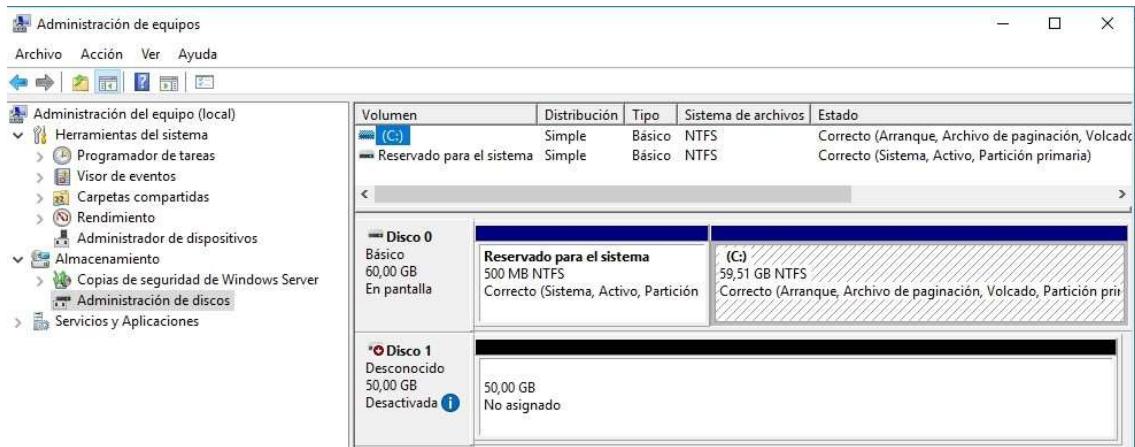
- La *base de datos de registros de clases COM+*. Contiene información sobre servicios de aplicaciones
- *Base de datos del servicio de certificados*. Esta base de datos contiene los certificados del servidor que Windows Server utiliza para autenticar usuarios, por ejemplo, con el *escritorio remoto*. Esta base solamente está presente si el servidor está funcionando como *servidor de certificados*.

Para realizar la operación de *backup* utilizaremos la herramienta provista por Windows Server. Esta herramienta, al tratarse de algo de uso local no es una función (rol) sino una característica, así que nos vamos a las características (*Añadir roles y características*), la seleccionamos y la instalamos:

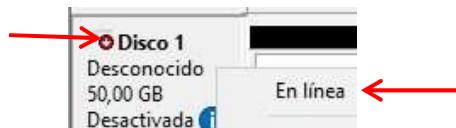


### 3.1 Proceso de copia de seguridad

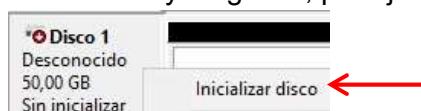
Antes de empezar este proceso crearemos en la máquina virtual (menú *VM>Settings>Hardware>Add>Hard disk*) que aloja al controlador de dominio, un nuevo disco (E:) de 50 GB. donde almacenaremos nuestra copia. A pesar de haberlo añadido no nos aparece en el *Explorador de archivos* ya que hay que activarlo. Para ello en el menú *Herramientas* del controlador de dominio elegimos *Administrador de equipos* y ahí *Administrador de discos* en el que nos aparecerá el disco recién añadido, pero desactivado.



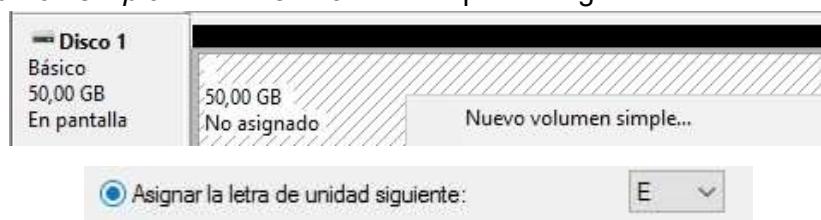
Para activarlo pulsamos con el botón derecho del ratón sobre la zona izquierda, donde pone *Disco 1* y pulsamos *En línea*:



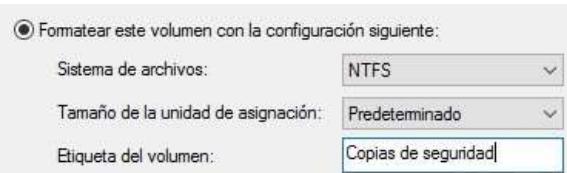
A continuación, volvemos a pulsar con el botón derecho del ratón sobre la zona izquierda y pinchamos en *Inicializar disco* y elegimos, por ejemplo *MBR*.



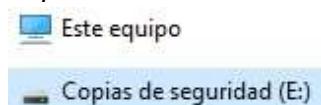
Y ahora pulsando con el botón derecho del ratón sobre la zona derecha creamos un *Nuevo volumen simple* con los 51.197 MB al que le asignaremos la letra E:



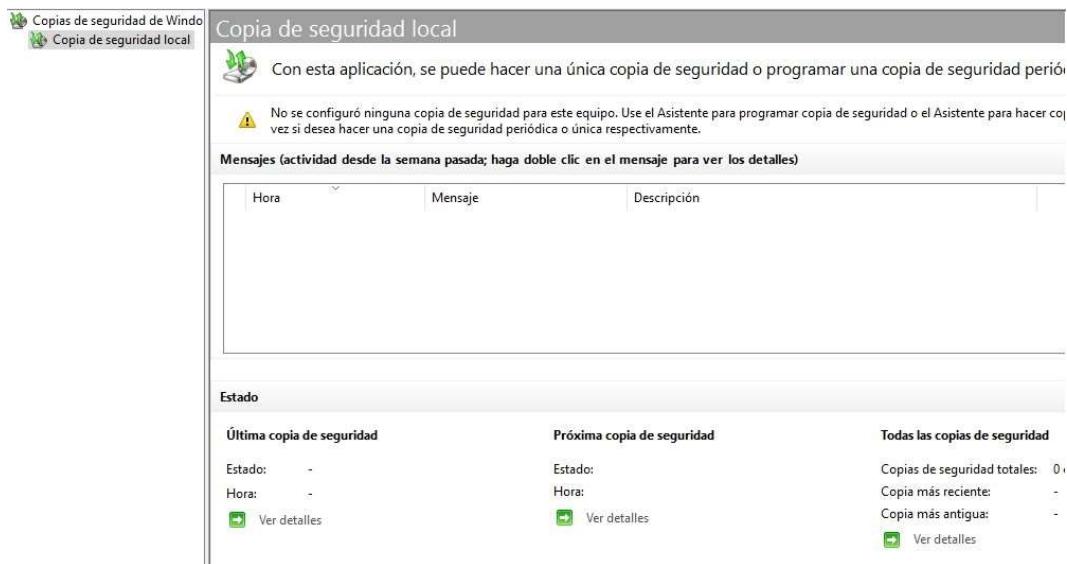
y le pondremos la etiqueta *Copias de seguridad* antes de formatearlo:



Ahora ya nos aparecerá en el *Explorador de archivos*:



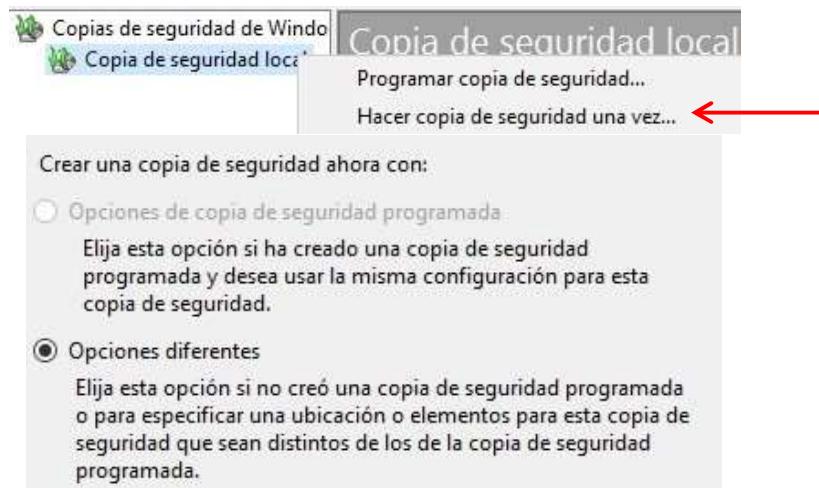
Utilizaremos este disco para guardar en él algunas copias de seguridad. Para ello en el menú *Herramientas* elegimos *Copias de Seguridad de Windows Server*. Aparecerá una pantalla como ésta:



Este programa permite crear tareas repetitivas de copias de seguridad. Es decir, programar una tarea para que todos los días a las 23:00 h. realice una copia de seguridad completa del servidor, por ejemplo.

Vamos a realizar una copia de seguridad (una vez) del *Estado del sistema* en el disco que hemos creado *Copias de seguridad (E:)*.

Pulsamos con el botón y elegimos la segunda opción de *Hacer copia de seguridad una vez>Opciones diferentes*:



Comenzamos con un mensaje de inicio donde nos indica que utilizaremos unas *Opciones diferentes* ya que no se trata de una tarea programada. Pulsaremos en *Siguiente:*



### Seleccionar configuración de copia de seguridad

Opciones de copia de seg...

**Seleccionar configuració...**

Seleccionar elementos pa...

Especificar tipo de destino

Confirmación

Progreso de la copia de s...

¿Qué tipo de configuración desea programar?

Servidor completo (recomendado)

Deseo hacer una copia de seguridad de todos los datos del servidor, las aplicaciones y el estado del sistema.

Tamaño de copia de seguridad: 13,13 GB

Personalizada

Deseo elegir volúmenes personalizados y archivos para la copia de seguridad.

Seleccionaremos la opción de *Personalizada* para ver qué opciones nos muestra. Pulsamos en el botón *Agregar elementos*. Fíjate que hay una opción que salvará el *Estado del sistema* en la están todos los datos principales como controlador de dominio. En todo caso elegiremos *Reconstrucción completa*, sigamos:



### Seleccionar elementos para copia de seguridad

Opciones de copia de seg...

Seleccionar configuració...

**Seleccionar elementos pa...**

Especificar tipo de destino

Confirmación

Progreso de la copia de s...

Seleccione los elementos que deseé incluir en la copia de seguridad. Si elige la reconstrucción completa tendrá más opciones en el caso de requerir una recuperación.

Nombre

Reconstrucción completa

Estado del sistema

Disco local (C:)

Reservado para el sistema

El tipo de almacenamiento para la copia de seguridad, en este caso, será *Unidades locales*:

Opciones de copia de seg...

Seleccionar configuració...

Seleccionar elementos pa...

**Especificar tipo de destino**

Seleccionar destino de la ...

Elija el tipo de almacenamiento para la copia de seguridad:

Unidades locales

Ejemplo: disco local (D:), unidad de DVD (E:)

Carpeta compartida remota

Ejemplo: \\miServidorDeArchivos\nombreDeCarpetaCompartida

Según el hardware instalado en el servidor podremos almacenar la copia en distintos sitios, seleccionaremos la unidad de disco (E:) que hemos creado anteriormente.

Opciones de copia de seg...

Seleccionar configuració...

Seleccionar elementos pa...

Especificar tipo de destino

**Seleccionar destino de la ...**

Confirmación

Progreso de la copia de s...

Seleccione un volumen para almacenar la copia de seguridad. Hay un disco externo conectado a este equipo que aparece como volumen.

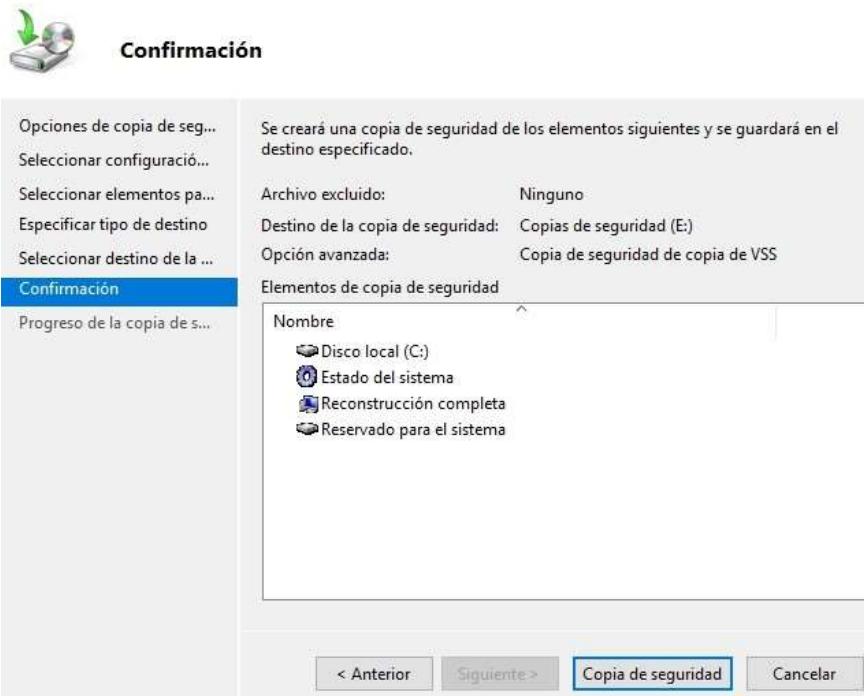
Destino de la copia de seguridad:

Copias de seguridad (E:)

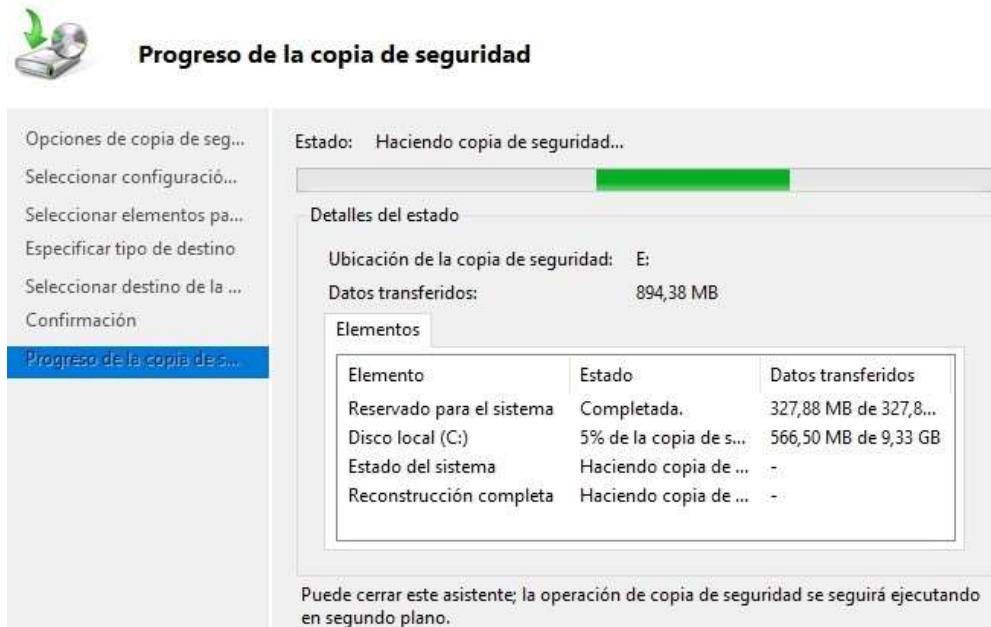
Espacio total en el destino de la copia de seguridad: 50,00 GB

Espacio disponible en el destino de la copia de seguridad: 49,90 GB

Antes de empezar el proceso de creación de la copia nos pide *Confirmación*.



Ya tenemos todo listo, así que pulsamos en el botón de *Copia de seguridad*:



La pantalla anterior nos mostrará el progreso de la copia, y si finalmente es correcto veremos un mensaje como el de la pantalla de *Copia de seguridad completada*. Bien, hemos hecho algo imprescindible, pero ojo, esto se debe hacer todos los días.

Ahora en la pantalla principal del programa nos mostrará un registro con las copias realizadas y su estado.

Vamos a crear en el controlador de dominio una carpeta llamada *Borrada* en la carpeta *Documentos de Este equipo*. Haremos una copia de seguridad (una vez) de *Documentos*, en una carpeta compartida llamada *Backup* que esté en un disco nuevo

de 20 GB., llamado *Copias*, del Windows 10 (*ClTuNombreW10*). Una vez que tengamos hecha la copia de seguridad de la carpeta *Documentos*, borraremos la carpeta *Borrada* y comprobaremos que ya no está.

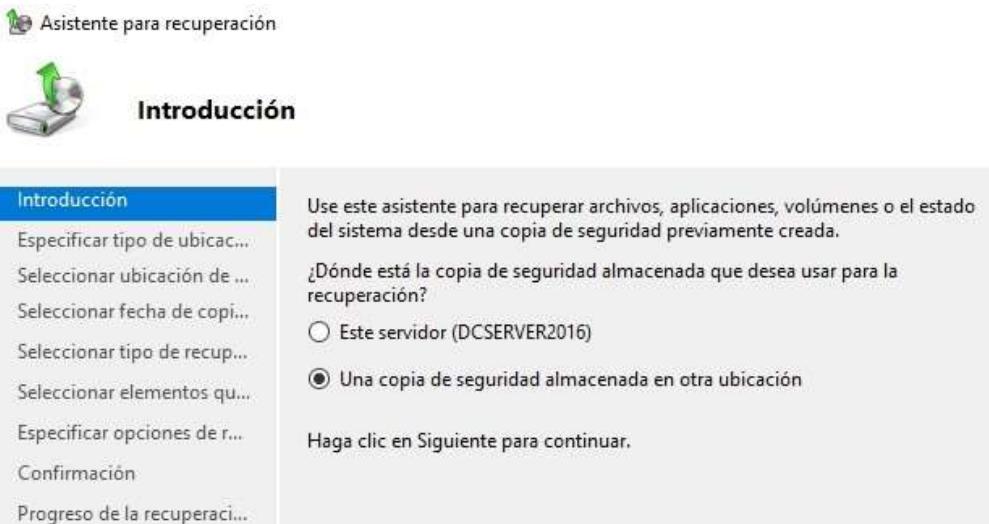
Vamos ahora al proceso contrario del de hacer una copia de seguridad, el de recuperar las copias hechas.

### 3.2 Restauración

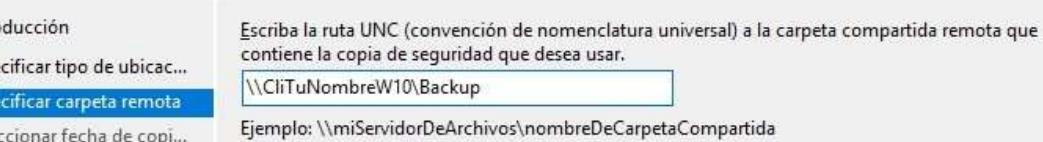
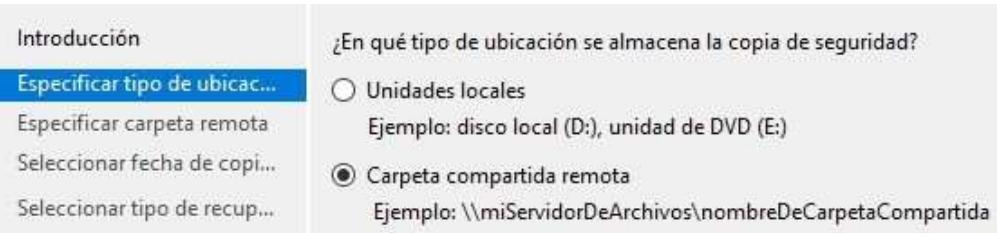
Veamos cómo podemos restaurar las copias de seguridad realizadas.

Vamos a recuperar la carpeta *Documentos*, desde la copia de seguridad creada y comprobar si está la carpeta borrada anteriormente.

Ejecutamos la consola de *Copias de seguridad* y seleccionamos ahora la opción de *Recuperar*:

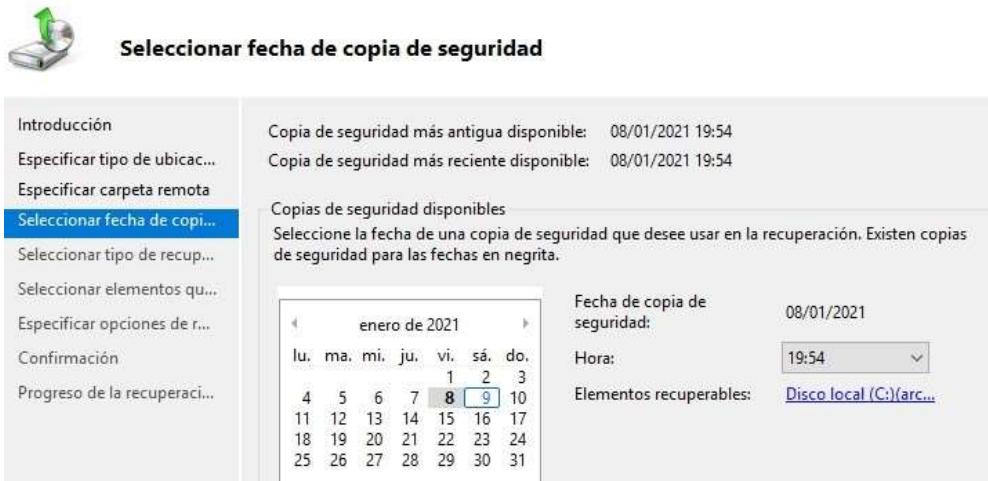


Pulsamos en *Siguiente* y elegimos la segunda opción *Carpeta compartida remota* ya que nuestra copia de seguridad está en la carpeta compartida llamada *Backup* en el equipo cliente Windows 10 (*ClTuNombreW10*):

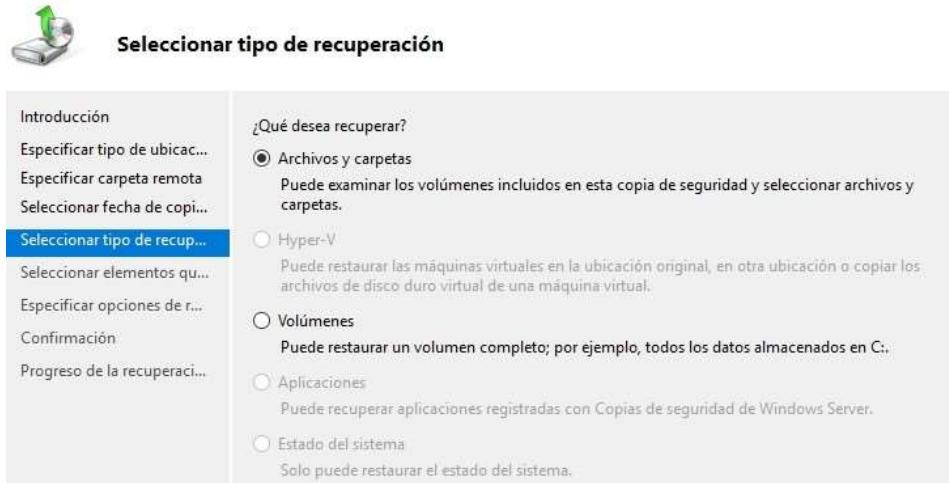


Ahora fíjate que nos indica que nos indica que *Seleccionemos la fecha de una copia de seguridad que deseamos usar en la recuperación*.

**NOTA:** En caso de que hagamos varias copias diferentes podremos recuperar la copia de la fecha que le indiquemos aquí.



Ahora le podemos indicar si es un archivo o carpeta lo que hay que recuperar o un volumen o todo el *Estado del sistema*, etc. En nuestro caso indicamos la primera opción porque solo queremos recuperar dos carpetas:



Le indicamos las carpetas a recuperar:



## Seleccionar elementos que se van a recuperar

Introducción

Especificar tipo de ubicac...

Especificar carpeta remota

Seleccionar fecha de copi...

Seleccionar tipo de recup...

Seleccionar elementos qu...

Especificar opciones de r...

Confirmación

Progreso de la recuperaci...

Examine el árbol de Elementos disponibles para buscar los archivos o las carpetas que desea recuperar. Haga clic en un elemento del árbol o en Nombre para seleccionarlo para la recuperación.

Elementos disponibles:



Elementos para recuperar:

Nombre	Fecha de modificación
Documents	09/01/2021 20:06

Definimos una ubicación para la restauración, por ejemplo, en el disco creado en el controlador de dominio llamado *Copias de seguridad (E:)* y confirmamos:



## Especificar opciones de recuperación

Introducción

Especificar tipo de ubicac...

Especificar carpeta remota

Seleccionar fecha de copi...

Seleccionar tipo de recup...

Seleccionar elementos qu...

Especificar opciones de r...

Confirmación

Progreso de la recuperaci...

Destino de la recuperación

Ubicación original

Otra ubicación

E:\

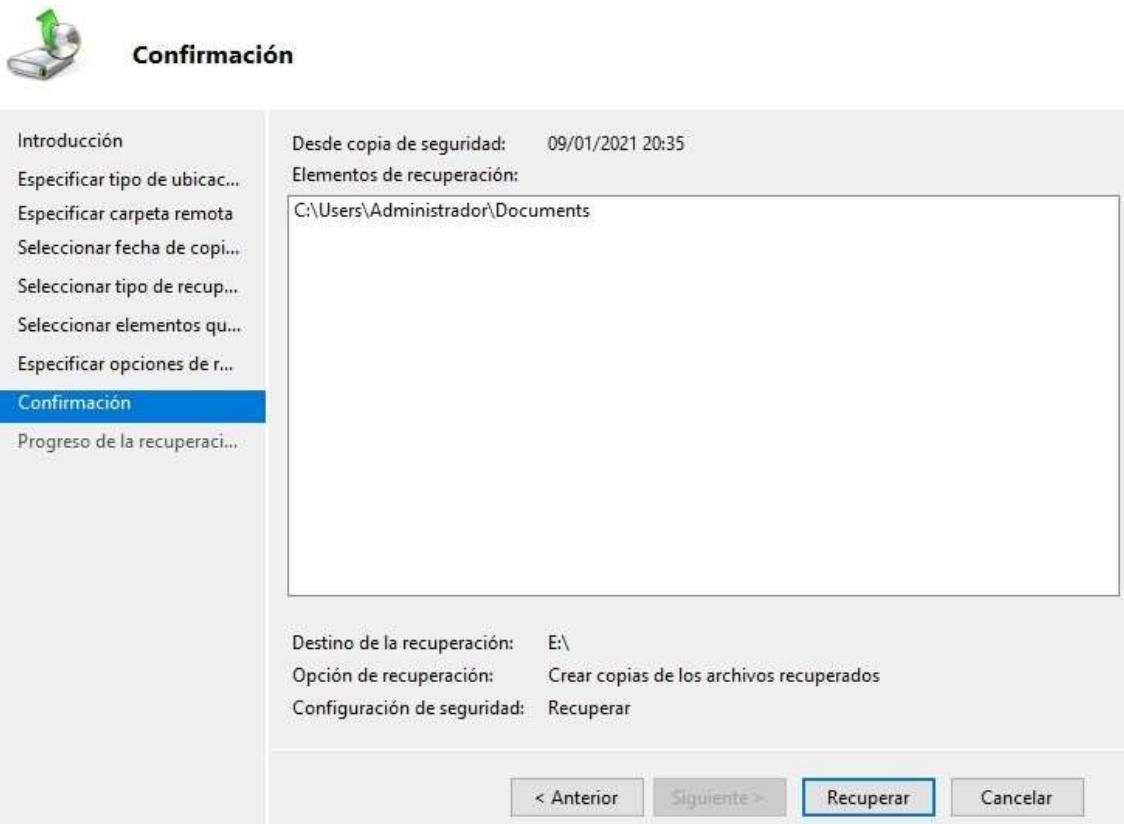
Examinar

Cuando se encuentren elementos en la copia de seguridad que ya estén en el destino

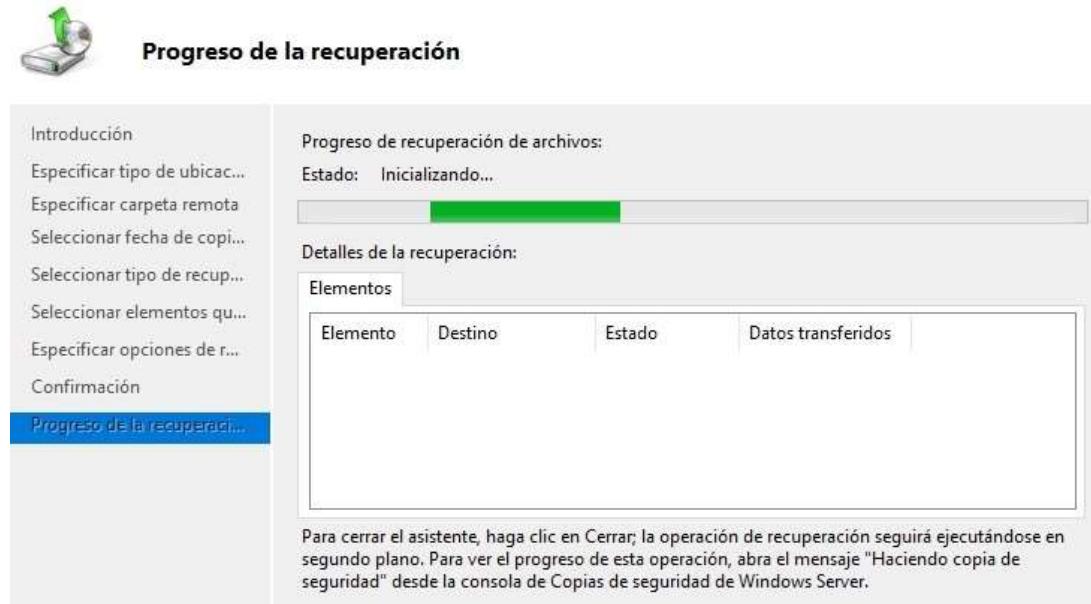
Crear copias para tener ambas versiones

Sobrescribir las versiones existentes con las recuperadas

No recuperar los elementos ya existentes en el destino de recuperación



Pulsamos el botón *Recuperar* e iniciamos la restauración:



Y si ha ido todo bien tenemos recuperado las carpetas borradas.



## Progreso de la recuperación

Introducción  
Especificar tipo de ubicac...  
Especificar carpeta remota  
Seleccionar fecha de copi...  
Seleccionar tipo de recup...  
Seleccionar elementos qu...  
Especificar opciones de r...  
Confirmación  
**Progreso de la recuperaci...**

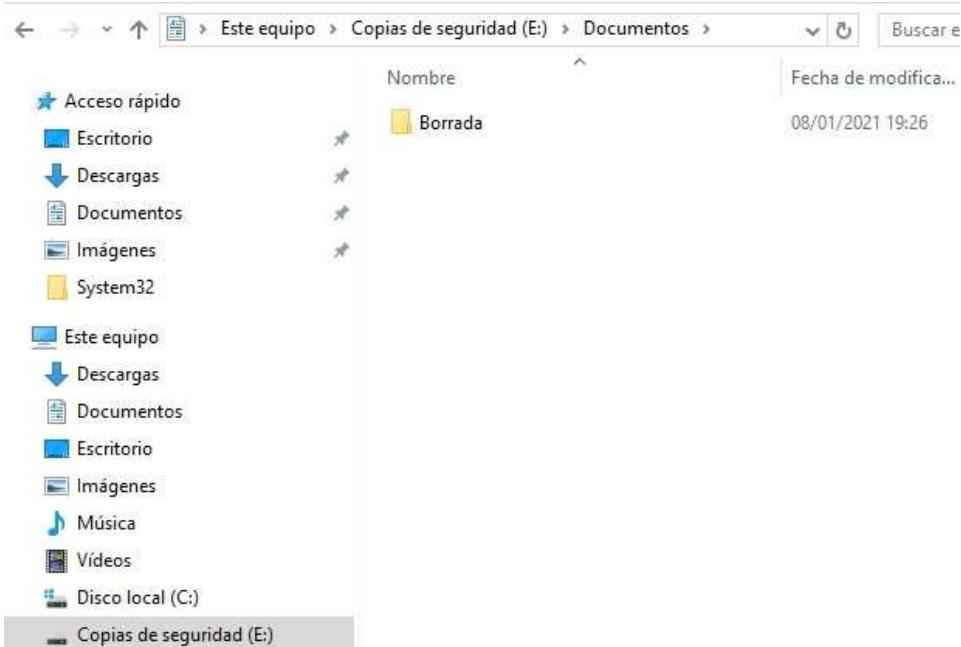
Progreso de recuperación de archivos:  
Estado: Completada.

Detalles de la recuperación:

Elemento	Destino	Estado	Datos transferidos
C:\Users\Administrador\Documents	E:\	Completada.	1 KB de 1 KB

Para cerrar el asistente, haga clic en Cerrar; la operación de recuperación seguirá ejecutándose en segundo plano. Para ver el progreso de esta operación, abra el mensaje "Haciendo copia de seguridad" desde la consola de Copias de seguridad de Windows Server.

Y comprobamos que se ha restaurado en la ubicación indicada:



En la consola de *Copias de seguridad* nos indica las acciones realizadas:

**Copia de seguridad local**

Con esta aplicación, se puede hacer una única copia de seguridad o programar una copia de seguridad periódica.

**⚠️** No se configuró ninguna copia de seguridad para este equipo. Use el Asistente para programar copia de seguridad o el Asistente para hacer copia de seguridad vez si desea hacer una copia de seguridad periódica o única respectivamente.

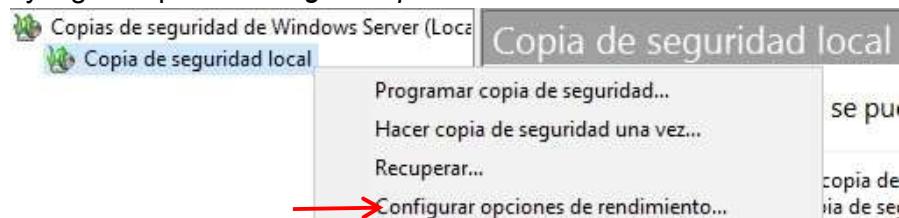
Mensajes (actividad desde la semana pasada; haga doble clic en el mensaje para ver los detalles)

Hora	Mensaje	Descripción
09/01/2021 20:06	Recuperación de archivos	Correcta
08/01/2021 19:54	Copia de seguridad	Correcta

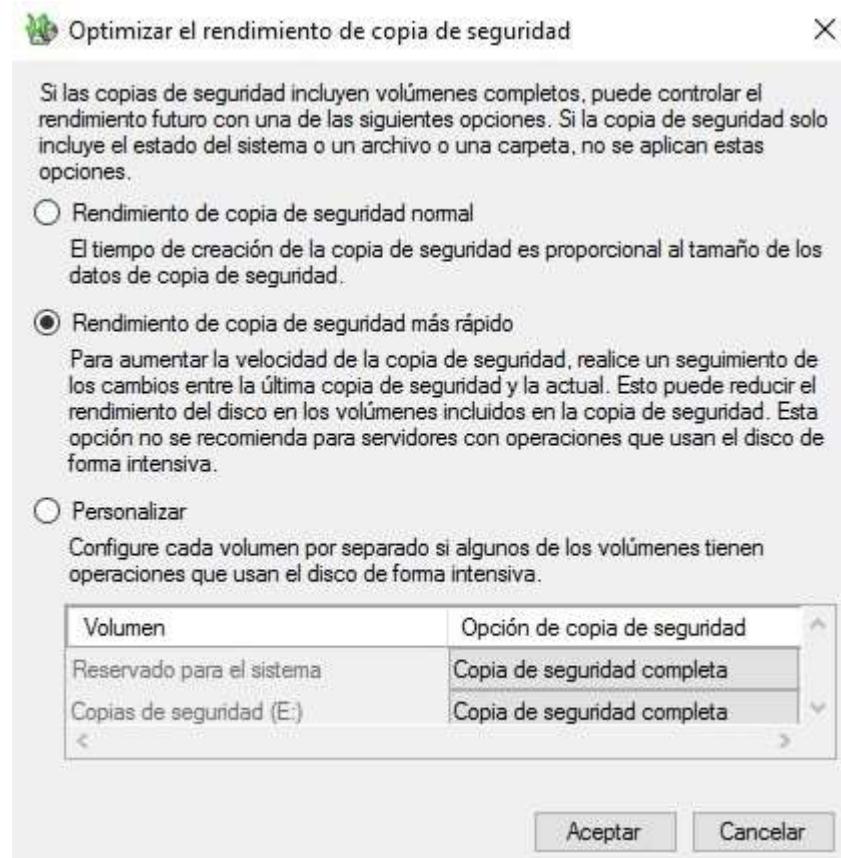
Estado

Última copia de seguridad	Próxima copia de seguridad	Todas las copias de seguridad
Estado: <span style="color: green;">●</span> Correcta Hora: 08/01/2021 19:54 <a href="#">Ver detalles</a>	Estado: No programada Hora: - <a href="#">Ver detalles</a>	Copias de seguridad totales: 1 copias Copia más reciente: 08/01/2021 19:54 Copia más antigua: 08/01/2021 19:54 <a href="#">Ver detalles</a>

Un detalle más que se refiere al método para realizarla. Haz clic con el botón derecho del ratón y elige la opción *Configurar opciones de rendimiento*:



Y nos aparecen diversas opciones que se refieren a cómo debe hacer una determinada copia de seguridad, si *completa* (por defecto), *incremental* (solo los cambios desde la última copia de seguridad) o *personalizada* (indicamos en cada volumen el tipo de copia de seguridad):



## 4. Almacenamiento en Windows Server

Hemos instalado un servidor en una máquina virtual para poder practicar. Imaginemos ahora que lo vamos a instalar en un servidor real (ya sea virtualizando o no) tenemos que conocer qué métodos tenemos para poder tener cierta protección en los datos almacenados en los discos.

Vamos a instalar un servidor que va a ser el centro del sistema informático. Merece la pena invertir un poco de dinero en un sistema de discos fiable. Esto nos va a ofrecer una garantía de funcionamiento, rendimiento y sobre todo tolerancia a fallos.

Hay varios tipos de discos duros: los IDE, los serial ATA, los SCSI y los de estado sólido. Éstos dos últimos son especiales y están especialmente mejorados para trabajar con servidores.

Afirmar que la información es el activo más valioso e importante de cualquier empresa y que los datos han de estar disponibles en todo momento (24 horas x 7 días a la semana x 365 días al año) y asegurados contra incidencias, es un hecho sumamente aceptado en la actualidad. El coste de una posible pérdida de información y el tiempo durante el cual el sistema no está en explotación mientras se soluciona el problema, es un lujo que cada vez menos empresas pueden permitirse. Así pues, **disponer de un sistema de almacenamiento seguro y tolerante al fallo**, como los sistemas RAID, es algo imprescindible.

## 4.1. Sistemas RAID

El término **RAID** es un acrónimo del inglés "**Redundant Array of Independent Disks**". Significa **matriz redundante de discos independientes**. RAID es un método de combinación de varios discos duros para formar una única unidad lógica en la que se almacenan los datos de forma redundante. Ofrece mayor tolerancia a fallos y más altos niveles de rendimiento que un sólo disco duro o un grupo de discos duros independientes.

Una matriz consta de dos o más discos duros que ante el sistema principal funcionan como un único dispositivo. Un RAID, para el sistema operativo, aparece ser un sólo disco duro lógico (LUN). Los datos se desglosan en fragmentos que se escriben en varias unidades de forma simultánea. La información se reparte entre varios discos, usando técnicas como el entrelazado de bloques (RAID nivel 0) o la duplicación de discos (RAID nivel 1) para proporcionar redundancia, reducir el tiempo de acceso u obtener mayor ancho de banda para leer o escribir, así como la posibilidad de recuperar un sistema tras la avería de uno de los discos.

La tecnología RAID protege los datos contra el fallo de una unidad de disco duro. Si se produce un fallo, RAID mantiene el servidor activo y en funcionamiento hasta que se sustituya el disco defectuoso.

La tecnología RAID se utiliza también con mucha frecuencia para mejorar el rendimiento de servidores y estaciones de trabajo. Estos dos objetivos, protección de datos y mejora del rendimiento, no se excluyen entre sí.

RAID ofrece varias opciones, llamadas niveles RAID, cada una de las cuales proporciona un equilibrio distinto entre tolerancia a fallos, rendimiento y coste. Todos los sistemas RAID suponen la pérdida de parte de la capacidad de almacenamiento de los discos, para conseguir la redundancia o almacenar los datos de paridad.

Características:

- **Tolerancia a fallos:** RAID protege contra la pérdida de datos y proporciona recuperación de datos en tiempo real.
- **Mejora del Rendimiento/Velocidad:** Una matriz consta de dos o más discos duros que ante el sistema principal funcionan como un único dispositivo. Los datos se desglosan en fragmentos que se escriben en varias unidades de forma simultánea. RAID permite a varias unidades trabajar en paralelo, lo que aumenta el rendimiento del sistema.
- **Mayor Fiabilidad:** Las soluciones RAID emplean dos técnicas para aumentar la fiabilidad: la redundancia de datos y la información de paridad. La redundancia implica el almacenamiento de los mismos datos en más de una unidad. De esta forma, si falla una unidad, todos los datos quedan disponibles en la otra unidad, de inmediato. Aunque este planteamiento es muy eficaz, también es muy costoso, ya que exige el uso de conjuntos de unidades duplicados. El segundo planteamiento para la protección de los datos consiste en el uso de la paridad de datos. Cuando se produce un fallo en una unidad se leen los datos correctos que quedan y se comparan con los datos de paridad

almacenados por la matriz. El uso de la paridad para obtener fiabilidad de los datos es menos costoso que la redundancia, ya que no requiere el uso de un conjunto redundante de unidades de disco.

Existen dos tipos de tecnología RAID: basada en software y basada en hardware. Cada uno de ellos tiene sus ventajas y sus inconvenientes.

La ventaja de los RAID basados en hardware es su independencia de la plataforma o sistema operativo, ya que son vistos por éste como un gran disco duro más, y además son mucho más rápidos, entre otras ventajas. Los sistemas RAID software no son implementaciones adecuadas en la mayoría de los casos, y cada vez son menos empleados.

A diferencia de las matrices (RAID) basadas en software, las que están basadas en hardware utilizan controladores RAID que se conectan a una ranura PCI del host. Con tan sólo una diferencia mínima de precio con respecto al coste del controlador que se necesita para el software RAID, el hardware RAID ofrece ventajas significativas en lo que respecta a:

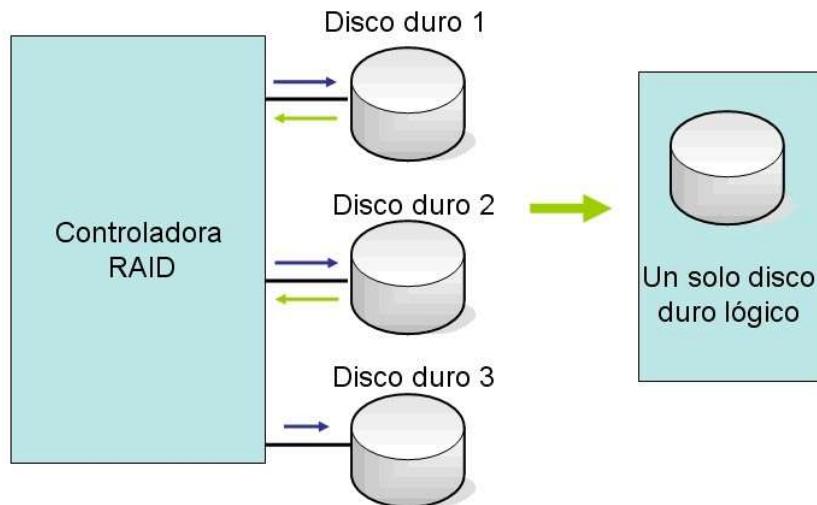
- Rendimiento
- Integridad de los datos
- Gestión de matrices

No dudamos entonces de que nuestro RAID debe ser por hardware. Si adquirimos el servidor indicando que queremos que tenga un sistema RAID con toda seguridad será por hardware y de uno de los principales tipos que son:

### Niveles de RAID

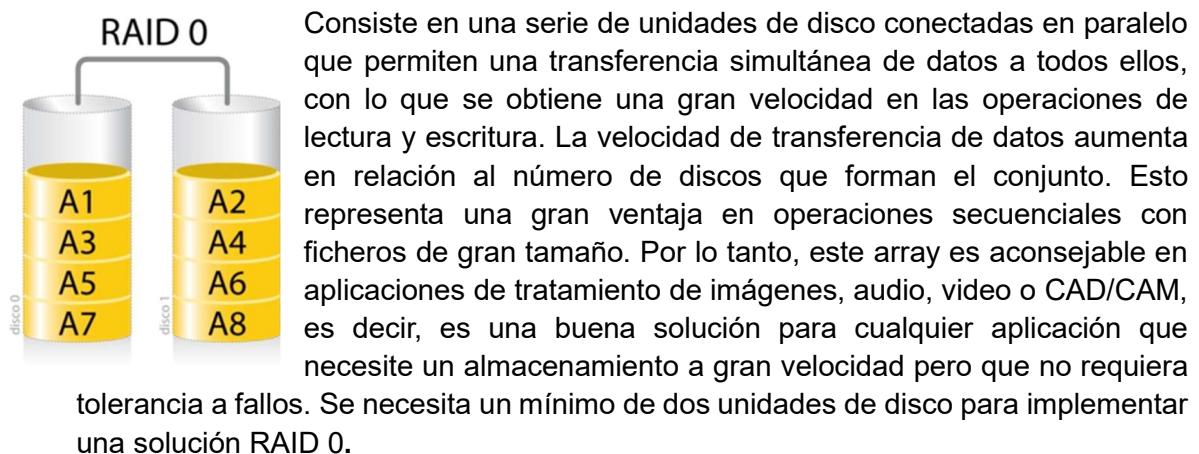
La elección de los diferentes niveles de RAID va a depender de las necesidades del usuario en lo que respecta a factores como seguridad, velocidad, capacidad, coste, etc. Cada nivel de RAID ofrece una combinación específica de tolerancia a fallos (redundancia), rendimiento y coste, diseñadas para satisfacer las diferentes necesidades de almacenamiento. La mayoría de los niveles RAID pueden satisfacer de manera efectiva sólo uno o dos de estos criterios. No hay un nivel de RAID mejor que otro; cada uno es apropiado para determinadas aplicaciones y entornos informáticos. De hecho, resulta frecuente el uso de varios niveles RAID para distintas aplicaciones del mismo servidor.

Por ejemplo, la más implementada es la de RAID 5 que se muestra en esquema:



- **RAID 0: Disk Striping "La más alta transferencia, pero sin tolerancia a fallos".**

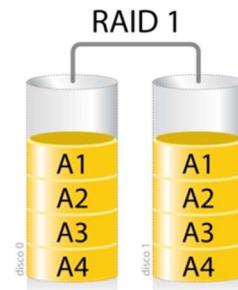
También conocido como "**separación o fraccionamiento/Striping**". Los datos se desglosan en pequeños segmentos y se distribuyen entre varias unidades. Este nivel de "array" o matriz no ofrece tolerancia al fallo (es decir, crea una sola unidad con varios discos, pero la información no se replica, por lo tanto, si se estropea uno perderemos la información). La ventaja es que por hardware creamos una unidad lógica que se compone de varios discos: transparente para nosotros y muy rápida). Al no existir redundancia, RAID 0 no ofrece ninguna protección de los datos. El fallo de cualquier disco de la matriz tendría como resultado la pérdida de los datos y sería necesario restaurarlos desde una copia de seguridad. Por lo tanto, RAID 0 no se ajusta realmente al acrónimo RAID.



- **RAID 1: (Espejo). "Redundancia. Más rápido que un disco y más seguro"**

También llamado "Mirroring" o "Duplicación" (Creación de discos en espejo). Se basa en la utilización de discos adicionales sobre los que se realiza una copia en

todo momento de los datos que se están modificando. RAID 1 ofrece una excelente disponibilidad de los datos mediante la redundancia total de los mismos. Para ello, se duplican todos los datos de una unidad o matriz en otra. De esta manera se asegura la integridad de los datos y la tolerancia a fallos, pues en caso de avería, la controladora sigue trabajando con los discos no dañados sin detener el sistema. Los datos se pueden leer desde la unidad o matriz duplicada sin que se produzcan interrupciones.



RAID 1 es una alternativa costosa para los grandes sistemas, ya que las unidades se deben añadir en pares para aumentar la capacidad de almacenamiento. Sin embargo, RAID 1 es una buena solución para las aplicaciones que requieren redundancia cuando hay sólo dos unidades disponibles. Los servidores de archivos pequeños son un buen ejemplo. Se necesita un mínimo de dos unidades para implementar una solución RAID 1.

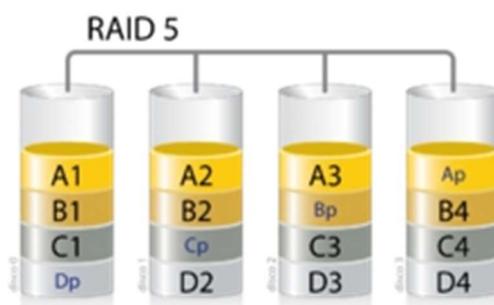
- **RAID 5: "Acceso independiente con paridad distribuida."**

Este array ofrece tolerancia al fallo, pero, además, optimiza la capacidad del sistema. Esto lo consigue mediante el cálculo de información de paridad y su almacenamiento alternativo por bloques en todos los discos del conjunto.

La información del usuario se graba por bloques y de forma alternativa en todos ellos. De esta manera, si cualquiera de las unidades de disco falla, se puede recuperar la información en tiempo real, sin que el servidor deje de funcionar.

**RAID 5 es el nivel de RAID más eficaz y el de uso preferente para las aplicaciones de servidor básicas para la empresa.** Comparado con otros niveles

RAID con tolerancia a fallos, RAID 5 ofrece la **mejor relación rendimiento-coste en un entorno con varias unidades**. Gracias a la combinación del fraccionamiento de datos y la paridad como método para recuperar los datos en caso de fallo, constituye una solución ideal para los entornos de servidores en los que la protección y disponibilidad de los datos es fundamental y el coste es un factor importante.



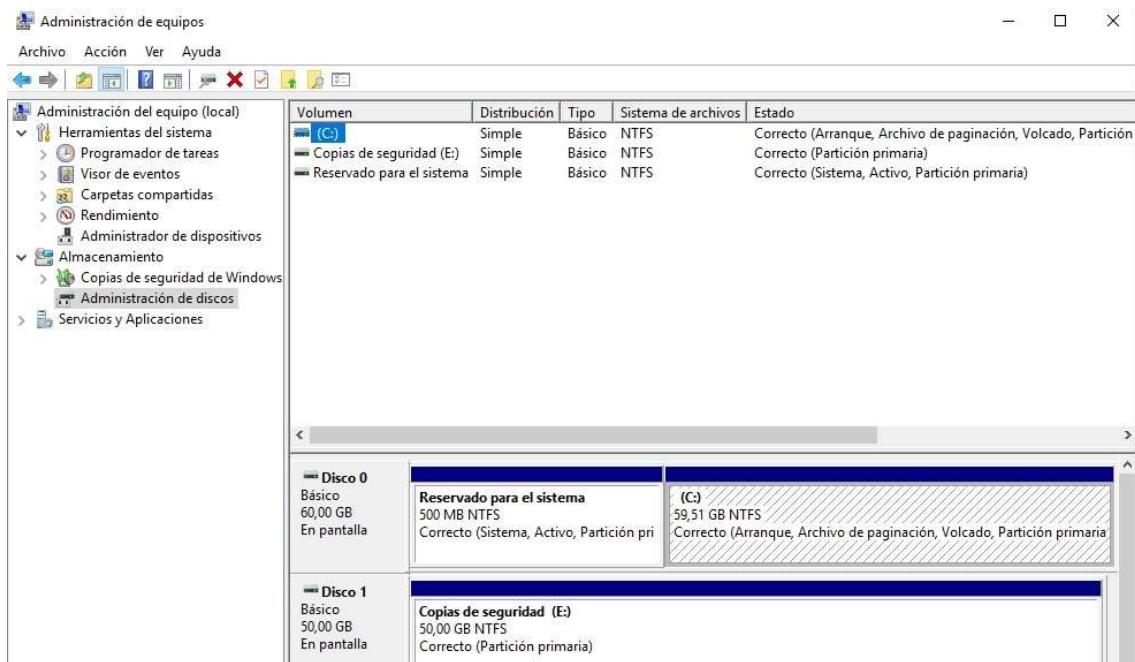
Se necesita un mínimo de tres unidades para implementar una solución RAID 5.

#### 4.3. Consola de administración de discos

---

Una vez arrancado el sistema, la consola de administración de discos, será la principal utilidad para manejar los discos físicos y lógicos de nuestra máquina. Ésta puede ser utilizada por usuarios miembros del grupo *Administradores*. Se utiliza tanto para configurar nuevos discos, como para administrar la tolerancia a fallos de los mismos.

Para ejecutar la consola de administración de discos, en el controlador de dominio, en el menú *Herramientas*, selecciona *Administración de Equipos* y ahí *Almacenamiento>Administración de discos*.



Antes de continuar comentaremos un par de detalles. Cuando añadimos un nuevo disco a Windows tendremos que configurarlo indicando el tipo de disco, tipo de volumen y su formato.

Podremos dar formato a los volúmenes de disco con los dos formatos de archivos comunes: FAT y NTFS. El primero se utiliza en disquetes, memorias USB y sistemas operativos antiguos. Es un formato muy inseguro y con pocas opciones avanzadas. NTFS que es el formato de Windows NT, proporciona seguridad y muchos más servicios que veremos ahora.

#### 4.4. Los discos en Windows Server

Windows Server nos va a permitir definir cómo serán presentados los discos. Dependiendo del tipo y del tamaño podremos elegir entre un tipo de disco y volúmenes para instalar en él nuestros programas. Vamos a ver ahora una serie de conceptos. Para empezar, podemos definir si va a ser un disco básico o dinámico y en los dos casos podemos definirlos como un *Master Boot Record (MBR)* o *discos de tablas de particiones (GPT)*. Los discos básicos solo permiten volúmenes simples y los discos dinámicos permiten crear volúmenes lógicos con varios discos. La elección luego entre MBR y GPT depende del tamaño del disco y de la cantidad de particiones que necesitemos crear en nuestros discos.

##### Discos "Master Boot Record" (MBR)

Es la estructura utilizada tradicionalmente. La configuración del disco, información de la partición y formato se almacena en el disco en el MBR. Este sector es vital, ya que, si se corrompe esta información o se mueve, el disco se queda inaccesible. Tienen un límite de tres particiones primarias y una extendida que puede albergar distintas

unidades lógicas. Si elegimos este formato sabremos que es un formato compatible y que es fácil montar y desmontar unidades e instalar diferentes sistemas operativos.

### **Discos con tabla de partición GUID (GPT)**

Este formato apareció por primera vez en Windows 2003 Server SP1 y es el formato recomendado para discos mayores de 2 TB. Permite ilimitadas particiones primarias y es muy útil si queremos crear grandes matrices de discos.

#### **Disco básico**

Un disco básico solo soporta volúmenes simples. No tienen mecanismos de tolerancia a fallos. Los volúmenes simples pueden extenderse añadiendo porciones del mismo disco o de otros discos, pero no se puede reducir su tamaño una vez extendido ni eliminar porciones que se añadieron, sólo se podrá eliminar el volumen completo. Un volumen simple puede extenderse por otros discos hasta ocupar un máximo de 32 discos dinámicos.

#### **Disco dinámico**

Los discos dinámicos pueden utilizarse para crear grandes volúmenes, volúmenes con tolerancia a fallos o volúmenes que pueden leer y escribir a través de varios discos físicos para una alta disponibilidad. Estos discos son administrados por el "servicio de discos virtuales" (VDS)

#### **Partición o volumen**

Cuando hablamos de discos en Windows podemos decir indistintamente volúmenes o particiones. De hecho, en la consola gráfica no hay diferencias. Pero en la realidad sí, los volúmenes pueden existir en discos básicos (serán particiones) o dinámicos (y repartirse en varios de ellos) y las particiones solo existen en discos básicos.

#### **Punto de montaje**

Cuando creamos un volumen en Windows, puede asignarse a una letra de unidad o montarse en una carpeta vacía existente o en un volumen ya existente. Cuando montamos un volumen en una carpeta se dice que es el punto de montaje.

Los puntos de montaje son muy útiles en el caso de que queremos simplificar el acceso a disco de los usuarios, además de poder crear un disco grande con varios pequeños. Por ejemplo, en un servidor de base de datos con tres discos en el que asignamos el disco1 a la unidad *D:\*, el disco2 lo podemos montar en *D:\datos* y el disco 3 lo podemos montar en *D:\logfiles*.

#### **Volúmenes simples**

Un volumen simple es una partición creada en un disco básico o dinámico. En un disco básico los volúmenes simples pueden ampliarse para utilizar el espacio de disco no utilizado que exista en la parte siguiente del disco, es decir, ese espacio debe ser contiguo. Para ampliar un volumen simple con zonas no contiguas o espacio libre del mismo disco o de otro debemos actualizarlo primero a un disco dinámico.

### **Volúmenes *Spanned* o distribuidos**

Los volúmenes distribuidos, también conocidos como spanned volumes o volúmenes extendidos, están formados por el espacio libre enlazado de hasta 32 discos dinámicos. Estos volúmenes no pueden ser configurados en espejo, tampoco tienen tolerancia a fallos por lo que si uno de los discos que lo componen falla no habrá manera de recuperar datos, aunque estos teóricamente se encuentran en otro disco físico por lo que es muy importante realizar backups de los datos más sensibles que se almacenen en este tipo de volumen.

La ventaja la tenemos en la facilidad para ampliar el tamaño si no podemos mover los datos a un disco mayor. Podemos ampliar el espacio con el que hay disponible en el disco o en otro disco. Un volumen simple al que le hemos ampliado con espacio libre del mismo disco se le considera todavía un volumen simple. Pero si ampliamos un volumen simple con espacio de otro disco automáticamente pasa a ser un volumen distribuido.

### **Volúmenes *Striped* o seccionado**

Un volumen seccionado o un volumen compatible RAID-0 necesita dos o más discos dinámicos proporcionando la configuración más rápida de ellos. Leen y escriben de cada disco simultáneamente para mejorar el tiempo de acceso. Utilizan todo el espacio disponible pero no tienen tolerancia a fallos: si un disco falla, no podremos acceder a los demás. Estos volúmenes necesitan una cantidad exacta de espacio en disco en cada uno de ellos. Por ejemplo, para crear un volumen seccionado de 15 GB con tres discos, utilizaremos 5 GB de cada uno de ellos.

Un volumen seccionado es un volumen que está formado por un conjunto de porciones o bandas de igual tamaño (64 Kbytes) de varios discos, hasta un máximo de 32 discos. La información se reparte entre las bandas de los distintos discos. El reparto de información es equitativo y alternativo, ocupando de este modo todas las bandas o porciones de los discos integrantes. Como resultado, el rendimiento de E/S es más alto.

Los discos no tienen por qué ser del mismo tamaño, pues lo que es igual son las bandas que se crean en los discos. Además, no pueden variar de tamaño una vez creados.

Estos volúmenes sólo pueden crearse en discos dinámicos y no ofrecen tolerancia a errores sino todo lo contrario. Si uno de los discos, o una banda, tuviese errores, el volumen completo falla y la información se pierde. Se corresponde con lo que en Windows NT se conocía como conjunto de bandas (RAID 0). La fiabilidad de este sistema es siempre menor que la fiabilidad del disco menos fiable.

Los volúmenes seccionados son el sistema de almacenamiento que ofrece el mejor rendimiento de todos los tipos de volúmenes de Windows 2008, tanto en escritura como lectura, por lo que se puede escoger por su rendimiento.

### **Volúmenes con tolerancia a fallos**

Si no disponemos de un sistema de hardware que nos proporcione tolerancia a fallos, podemos crear volúmenes con esta ventaja por software para poder proteger los datos.

Windows Server tiene dos formas de proporcionarnos esta tolerancia a fallos y que ya vimos antes: RAID 1 (espejo) y RAID 5.

### **Volúmenes *mirror* o en espejo**

Un espejo o RAID-1 necesita dos discos independientes, sin embargo, el espacio en discos será el equivalente a uno de ellos ya que la información está repetida en los dos discos físicos. Es una forma sencilla de tener un sistema de tolerancia a fallos, pero "desperdiciamos" mucho espacio. Es más eficiente el RAID-5.

Las dos copias siempre deben encontrarse en dos discos distintos, y preferentemente en controladoras de disco distintas, a este mecanismo se le denomina **duplexación**. Si uno de los discos fallase, el sistema se repondrá utilizando la copia. Esto es recomendable, por ejemplo, para el volumen del sistema. Además, desde el disco de reparación de emergencia, se puede arrancar de una copia en espejo. Como inconveniente, el espacio útil de disco se reduce en un 50%.

Sólo pueden crearse en discos dinámicos. Son más lentos a la hora de escribir, puesto que se han de realizar las escrituras por duplicado.

Para reflejar el volumen, es necesario que en el sistema exista al menos otro disco en modo dinámico, además del que queremos reflejar. En ese momento, pulsando con el botón derecho sobre el volumen, el sistema ofrece la posibilidad de reflejarlo utilizando espacio no asignado de alguno de los discos. Para eliminar un volumen reflejado tenemos dos opciones:

- **Romper el espejo:** Esta opción descompone el volumen reflejado dividiéndola en dos volúmenes independientes. Como resultado tenemos dos volúmenes idénticos en tamaño y con la misma información en ambos, pero ya no están reflejados.
- **Quitar el espejo:** Esta opción libera una de las dos copias integrantes del espejo, dejando el espacio que ocupaba tal copia como no asignado. La otra copia sigue funcionando, pero ahora no está reflejada.

### **Volúmenes en RAID-5**

Para estos volúmenes necesitamos tres discos o más discos dinámicos y proporcionan una gran velocidad de acceso porque se puede leer de todos simultáneamente. La escritura esa algo más lenta por utilizar unas "bandas" para la escritura. En el caso de fallo en un disco, la información se recoge automáticamente de la redundancia, pero con cierta pérdida de rendimiento hasta que se sustituya la unidad y se restablezca el RAID.

Se pierde un disco en la redundancia, es decir, si tenemos 3 discos de 50 GB el espacio final será de 100 GB disponibles. Si tenemos 4 discos de 25 GB el espacio total será de 75 GB disponibles.

Los volúmenes de RAID5 son tolerantes a fallos. Si un disco o una banda contiene errores, Windows Server puede reconstruir la información que se pierde a partir de los datos que quedan en las otras bandas junto con la paridad. El sistema puede por tanto soportar la pérdida de un disco sin pérdida de datos.

Como hemos comentado no dispondremos de toda la capacidad de un volumen RAID5 para guardar datos, puesto que siempre una de las bandas se destina a guardar los datos de paridad. El tamaño disponible dependerá del número de discos que componen el RAID5, como siempre se destina una banda a la paridad, al incrementar el número de discos del RAID5 aumenta el espacio de almacenamiento útil disponible.

Los volúmenes RAID5 consumen más memoria del sistema. Su uso es para información importante que en la medida de lo posible no sea muy cambiante, pues el rendimiento en escrituras es algo peor.

#### 4.5. Administrar discos con Server

La administración laaremos con la consola administrativa que vimos antes. Veamos diferentes operaciones con discos:

##### Añadir un nuevo disco a Windows

Añadiremos dos nuevos discos a nuestro controlador de dominio de tamaños 8 GB y 16 GB. Recuerda que desde *Herramientas > Administración de equipos > Almacenamiento > Administración de discos* hay que ponerlos en línea e inicializarlos.



Y a continuación los formateamos dándoles un *nuevo volumen simple* (botón derecho del ratón), de momento no ponemos etiquetas a los discos:

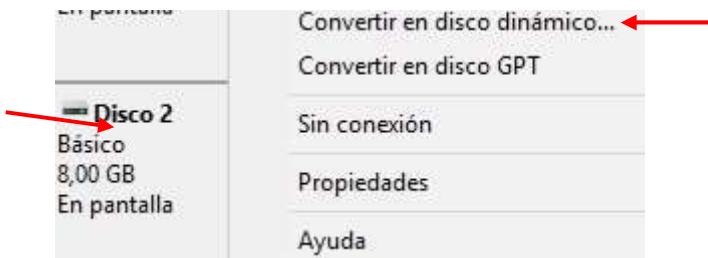


Una vez hecho esto nos quedará en el *administrador de archivos*:



##### Convertir un disco sencillo en dinámico.

Si queremos crear un sistema de tolerancia a fallos los discos tendrán que convertirse en dinámicos, así después le aplicaremos la tolerancia a fallos que queramos. Para convertirlo en dinámico, pulsamos en la zona izquierda con el botón derecho y elegimos la opción *Convertir en disco dinámico*:



Nos advierte de que en discos dinámicos no se pueden instalar sistemas operativos, pero en nuestro caso no nos importa porque los usaremos para crear RAIDs en ellos.

Administración de discos

**i** La operación elegida convertirá los discos básicos seleccionados en discos dinámicos. Si los discos se convierten en dinámicos, no podrá iniciar ningún sistema operativo instalado en los volúmenes de los mismos, a excepción del volumen de arranque actual. ¿Está seguro de que desea continuar?

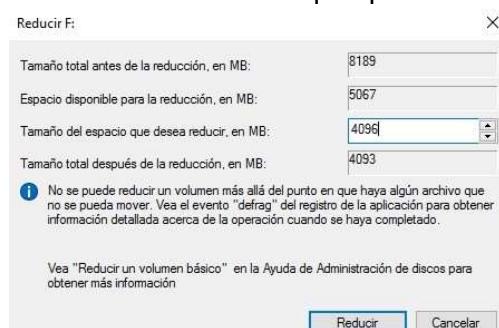
Una vez creado figurará ya como dinámico con un volumen simple:



**Importante:** Este proceso NO es reversible, es decir, no podremos convertirlo en básico sin eliminar todos los volúmenes y perdiendo los datos.

#### Crear un sistema de tolerancia a fallos

Como ya sabemos, tendremos que disponer de varios discos dinámicos. Para el ejemplo que vamos a hacer, un RAID1 o espejo, necesitaremos dos discos. Lo primero será obtener espacio libre en ambos discos (que anteriormente hemos convertido en discos dinámicos y ahora son volúmenes simples, sin espacio libre). Para ello pulsamos con el botón derecho y elegiremos *Reducir volumen* (lo haremos en ambos discos) **Reducir volumen...** Introduciremos el tamaño que queremos reducir 4.096 MB (4 GB):



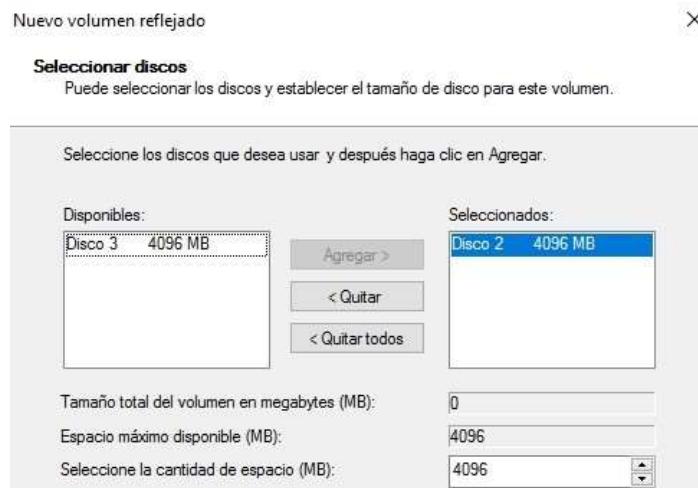
con lo que en ambos discos tendremos 4 GB de espacio libre (sin asignar):

<b>Disco 2</b> Dinámico 8,00 GB En pantalla	<b>Nuevo vol (F:)</b> 4,00 GB NTFS Correcto	4,00 GB No asignado
<b>Disco 3</b> Dinámico 16,00 GB En pantalla	<b>Nuevo vol (G:)</b> 12,00 GB NTFS Correcto	4,00 GB No asignado

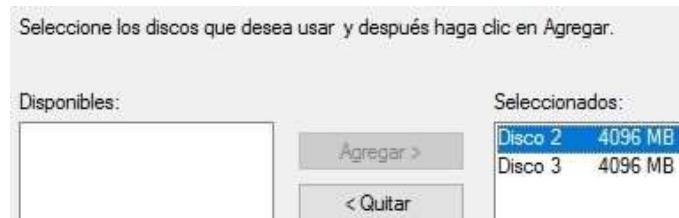
Ahora vamos a crear un RAID1 en estos espacios no asignados (necesitábamos espacio libre en dos discos). Para ello pulsamos con el botón dercho sobre la zona libre y elegimos *Nuevo volumen reflejado*:



Como ves tenemos habilitadas todas las opciones de volúmenes que hemos visto antes en la teoría, excepto la de RAID5 ya que solo disponemos de dos discos con espacio libre y para crear un RAID5 necesitamos al menos 3 discos con espacio no asignado. En nuestro caso seleccionamos *Nuevo volumen reflejado* y continuamos:



Ahora elegimos el Disco 3 (que usaremos para crear el RAID1) y pulsamos en *Agregar*:



Asignamos una unidad lógica (H:) al RAID1 y lo formateamos:

#### Nuevo volumen reflejado

##### Asignar letra de unidad o ruta de acceso

Para obtener acceso más fácilmente, puede asignar una letra de unidad o ruta de unidad a su volumen.

Asignar la letra de unidad siguiente:

H

Montar en la siguiente carpeta NTFS vacía:

Examinar...

No asignar una letra o ruta de acceso de unidad

#### Nuevo volumen reflejado

##### Formatear volumen

Debe formatear este volumen antes de poder almacenar datos en él.

Elija si desea formatear este volumen y, de ser así, la configuración que desea usar.

No formatear este volumen

Formatear este volumen con la configuración siguiente:

Sistema de archivos:

NTFS

Tamaño de la unidad de asignación:

Predeterminado

Etiqueta del volumen:

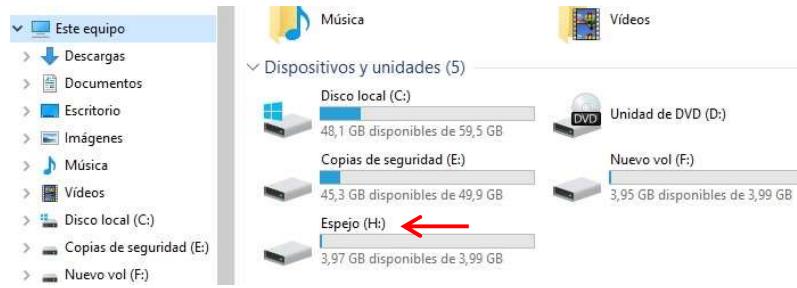
Espejo

Aquí le ponemos un nombre al volumen (*Espejo*) y le damos un formato rápido. Una vez creado nos mostrará el RAID1 creado:

<b>Disco 2</b> Dinámico 8,00 GB En pantalla	<b>Nuevo vol (F:)</b> 4,00 GB NTFS Correcto	<b>Espejo (H:)</b> 4,00 GB NTFS Correcto
<b>Disco 3</b> Dinámico 16,00 GB En pantalla	<b>Nuevo vol (G:)</b> 12,00 GB NTFS Correcto	<b>Espejo (H:)</b> 4,00 GB NTFS Correcto
 CD-ROM 0 <input type="checkbox"/> No asignado	<input type="checkbox"/> Partición primaria  Volumen simple  Volumen reflejado	

Es decir, tenemos en rojo un *volumen reflejado* que ha utilizado el mismo espacio libre de dos discos.

Hay que hacer notar que desde el punto de vista lógico el volumen reflejado (H:), sólo aparece como una única unidad en el *Explorador de archivos* (a pesar de formar parte de dos discos diferentes):



**NOTA:** También podríamos crear volúmenes reflejados (RAID1) sin necesidad de convertir los dos discos necesarios para ello en dinámicos y después *Reducir sus volúmenes* para crear en sendos espacios vacíos el volumen reflejado, tal y como hemos hecho anteriormente. Para ello podemos pulsar con el botón derecho en la zona derecha de uno de los discos y elegir *Nuevo volumen reflejado*. A continuación, tendremos que elegir otro disco (o parte libre) para completar el proceso. Notar que como el volumen reflejado debe ocupar el mismo espacio en cada una de las dos componentes, su espacio vendrá dado por el tamaño del menor de los discos (recuerda que en este caso estamos haciéndolo directamente) y así éste quedará completamente lleno con el volumen reflejado y el más grande quedará con espacio sin asignar. Se verá este caso.



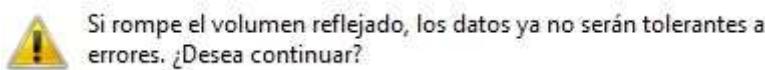
Veamos ahora las tres acciones que se pueden realizar sobre un volumen reflejado (RAID1): *Romper el espejo*, *Quitar el espejo*, probar la *tolerancia a fallos*.

### Romper el espejo

Si pulsamos con el botón derecho del ratón sobre el volumen reflejado y pulsamos en *Romper volumen reflejado*



nos advertirá que ya no es tolerante a fallos



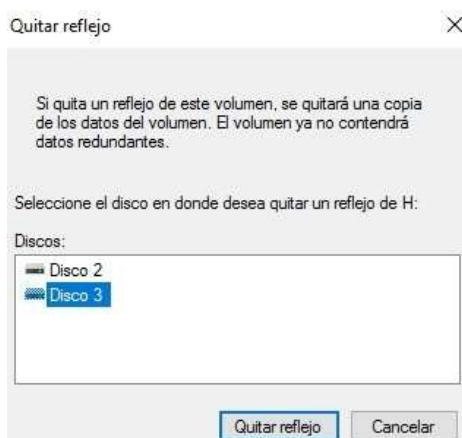
y el volumen reflejado se convertirá en dos volúmenes simples independientes cada uno con su unidad lógica distinta (I:) y (H:). La información que hubiera en el volumen ahora estará repetida, en cada uno de los dos volúmenes independientes.

### **Quitar el espejo**

Si pulsamos con el botón derecho del ratón sobre el volumen reflejado y pulsamos en *Quitar reflejo*



nos avisa de que desaparecerá una de las partes del RAID1 y por tanto la redundancia



Nos quedará un espacio libre (donde hemos quitado el reflejo) y un volumen simple, donde estarán todavía los datos anteriormente contenidos en el volumen reflejado.

Ahora a partir del volumen que ha quedado del anterior espejo (en él permanecen los datos), podemos reestablecer el espejo pulsando con el botón contextual en *Agregar reflejo* (lo haremos tomando el espacio no asignado del otro disco):

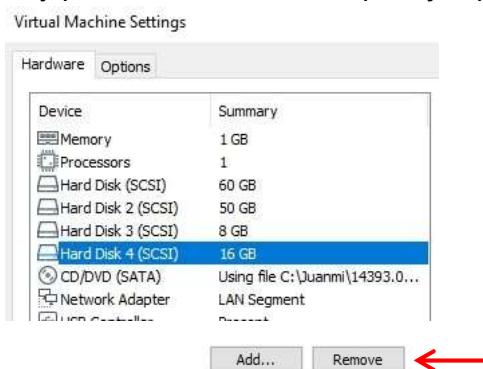
Ahora volvemos a tener un volumen reflejado con redundancia de datos:



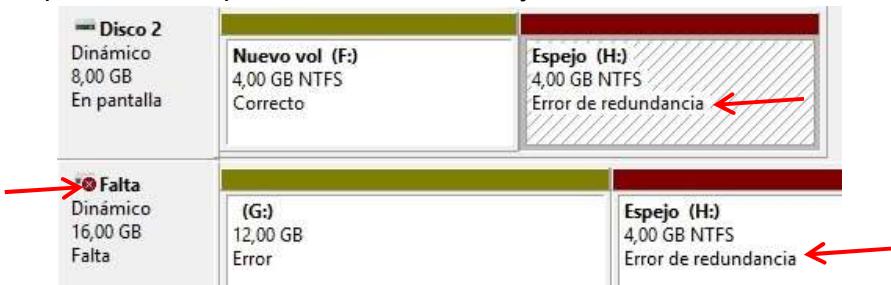
### Tolerancia a fallos

Lo más interesante del RAID1 o RAID5 es que son tolerantes a fallos (no así el RAID0), es decir, si nos falla uno de los discos que los que forman parte, los datos incluidos en ellos no se perderán. Veámoslo para el caso RAID1:

En primer lugar, eliminaremos uno de los discos que contiene el volumen reflejado que debemos tener en este momento. Para ello en VMware desde el menú *VM>Settings* elegimos el disco a eliminar y pulsamos en *Remove*, por ejemplo, el de 16 GB:

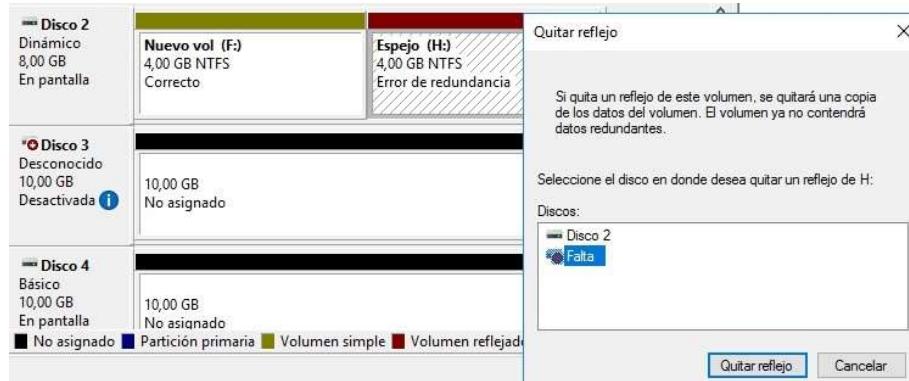


Nos informará de que falta un disco (el que hemos eliminado) y que en RAID1 hay un error de redundancia, ya que ahora los datos ya no están repetidos, al faltar uno de los discos que formaban parte del volumen reflejado:

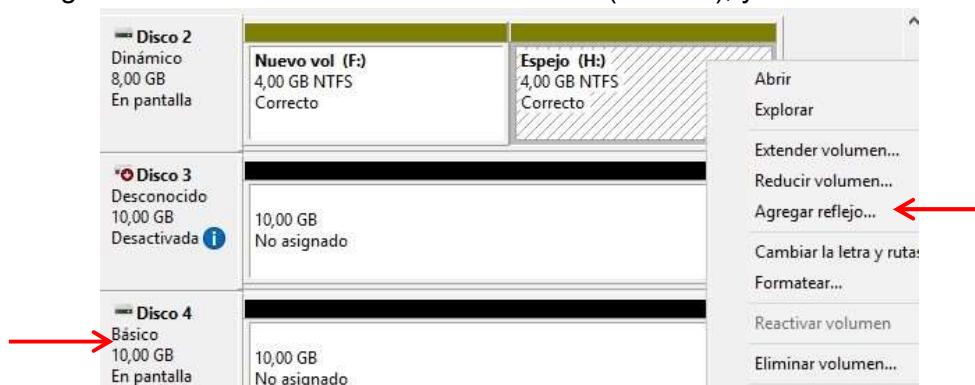


Si queremos reestablecer el volumen reflejado debemos añadir un nuevo disco (desde el menú *VM>Settings>Add*). En este caso será, por ejemplo, de 10 GB.

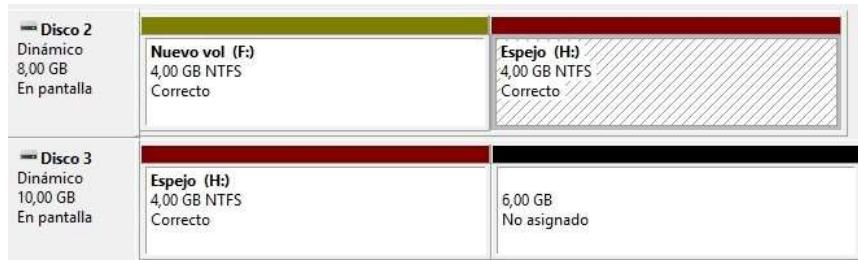
Ahora quitaremos el reflejo del volumen del disco que ya no existe (Disco 3):



Finalmente agregaremos el reflejo a partir del volumen (*Espejo (H:)*) del disco que todavía guardaba la información del RAID1 inicial (Disco 2), y con este nuevo disco:



Y volveremos a tener el volumen reflejado y además todavía estarán los datos iniciales de la parte que quedó del RAID1, *Espejo (H:)*, ahora en ambos discos (con redundancia).



### Crear un volumen distribuido

Para finalizar veamos cómo crear un volumen distribuido<sup>1</sup>. Partimos, por ejemplo, de la siguiente configuración, que ya teníamos anteriormente y a la que hemos añadido un disco de 25 GB:

---

<sup>1</sup> Un volumen distribuido forma parte de varios discos y no tiene por qué tener el mismo tamaño en cada uno de ellos como ocurría con los RAIDs. Además no es tolerante a fallos, así que si se estropea uno de los discos de los que forma parte el volumen distribuido se perderá la información, por lo que es muy habitual hacer copias de seguridad de dichos volúmenes distribuidos.

■ Disco 0 Básico 60,00 GB En pantalla	<b>Reservado para el sistema</b> 500 MB NTFS Correcto (Sistema, Activo, Partición primaria)	(C) 59,51 GB NTFS Correcto (Arranque, Archivo de paginación, Volcado, Partición primaria)
■ Disco 1 Básico 50,00 GB En pantalla	<b>Copias de seguridad (E:)</b> 50,00 GB NTFS Correcto (Partición primaria)	
■ Disco 2 Dinámico 8,00 GB En pantalla	<b>Nuevo vol (F:)</b> 3,05 GB NTFS Correcto	971 MB No asignado
■ Disco 3 Dinámico 10,00 GB En pantalla	Espejo (H:) 4,00 GB NTFS Correcto	6,00 GB No asignado
■ Disco 4 Básico 25,00 GB En pantalla	25,00 GB No asignado	

■ No asignado ■ Partición primaria ■ Volumen simple ■ Volumen reflejado

Queremos ampliar el espacio libre del Disco 2 con el espacio disponible de los Disco 3 y Disco 4 (podríamos hacerlo sólo con dos discos o con más de tres). Simplemente Pulsaremos con el menú contextual en el espacio libre del Disco 2 y elegiremos la opción *Nuevo volumen distribuido*:



Como tenemos otros discos con espacio disponible nos los muestra:

Nuevo volumen distribuido

**Seleccionar discos**  
Puede seleccionar los discos y establecer el tamaño de disco para este volumen.

Seleccione el disco que desea usar y después haga clic en Agregar.

<b>Disponibles:</b>	<b>Seleccionados:</b>
Disco 3 6141 MB	Disco 2 970 MB
Disco 4 25597 MB	

Aregar >

< Quitar

< Quitar todos

Tamaño total del volumen en megabytes (MB):

Espacio máximo disponible (MB):

Seleccione la cantidad de espacio (MB):

En este caso añadiremos 3000 MB del espacio libre del Disco 3 y 5000 MB del espacio libre del Disco 3, por ejemplo:

### Nuevo volumen distribuido

#### Seleccionar discos

Puede seleccionar los discos y establecer el tamaño de disco para este volumen.

Seleccione el disco que desea usar y después haga clic en Agregar.

Disponibles:	Seleccionados:
<input type="button" value="Añadir &gt;"/>	Disco 2 970 MB Disco 3 3000 MB <b>Disco 4 5000 MB</b>
<input type="button" value="&lt; Quitar"/>	
<input type="button" value="&lt; Quitar todos"/>	

Tamaño total del volumen en megabytes (MB):

Espacio máximo disponible (MB):

Seleccione la cantidad de espacio (MB):

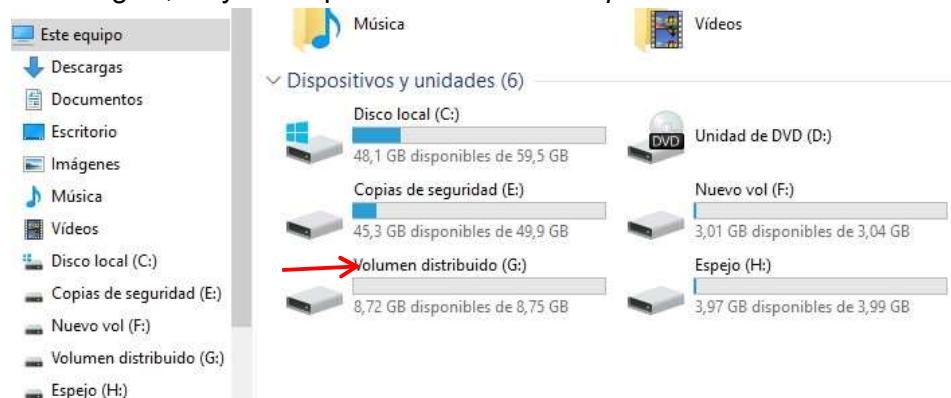
Le asignaremos una letra (G), le pondremos una etiqueta (*Volumen distribuido*) y lo formatearemos y tendremos nuestro volumen distribuido:

Disco 2 Dinámico 8,00 GB En pantalla	<b>Nuevo vol (F:)</b> 3,05 GB NTFS Correcto	<b>Volumen distribuido (G:)</b> 970 MB NTFS Correcto	Espejo (H:) 4,00 GB NTFS Correcto
Disco 3 Dinámico 10,00 GB En pantalla	Espejo (H:) 4,00 GB NTFS Correcto	<b>Volumen distribuido (G:)</b> 2,93 GB NTFS Correcto	3,07 GB No asignado
Disco 4 Dinámico 25,00 GB En pantalla	<b>Volumen distribuido (G:)</b> 4,88 GB NTFS Correcto		20,12 GB No asignado

■ No asignado ■ Partición primaria ■ Volumen simple ■ Volumen distribuido ■ Volumen reflejado

que es exactamente lo que hablamos antes de un volumen distribuido: volúmenes dinámicos en discos distintos.

Como ves, aunque el volumen distribuido forme parte de diferentes discos, constituye una unidad lógica, tal y como podemos ver en el *Explorador de archivos*:



Siempre hay que tener cuidado con estas operaciones y hacer copia de seguridad de los datos, antes de nada.

Un claro ejemplo de porqué usar un volumen distribuido es cuando, por ejemplo, estamos a punto de llenar un disco de datos y en lugar de sustituirlo por otro de más tamaño y volcar toda la información en este, lo que hacemos es añadir otro disco y hacer un volumen distribuido con la parte que todavía queda libre del primer disco y parte o todo del segundo. La información estará distribuida en ambos (o más) discos, pero estará en una unidad lógica.

## 5. Cuotas

---

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.

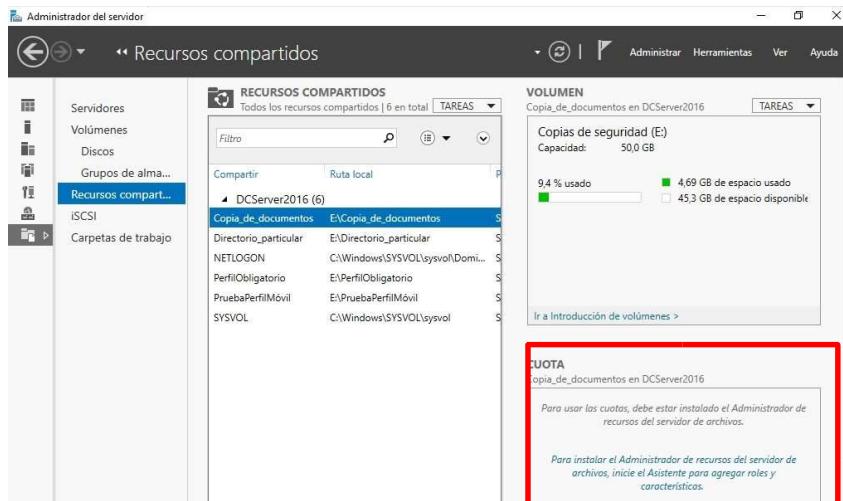
Mediante el *Administrador de recursos del servidor de archivos* se pueden acometer las siguientes tareas:

- 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 en el servidor, 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.

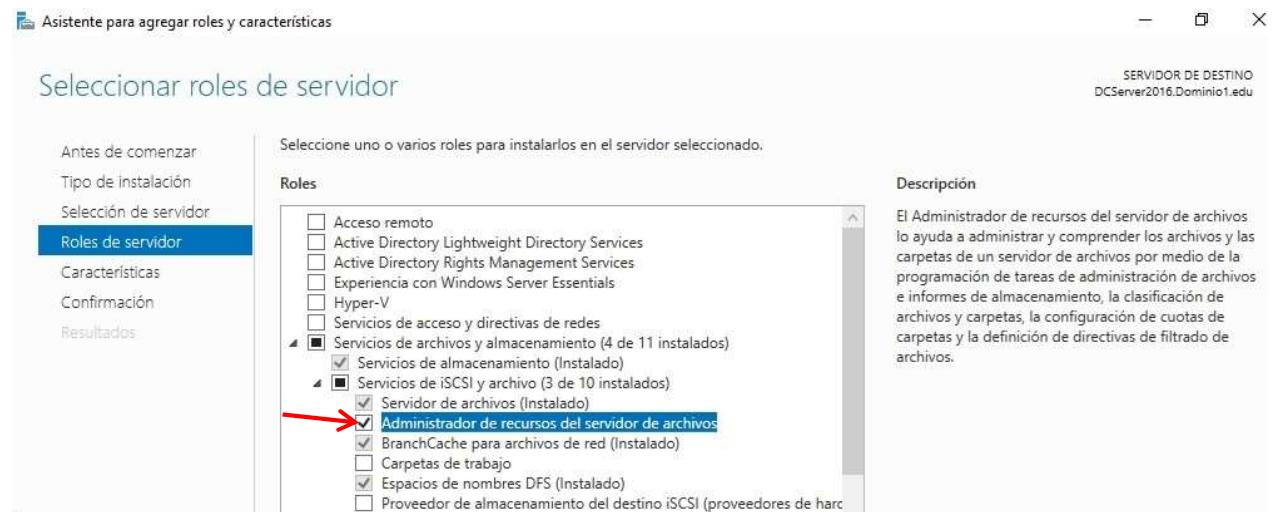
El *Administrador de recursos del servidor de archivos* es un servicio del rol *Servicios de archivo* en Windows Server. Puede instalarse como parte de este rol mediante el *Administrador de servidores*. El requisito mínimo para utilizar el *Administrador de recursos del servidor de archivos* es pertenecer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

Este *Administrador de recursos del servidor de archivos* se puede usar en cualquier Server de Windows, es decir no es necesario que sea un controlador de dominio.

Antes de la instalación podemos comprobar que no se pueden crear cuotas. Lo podemos ver si accedemos en el *Administrador del servidor* en el panel de la izquierda *Servicios de archivo y almacenamiento > Recursos compartidos*:

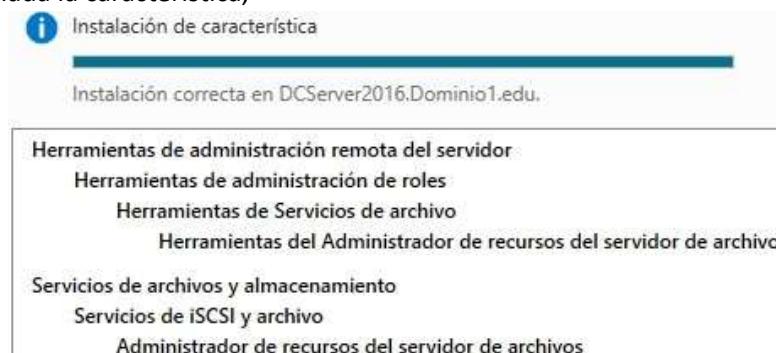


Para su instalación vamos, en nuestro controlador de dominio, al *Administrador del servidor > Agregar roles y características > Instalación basada en características o en roles > Servicios de archivos y almacenamiento > Servicios de iSCSI y archivo > Administrador de recursos del servidor de archivos (marcar opción)*:

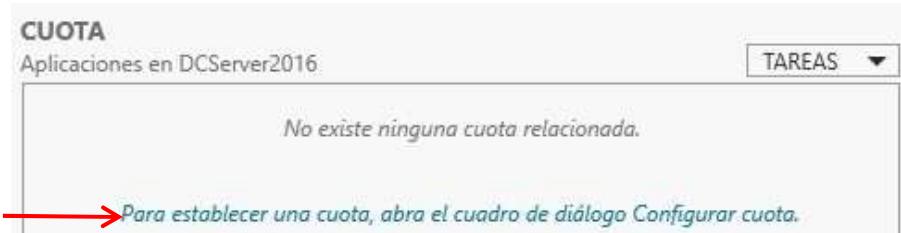


En las siguientes opciones los limitaremos a marcar la opción *Siguiente* hasta que nos ofrezca la opción *Instalar*.

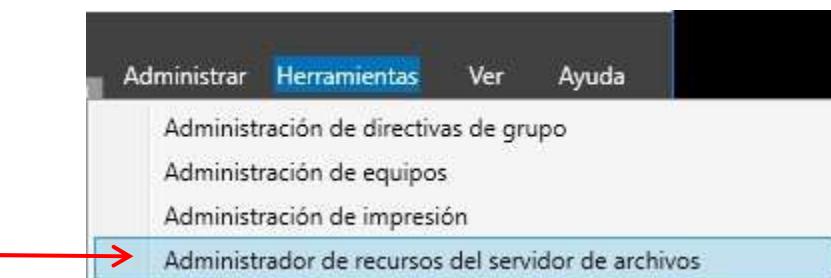
Una vez instalada la característica,



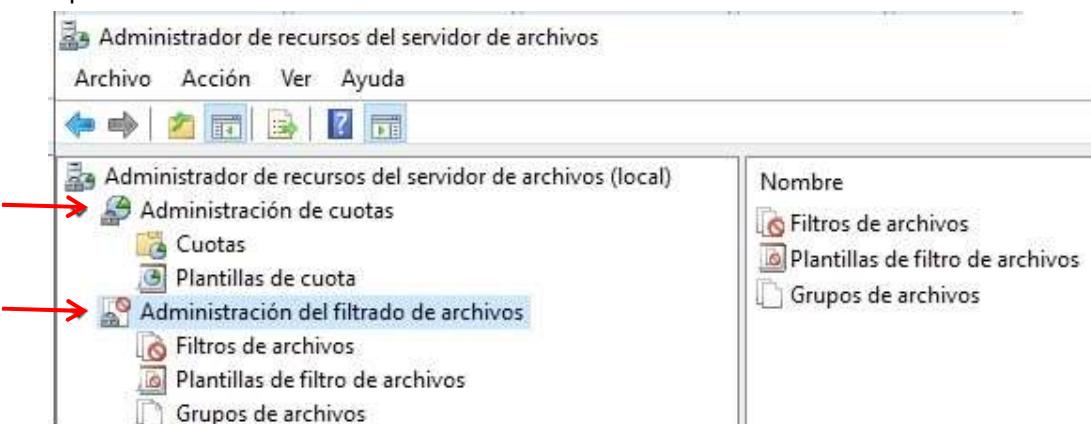
si volvemos a *Administrador del servidor > Servicios de archivos y de almacenamiento* (panel de la izquierda)> *Recursos compartidos*, veremos que ahora sí nos permite crear cuotas.



Una vez instalado abriremos la consola *Administrador de recursos del servidor de archivos* desde el *Administrador del servidor > Herramientas*:



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 dos primeras:



#### **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.

## 5.1 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.

Podemos crear dos tipos de cuotas:

- 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. Estas cuestiones no las haremos porque se escapan de los objetivos del curso.

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.

## 5.2 Acerca de las 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 las 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*:

Plantilla de cuota	Límite	Tipo de cuota	Descripción
Límite ampliado de 250 MB	250 MB	Máxima	
Límite de 10 GB	10,0 GB	Máxima	
Límite de 100 MB	100 MB	Máxima	
Límite de 2 GB	2,00 GB	Máxima	
Límite de 200 MB con extensión de 50 MB	200 MB	Máxima	
Límite de 200 MB en informes a usuario	200 MB	Máxima	
Límite de 5 GB	5,00 GB	Máxima	
Supervisar 10 TB de uso de volumen	10,0 TB	De advertencia	
Supervisar 200 GB de uso de volumen	200 GB	De advertencia	
Supervisar 3 TB de uso de volumen	3,00 TB	De advertencia	
Supervisar 5 TB de uso de volumen	5,00 TB	De advertencia	
Supervisar 500 MB de recursos compartidos	500 MB	De advertencia	

Más adelante veremos cómo se crea una plantilla de cuota y cómo se aplican las ya existentes.

### 5.3 Crear una cuota

---

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

Antes de nada, en el disco *Copias de seguridad (E:)* crearemos una carpeta llamada *Datos\_cuota*, y la compartiríremos con los *Usuarios del dominio* (aunque podríamos restringirlo a cualquier otro grupo o usuario), con permisos de *Lectura y escritura*:

Copias de seguridad (E:)

Nombre	Fecha de modifica...	Tipo
Datos_cuota	10/02/2021 19:29	Carpeta de archivos

Archivos compartidos

Elija los usuarios de la red con los que desea compartir recursos.

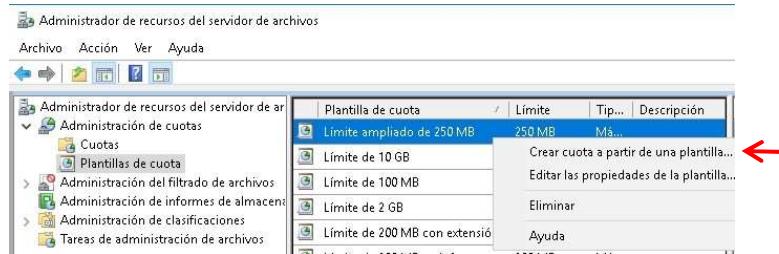
Escriba un nombre y haga clic en Agregar, o haga clic en la flecha para buscar usuarios.

Nombre	Nivel de permiso
Administrador	Lectura y escritura ▾
Administradores	Propietario
Usuarios del dominio	Lectura y escritura ▾

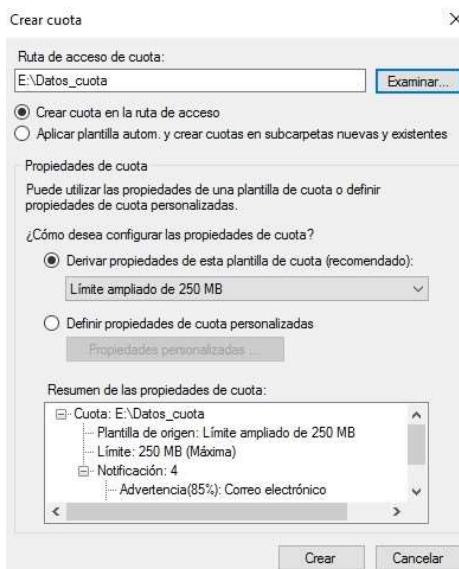
Agregar

### 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 ...**



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 preseleccionada 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**.

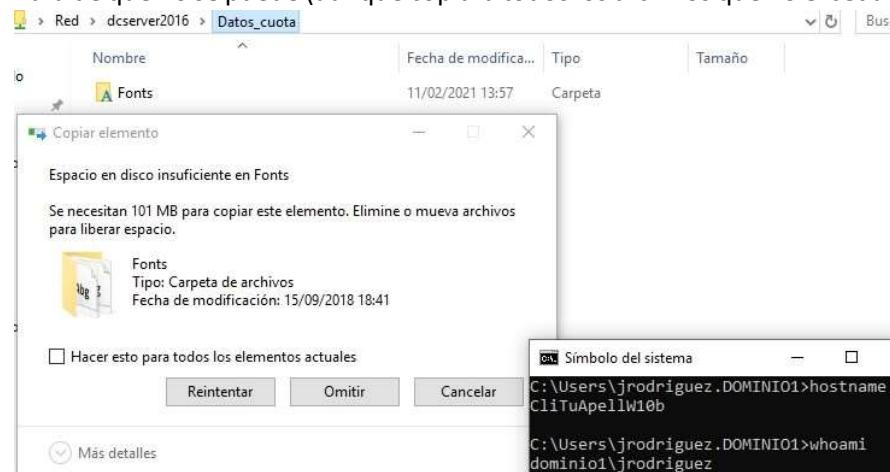
**NOTA:** Si no deseamos basar la cuota en una plantilla, o si queremos editar las propiedades que se copiaron desde una plantilla, en el cuadro de diálogo **Crear cuota** elegimos **Definir propiedades de cuota personalizadas** y, a continuación, hacemos clic en **Propiedades personalizadas**. Tengamos 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.

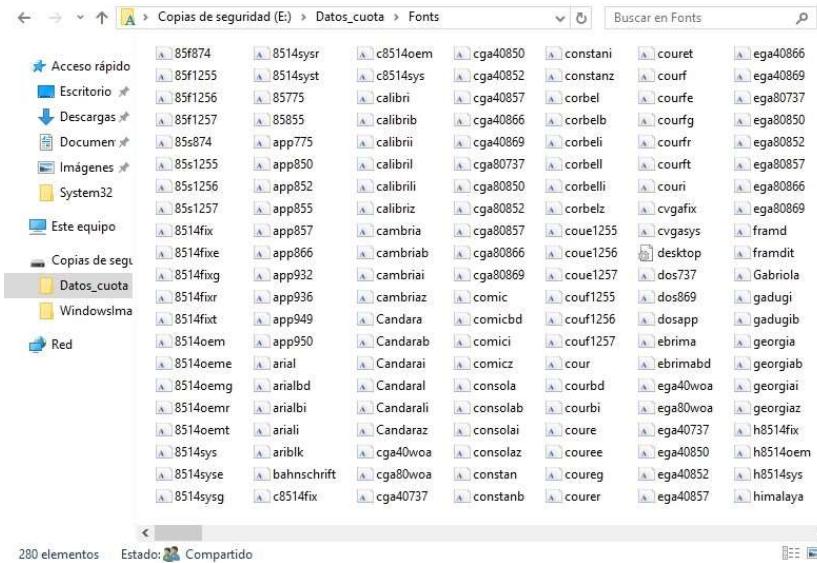
Para probarlo intentaremos copiar el contenido de la carpeta *C:\Windows\Fonts* (de 343 MB) del equipo *CliTuApellW10B* en la carpeta compartida *Datos\_cuota*, con *jrodriguez*, sobre la que hemos establecido la cuota máxima de 250 MB.

Para copiarlo lo haremos a través de la ruta UNC en el *Explorador de archivos*, del equipo cliente:



Nos informará de que no se puede (aunque copiará todos los archivos que no excedan la cuota):





## 5.3 Crear una plantilla de cuota

Para ello seguiremos los siguientes pasos:

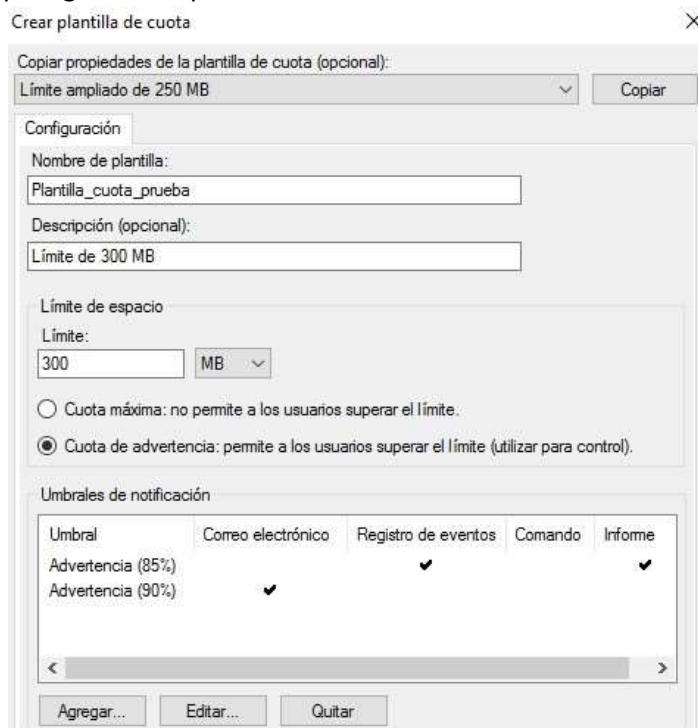
1. En **Administración de cuotas**, hacemos clic en el nodo **Plantillas de cuota**.
2. Hacemos clic con el botón secundario en **Plantillas de cuota** y, a continuación, pulsamos en **Crear plantilla de cuota**.



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**. Ahora no lo haremos así.
4. En el cuadro de texto **Nombre de plantilla**, escribimos el nombre de la nueva plantilla, por ejemplo, **Plantilla\_cuota\_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.

- Podemos configurar uno o varios umbrales de notificación opcionales para la plantilla de cuota (aunque en nuestro caso no se enviarán los mensajes ya que como dijimos la configuración necesaria se escapa de los objetivos del curso). 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	Tipo de cuota	Descripción
Límite ampliado de 250 MB	250 MB	Máxima	
Límite de 10 GB	10,0 GB	Máxima	
Límite de 100 MB	100 MB	Máxima	
Límite de 2 GB	2,00 GB	Máxima	
Límite de 200 MB con extensión de 50 MB	200 MB	Máxima	
Límite de 200 MB en informes a usuario	200 MB	Máxima	
Límite de 5 GB	5,00 GB	Máxima	
<b>Plantilla_cuota_prueba</b>	<b>300 MB</b>	<b>De advertencia</b>	<b>Límite de 300 MB</b>
Supervisar 10 TB de uso de volumen	10,0 TB	De advertencia	
Supervisar 200 GB de uso de volumen	200 GB	De advertencia	
Supervisar 3 TB de uso de volumen	3,00 TB	De advertencia	
Supervisar 5 TB de uso de volumen	5,00 TB	De advertencia	
Supervisar 500 MB de recursos compartidos	500 MB	De advertencia	

Ahora podríamos crear cuotas sobre volúmenes o carpetas tal y como hemos hecho en el apartado anterior, para esta plantilla de cuota.

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

Filtro: Mostrar todo: 2 elementos					
	Ruta de acceso de cuota	% u...	Limi...	Tipo de cu...	Plantilla de origen
<b>Coincide con plantilla: Sí (2 elementos)</b>					
	E:\Datos_cuota	99%	250 ...	Máxima	Límite ampliado de 250 MB
	E:\Cuota_informatica	0%	300 ...	De adverte...	Plantilla_cuota_prueba
					Sí

## 5.5 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. En nuestro caso no lo haremos, por razones ya comentadas.

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.

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. 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*.

Plantilla de filtro de archivos	Tipo de filtrado	Grupos de archivos
Bloquear archivos de audio y vídeo	Activo	Bloquear: Archivos de audio y vídeo
Bloquear archivos de correo electrónico	Activo	Bloquear: Archivos de correo electrónico
Bloquear archivos de imagen	Activo	Bloquear: Archivos de imagen
Bloquear archivos ejecutables	Activo	Bloquear: Archivos ejecutables
Supervisar archivos ejecutables y de sistema	Pasivo	Advertir: Archivos ejecutables, Archivos de sistema

## 5.6 Crear un filtro de archivos

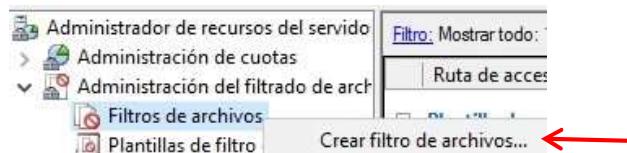
A continuación, crearemos un filtro de archivos y veremos sus efectos sobre una carpeta:

**Ejemplo:** Crea en una carpeta, llamada *Prueba\_filtro* dentro del disco *Copias de seguridad (E:)*. La carpeta *Prueba\_filtro* estará compartida para los usuarios de la UO *Informatica*, con permisos de *Lectura y escritura*. Inclúyelos a todos los usuarios de esta unidad organizativa en un grupo llamado *GInformatica*.

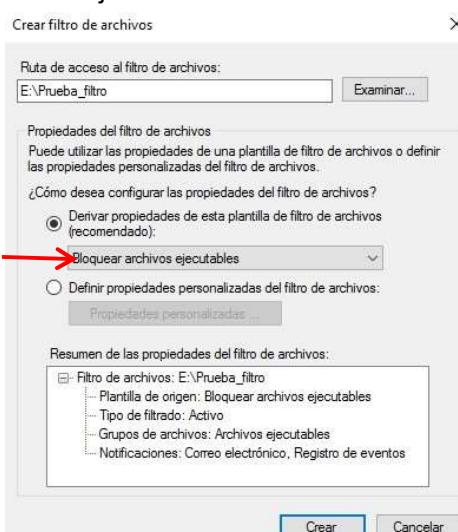
Crea un filtro (activo) para que no deje copiar archivos *ejecutables* en la carpeta *Prueba\_filtro*. Crea una excepción en el filtro anterior para que en esta carpeta permita copiar los archivos por lotes *.bat*.

Comprueba ambas acciones (no se pueden copiar ejecutables en *Prueba\_filtro*, pero sí otro tipo de archivos y sí se pueden copiar archivos .bat en ella) con *jrodriguez* que pertenece a la UO *Informatica*. ¿Qué ocurre con otro usuario que no sea de la UO *Informatica*, por ejemplo, con *usumadrid*?

En primer lugar, crearemos el filtro con el botón secundario:



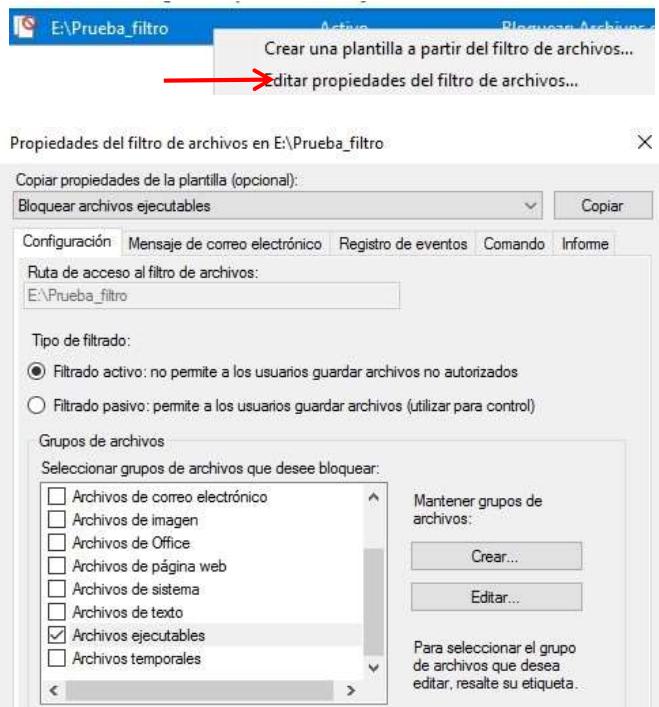
y seleccionaremos la carpeta sobre la que va a actuar y derivamos sus propiedades de la plantilla que bloquea los archivos ejecutables:



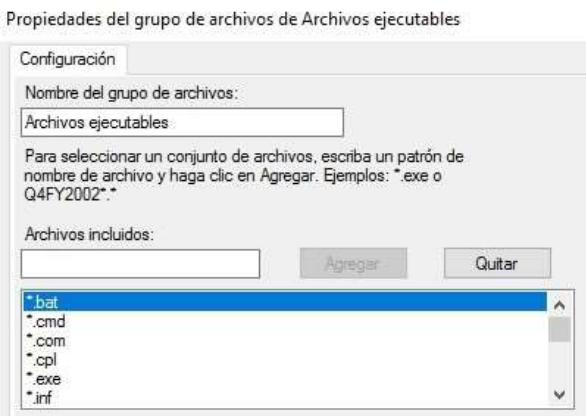
y al pulsar en *Crear* se creará el filtro sobre la carpeta *Prueba\_filtro*.



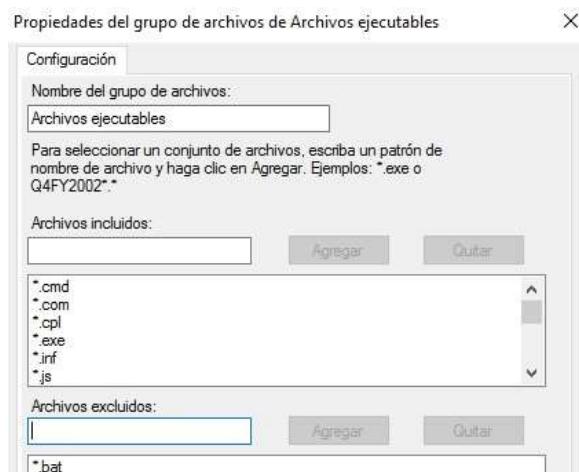
Para crear una excepción (que permita copiar archivos por lotes en la carpeta), pulsaremos sobre *Editar propiedades del filtro de archivos*:



y a continuación después de pulsar sobre el botón *Editar* nos aparecerá:



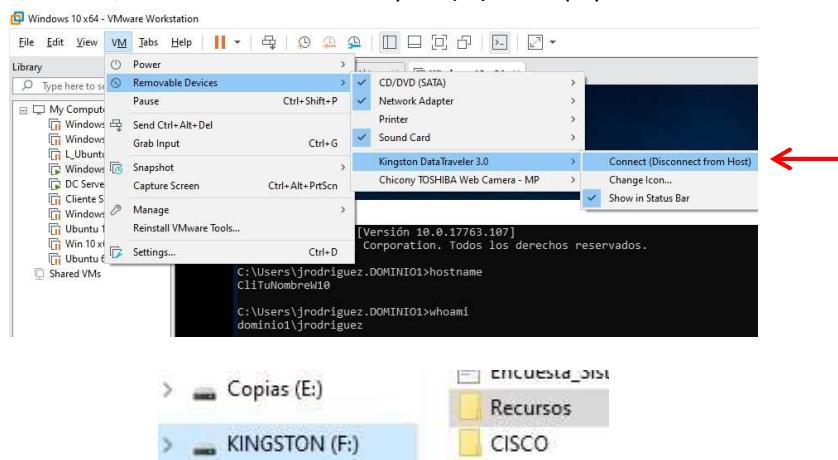
del que quitaremos **\*.bat** de los *Archivos incluidos* y lo agregaremos en *Archivos excluidos*:



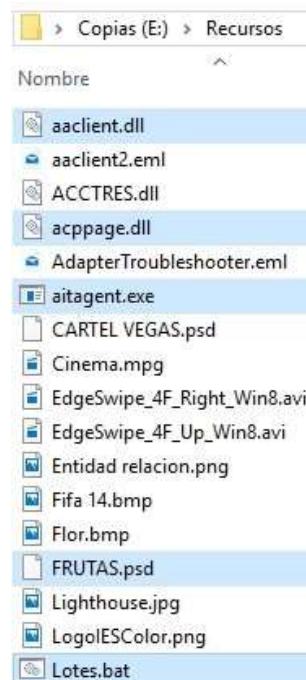
Ahora ya podrán los usuarios de la UO *Informatica* copiar archivos .bat en la carpeta *Prueba\_filtro*, aunque no podrán copiar ningún otro ejecutable.

**Prueba:** Veámoslo desde el equipo *CliTuNombreW10* con el usuario *jrodriguez*.

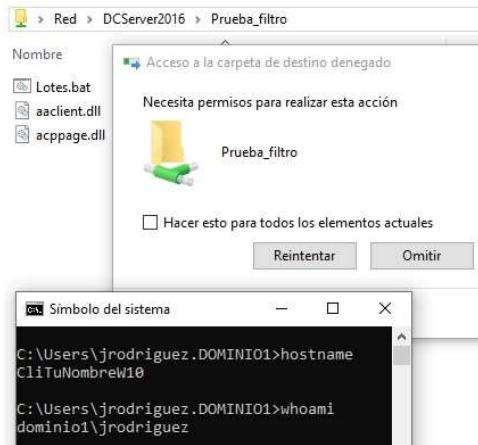
Antes copiamos la carpeta *Recursos* en este equipo cliente. Para ello en el menú *VM* de la máquina virtual, elegimos *Removable Devices>Nuestro USB>Connect (Disconnect from Host)*, con lo que lo conectaremos a la máquina virtual y así podremos copiar su contenido, en este caso la carpeta *Recursos*, en el disco llamado *Copias (E:)* del equipo *CliTuNombreW10*:



Ahora seleccionamos archivos, que incluyan .exe y .bat, además de algún archivo de otro tipo, por ejemplo, los siguientes:

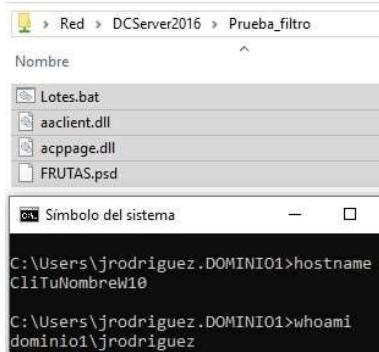


y los intentamos copiar, usando la dirección UNC desde el *Explorador de archivos* del cliente, en la carpeta *Prueba\_filtro*:



```
C:\> Símbolo del sistema
C:\Users\jrodriguez.DOMINIO01>hostname
ClTuNombreW10
C:\Users\jrodriguez.DOMINIO01>whoami
dominio1\jrodriguez
```

se detiene porque está intentando copiar el archivo *aitagent.exe* y no puede, pulsamos en *Omitir* y seguimos:



y así vemos que ha copiado todos los archivos seleccionados, incluido el *.bat* y excepto el *.exe*.

## 5.7 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.

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

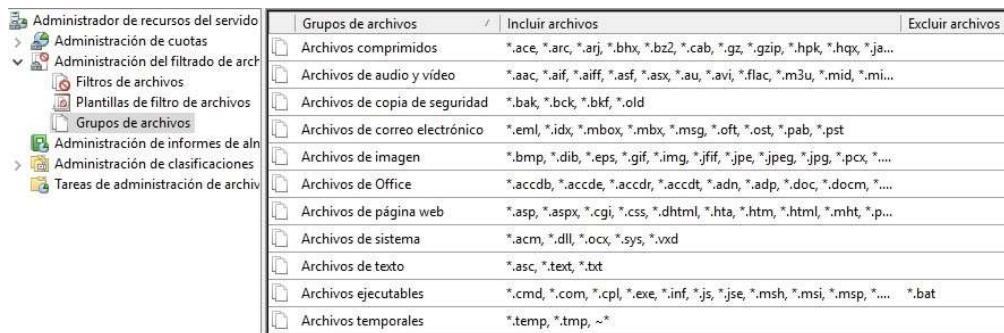
- **Archivos incluidos:** archivos que pertenecen al grupo.
- **Archivos excluidos:** archivos que no pertenecen al grupo.

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 en cualquier grupo de archivos. Cualquier cambio que hagamos a un grupo de archivos afectará a todos los filtros, plantillas e informes existentes a los cuales se ha agregado el grupo de archivos.

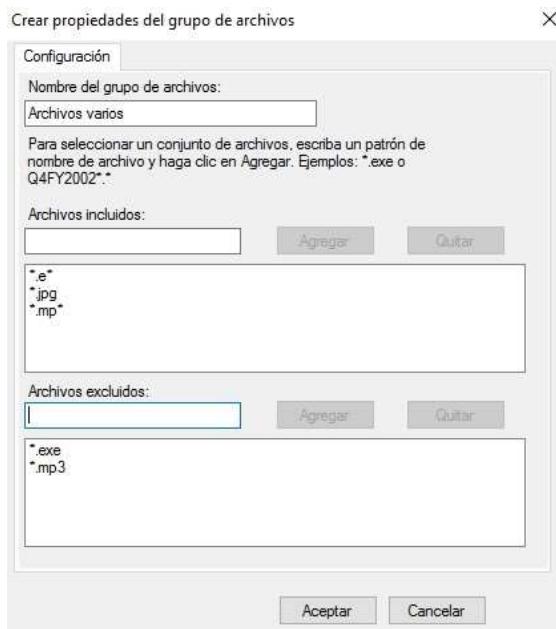
#### **Para crear un grupo de archivos:**

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 varios*.
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 (será los que bloquee), en **Archivos incluidos**, escribiremos un patrón de nombre de archivo y luego pulsaremos 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 (no los bloqueará), 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**.

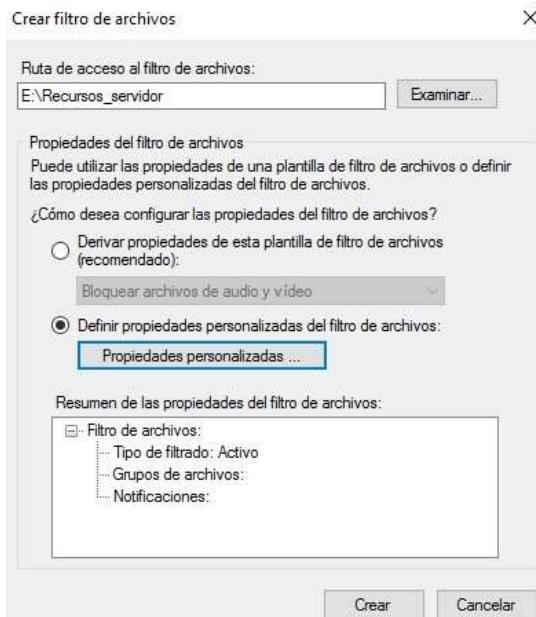
## 5.7 Crear un filtro de archivos basado en un grupo de archivos personalizado

En el siguiente procedimiento, crearemos un nuevo filtro de archivos (a partir del grupo de archivos que hemos creado en el anterior párrafo) 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.

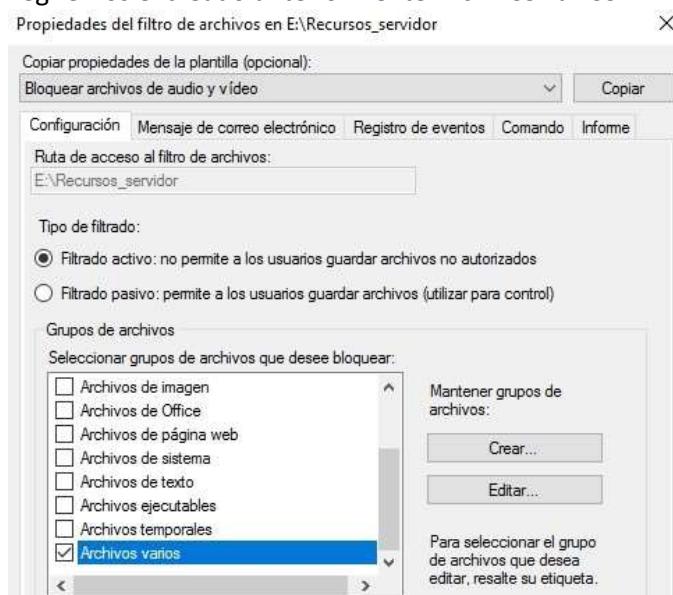
De manera similar, podemos crear una nueva *plantilla de filtro de archivos* que se base en las propiedades de un *filtro de archivos* que creamos.

**Para crear un filtro de archivos (basado en un grupo de archivos personalizado):**

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**. 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\_servidor**, en el disco *Copias de seguridad (E:)* del controlador de dominio. Esta carpeta la compartiremos para todos los *Usuarios del dominio* con permisos de *Lectura y escritura*.
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**.

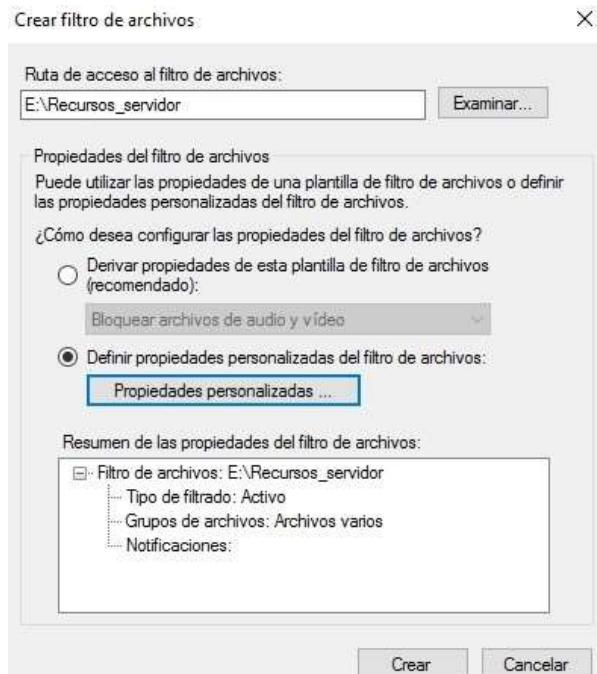


5. Se abrirá el cuadro de diálogo **Propiedades del filtro de archivos**. En **Grupos de archivos**, seleccionamos cada grupo de archivos que deseamos incluir en el filtro de archivos. Elegiremos el creado anteriormente **Archivos varios**.



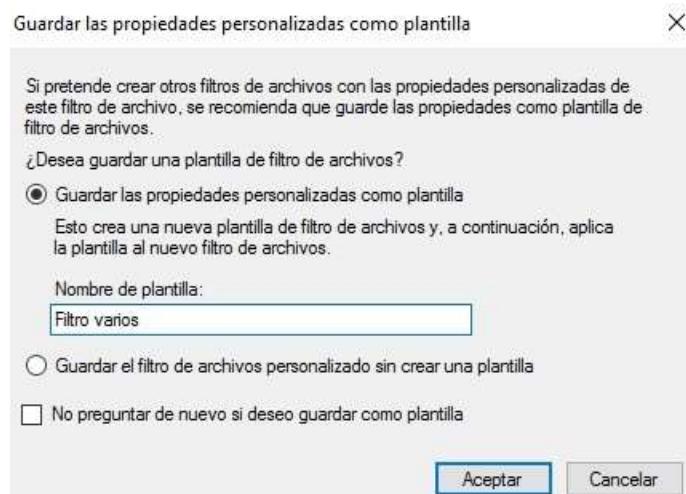
6. Si deseamos copiar las propiedades de una plantilla existente para usarla como base de su nuevo filtro de archivos, seleccionamos una plantilla de la lista desplegable **Copiar propiedades de la plantilla**. A continuación, hacemos clic en **Copiar**, pero en nuestro caso no lo basaremos en ninguna plantilla por lo que no pulsaremos este botón.
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\_servidor**.
8. Si deseamos generar notificaciones de correo electrónico, en la ficha **Mensaje de correo electrónico**, configuramos 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 lo 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. Despues de seleccionar todas las propiedades del filtro de archivos que deseamos usar, haremos clic en **Aceptar** para cerrar el cuadro de diálogo **Propiedades del filtro de archivos**.



10. En el cuadro de diálogo **Crear filtro de archivos**, haremos clic en **Crear** para guardar el filtro de archivos. De este modo se abre el cuadro de diálogo **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 varios**. 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**.

Con lo anterior habremos creado un *filtro de archivos* y una *plantilla de filtro de archivos* que bloquea los archivos **\*.jpg**, **\*.e\*** y **\*.mp\*** con las excepciones de **\*.exe** y **\*.mp3** para la carpeta **Recursos\_servidor**:

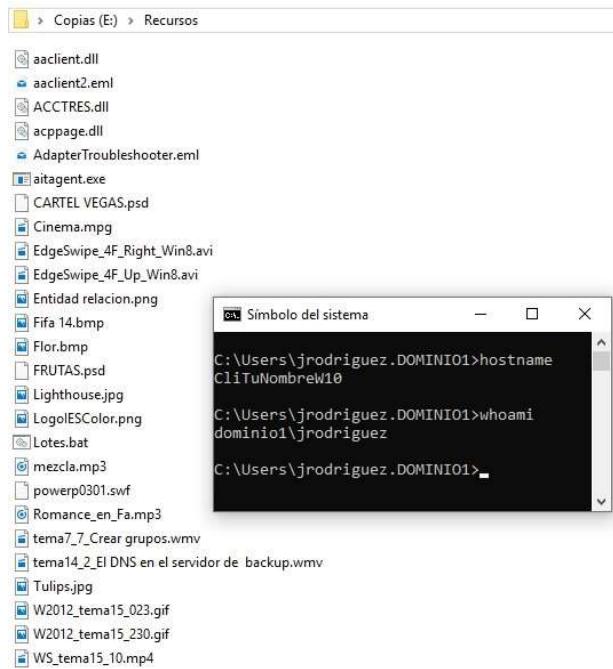
Plantilla de origen: Bloquear archivos ejecutables (1 elemento)			
E:\Prueba_filtro	Activo	Bloquear: Archivos ejecutables	Bloquear archivos ejecutables

Plantilla de origen: Filtro varios (1 elemento)			
E:\Recursos_servidor	Activo	Bloquear: Archivos varios	Filtro varios

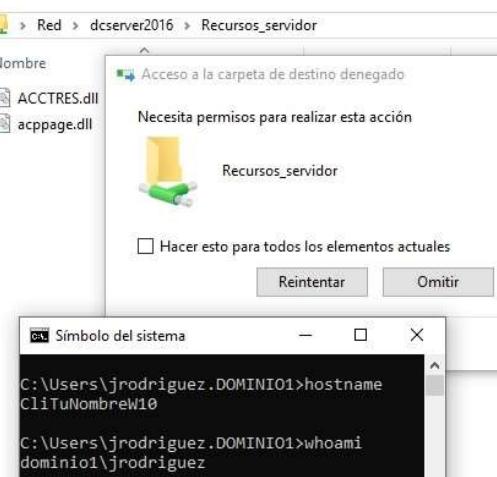
Plantilla de filtro de archivos	Tipo de filtrado	Grupos de archivos
Bloquear archivos de audio y video	Activo	Bloquear: Archivos de audio y video
Bloquear archivos de correo electrónico	Activo	Bloquear: Archivos de correo electrónico
Bloquear archivos de imagen	Activo	Bloquear: Archivos de imagen
Bloquear archivos ejecutables	Activo	Bloquear: Archivos ejecutables
Filtro varios	Activo	Bloquear: Archivos varios
Supervisar archivos ejecutables y de sistema	Pasivo	Advertir: Archivos ejecutables, Archivos de sistema

Para **probarlo**, abrimos sesión en el equipo *CliTuNombreW10* con *jrodriguez* y entramos en la carpeta *Recursos* que contiene archivos **\*.exe**, **\*.jpg**, **\*.eml** (correo de Outlook), **\*.mp3** y **\*.mp4**.

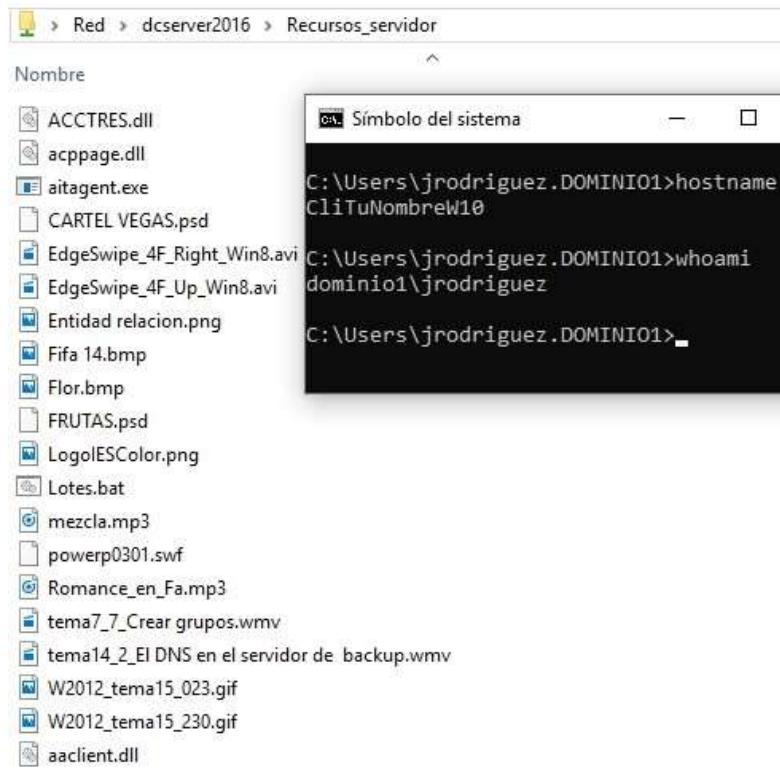


Ahora intentamos copiar todos los archivos anteriores en la carpeta compartida **Recursos\_servidor** a través del entorno red (`\|Nombre del servidor\carpeta compartida`):

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



Finalmente, sólo copiará aquellos archivos cuya extensión hemos permitido, incluidos los *.mp3* y *.exe*:



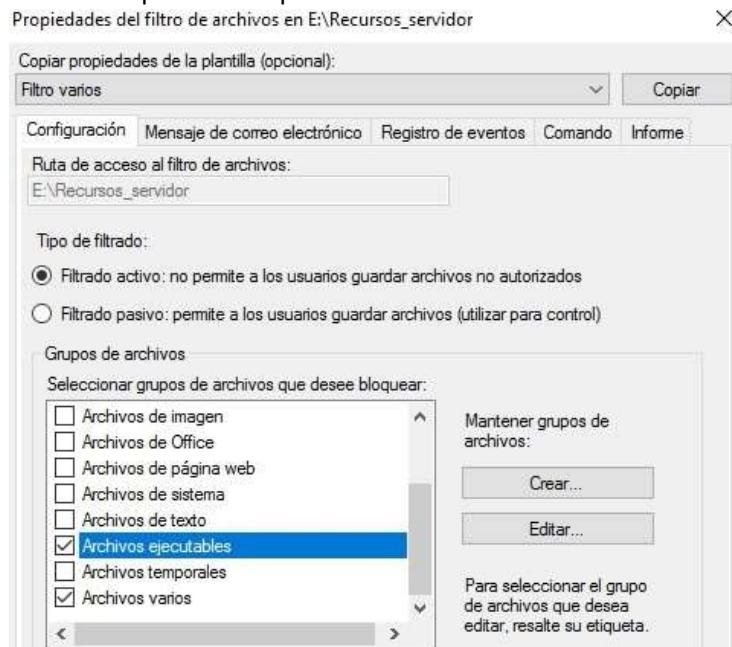
pero no otros archivos bloqueados como los siguientes:

Nombre	Fecha de modifica...	Tipo	Tamaño
aclient.dll	10/07/2015 21:51	Extensión de la apl...	155 KB
aclient2.eml	11/02/2021 13:43	Archivo EML	155 KB
ACCTRES.dll	14/07/2009 5:24	Extensión de la apl...	39 KB
acppage.dll	15/01/2011 17:52	Extensión de la apl...	52 KB
AdapterTroubleshooter.eml	12/02/2021 4:30	Archivo EML	40 KB
aitagent.exe	15/01/2011 17:52	Aplicación	120 KB
CARTEL VEGAS.psd	03/07/2008 15:07	Archivo PSD	222 KB
Cinema.mpg	16/07/2002 11:41	Archivo MPG	10.170 KB
EdgeSwipe_4F_Right_Win8.avi	02/04/2013 11:32	Archivo AVI	1.046 KB
EdgeSwipe_4F_Up_Win8.avi	02/04/2013 11:32	Archivo AVI	244 KB
Entidad relacion.png	06/03/2014 10:58	Archivo PNG	109 KB
Fifa 14.bmp	19/02/2014 21:15	Archivo BMP	149 KB
Flor.bmp	07/06/1998 18:29	Archivo BMP	78 KB
FRUTAS.psd	03/07/2008 15:08	Archivo PSD	262 KB
Lighthouse.jpg	14/07/2009 9:32	Archivo JPG	549 KB
LogoIESColor.png	11/02/2014 14:45	Archivo PNG	180 KB
Lotes.bat	11/02/2021 20:12	Archivo por lotes ...	0 KB
mezcla.mp3	15/11/2010 21:46	Archivo MP3	138 KB
powerp0301.swf	07/07/2011 19:39	Shockwave Flash ...	3.758 KB
Romance_en_Fa.mp3	18/11/2010 21:28	Archivo MP3	4.018 KB
tema7_7_Crear grupos.wmv	30/04/2010 16:48	Archivo WMV	426 KB
tema14_2_El DNS en el servidor de backup.wmv	07/05/2010 14:58	Archivo WMV	923 KB
Tulips.jpg	14/07/2009 9:32	Archivo JPG	607 KB
W2012_tema15_023.gif	20/06/2013 14:32	Archivo GIF	14 KB
W2012_tema15_230.gif	20/06/2013 14:32	Archivo GIF	4 KB
WS_tema15_10.mp4	20/06/2013 14:25	Archivo MP4	4.736 KB

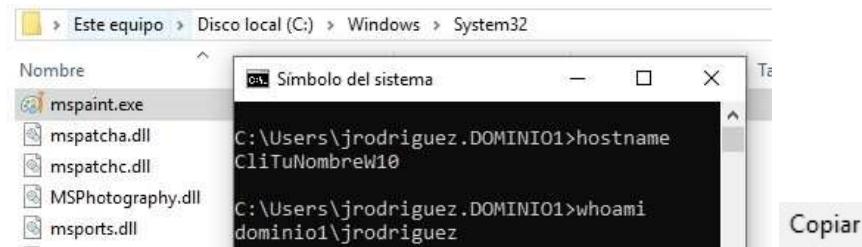
Ahora podríamos editar el filtro creado anteriormente para que bloquee, además, los archivos ejecutables, con la opción *Editar propiedades del filtro de archivos*:



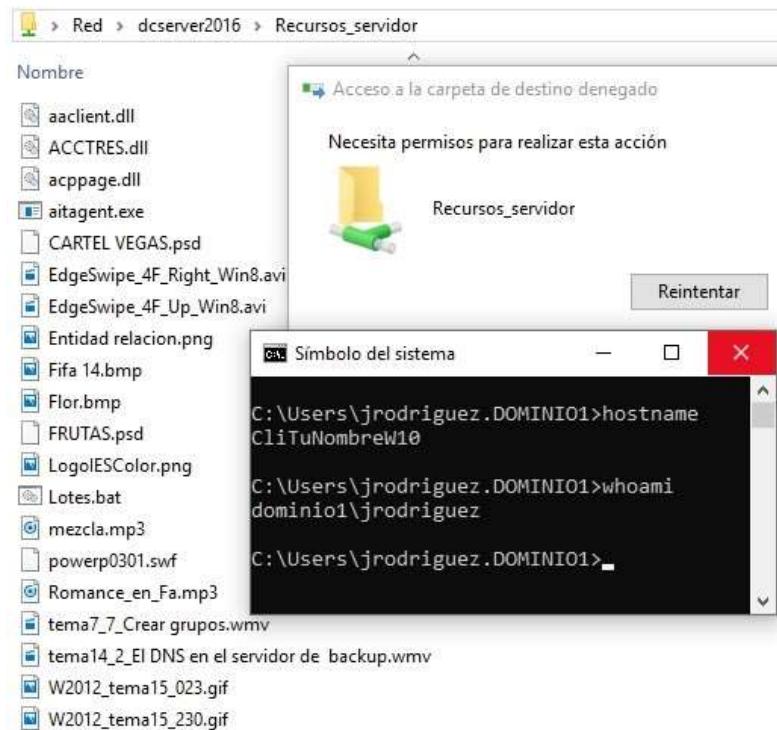
Marcamos, en sus propiedades, Archivos ejecutables, para que los bloquee y no puedan, ahora, copiarse archivos de este tipo en la carpeta **Recursos**:



Ahora si intentamos copiar el archivo de *Windows>System32, mspaint.exe* del equipo cliente



en la carpeta **Recursos\_servidor** evidentemente no nos lo permitirá, al estar bloqueados este tipo de archivos (ejecutables):



## 6. Definición de Escritorio remoto.

El Escritorio remoto de Windows Server (no es necesario que sea un controlador de dominio) es la base para conectarse al servidor de forma remota y realizar tareas administrativas. Proporciona funciones de administración de servidor remoto para los sistemas operativos de la familia Windows Server. Con esta característica se puede administrar un servidor desde cualquier equipo de la red. No se necesitan licencias para disponer de hasta dos conexiones remotas simultáneas, además de la sesión de la consola del servidor. Para acceder al servidor mediante una conexión a Escritorio remoto hay que autenticarse previamente en el dominio como un usuario habilitado para ello.

Los usuarios que inician una sesión de Escritorio remoto en su estación de trabajo sólo ven su sesión, administrada de manera transparente por el sistema operativo del servidor e independiente de cualquier otra sesión de cliente que se pudiera estar ejecutando. El software de cliente puede ejecutarse en varios dispositivos hardware de cliente, incluidos equipos y terminales basados en S.O. Windows. Son varias las ventajas del Escritorio remoto, entre las que podemos citar:

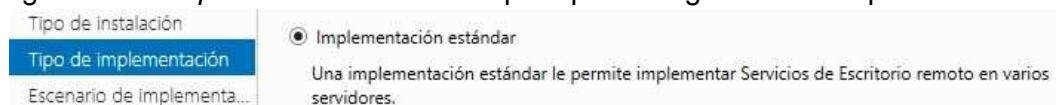
- Los servicios de Escritorio remoto de Windows permiten agregar y volver a conectar automáticamente impresoras, de forma que podamos imprimir de forma remota en dichas impresoras.
- Pueden ser configuradas ciertas características en el acceso a la máquina remota, tales como el fondo de Escritorio, la resolución de la pantalla, las unidades locales a las que deseamos tener acceso en la máquina remota, etc.

### 6.1 Instalación de Servicios de Escritorio remoto

Para empezar, deberemos agregar el rol de *Instalación de Servicios de Escritorio remoto*:



Elegiremos la *Implementación estándar* para poder seguir todos los pasos.



y a continuación elegimos *Implementación de escritorio basada en sesión*, ya que en nuestro caso no queremos virtualizar.

● **Implementación de escritorio basada en sesión**

La implementación de escritorio basada en sesión permite a los usuarios conectarse a colecciones de sesiones que incluyan programas RemoteApp publicados y escritorios basados en sesión.

Nos informará de los servicios que se instalarán y configurarán:

Se instalarán y configurarán los siguientes servicios de rol de Servicios de Escritorio remoto para esta implementación.



**Agente de conexión a Escritorio remoto**

El Agente de conexión a Escritorio remoto conecta o reconecta un dispositivo cliente a programas RemoteApp, escritorios basados en sesión y escritorios virtuales.



**Acceso web a Escritorio remoto**

Acceso web a Escritorio remoto permite que los usuarios se conecten a recursos proporcionados por colecciones de sesiones y colecciones de escritorios virtuales mediante el menú Inicio o un explorador web.



**Host de sesión de Escritorio remoto**

El host de sesión de Escritorio remoto permite que un servidor hospede programas RemoteApp o escritorios basados en sesión.



Se usarán las credenciales de la cuenta DOMINIO1\Administrador para crear la implementación.

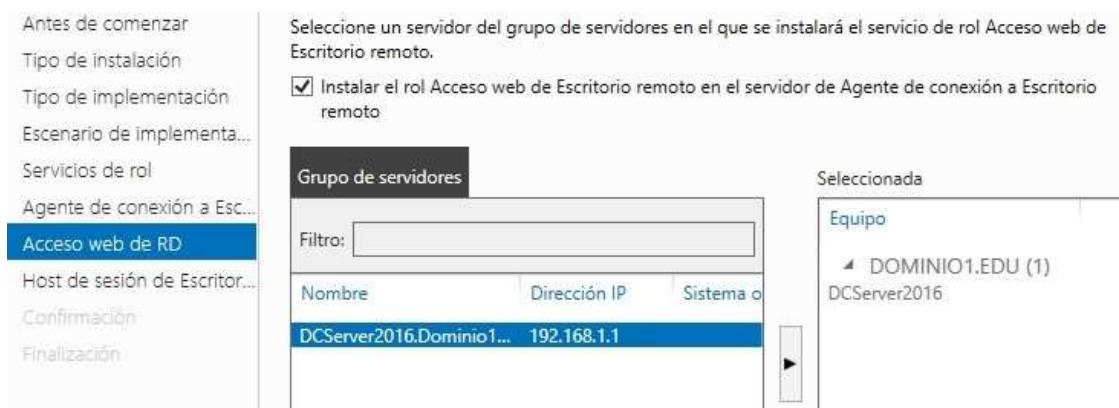
A continuación, elegiremos nuestro servidor para poder implementar el servicio de Escritorio remoto en él y lo pasamos a la derecha:

Grupo de servidores		
Filtro:		
Nombre	Dirección IP	Sistema o
DCServer2016.Dominio1...	192.168.1.1	

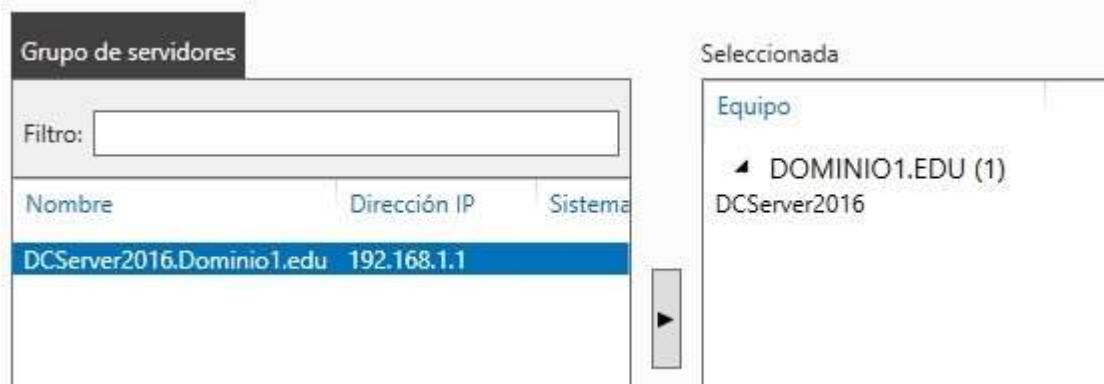
Seleccionada

Equipo
DOMINIO1.EDU (1)
DCServer2016

Incluirémos también nuestro servidor para poder tener acceso a través de la web:



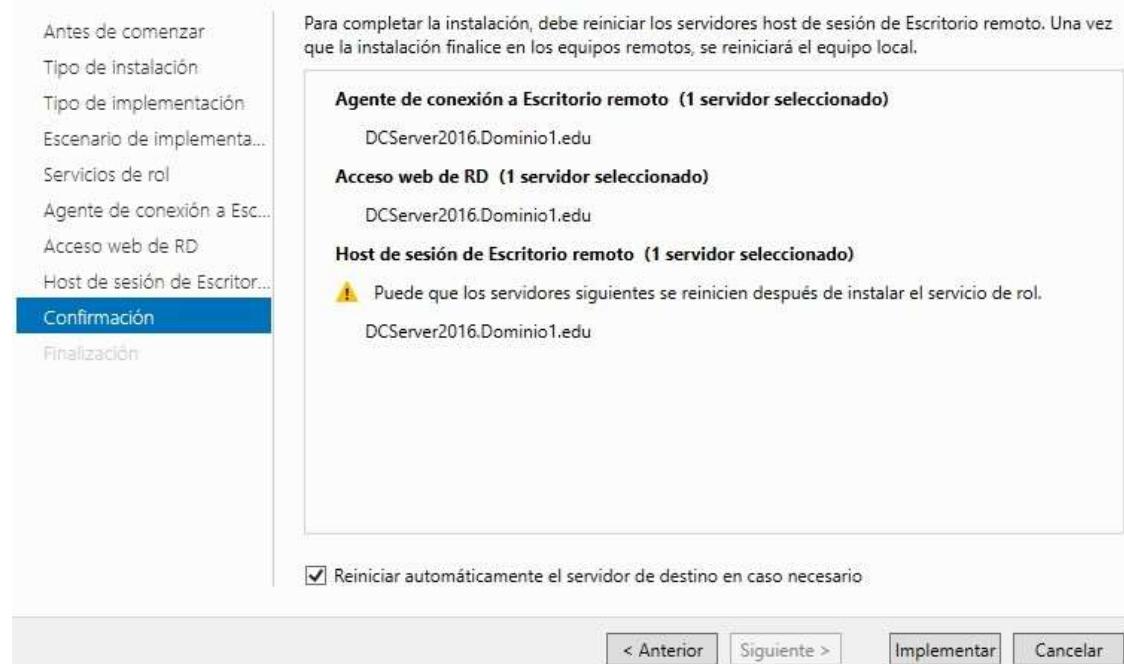
y finalmente incluiremos nuestro servidor para poder usar el servicio *Host de sesión de Escritorio remoto*:



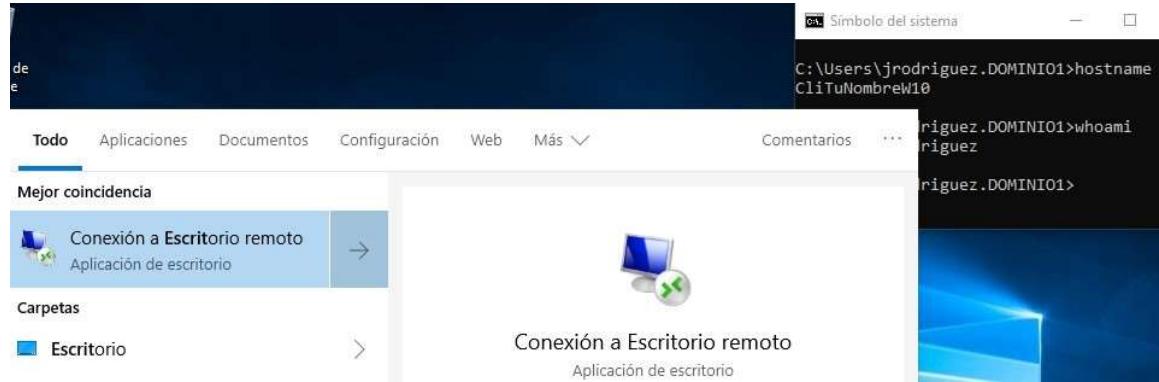
Ahora confirmamos y pulsamos *Implementar* para iniciar la instalación:

Confirmar selecciones

SERVIDOR DE DESTINO  
Implementación estándar seleccionada



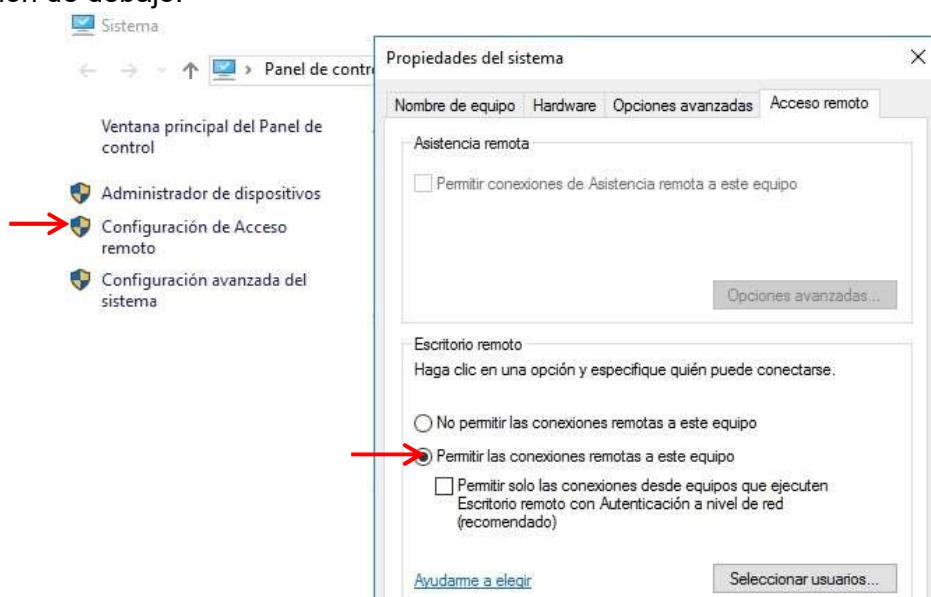
Desde el punto de vista de la estación de trabajo donde se ejecuta el cliente de Escritorio remoto, éste aparece como una ventana en el entorno de escritorio local que contiene sólo la cantidad mínima de software necesaria para establecer una conexión con el servidor y presentar la interfaz de usuario, el resto de las funciones del S.O., así como las aplicaciones, se ejecutan en el servidor. El cliente puede ejecutarse en distintos S.O. de Microsoft: p.ej. "Windows XP", "Windows 7" o "Windows 10", tal y como podemos ver en el siguiente cliente de Windows 10:



## 6.2 Habilitar el Escritorio remoto en el servidor.

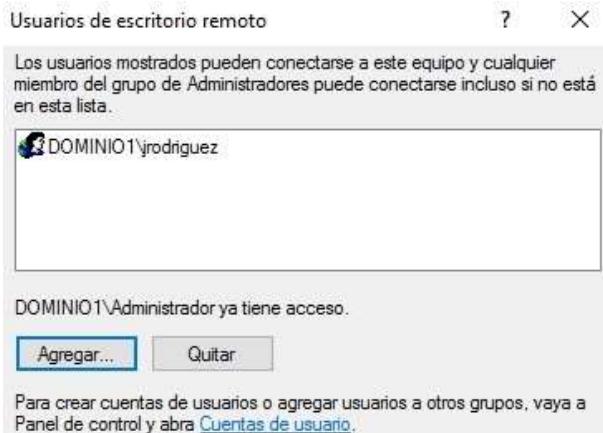
**NOTA:** No es necesario para lo siguiente tener instalado el rol de Escritorio remoto.

Para habilitar el *Escritorio remoto* en *Windows Server*, de modo que podamos acceder al servidor de forma remota desde otros equipos clientes, nos ubicamos sobre nuestro servidor Windows, pulsaremos con el botón derecho del ratón sobre *Este equipo*, y seleccionaremos la opción *Propiedades*, pulsamos en *Configuración de Acceso remoto* y a continuación elegimos la pestaña *Acceso remoto*. En dicha ventana activaremos la opción *Permitir las conexiones remotas a este equipo*, sin marcar la opción de debajo.



Si deseamos permitir el acceso mediante la Conexión a Escritorio remoto a otros usuarios que no sean el propio Administrador de nuestro servidor Windows, en la

pestaña anterior *Acceso remoto* pulsaremos sobre el botón *Seleccionar usuarios ...* pulsamos en *Agregar* e indicaremos los usuarios a los que deseamos dar acceso. Como veremos esta es una condición que no permitirá la administración completa del servidor.



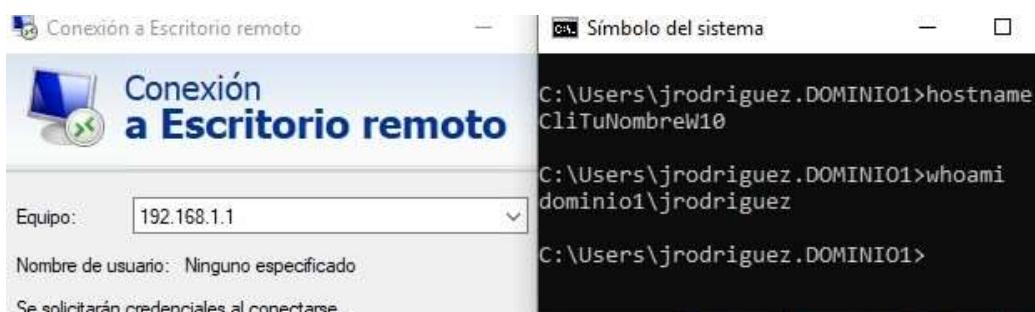
Así el usuario *jrodriguez* queda añadido como *usuario de Escritorio remoto*:



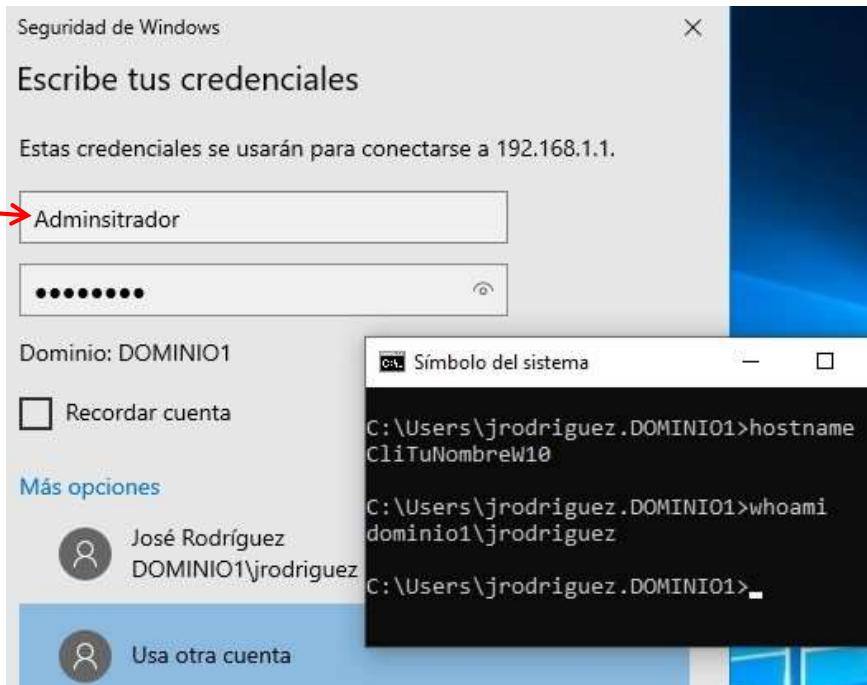
### 6.3 Ejecución del cliente de escritorio remoto.

Para lanzar el cliente de *Conexión a Escritorio remoto*, en Windows 10, vamos al botón *Iniciar > Accesorios de Windows > Conexión a Escritorio remoto*.

Al lanzar la aplicación se mostrará la siguiente ventana, en la cual especificaremos la dirección IP o el nombre del equipo al cual nos queremos conectar de modo remoto, en nuestro caso al servidor controlador de dominio.



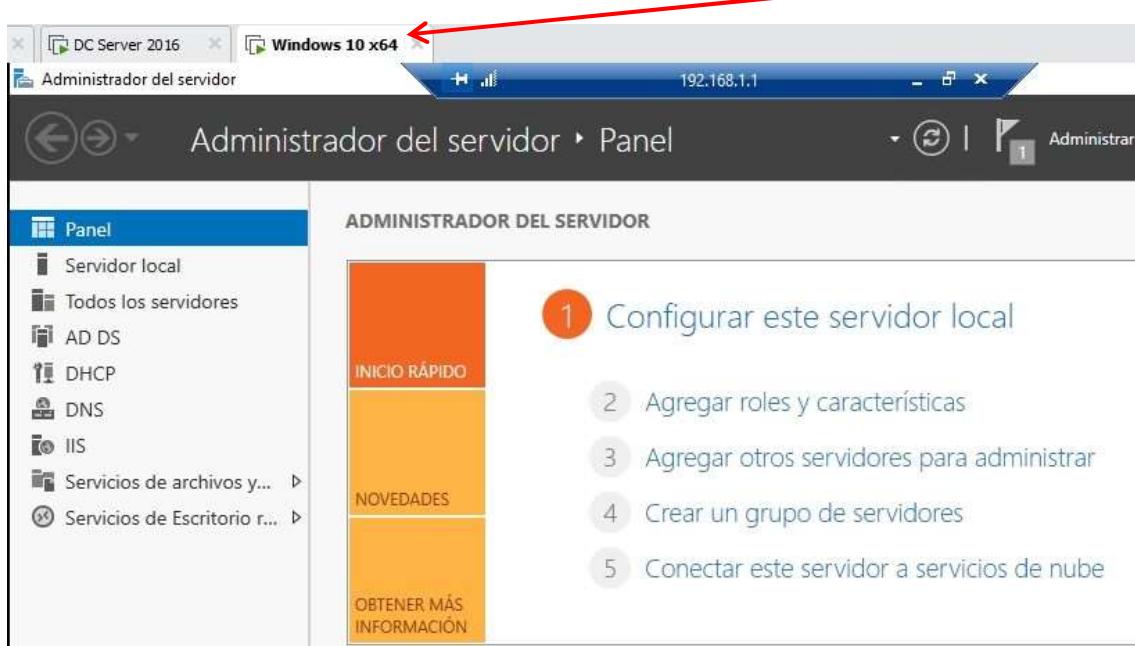
Pulsando sobre el botón *Conectar* se nos presenta una pantalla de autenticación en el servidor Windows. Como estábamos en una sesión de *jrodriguez*, elegiremos la opción *Usar otra cuenta* para autenticarnos como *Administrador del dominio*:



Nos pedirá confirmar la conexión al no tener un certificado de seguridad (si lo tuviéramos instalado, no lo pediría), pulsaremos en el botón Sí:

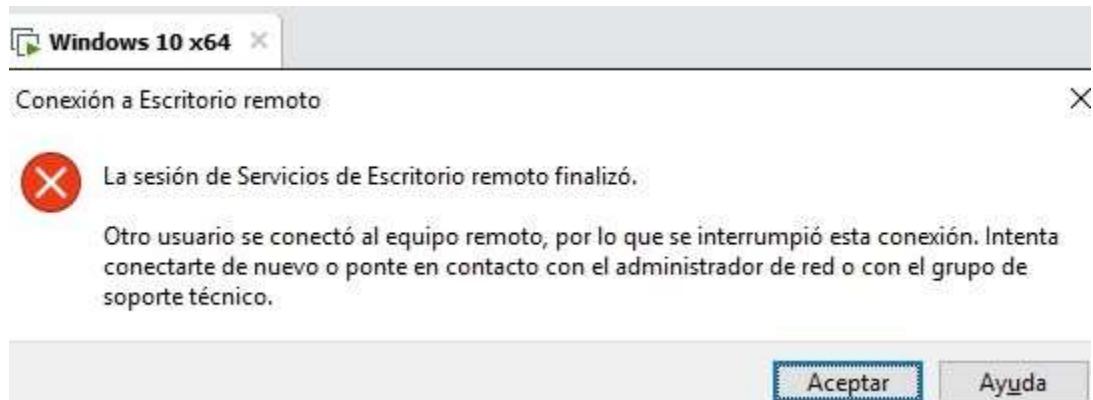


Tras ello accedemos a una pantalla con el Administrador del servidor de nuestro Windows Server (DCServer2016), igual que si nos encontrásemos físicamente sobre dicha máquina, trabajando con la misma libertad que si estuviéramos sentados físicamente frente a la consola, pero el equipo físico es el Windows 10:



**NOTA:** La máquina real del servidor está con la sesión cerrada mientras que está abierta la sesión por *Escritorio remoto* desde el cliente y viceversa.

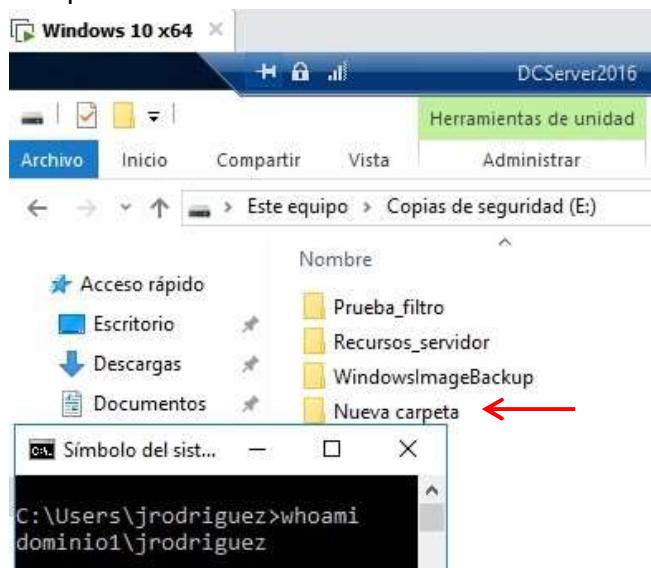
Si volvemos a iniciar sesión en el dominio, con el *Administrador*, el equipo cliente se desconectará de la sesión de *Escritorio remoto*:



Si queremos conectarnos al servidor (en este caso en lugar de a través de su IP lo haremos con su nombre) desde un equipo cliente con un usuario que no tenga permisos de Administrador (pero que esté en el grupo *Usuarios de escritorio remoto*), por ejemplo, con *jrodriguez*:

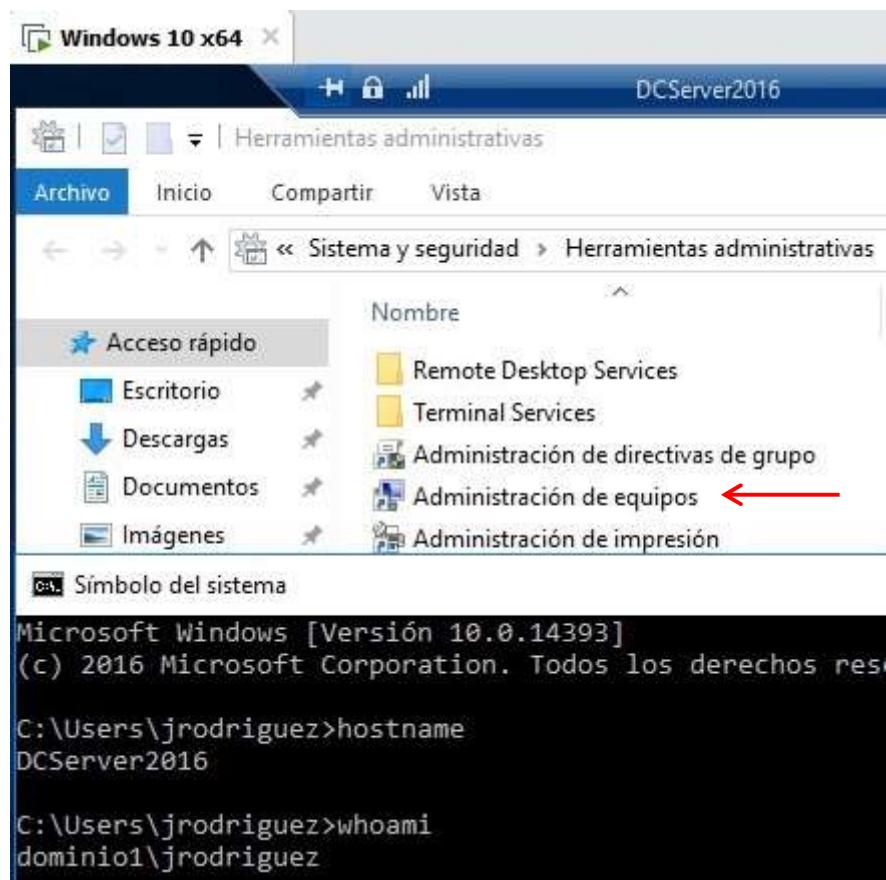


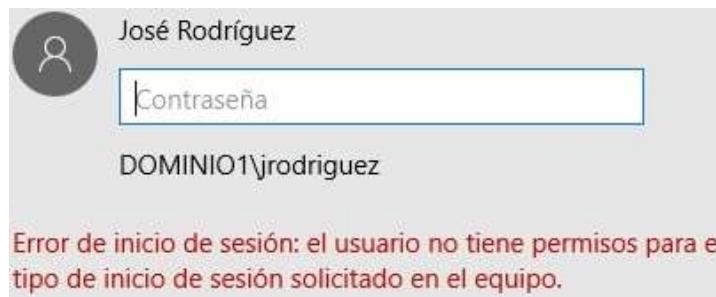
nos permitirá ver determinadas consolas y realizar algunas acciones en el servidor, por ejemplo, crear carpetas:



pero no podremos administrar el servidor.

Si intentamos abrir, por ejemplo, la consola *Administración de equipos*, nos indicará que no tenemos permisos para esa acción, con *jrodriguez*:





Ahora cerraremos la sesión de *Escrivtorio remoto*, pero tener en cuenta que:

**NOTA IMPORTANTE:** Cuando cerremos la sesión de *Escrivtorio remoto*, no debemos seleccionar la opción *Apagar* dentro de la ventana del equipo cliente de *Escrivtorio remoto*, pues en dicho caso apagaremos la máquina servidora Windows Server; la opción que hemos de seleccionar debe ser Desconectar o Cerrar sesión, para que la máquina Windows Server siga levantada y activa. La opción *Desconectar* deja la sesión temporalmente desactivada, pudiendo retomarla en cualquier momento; por contra *Cerrar sesión*, termina la sesión actual de *Escrivtorio remoto* en el equipo cliente.

Si intentamos entrar remotamente al servidor con un usuario que no ha sido incluido como *Usuario de escritorio remoto*, como por ejemplo *usumadrid*, no nos lo permitirá:

