Sistemas Informáticos

Tema 12. Windows Server.
Permisos, directivas de grupo y perfiles

Índice

1. Objetivos

- Creación de recursos compartidos.
- Configuración y administración de permisos de carpetas compartidas.
- Configuración y administración de permisos NTFS
- Gestión del dominio mediante directivas de grupo.
- Configuración del entorno de trabajo del usuario mediante perfiles.
- Establecimiento de carpetas particulares de los usuarios del dominio.
- Ejecución de comandos de inicio de sesión.

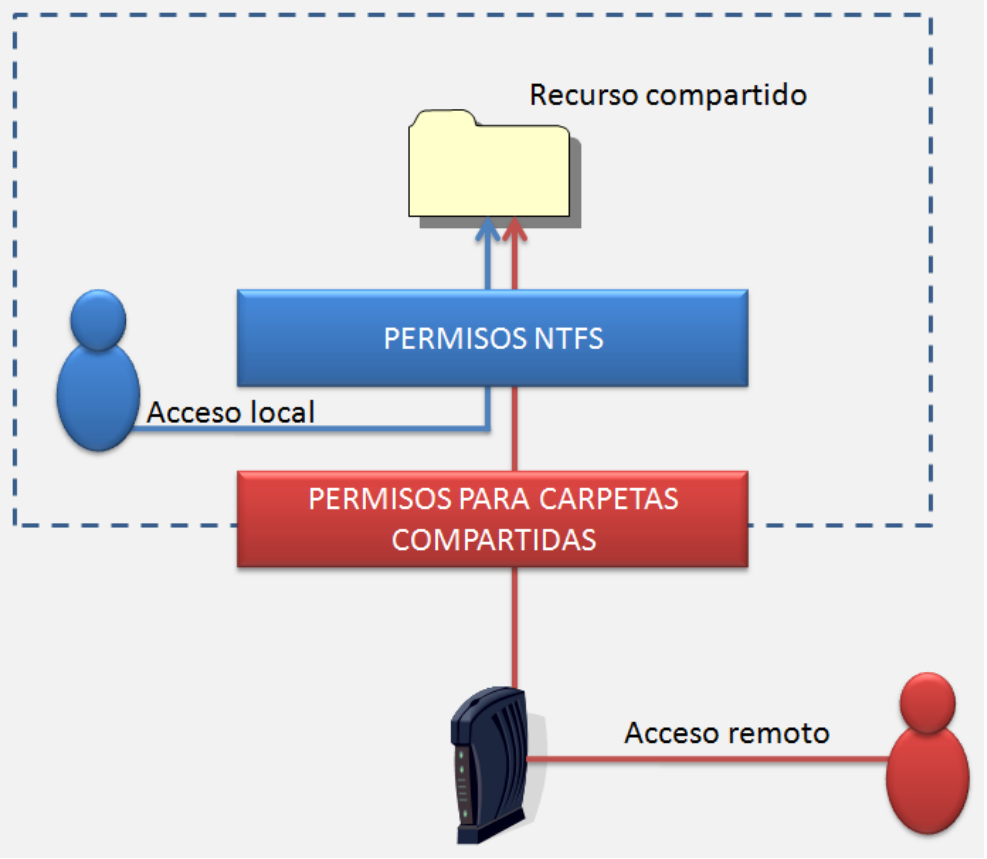
2. Permisos

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

- Permisos para recursos o carpetas compartidas: se aplican cada vez que un usuario quiere acceder a un archivo o carpeta de la red.
- Permisos para archivos y carpetas NTFS: se aplican sobre dispositivos con **formato NTFS** para definir en mayor detalle las acciones permitidas.

De lo anterior se extrae que cuando se accede en modo local a los archivos o carpetas sólo intervienen los permisos asociados al sistema de ficheros, en este caso NTFS, sin embargo si se accede a través de la red se aplican los dos niveles de permisos: en primer lugar se aplican los permisos de carpetas compartidas y posteriormente los permisos NTFS.

Como veremos más adelante, en caso de que haya inconsistencias entre los permisos de cada tipo, se aplicarán los más restrictivos.

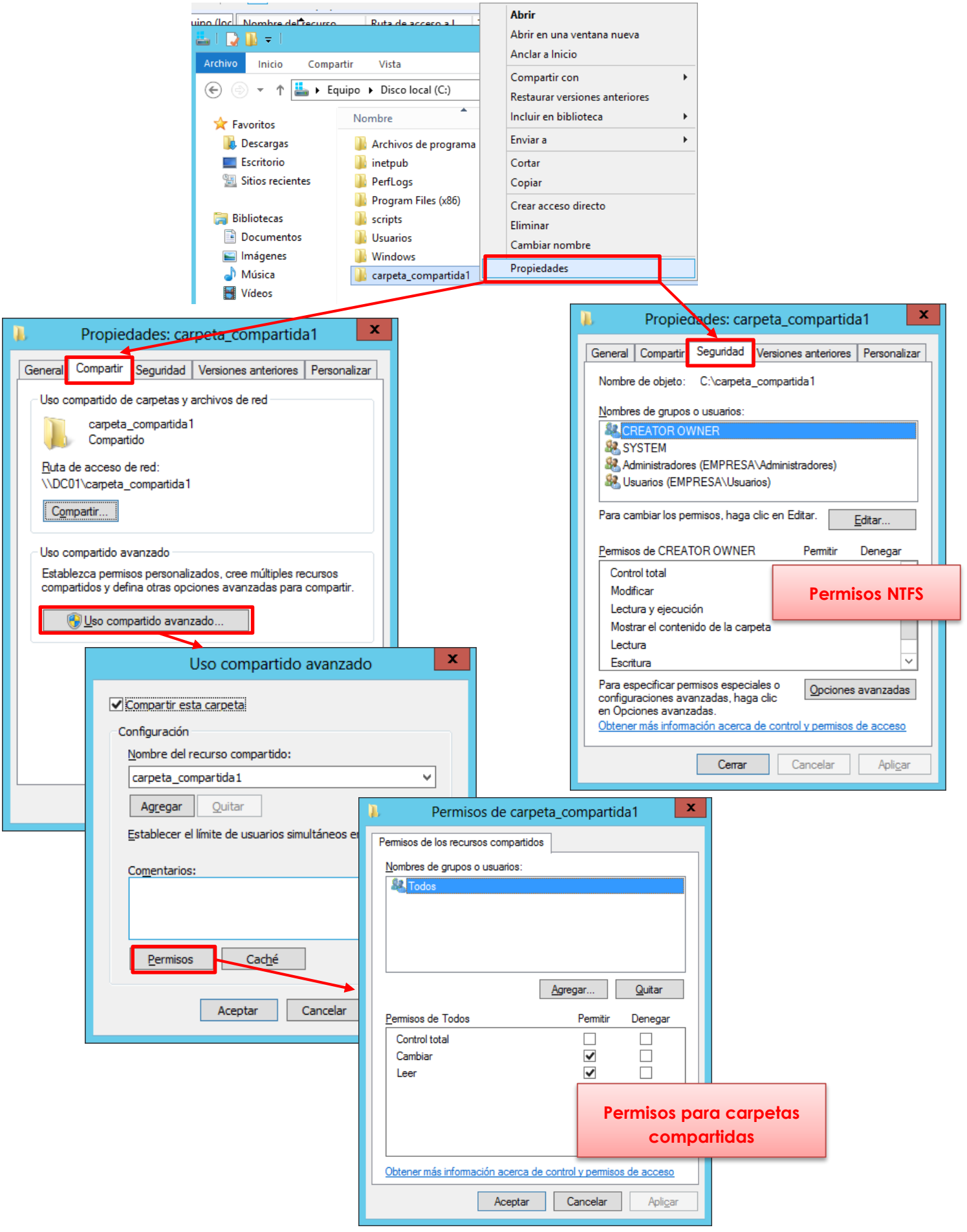


¿Qué ocurrirá si el volumen está formateado con FAT?

Finalmente remarcar que, como veremos a continuación, una correcta labor de administración, requerirá una adecuada planificación de la estructura de los usuarios, asignándolos en la medida de lo posible a grupos. De esta manera, los permisos sobre los recursos se asignarán a los grupos de usuarios creados, evitando (en la medida de lo posible) que usuarios concretos posean unos permisos determinados, lo que acabaría dificultando a la larga las tareas de administración.

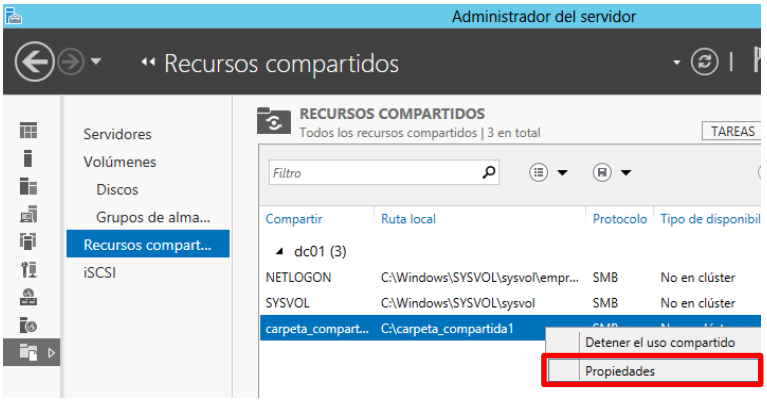
2.1. Cómo consultar los permisos que tiene un recurso

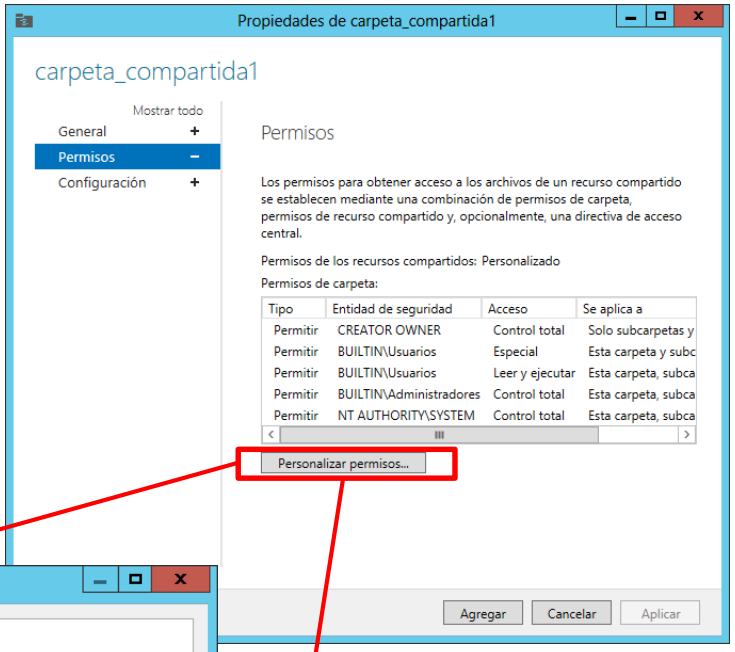
Desde **la carpeta a consultar sus permisos→Botón derecho-Propiedades:**

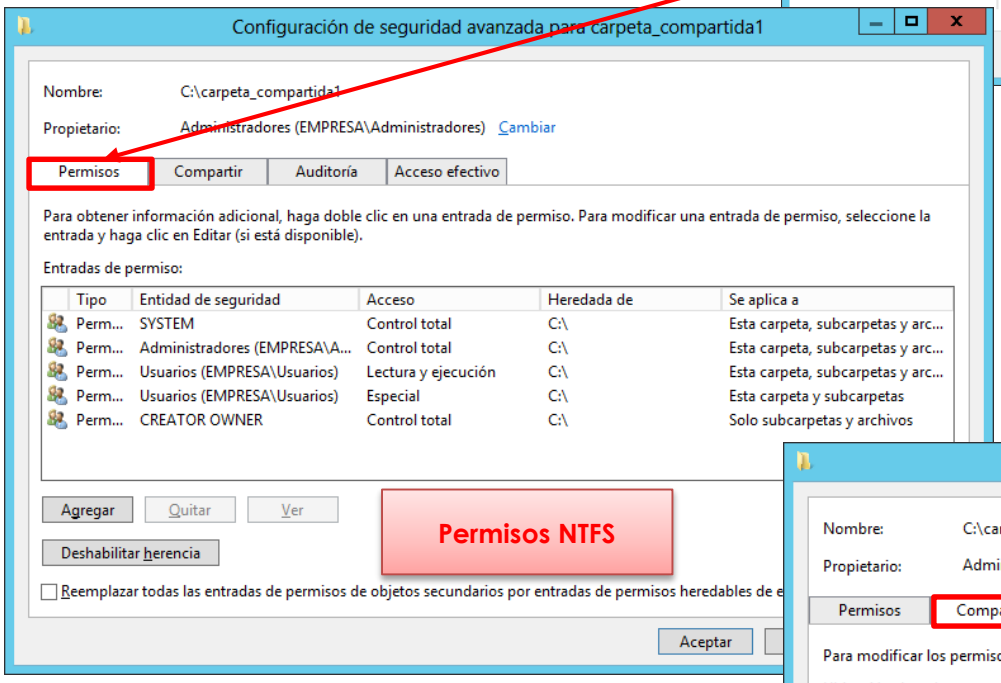


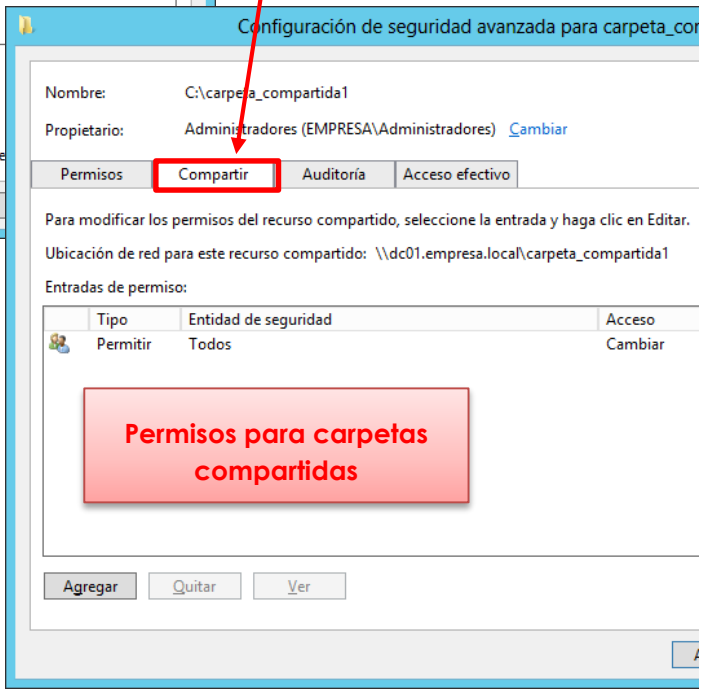
2.1.1. Otras formas de consultar los permisos de un recurso

a) Desde **Administrador del servidor → Servicios de archivos y de almacenamiento → Recursos compartidos → Botón derecho-Propiedades**:

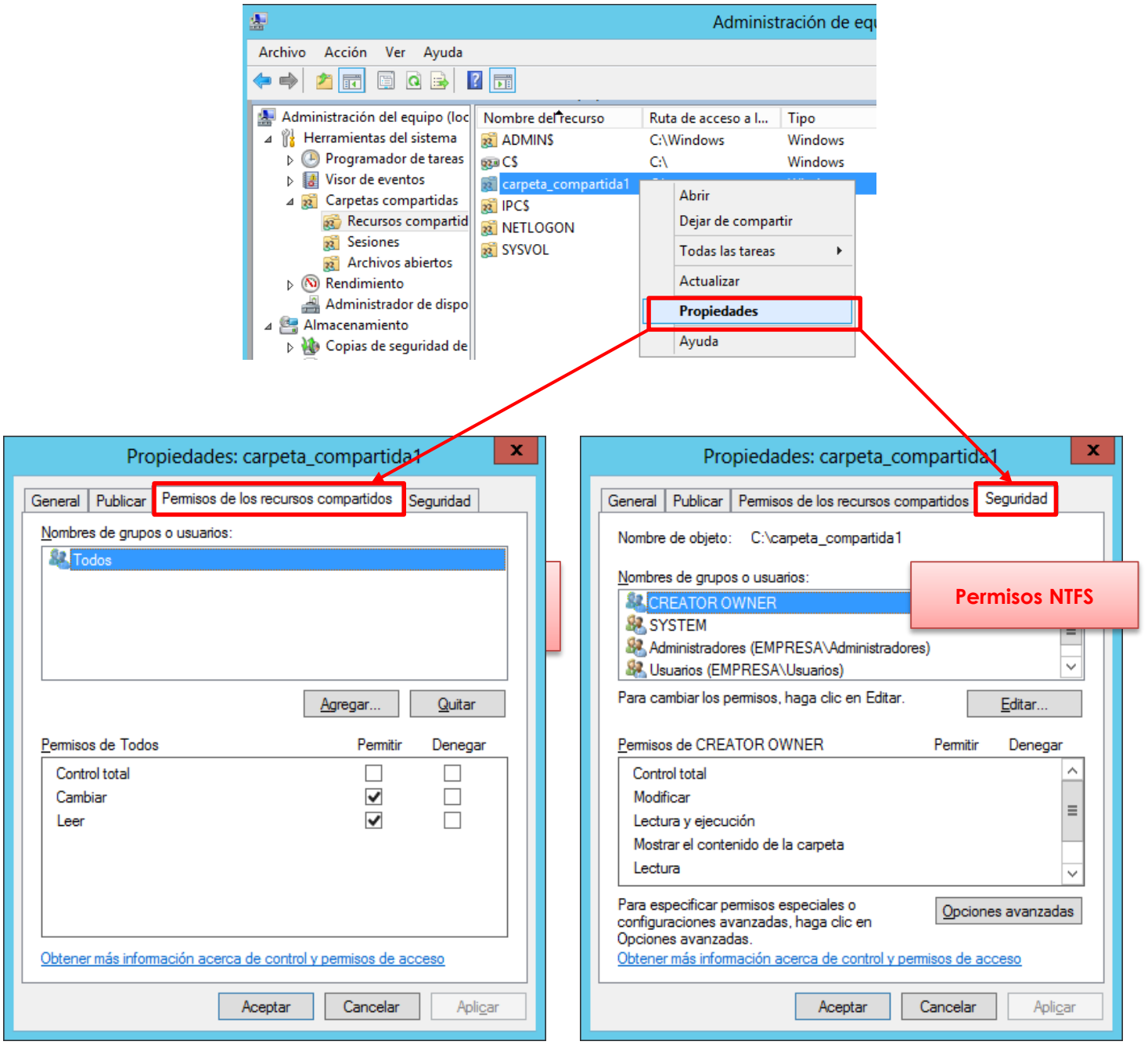




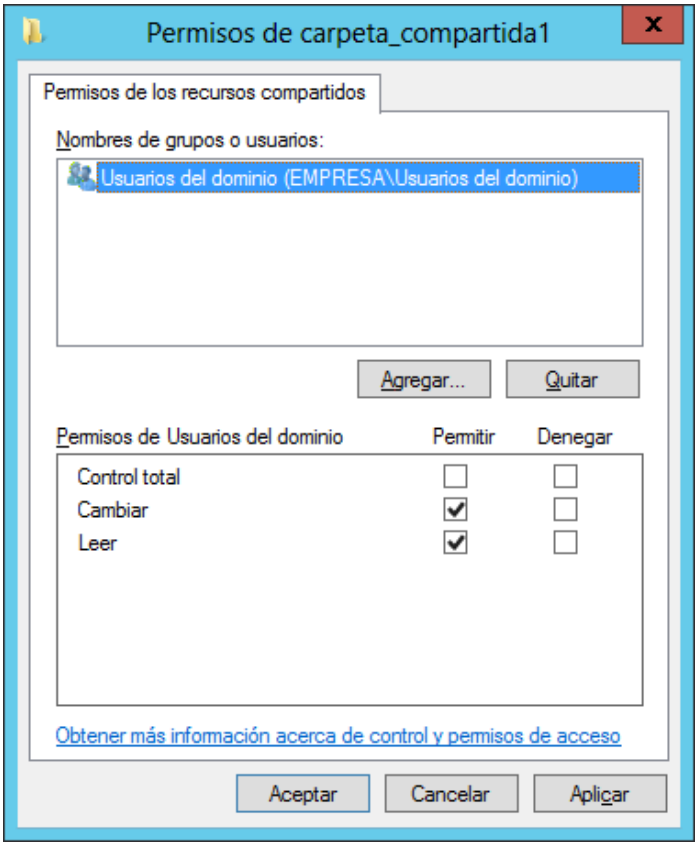




b) Desde **Administrador del servidor → Herramientas → Administración de equipos → Carpetas compartidas → Recursos compartidos→Botón derecho-propiedades:**



2.2. Permisos de recursos compartidos



En el caso de los permisos de recursos compartidos, estos pueden ser de tres tipos:

- **Control total**: no solo permite cambiar y leer, sino modificar los permisos sobre el recurso compartido.
- **Cambiar:** se permite crear carpetas y archivos además de modificar y borrar los archivos y directorios existentes.
- **Lectura:** únicamente permite la lectura de archivos y la ejecución de archivos ejecutables que se hallen dentro del recurso compartido.

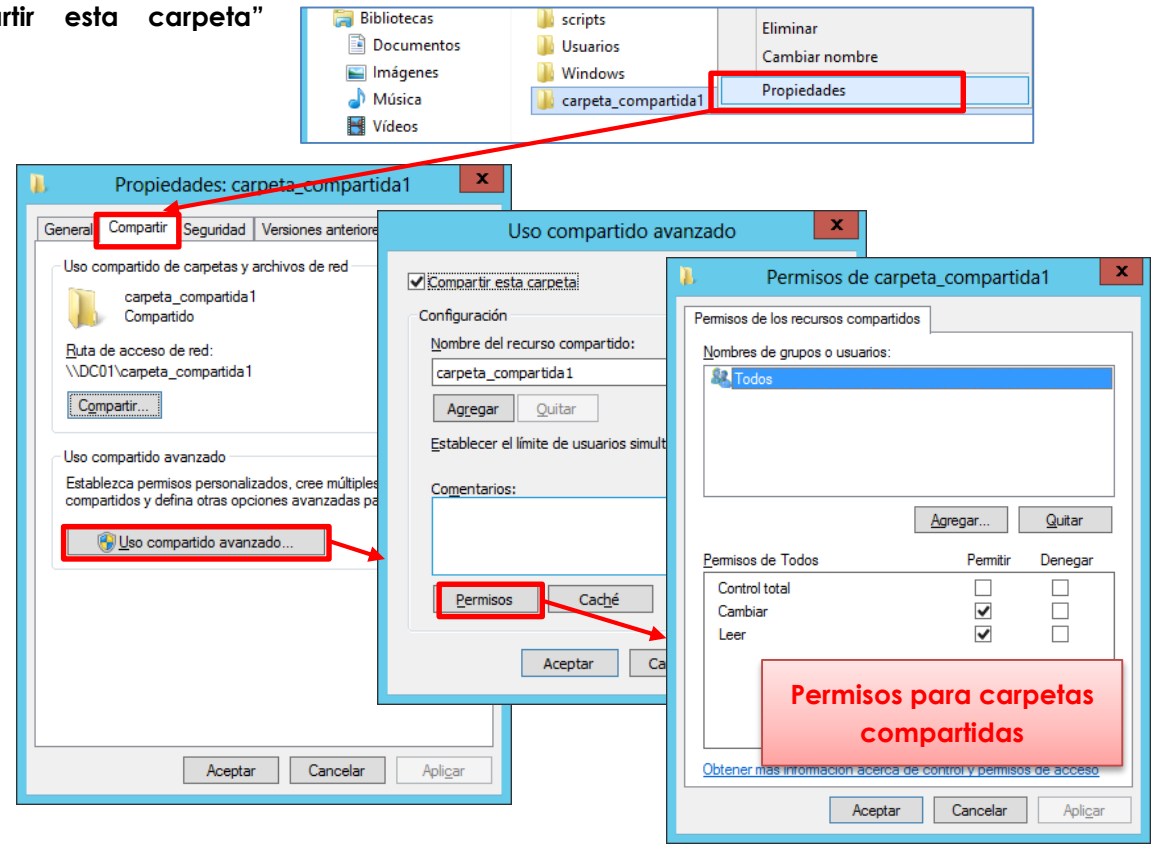
Como se puede comprobar, existen dos columnas donde asignar permisos: 'Permitir' y 'Denegar'. Es importante destacar que la opción 'Denegar' tiene prioridad sobre otros permisos asignados sobre el recurso compartido.

¿Qué ocurre si en los Permisos de los recursos compartidos no marcamos 'Permitir' ni 'Denegar'?

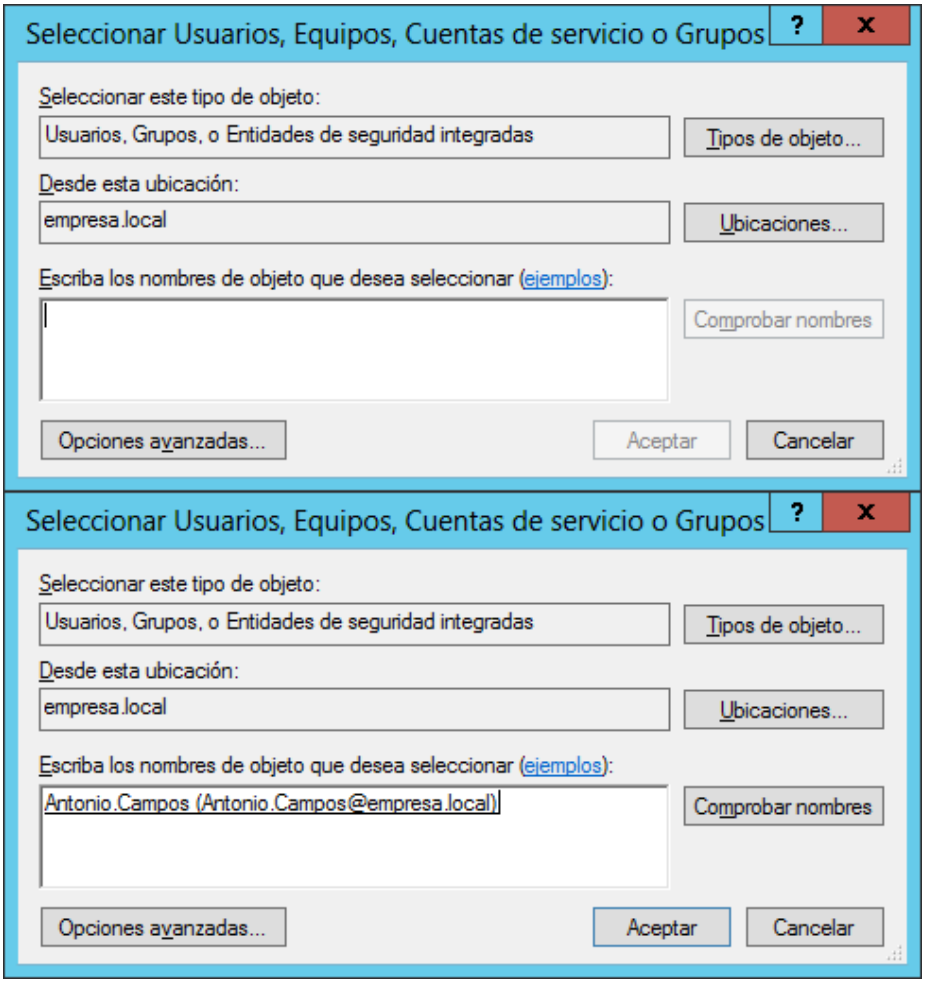
Si no se marca explícitamente un permiso, se entiende que está implícitamente denegado, por lo que un usuario que no tenga marcado ningún permiso ni en la casilla 'Permitir' ni en la casilla 'Denegar' no podrá acceder al recurso compartido.

2.2.1. Establecer permisos de recursos compartidos

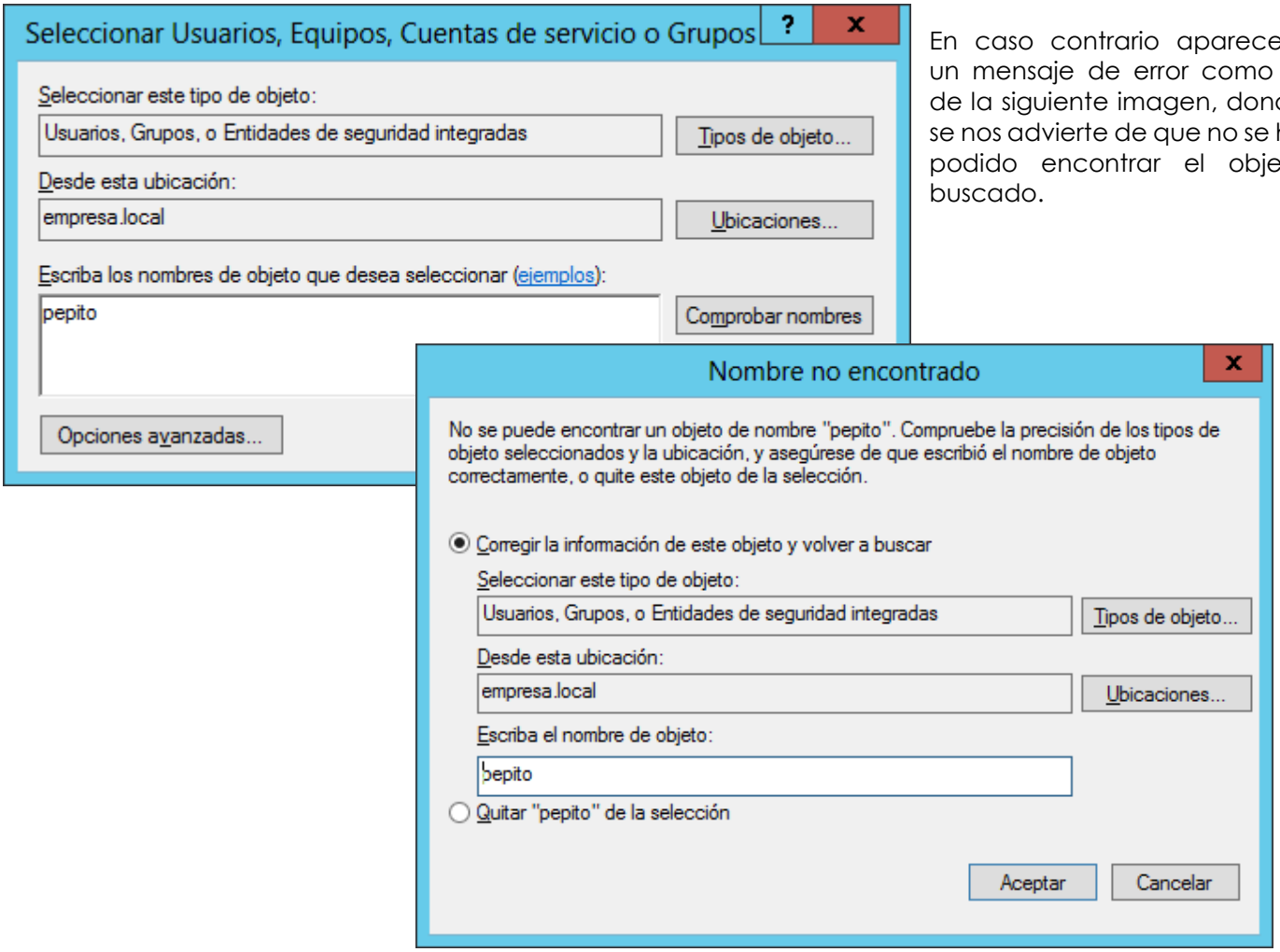
La configuración de los permisos de recursos compartidos se puede hacer de varias maneras. La más sencilla es seleccionar el recurso sobre el cual se desean configurar los permisos, y haciendo clic con el botón derecho, elegir la opción **Propiedades → Pestaña Compartir→ Botón "Uso compartido avanzado" → Marcamos "Compartir esta carpeta" →Botón permisos**



Si queremos añadir permisos a un usuario o a un grupo, haremos clic en el botón 'Agregar'. Se abrirá un cuadro de diálogo que nos permitirá buscar entre los usuarios y grupos del sistema.

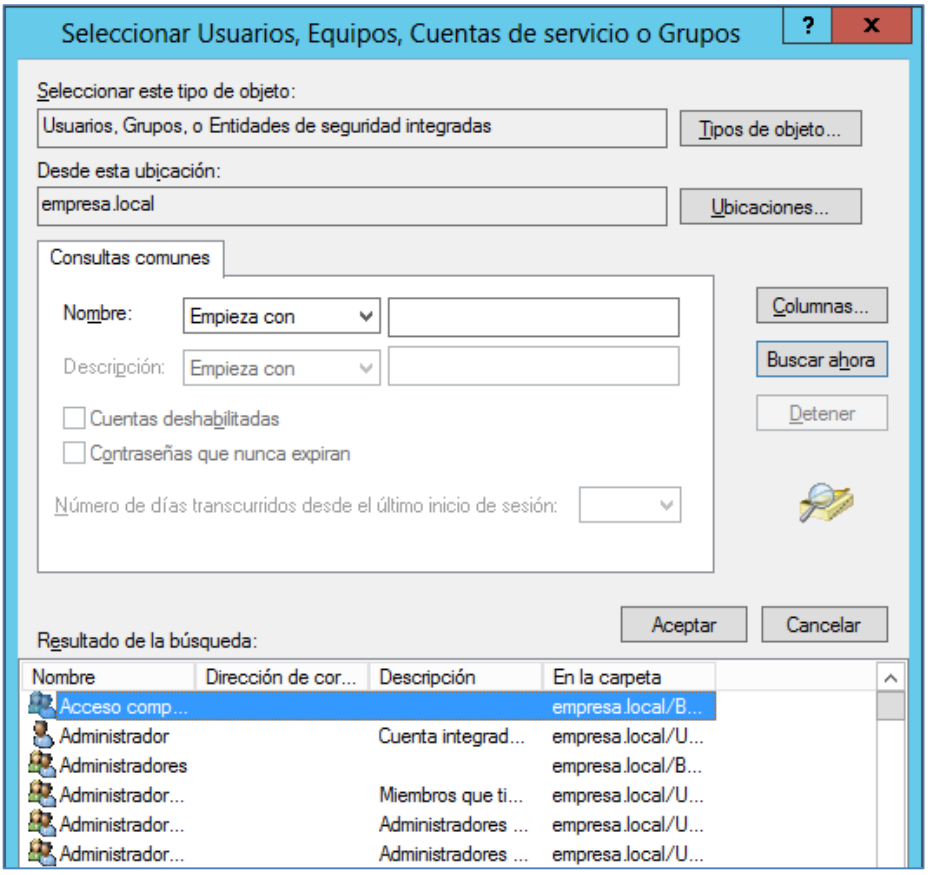


En ese cuadro escribiremos el nombre del usuario o grupo al que queremos asignar los permisos. Pulsando en 'Comprobar nombres' el sistema buscará el nombre escrito en el cuadro y comprobará si efectivamente está dado de alta en el dominio, en cuyo caso aparecerá subrayado.

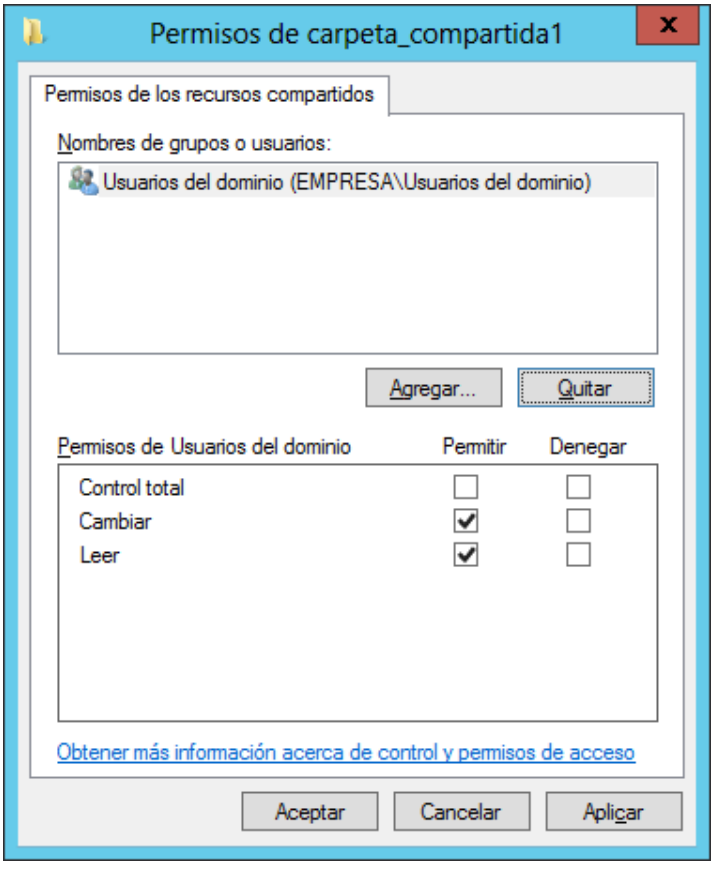


En caso contrario aparecerá un mensaje de error como el de la siguiente imagen, donde se nos advierte de que no se ha podido encontrar el objeto buscado.

Si no recordamos el nombre del grupo o usuario que queremos añadir podemos ir a "Opciones avanzadas"→"Buscar ahora" y seleccionar los usuarios o grupos que queremos:



Una vez que hayamos introducido el nombre de un usuario o grupo que exista en el dominio podremos asignar o quitar los permisos como se ha mostrado más arriba.

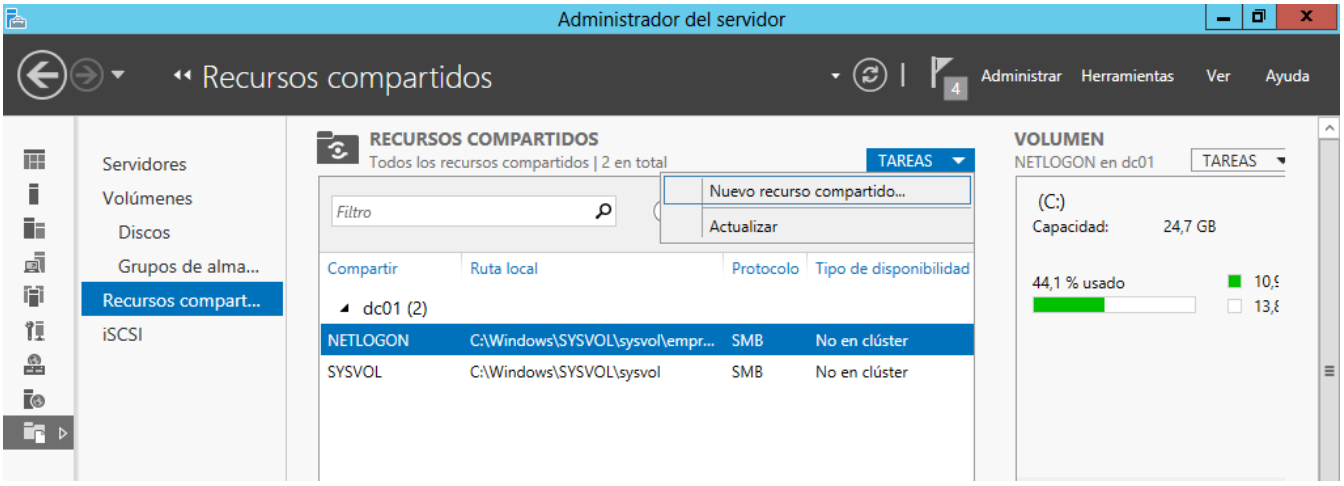


Como política adecuada de administración de sistemas, **en la medida de lo posible se evitarán las comparticiones con el grupo Todos** (en ese grupo están incluso las cuentas de invitado) aunque en el siguiente nivel de permisos (NTFS) se bloqueen accesos indebidos. Se tenderá a incluir únicamente en los permisos de recursos compartidos a aquellos grupos o usuarios que de verdad queramos que tengan algún tipo de acceso sobre el recurso.

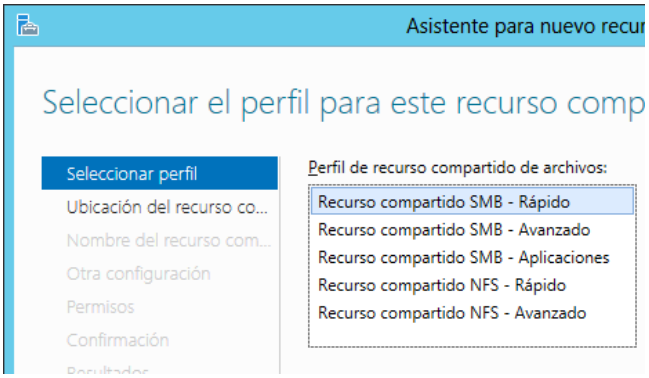
2.2.1.1. Otras formas de compartir recursos

Además del anterior modo, podemos crear recursos compartidos de las siguientes formas:

a) Administrador del servidor→Servicios de archivos y de almacenamiento→Recursos compartidos → Tareas → Nuevo recurso compartido



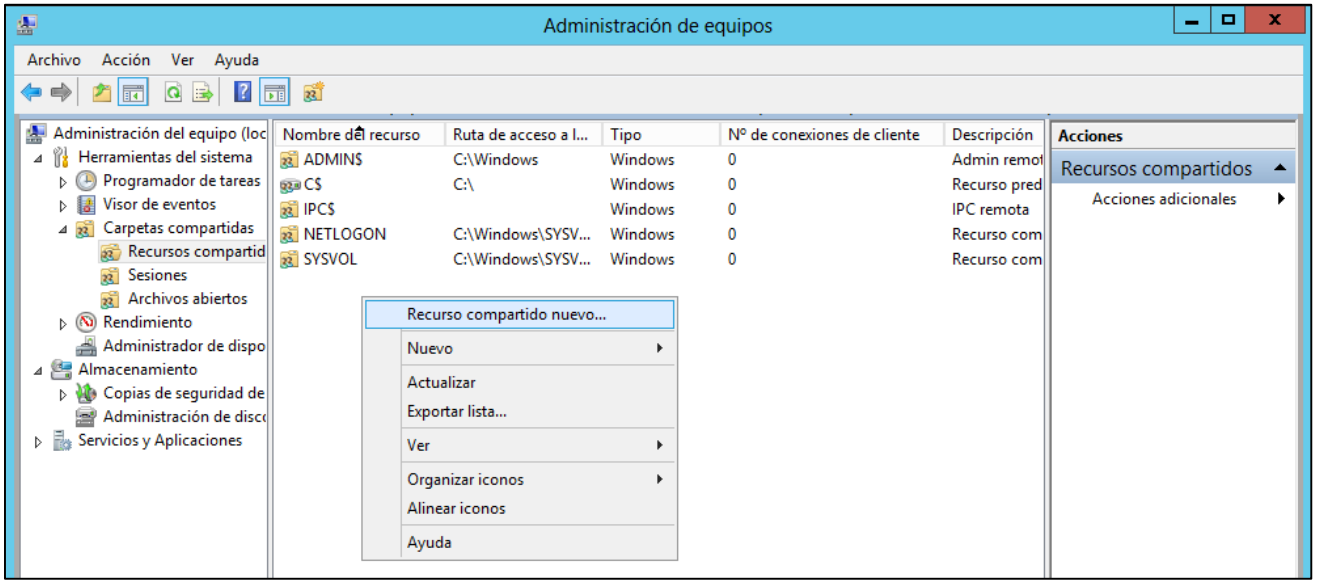
Un asistente nos solicitará que escojamos entre cinco formas diferentes de recurso compartido. Hay tres SMB (para Windows) y dos NFS (para Linux/Unix):



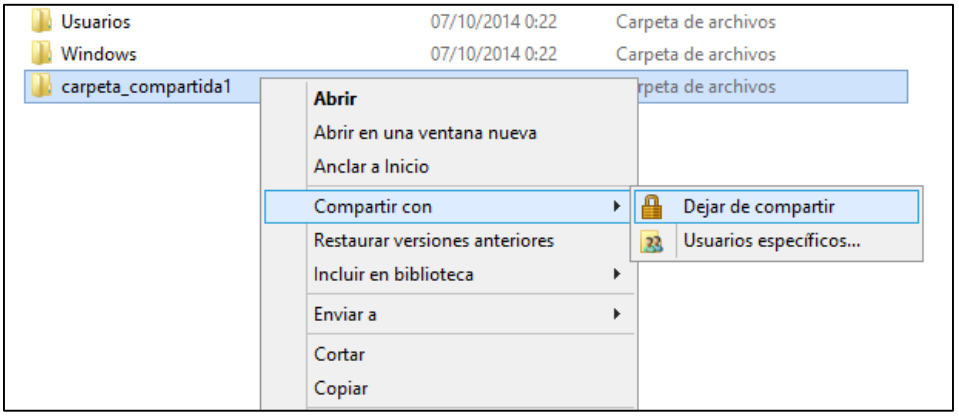
- SMB – Rápido.- es la forma más rápida de crear un share de archivos SMB. Será el que utilicemos por defecto para la compartición de ficheros desde un servidor. Posteriormente podremos configurar las opciones avanzadas.
- SMB – Avanzado.- Nos ofrece las opciones avanzadas de la compartición de archivos SMB, pudiendo:
  - Establecer propietarios de carpetas y quién accede a la información que contenga.
  - Configurar la clasificación de los datos a través de directivas de administración.
  - Habilitar el uso de cuotas.
- SMB – Aplicaciones.- Esta opción es la que está optimizada para el uso de SMB en Hyper-V, Bases de Datos y otras aplicaciones.
- NFS – Rápido.- Es la forma más rápida de crear un share de archivos NFS, utilizado en equipos basados en UNIX. Al igual que para SMB una vez creado el recurso posteriormente podemos realizar una configuración adicional.
- NFS – Avanzado.- Es idéntica a la SMB – Avanzado pero para equipos basados en UNIX.

Esta forma nos permite consultar qué recursos están siendo compartidos en el sistema.

b) Administrador del servidor → Herramientas → Administración de equipos → Carpetas compartidas → Recursos compartidos→botón derecho: Recurso compartido nuevo



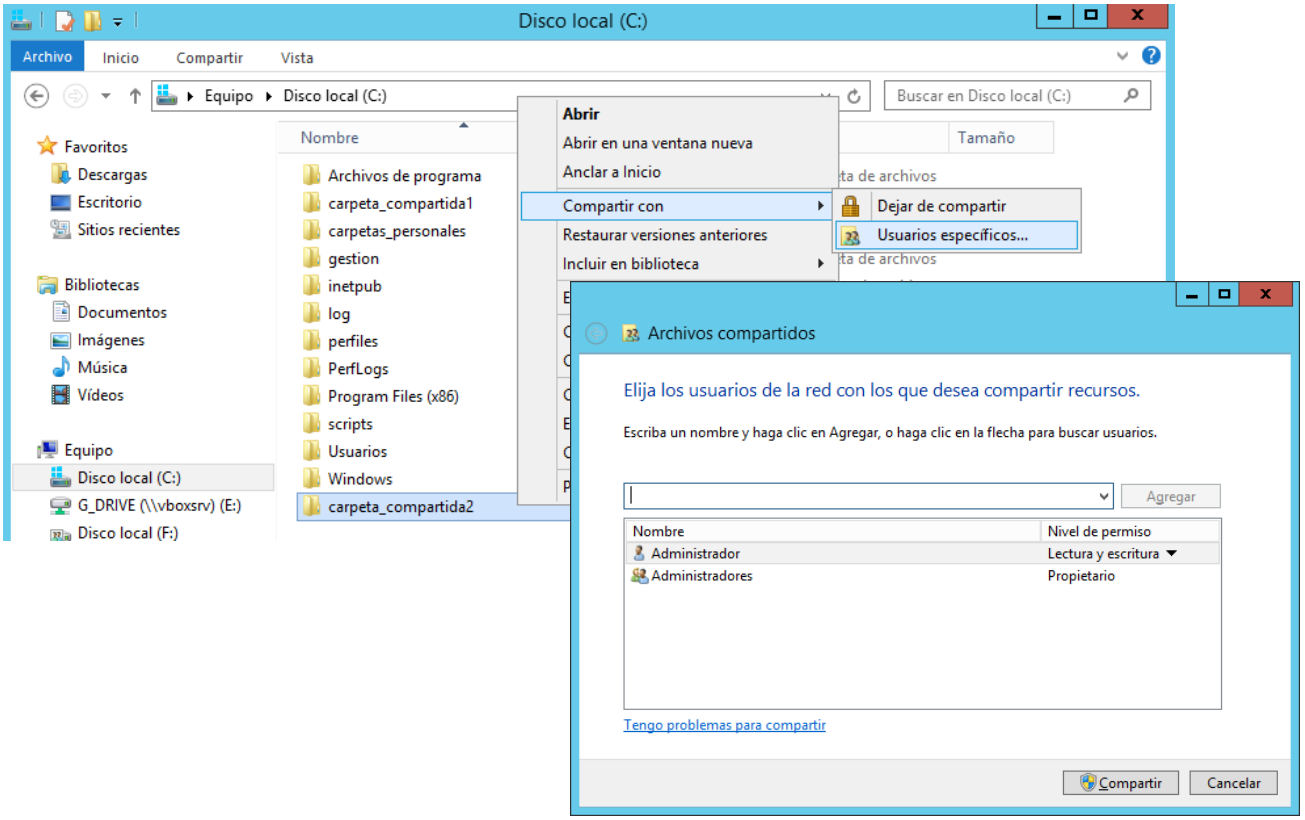
c) Botón derecho sobre la carpeta a compartir→ Compartir con



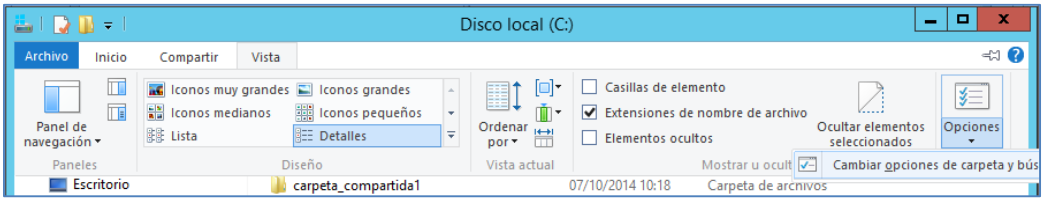
Durante el proceso de creación de un recurso compartido es muy importante la **configuración de los permisos de acceso a dicho recurso**. A continuación, se explica detalladamente el funcionamiento, niveles (tipos de permisos) y configuración de estos permisos.

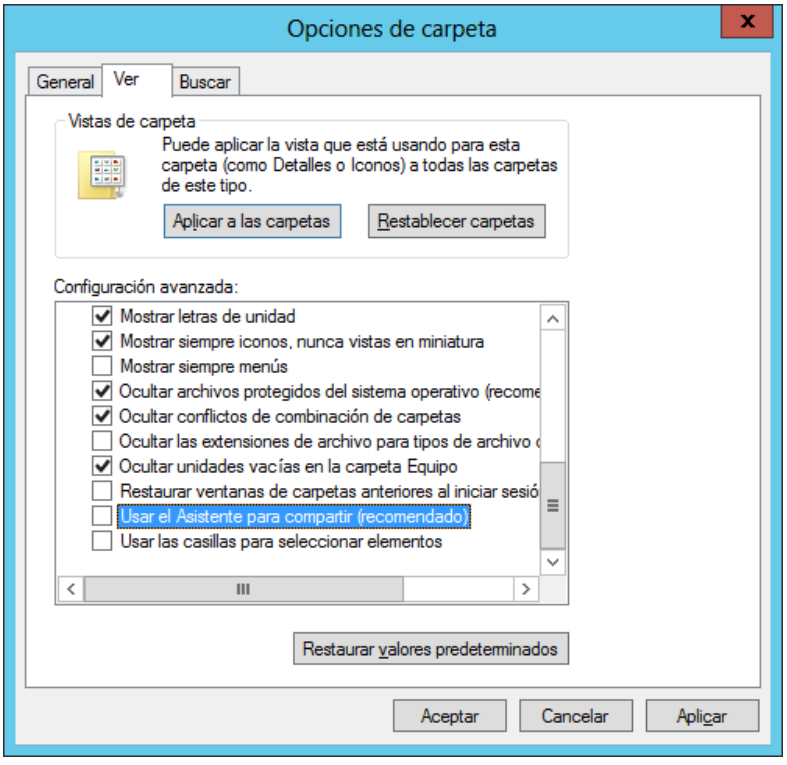
***Nota**: Si compartes una carpeta mediante la opción botón derecho "Compartir con" → "Usuarios específicos…" te saldrá un asistente que permite la configuración de carpetas compartidas. Habitualmente se desaconseja la utilización del asistente para compartir, ya que este resta cierta funcionalidad en comparación con las formas vistas anteriormente. De ahora en adelante todos los ejemplos se realizarán con el **asistente para compartir deshabilitado**.*

A continuación, se muestra cómo desactivar este asistente:



Si se desea inhabilitar el asistente basta con acceder dentro del Explorador de Windows a la pestaña Vista →Opciones →"Cambiar opciones de carpeta" y búsqueda y ahí en la pestaña 'Ver', desmarcar la opción 'Usar el asistente para compartir'.





2.3. Permisos NTFS

Como se ha comentado anteriormente, los permisos NTFS complementan y amplían los permisos de recursos compartidos, siendo **efectivo el más restrictivo.**

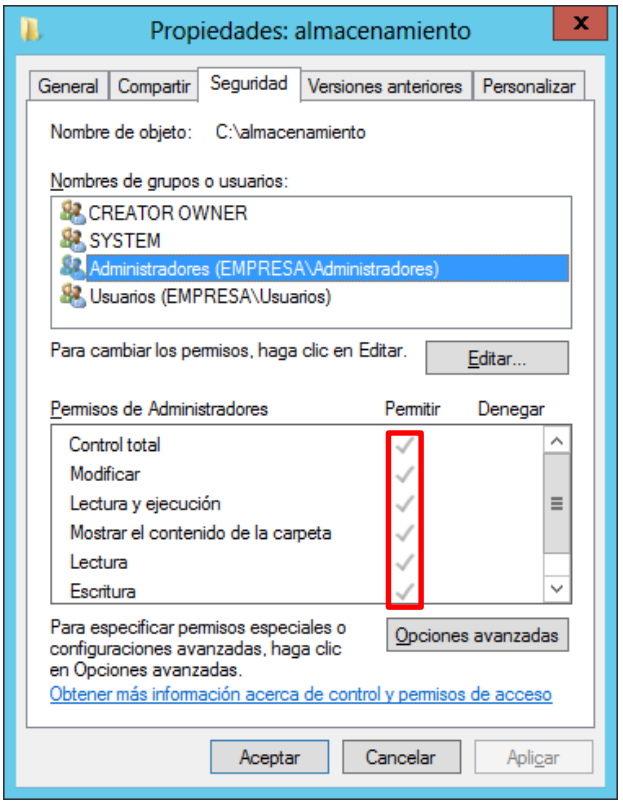
Todos los archivos y carpetas de un **volumen NTFS** tienen asociada una **ACL** o **lista de control de acceso** que fija el **nivel de acceso de un usuario o grupo que pretenda acceder al recurso**. Además, los permisos NTFS pueden ser aplicados a nivel de archivo, a diferencia de los permisos de recursos compartidos, los cuales únicamente pueden aplicarse a nivel de carpeta.

Por otra parte, surge un nuevo concepto al aplicar los permisos NTFS que los hace más complejos aunque también más potentes: **la herencia**, la cual determinará los permisos que se reciben sobre un determinado recurso provenientes de un nivel superior, aunque esto lo veremos detalladamente más adelante.

Tipos de permisos NTFS

Los permisos básicos (o predeterminados) que pueden aplicarse sobre archivos y carpetas son:

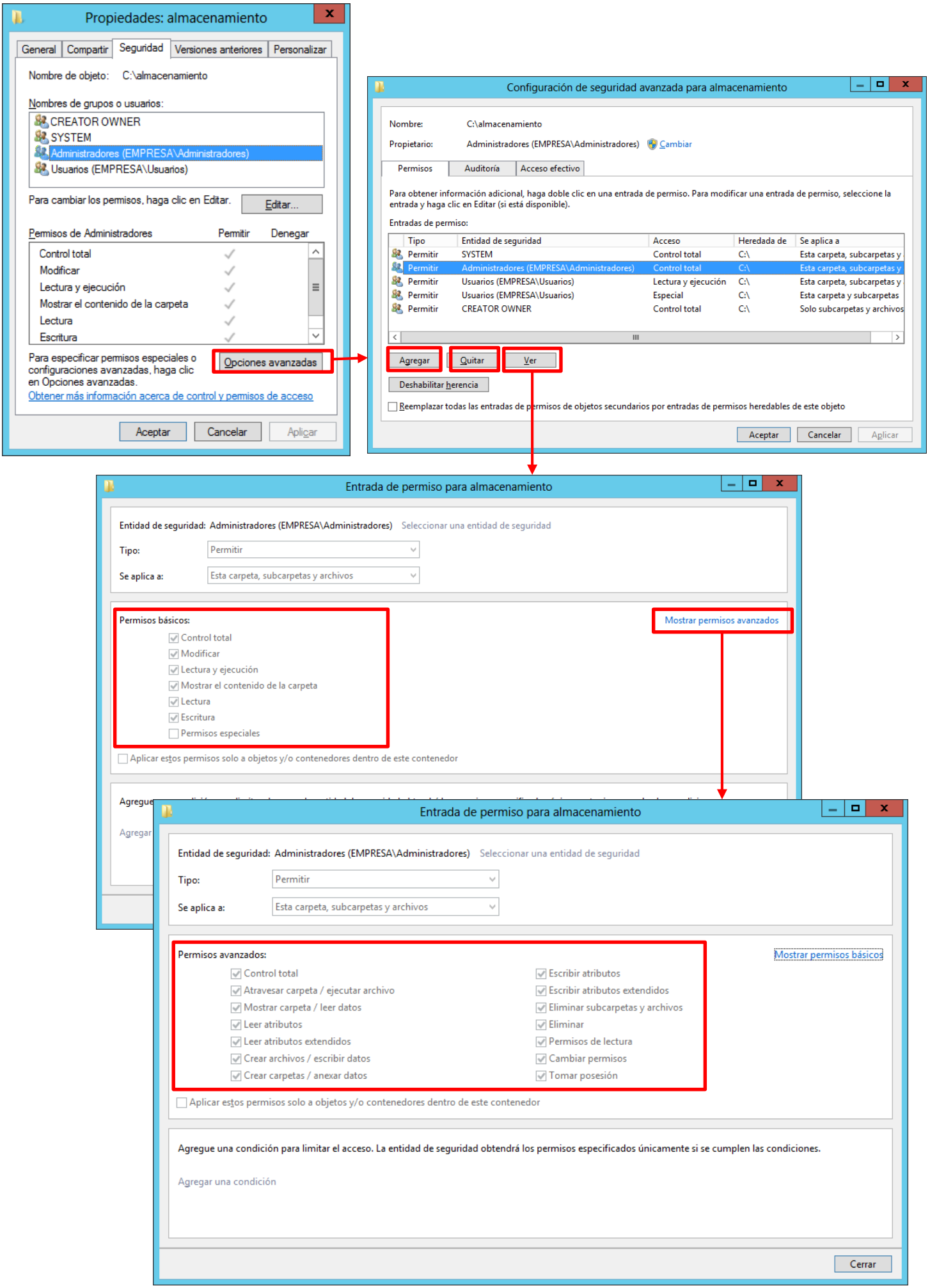
- Control total.
- Modificar.
- Lectura y ejecución.
- Mostrar el contenido de la carpeta.
- Lectura.
- Escritura.



No obstante, estos permisos en realidad representan varios aspectos mucho más concretos. Es decir, los permisos básicos o predeterminados, en realidad corresponden a unas combinaciones de **permisos avanzados** (o específicos). Para tratar de clarificar esta cuestión, la tabla que se muestra a continuación resume qué tareas pueden realizarse con cada tipo de permiso.

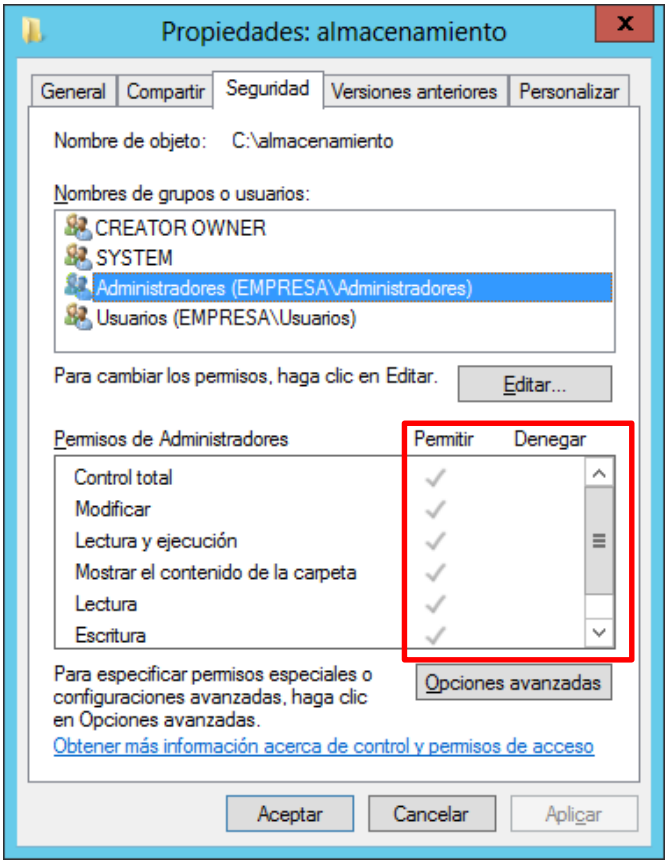
	Control total	Modificar	Lectura y ejecución	Mostrar el contenido de la carpeta	Lectura	Escritura
Atravesar carpeta/ejecutar archivo	✓	✓	✓	✓		
Mostrar carpeta/leer datos	✓	✓	✓	✓	✓	
Leer atributos	✓	✓	✓	✓	✓	
Leer atributos extendidos	✓	✓	✓	✓	✓	
Crear archivos/escribir datos	✓	✓				✓
Crear carpetas/anexar datos	✓	✓				✓
Escribir atributos	✓	✓				✓
Escribir atributos extendidos	✓	✓				✓
Eliminar subcarpetas y archivos	✓					
Eliminar	✓	✓				
Permisos de lectura	✓	✓	✓	✓	✓	✓
Cambiar permisos	✓					
Tomar posesión	✓					

Los permisos específicos puede editarse/consultarse individualmente, tal y como se muestra a continuación:



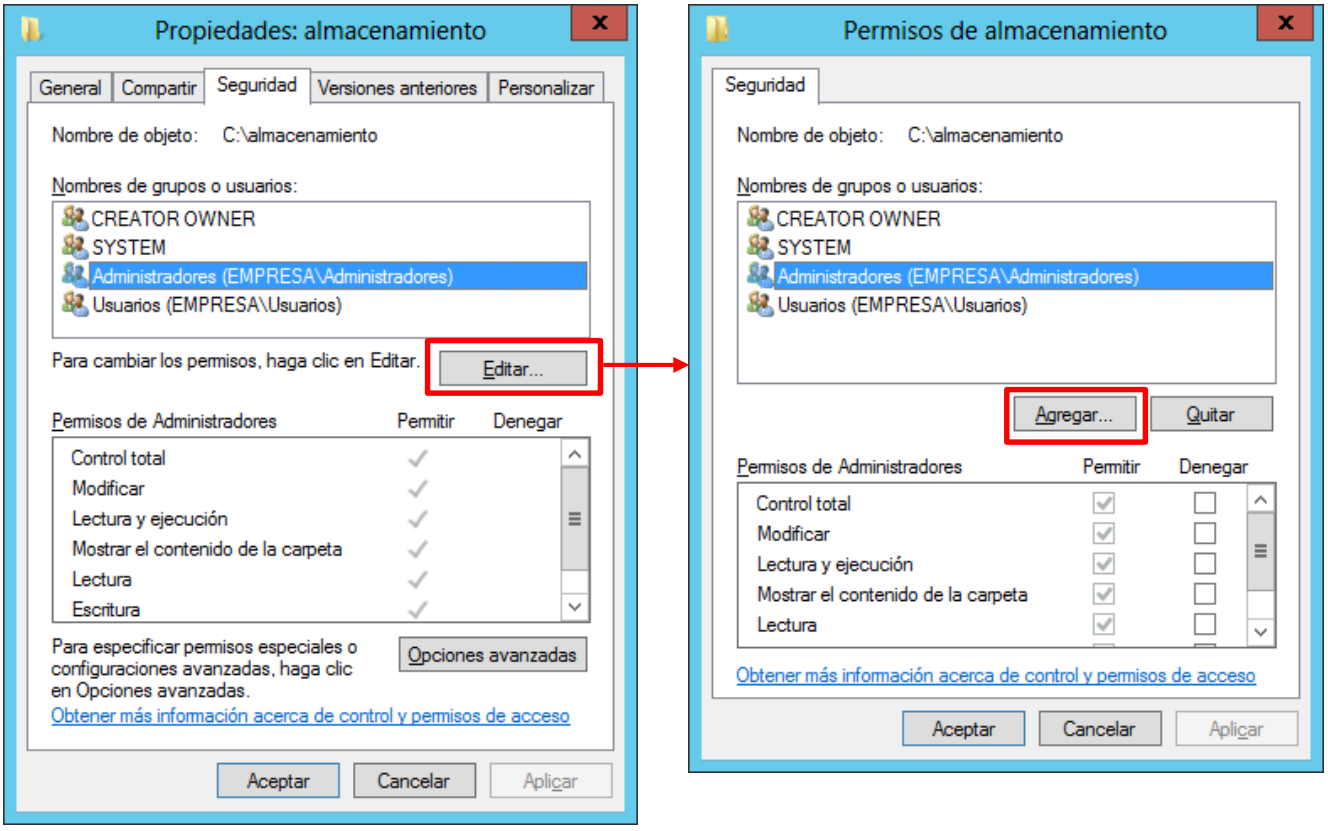
2.3.1. Asignación de permisos NTFS

Al definir un permiso NTFS este puede ser un permiso o una denegación.



Los permisos NTFS son acumulativos: se evalúan los permisos otorgados al usuario y a los grupos a los que pertenece el usuario. En el caso de que haya una incompatibilidad entre los permisos asignados a un usuario y los asignados a un grupo del cual sea miembro, prevalecerá la opción más restrictiva: Denegar (si está definido explícitamente).

Para asignar permisos NTFS a un recurso compartido bastará con hacer clic con el botón secundario sobre el recurso y acceder a la pestaña 'Seguridad'. A continuación pulsaremos el botón 'Editar'. El botón 'Agregar' permite añadir grupos o usuarios a los que otorgar o denegar permisos.



Cuidado con el grupo `Usuarios` (del dominio) porque aparece por defecto en los permisos NTFS (con permisos de lectura), y puede provocar que se produzcan accesos diferentes a nuestra planificación. Como norma general, si queremos limitar el acceso a un recurso compartido, eliminaremos el grupo `Usuarios` de los permisos NTFS y explicitaremos únicamente aquellos grupos o usuarios que efectivamente queramos que tengan acceso al recurso

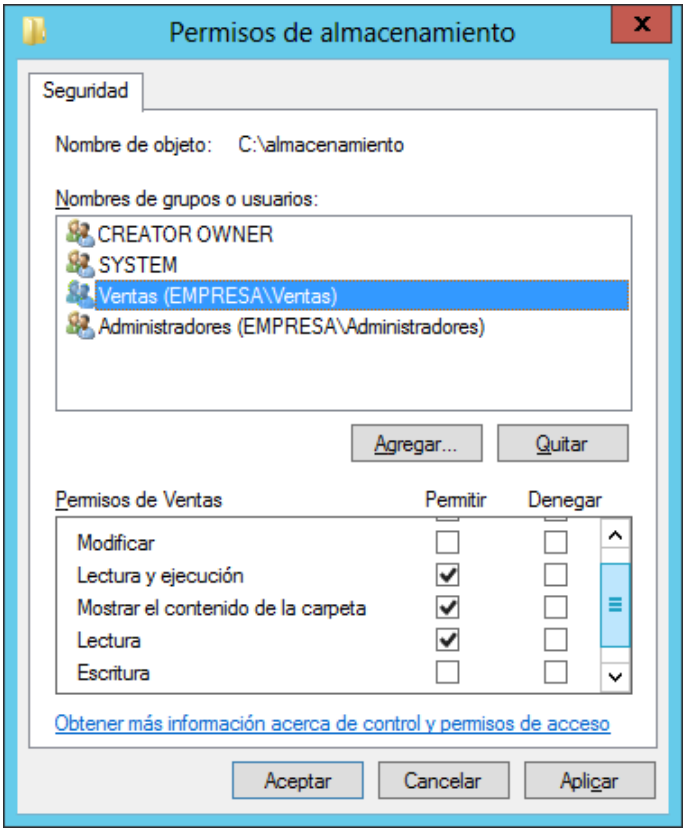
2.3.2. Permisos implícitos y permisos explícitos

Los permisos otorgados de manera implícita o explícita son una cuestión sencilla, en la que si no nos fijamos con atención, podemos hacer que los accesos a los recursos no funcionen como teníamos previsto.

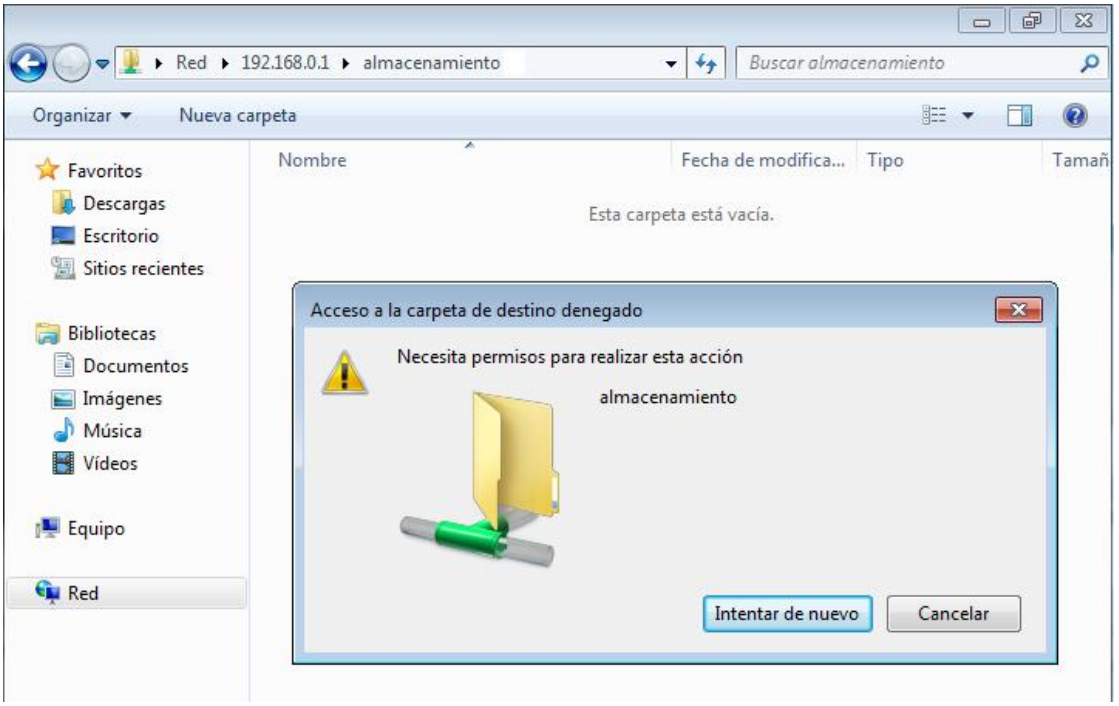
Para evitar problemas tendremos en cuenta que:

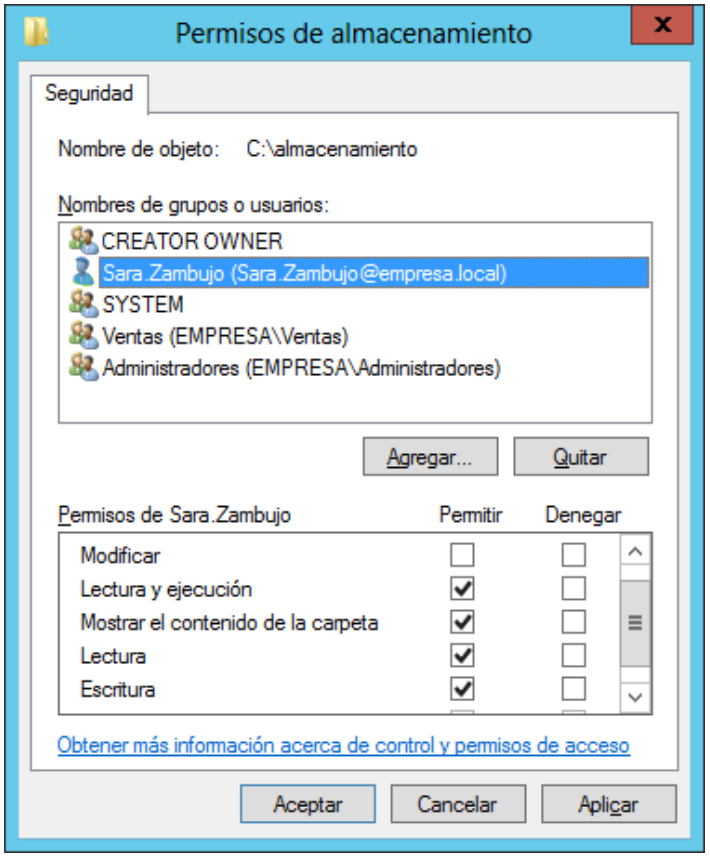
1. Un permiso definido de manera explícita siempre prevalecerá sobre un permiso definido de manera implícita.
2. Denegar un permiso siempre prevalece sobre otorgar ese permiso, siempre y cuando ambos estén definidos de la misma manera (implícita o explícitamente).

¿Cómo se define un permiso de manera explícita? Si nos fijamos en la siguiente imagen, el grupo Ventas no tiene (aparentemente) definidos permisos de escritura. Sin embargo esa aparente indefinición, en realidad indica que el permiso de escritura está denegado implícitamente.

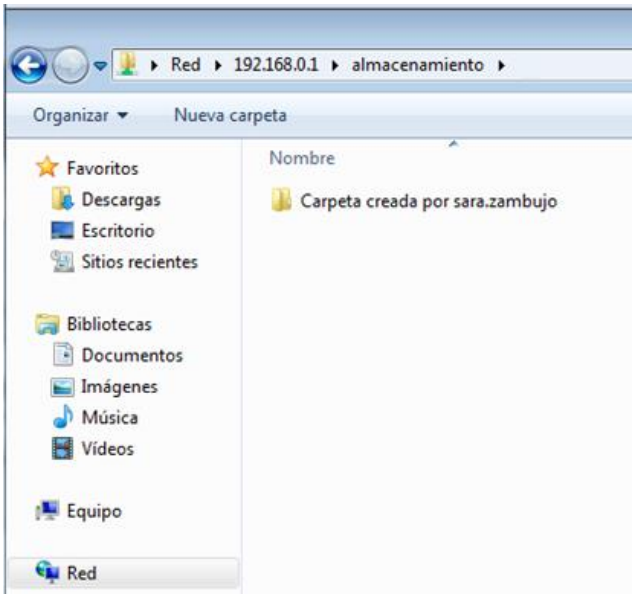


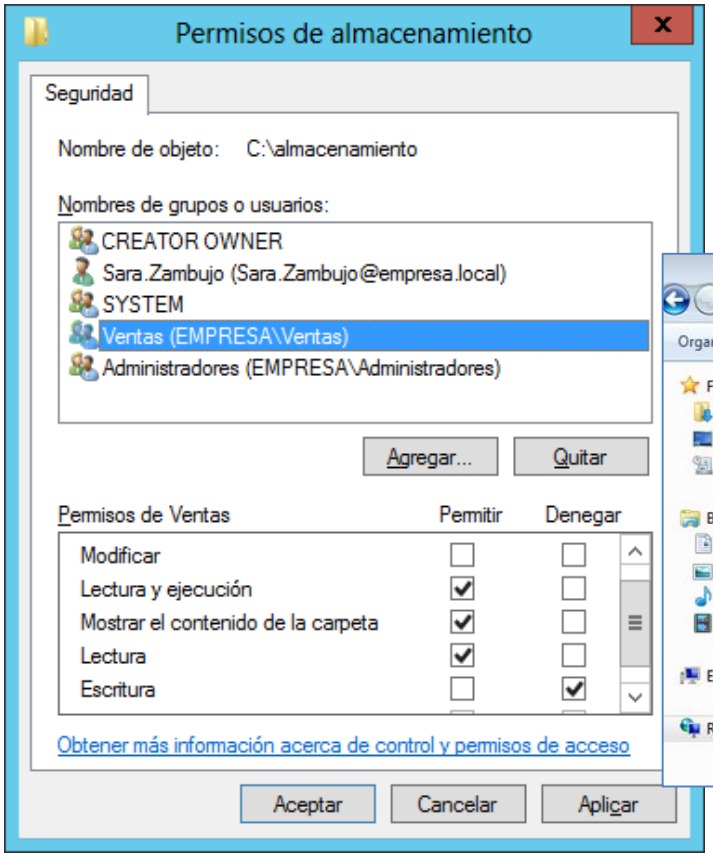
Si un usuario del grupo Ventas intenta escribir en la carpeta, se producirá un mensaje de error.



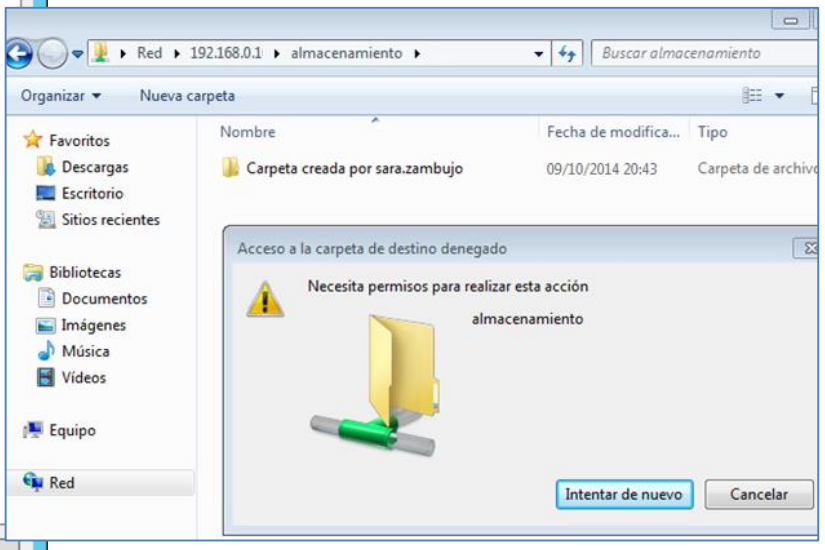


Sin embargo, si añadimos al usuario `sara.zambujo` que es miembro de `Ventas` en la ficha permisos, y le otorgamos el permiso explícito de escritura, veremos que efectivamente puede escribir en el recurso, ya que la definición explícita del permiso para escribir prevalece sobre la denegación implícita del permiso escribir.





Si explicitamos la denegación del permiso de escritura para los miembros del grupo `Ventas`, podremos comprobar que efectivamente `sara.zambujo` **no puede** escribir en la carpeta.



Se recomienda evitar el uso explícito de la denegación de permisos salvo que se considere que no existe otro modo para obtener un nivel específico de permiso para un determinado grupo.

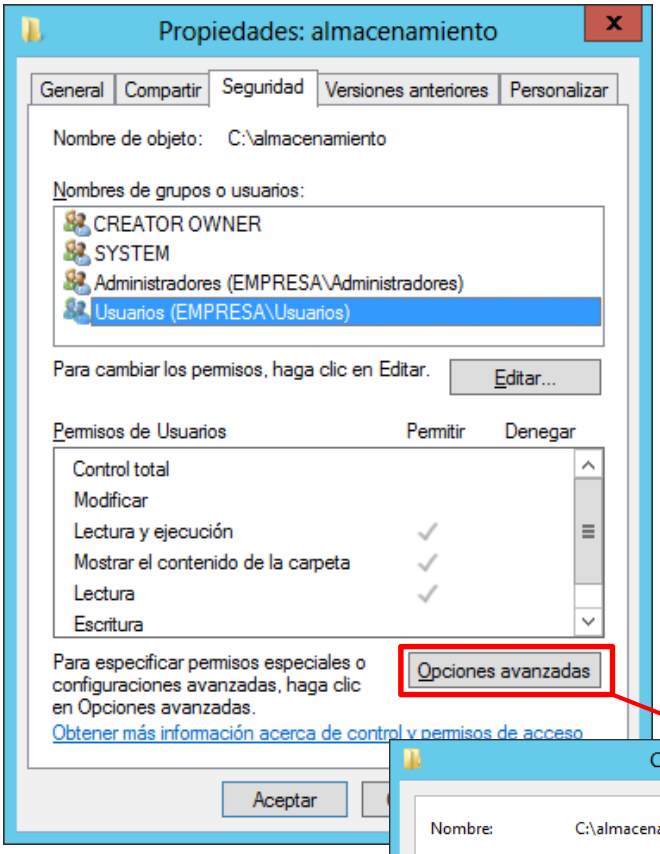
2.3.3. Herencia de permisos

Al crear un archivo o carpeta en un volumen NTFS ese objeto hereda automáticamente los permisos de su carpeta contenedora, y a la inversa: cuando asignamos permisos a una carpeta contenedora, los permisos se propagan automáticamente hacia los archivos y subcarpetas contenidas en el recurso.

Sin embargo, pueden darse ocasiones en las que queramos eliminar esa herencia de permisos. Esto puede ejecutarse de tres maneras diferentes:

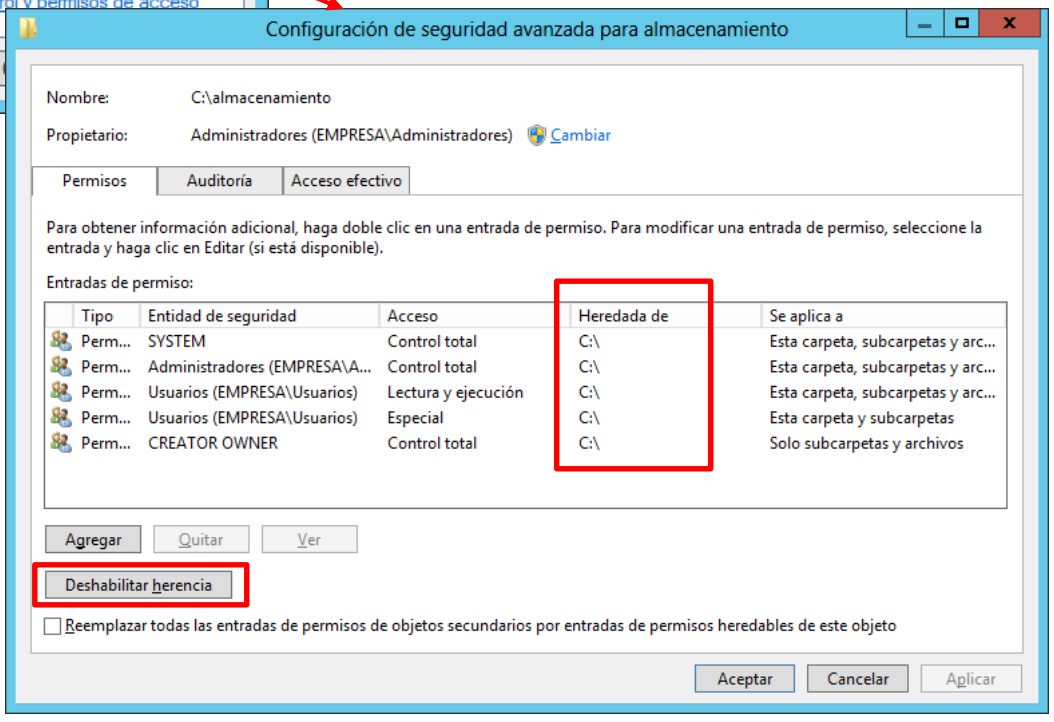
- Eliminar la herencia a nivel de la carpeta de nivel superior, los objetos contenidos en ella dejan de heredar los permisos.
- Eliminar la herencia a nivel de subcarpeta o archivo contenido dentro del recurso principal.
- Permitir o denegar **explícitamente** un permiso de manera diferente a como está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

Eliminación de herencia del recurso de nivel superior



Para eliminar la herencia de los permisos establecidos en la carpeta de nivel superior, se debe acceder a la ficha 'Seguridad' y a continuación se hace clic en 'Opciones Avanzadas'.

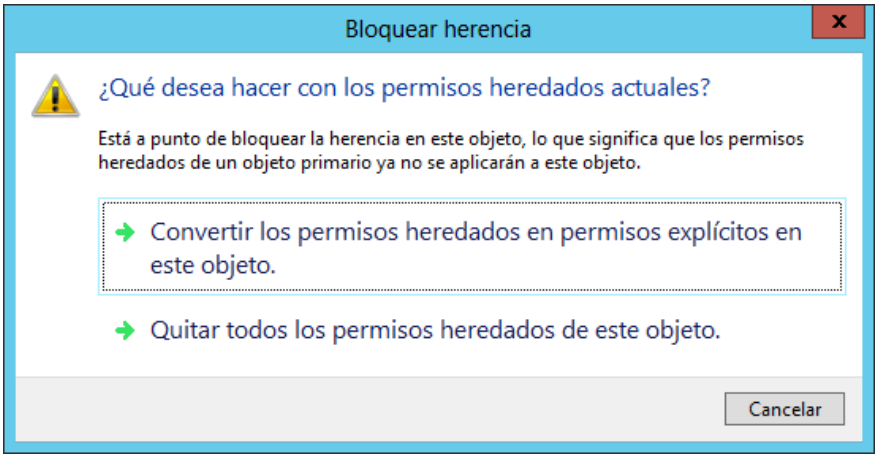
El cuadro de diálogo que aparece muestra los permisos actuales y en la columna 'Heredada de' se indica el origen del permiso.



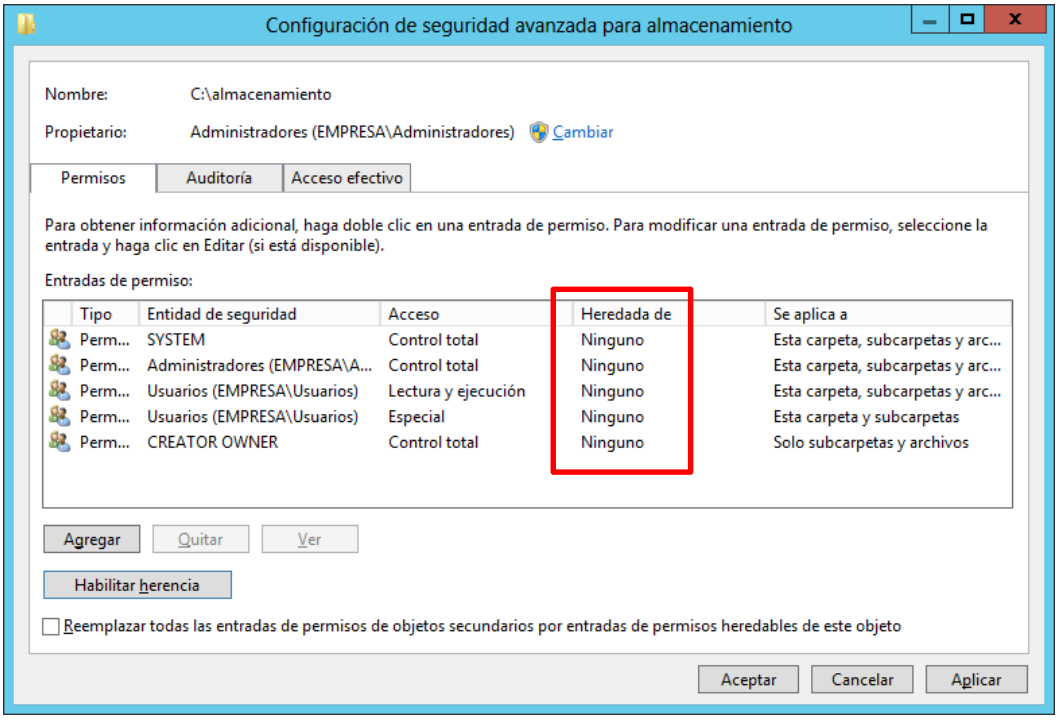
Para eliminar la herencia pulsaremos el botón Deshabilitar herencia'.

A continuación aparece un cuadro de diálogo que nos da la opción de:

- Convertir los permisos heredados en permisos explícitos en este objeto' (copiar): mantiene los permisos de todos los archivos y subcarpetas, pero no están vinculados a los del nivel superior.
- 'Quitar todos los permisos heredados de este objeto' (quitar): elimina todos los permisos heredados.

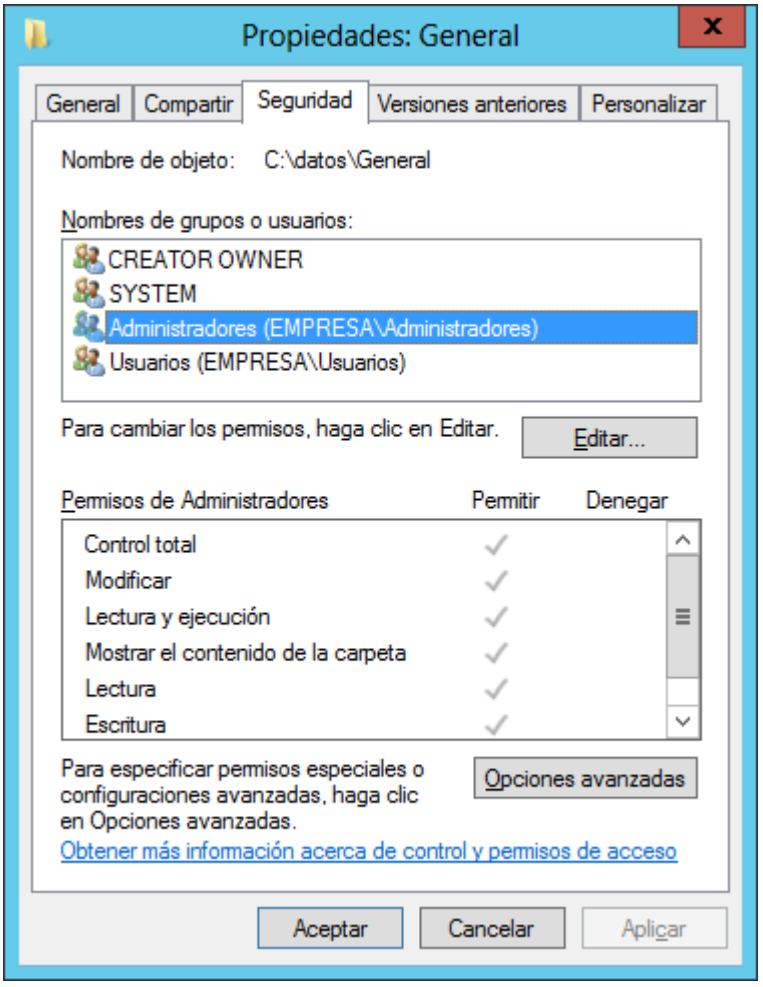


Como norma general haremos clic en 'Convertir…/Copiar'. En el cuadro de diálogo de 'Configuración de seguridad avanzada' se nos indican los permisos como 'Heredada de: ninguno' (no heredados).

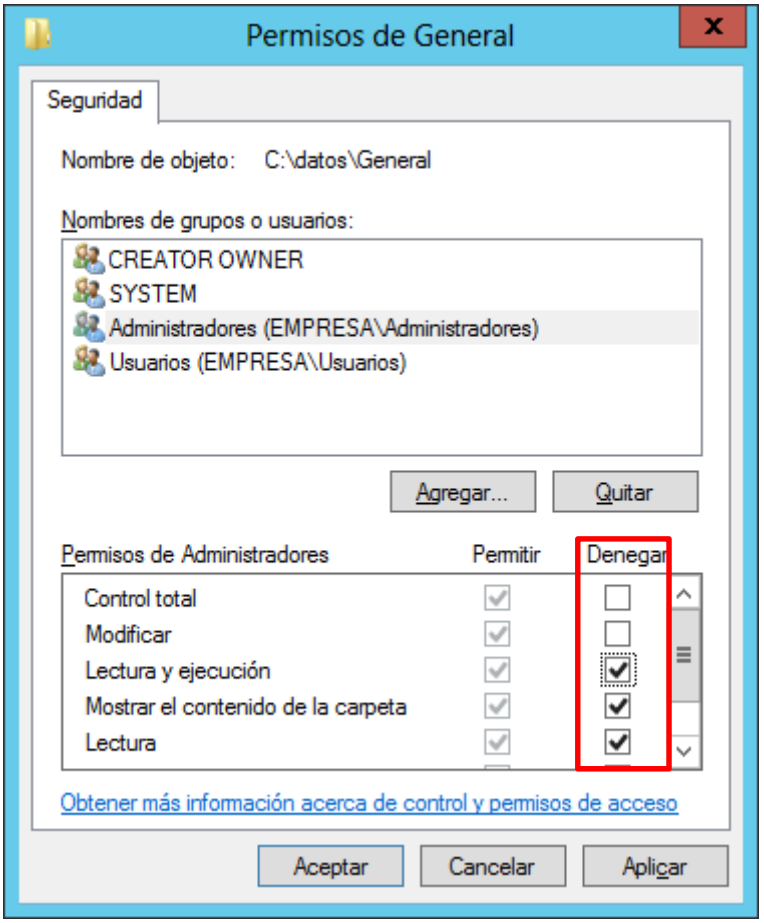


Cambio de los permisos del objeto hijo

Si observamos los permisos de un objeto que está heredando permisos, veremos que las casillas de verificación están (completa o parcialmente) inaccesibles.



En primer lugar podemos interrumpir la herencia, denegando explícitamente los permisos. Si el permiso heredado es de concesión, la denegación está habilitada.



Otra alternativa consiste en acceder a la 'Configuración de seguridad avanzada' del objeto hijo y eliminar el vínculo con el objeto padre de manera similar a como se planteó en el punto anterior.

2.4. Compartición de recursos por línea de comandos

La primera cuestión a resolver al compartir un recurso por línea de comandos, será la creación de la carpeta que queremos compartir. Supongamos que queremos crear dicha carpeta en C: y que se llamará Carpeta_Compartida. El comando para crearla sería:

```
>>mkdir C:\Carpeta_Compartida
```

A la hora de gestionar los permisos de acceso, daremos permiso de lectura y escritura a cualquier usuario del grupo, por ejemplo `Ventas` que se conecte a la carpeta compartida. Así, el comando para compartir la carpeta sería:

```
>>net share Compartida=C:\Carpeta_Compartida /grant:empresa\Ventas,change
```

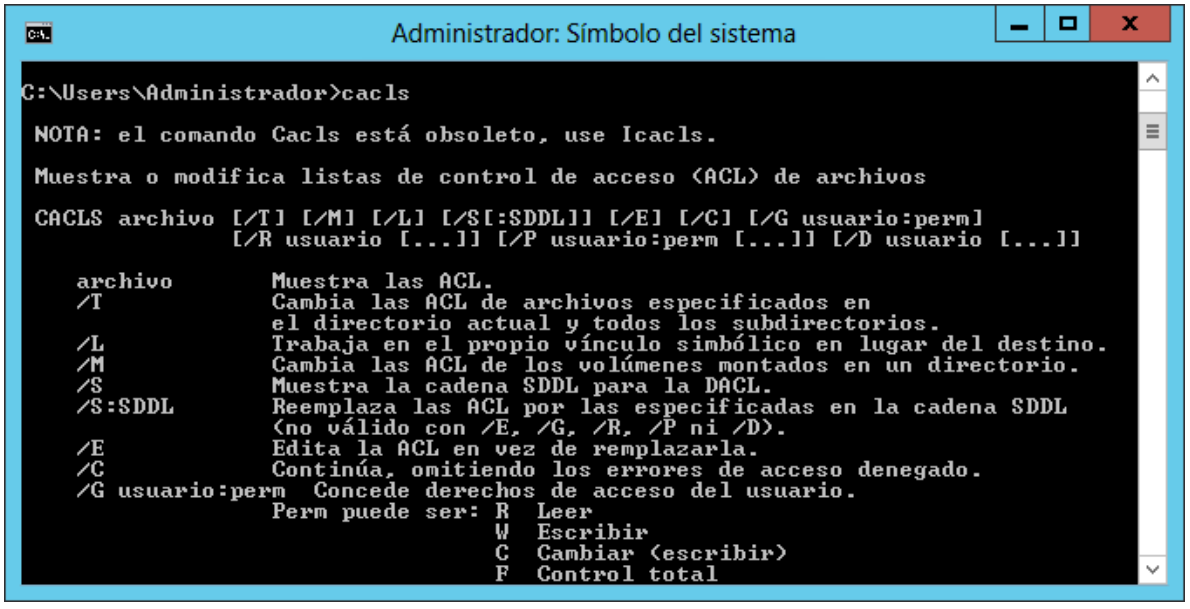
Detengámonos por un instante en esta sintaxis. El término `Compartida` que aparece a la izquierda del comando `net share`, indica el nombre de la carpeta que será visible para el usuario que se conecte a ella. A continuación se ha de escribir la ruta donde se halla la carpeta compartida. La siguiente parte del comando es `/grant:` donde han de indicarse los usuarios que tendrán acceso al recurso, y finalmente tras una coma se escribe el tipo de permiso que tendrá, `read, change o full`.

En la siguiente tabla se especifica qué nivel de acceso permite cada una de las opciones:

Permisos	Nivel de Acceso
Read	Únicamente permite visualizar el contenido de la carpeta compartida.
Change	Permite modificar el contenido de la carpeta compartida (escribir, borrar, crear archivos, etc.)
Full	Permite hacer todo lo anterior, y además cambiar los permisos de la carpeta.

2.5. Permisos NTFS por línea de comandos

Antiguamente las ACLs (*listas de control de accesos*), que se gestionaban en los permisos NTFS, se configuraban por línea de comandos mediante `cacls`. Al ejecutarlo actualmente, nos aparece una advertencia indicando que el comando está obsoleto.



Microsoft creó la herramienta `xcacls` para sustituir al anterior. Originariamente era un fichero `.exe`, aunque ahora está disponible para su descarga como `.vbs`. En el siguiente enlace podéis hallar la ayuda que brinda Microsoft para su utilización, no obstante sigue sin venir instalado en el propio sistema operativo. Posteriormente apareció subinacl.exe para sustituir a `xcacls`. Sin embargo la herramienta que viniendo instalada en el propio sistema operativo, mejores resultados ofrece es `iacls`.

`icacls` permite de una manera relativamente intuitiva gestionar y modificar las ACLs de los recursos compartidos. A continuación veremos algunos ejemplos:

Creemos en el controlador de dominio, por ejemplo, una carpeta en `C:`, llamada `Pruebas`:

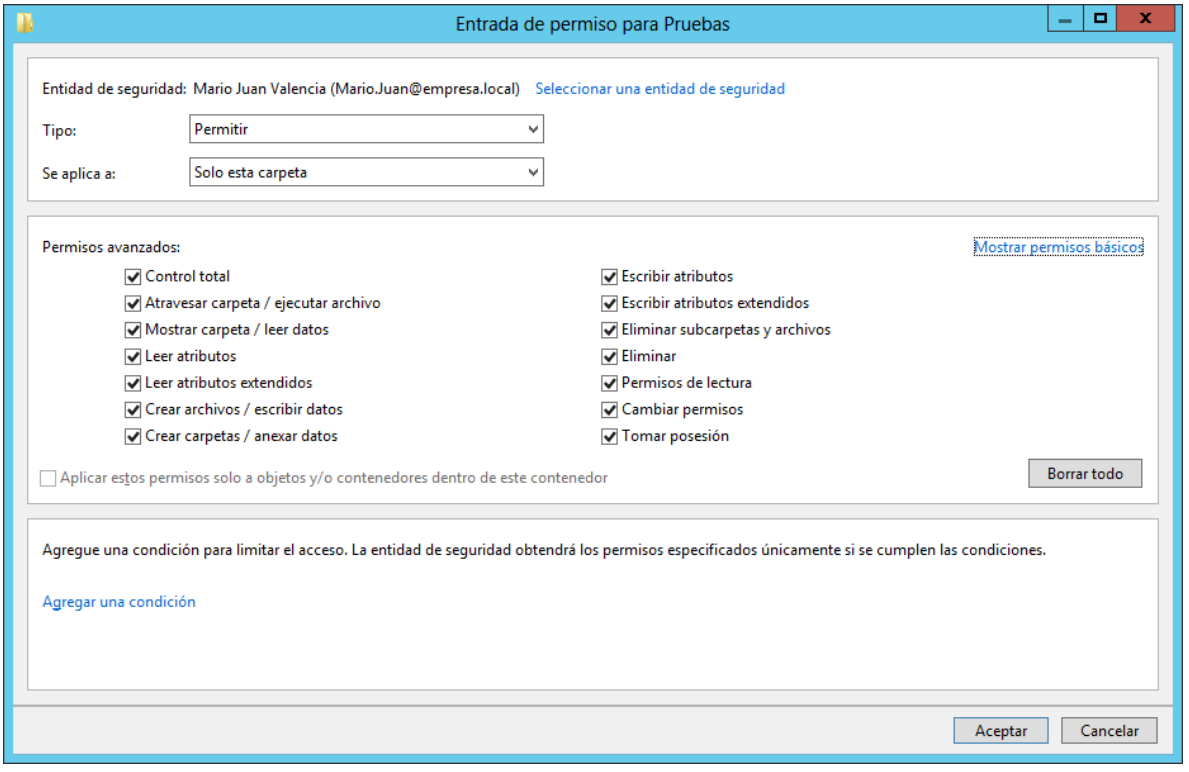
```
>>mkdir C:\Pruebas
```

Si ahora aplicamos el comando `iacls` para otorgar permisos al usuario `mario.juan` del dominio `empresa` escribiríamos:

```
>>icacls C:\Pruebas /GRANT empresa\mario.juan:(f)

>>icacls C:\Pruebas /inheritance:d

>>icacls C:\Pruebas /remove:g Usuarios
```

La primera línea de la serie de comandos anteriores **otorga** (`/GRANT:`) al usuario `mario.juan` control total (`f`) sobre `C:\Pruebas`. La segunda elimina (`:d`) la herencia (`/inheritance`) de permisos, y finalmente la tercera elimina (`/remove`) los permisos otorgados `:g` al grupo `Usuarios`.

Comprobemos el resultado de la acción anterior:

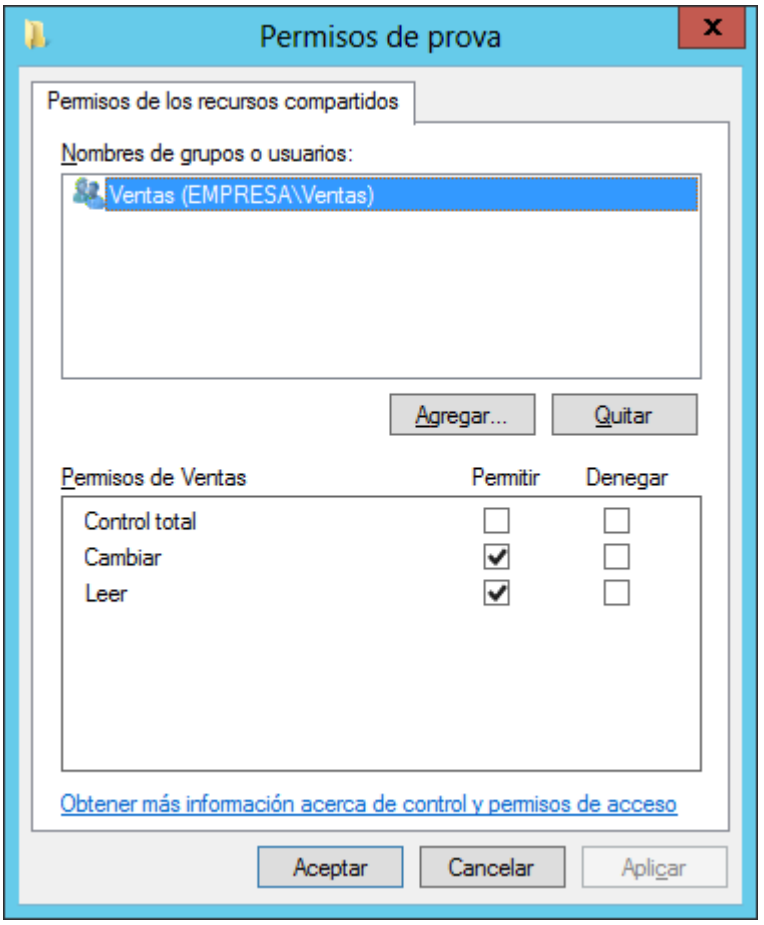


Tal y como se han configurado las ACLs ¿El usuario `mario.juan` tendrá acceso a la carpeta `Pruebas` del controlador de dominio desde un equipo cliente?

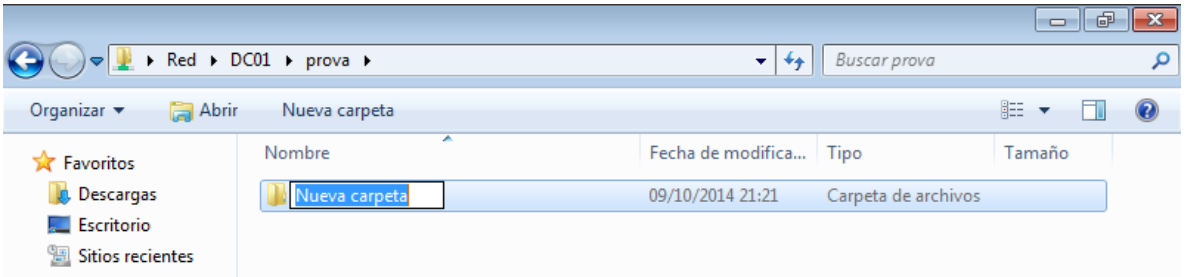
Compartamos la carpeta en red con los miembros del dominio que pertenezcan al grupo `Ventas` (`mario.juan` es miembro de `Ventas`). Es importante destacar que debemos indicar el dominio al que pertenece el grupo: `empresa\Ventas`.

```
>>net share prova=C:\Pruebas /grant:empresa\Ventas,change
```

Si comprobamos la compartición en red, vemos que está todo correcto.



Ahora efectivamente, el usuario `mario.juan` puede acceder al recurso compartido y, entre otras cosas, crear una carpeta dentro.

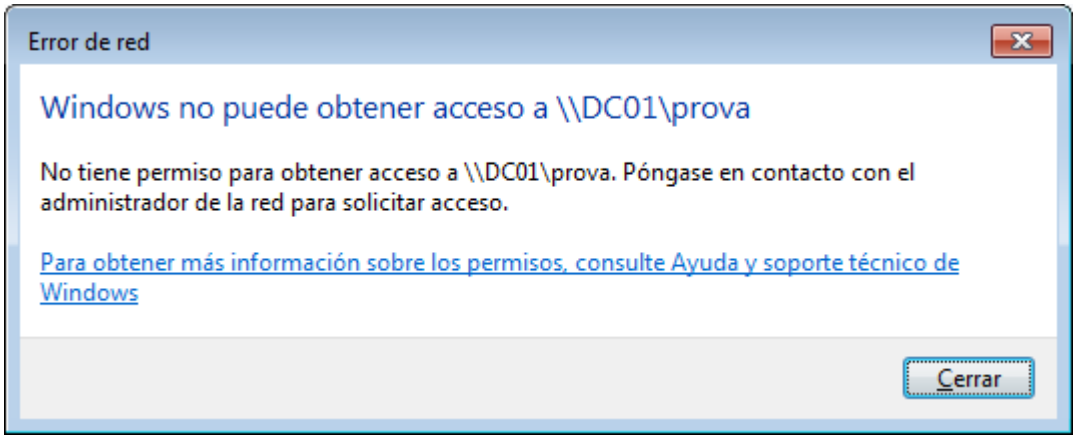


Modifiquemos los permisos de carpeta compartida para comprobar que los permisos NTFS (ACLs) bloquean el acceso a los usuarios que no tienen permiso.

```
>>net share prova /delete

>>net share prova=C:\Pruebas /grant:Todos,change
```

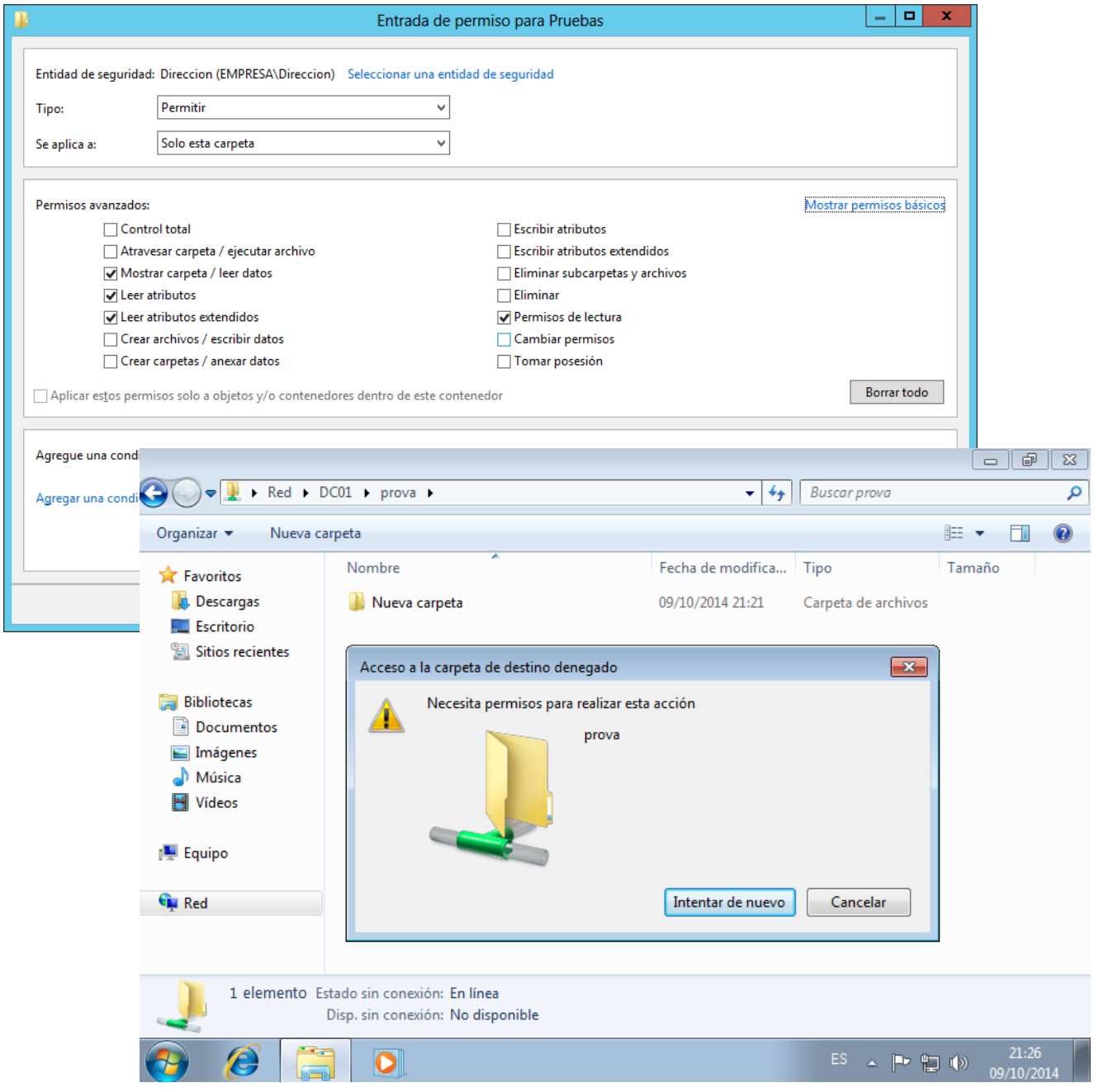
Ahora todos los usuarios del dominio tienen permiso de lectura y escritura, aunque este permiso luego estará limitado por las ACLs.

Veamos cómo se produce el error al intentar acceder un usuario al que no se le ha concedido un permiso NTFS: `basilio.pujol`.



Modifiquemos los permisos NTFS para que `basilio.pujol`, del grupo `Dirección`, pueda ver el contenido de la carpeta, pero no modificarlo, ni añadir archivos (daos cuenta de que hay que poner el nombre completo del grupo `empresa\Dirección`):

```
>>icacls C:\Pruebas /grant empresa\Dirección:(R)
```



Para concluir este apartado, vamos a proponer un pequeño script que:

1. Cree una carpeta en el servidor que se llamará `Documentación`.
2. Cree una subcarpeta por cada departamento de la organización
   - Dirección
   - Finanzas
   - Servicios
   - Producción
   - Ventas
3. Comparta las carpetas en red
4. Aplique permisos NTFS, de manera que los miembros de un departamento podrán leer y escribir en su carpeta, pero no podrán acceder al contenido del resto de carpetas
5. Los miembros del grupo local `Acceso_extra` (cuyos miembros eran los grupos globales de Dirección y Finanzas) podrán acceder pero no escribir en las carpetas de los demás departamentos.

La solución propuesta es como sigue:

```
@echo off
REM Comprobamos si existen las carpetas, en caso contrario las creamos
if NOT EXIST C:\Documentación mkdir C:\Documentación
if NOT EXIST C:\Documentación\Dirección mkdir C:\Documentación\Dirección
if NOT EXIST C:\Documentación\Finanzas mkdir C:\Documentación\Finanzas
if NOT EXIST C:\Documentación\Servicios mkdir C:\Documentación\Servicios
if NOT EXIST C:\Documentación\Producción mkdir C:\Documentación\Producción
if NOT EXIST C:\Documentación\Ventas mkdir C:\Documentación\Producción
REM Compartimos en red con 'Todos' las carpetas, con los permisos NTFS filtraremos
los accesos
net share Documentos_Dirección=C:\Documentación\Dirección /GRANT:Todos,full
net share Documentos_Finanzas=C:\Documentación\Finanzas /GRANT:Todos,full
net share Documentos_Producción=C:\Documentación\Producción /GRANT:Todos,full
net share Documentos_Servicios=C:\Documentación\Servicios /GRANT:Todos,full
net share Documentos_Ventas=C:\Documentación\Ventas /GRANT:Todos,full
REM Aplicamos las ACLs
icacls C:\Documentación\Dirección /GRANT empresa\Dirección:(R,W)
icacls C:\Documentación\Finanzas /GRANT empresa\Finanzas:(R,W)
icacls C:\Documentación\Producción /GRANT empresa\Producción:(R,W)
icacls C:\Documentación\Servicios /GRANT empresa\Servicios:(R,W)
icacls C:\Documentación\Ventas /GRANT empresa\Ventas:(R,W)
REM Eliminamos los permisos asignados al grupo 'Usuarios del dominio'
icacls C:\Documentación\Dirección /inheritance:d /T
icacls C:\Documentación\Dirección /remove:g Usuarios
icacls C:\Documentación\Finanzas /inheritance:d /T
icacls C:\Documentación\Finanzas /remove:g Usuarios
icacls C:\Documentación\Producción /inheritance:d /T
icacls C:\Documentación\Producción /remove:g Usuarios
icacls C:\Documentación\Servicios /inheritance:d /T
icacls C:\Documentación\Servicios /remove:g Usuarios
icacls C:\Documentación\Ventas /inheritance:d /T
icacls C:\Documentación\Ventas /remove:g Usuarios
REM Añadimos el permiso extra del grupo Acceso_extra
icacls C:\Documentación\Dirección /GRANT empresa\Acceso_extra:(R)
icacls C:\Documentación\Finanzas /GRANT empresa\Acceso_extra:(R)
icacls C:\Documentación\Producción /GRANT empresa\Acceso_extra:(R)
icacls C:\Documentación\Servicios /GRANT empresa\Acceso_extra:(R)
icacls C:\Documentación\Ventas /GRANT empresa\Acceso_extra:(R)
```

Se puede comprobar que la estructura se ha creado correctamente, y los permisos se ajustan a los requisitos establecidos.

En la web Technet de Microsoft se halla una referencia (algo escueta) al comando `iacls`. Particularmente interesantes son todas las opciones que permite para definir de una manera muy precisa los permisos otorgados, más alla del `f` (control total), `r` (lectura), y `w` (escritura) mostrados en los ejemplos anteriores.

3. Directivas de Grupo (GPO)

Las directivas de grupo (*Group Policy*) son una serie de **configuraciones** creadas por el administrador **que se aplican a objetos del dominio**. Por medio de estas directivas, el administrador **controla los entornos de trabajo de los usuarios del dominio, los equipos y el comportamiento de distintos objetos**. Son en definitiva un conjunto de **reglas que facilitan las labores de administración de los usuarios y equipos**.

Algunos de los aspectos más útiles que se pueden definir por parte del administrador mediante las directivas son:

- Los comandos de inicio de sesión.
- Características de las directivas de seguridad de las cuentas de usuario.
- Configuración de la apariencia de la sesión de usuario.
- Redirección del acceso a ciertas carpetas o archivos centralizados
- Distribución de software a los equipos clientes.
- Permisos otorgados a las cuentas de usuarios y grupos, etc.

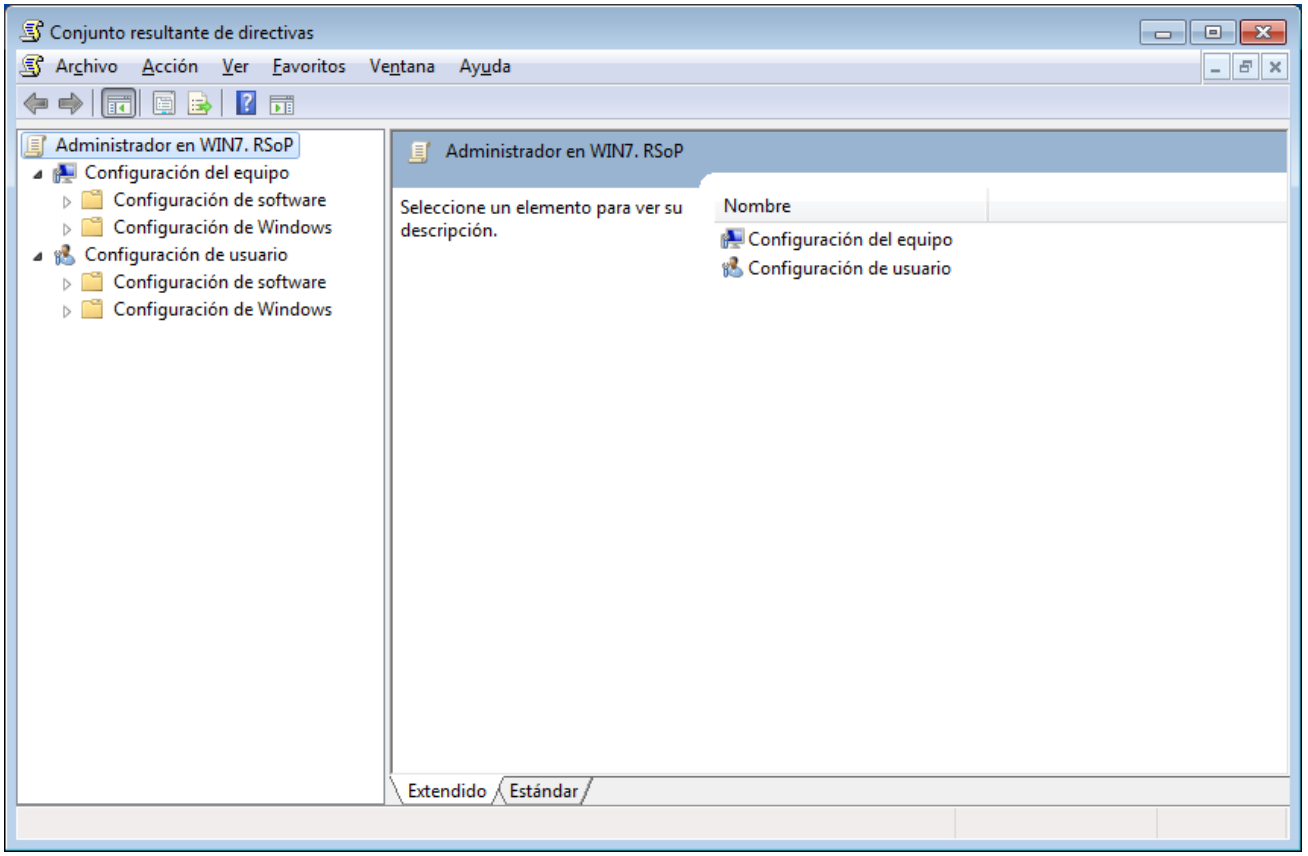
Acumulación de las directicas de grupo

Al existir diferentes niveles de directivas de grupo, estas pueden entrar en conflicto, haciendo que aparezcan efectos no deseados en la gestión del dominio. Al establecer directivas de grupo hay que tener en cuenta el orden de aplicación de las mismas:

- Directiva de grupo local.
- Directiva de grupo de sitio.
- Directiva de grupo de dominio.
- Directiva de grupo de unidad organizativa.

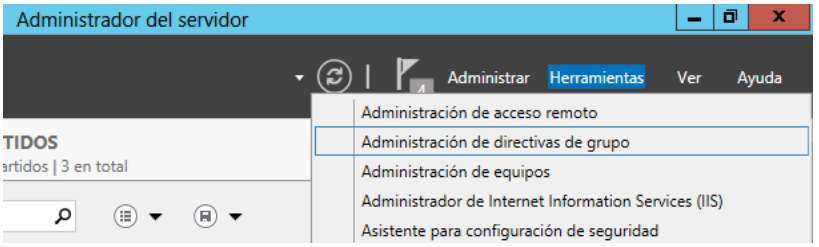
De manera predeterminada cuando existe una contradicción entre las directivas, la que prevalece será la que está en un nivel inferior de la lista anterior. Obviamente, en caso de no existir contradicciones, se aplican todas las directivas.

Si queremos saber las directivas que están aplicándose a un usuario o equipo, ejecutaremos `rsop.msc`. Más información en Technet de Microsoft.



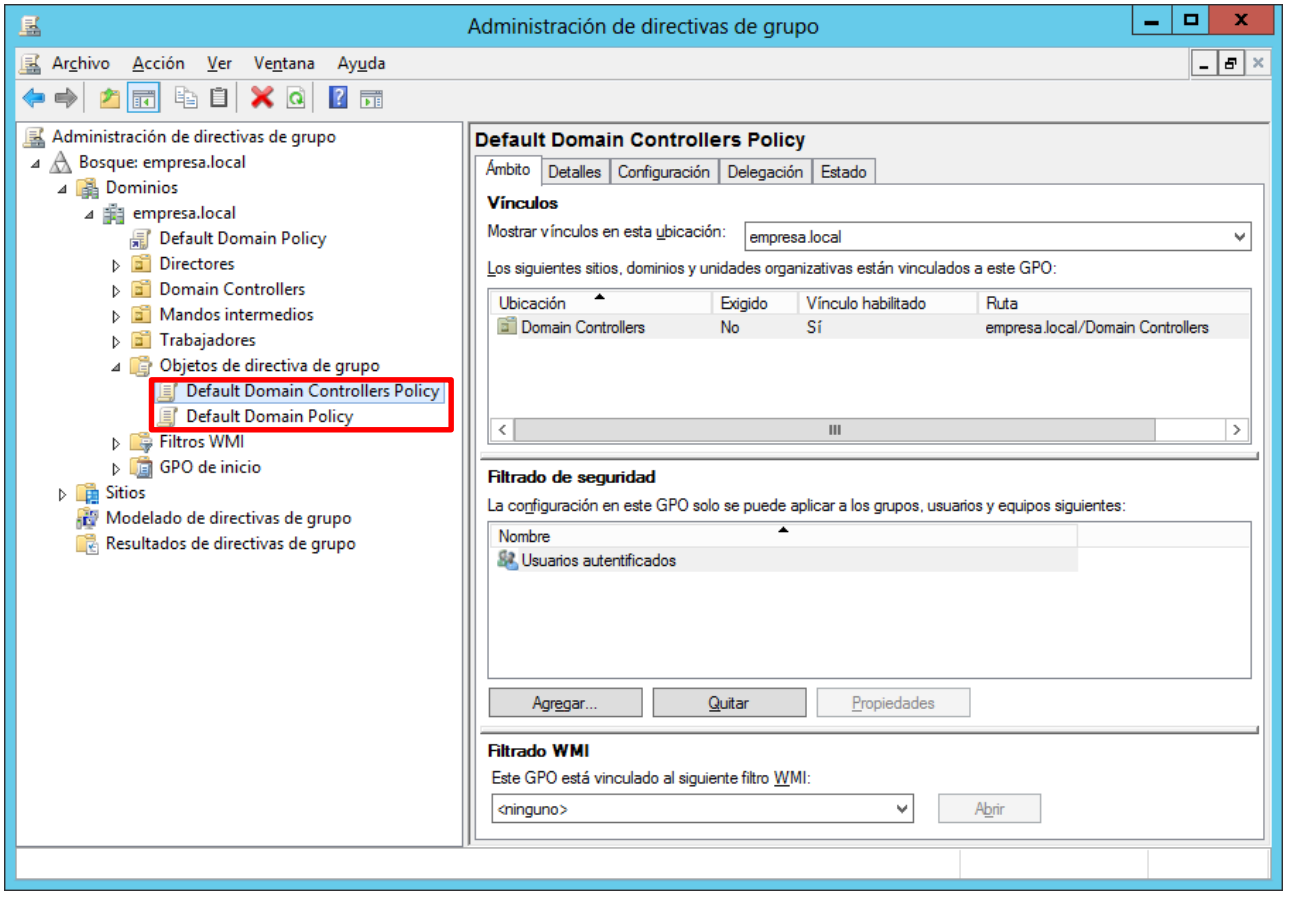
3.1. Edición de las directivas de grupo predefinidas

Para acceder a la consola de administración de directivas haremos clic en 'Administrador del servidor→Herramientas→Administración de directivas de grupo'.



Cuando se pone en marcha un dominio se crean dos directivas de grupo llamadas:

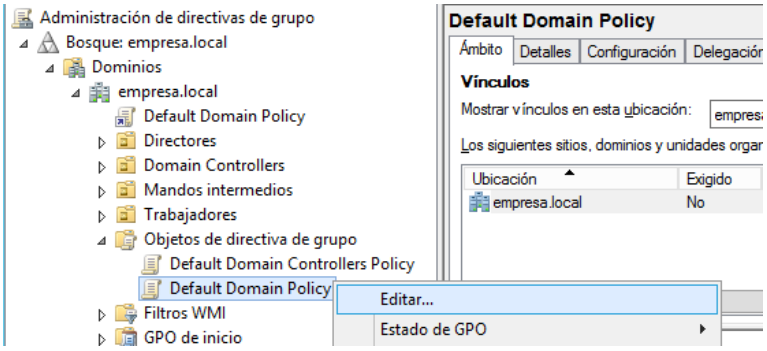
- Default Domain Controllers.
- Default Domain Policy.

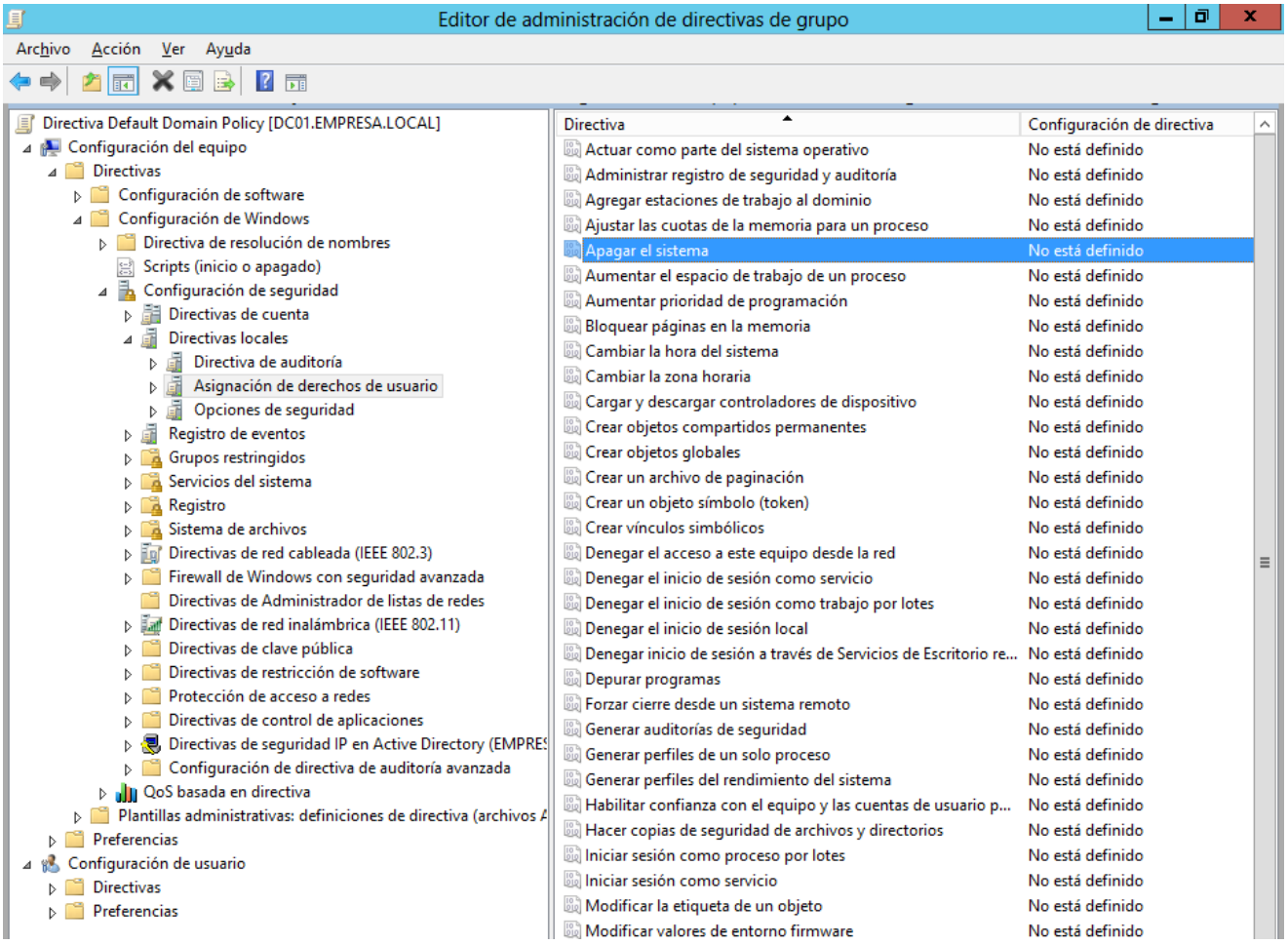


Estas dos directivas establecen la configuración básica de los objetos del dominio, y están vinculadas respectivamente a:

- La unidad organizativa `Domain Controllers`.
- El dominio.

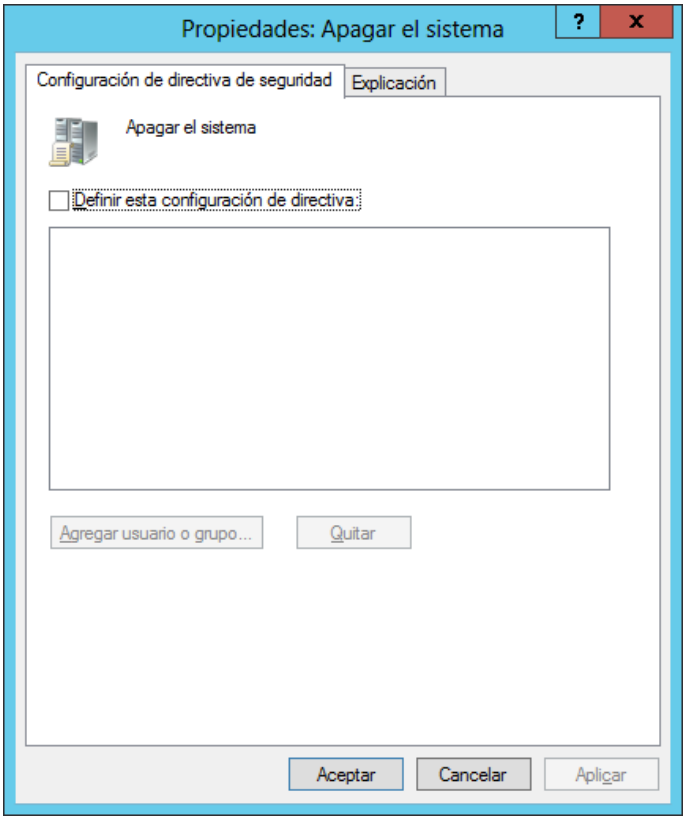
Estos dos GPO se componen de un conjunto muy amplio de directivas, como se puede ver al abrir el editor de directivas.

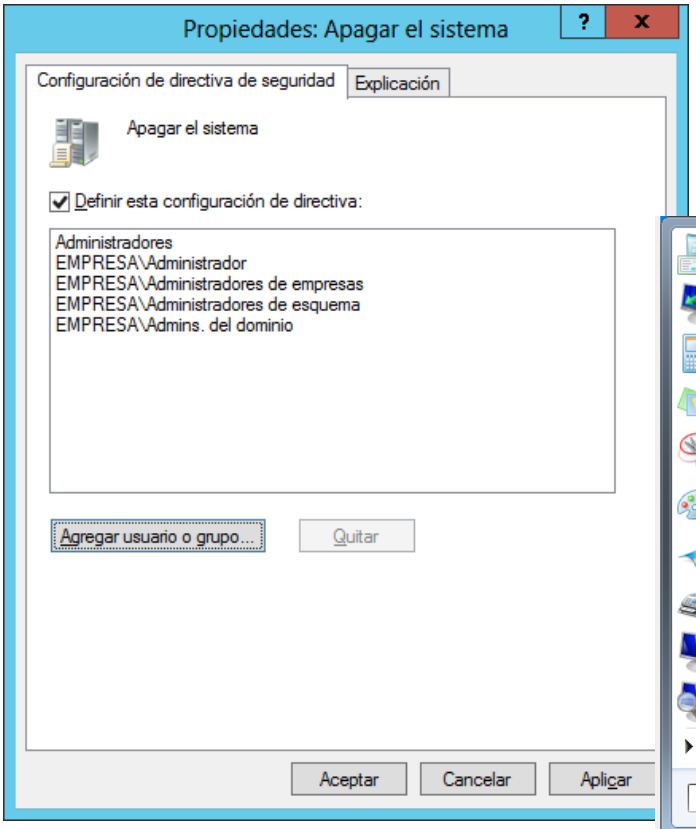




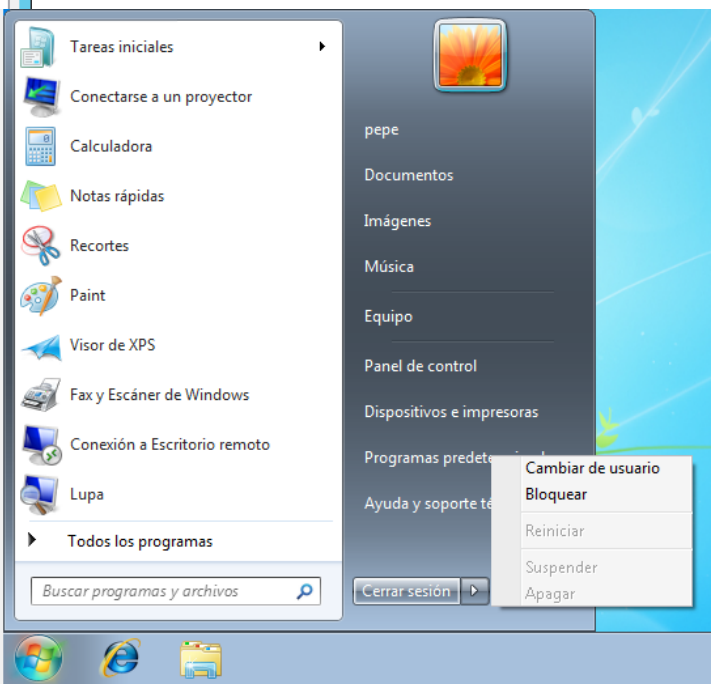
Supongamos que queremos cambiar la configuración de la directiva que aplica sobre el permiso para **apagar el equipo**. En ese caso la buscaríamos entre todo el conjunto de directivas dentro del GPO `Default Domain Policy` y haríamos doble clic sobre ella.

En el cuadro de diálogo que se ha abierto podemos comprobar que esta directiva no está habilitada.





Si la habilitamos y únicamente otorgamos permiso a los administradores del dominio, podremos comprobar que efectivamente un usuario del dominio que inicia sesión en un equipo cliente **no puede apagarlo**, solamente podría un usuario con privilegios de administración.



Para evitar generar un tráfico de gestión excesivo en la red, las directivas de grupo no se actualizan inmediatamente tras su modificación, sino que está establecido un intervalo de 5 minutos entre actualizaciones automáticas. No obstante, este intervalo se puede modificar en las propias directivas de grupo (ver página de Microsoft Technet). De todas maneras, no es necesario modificar este intervalo para comprobar la correcta aplicación de las directivas de grupo, basta con escribir en la consola `cmd`:

```
>>gpupdate
```

o

```
>>gpupdate /force
```

Esta última puede requerir el reinicio del controlador de dominio. (Más información acerca de las opciones y características de `gpupdate` en Technet).

Para ejemplificar todo lo anterior vamos a modificar la *Default Domain Policy* para implementar las siguientes configuraciones en el dominio:

1. Si el usuario se equivoca tres veces al introducir su contraseña, su cuenta queda bloqueada (solo la podrá desbloquear el administrador). Esto protege el sistema de posibles ataques.
2. La contraseña deberá tener un mínimo de 8 caracteres, pero no es necesario obligatoriamente que sean mayúsculas, minúsculas, caracteres alfanuméricos, obligatoriamente, etc.
3. La contraseña que se haya utilizado ya, no podrá volverse a utilizar hasta pasados al menos 10 cambios de contraseña (de esta manera forzamos al usuario a que no 'recicle' contraseñas antiguas, incrementando la seguridad del sistema).
4. El usuario debe cambiar la contraseña cada seis meses, al establecer una 'vida útil' de las contraseñas tenemos un sistema más seguro, ya que en caso de que alguien haya averiguado la contraseña del usuario, y no se haya detectado, como tarde a los seis meses, perderá el acceso a la cuenta.

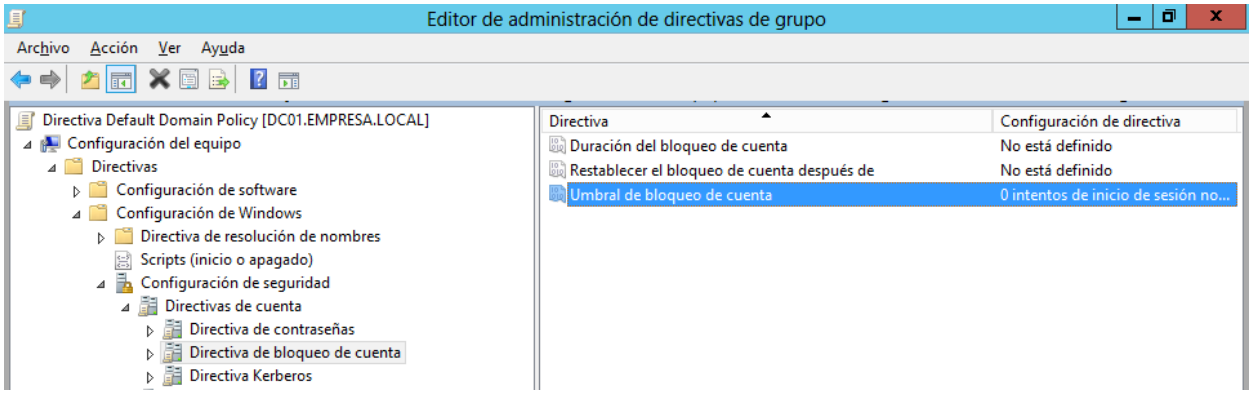
En las siguientes subsecciones se examina la manera de proceder para llevar a cabo estas configuraciones del sistema.

Las directivas de seguridad relacionadas con las contraseñas no pueden aplicarse sobre GPOs distintas de la *Domain Default Policy*.

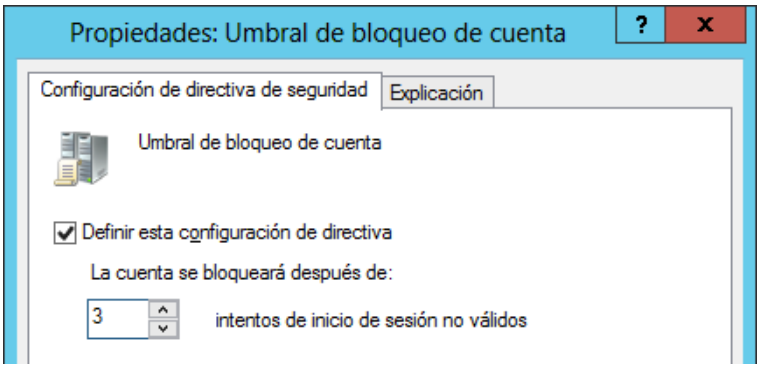
Si por ejemplo queremos que diferentes usuarios del dominio tengan diferentes características de sus contraseñas, deberemos utilizar la *Fine-Grained Password Policy*, la cual es algo compleja de configurar. En el siguiente enlace tenéis una guía que explica paso a paso cómo crearlas y configurarlas para conseguir la funcionalidad comentada anteriormente. No obstante la configuración de la *Fine-Grained Password Policy* queda fuera del alcance de este curso.

3.1.1. Bloqueo de cuenta al introducir en tres ocasiones una contraseña errónea

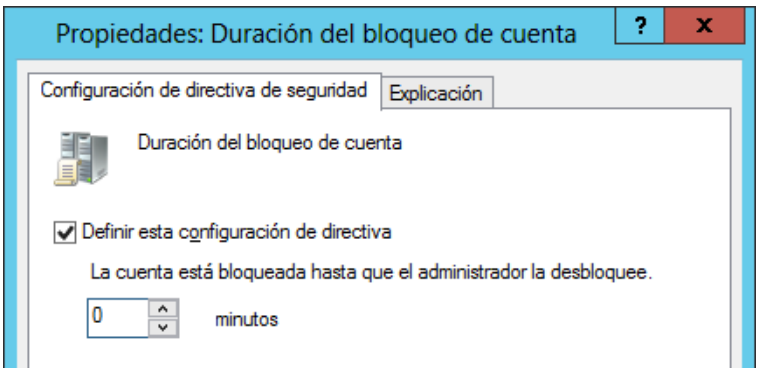
En primer lugar editaremos el GPO 'Default Domain Policy' para configurar la directiva de bloqueo de cuenta. Esta se halla en 'Configuración del equipo'→'Directivas'→'Configuración de Windows'→'Directiva de bloqueo de cuenta'→'Umbral de bloqueo de cuenta'



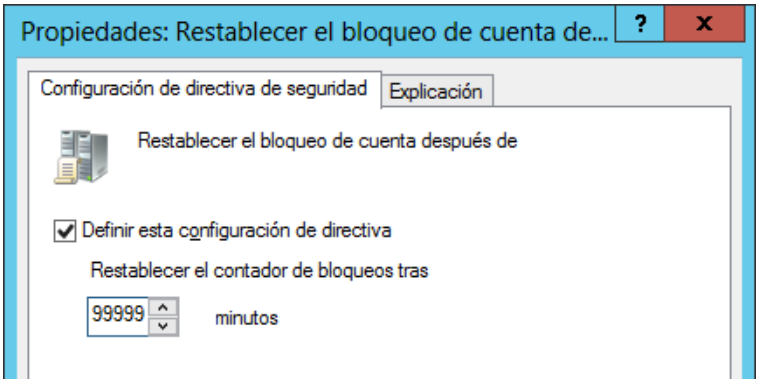
Modificamos el valor de umbral a '3 intentos' de inicio de sesión erróneos.



Además configuraremos la duración del bloqueo, donde un valor de 0 indica que la cuenta deberá ser desbloqueada manualmente por el administrador.

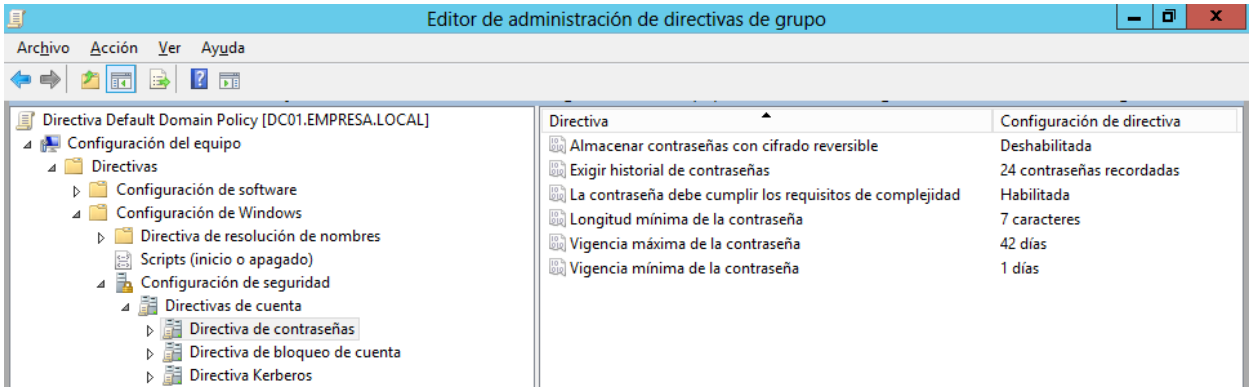


Finalmente también configuraremos el tiempo que debe transcurrir entre intentos para que el contador de fallos de inicio de sesión vuelva a cero antes de que se bloquee la cuenta. Pondremos el máximo valor permitido.

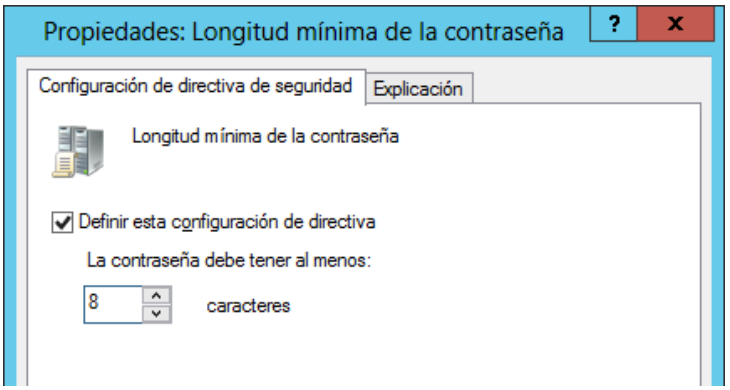


3.1.2. Longitud de la contraseña

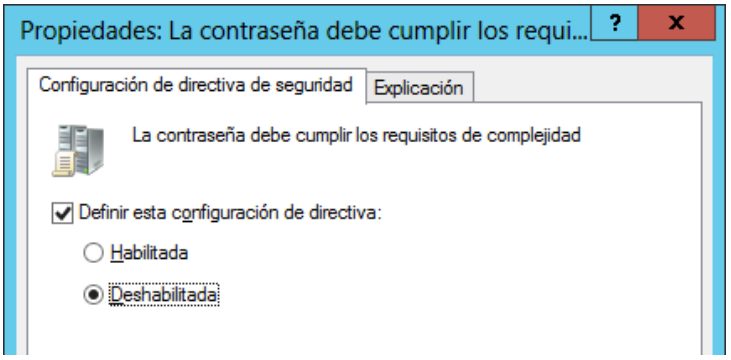
Como en el caso anterior editaremos el GPO 'Default Domain Policy' para configurar la longitud y complejidad de las contraseñas.



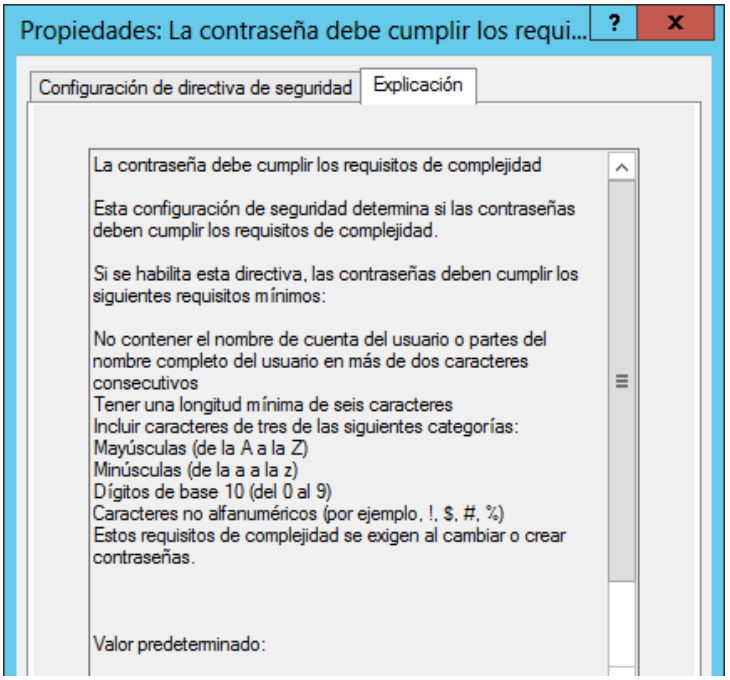
Modificamos el valor de la longitud a 8 caracteres.



A continuación deshabilitamos los requisitos de complejidad de las contraseñas.

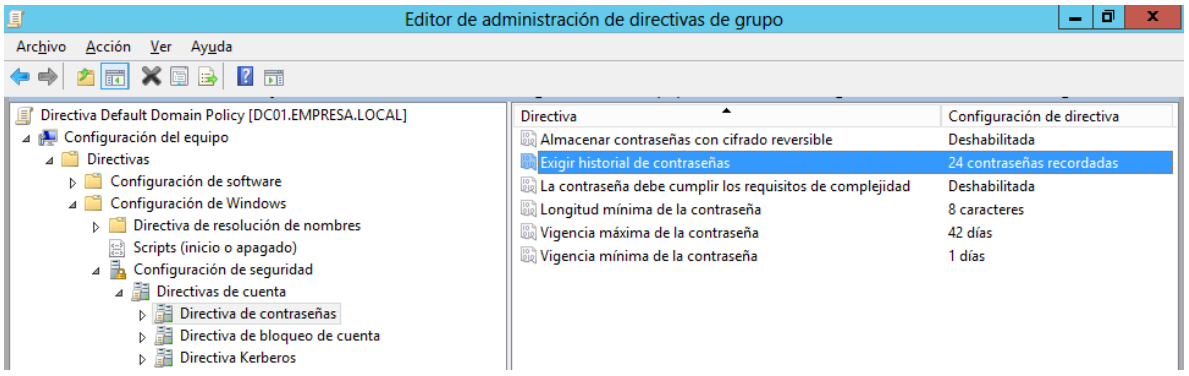


En esta imagen se puede ver las características de complejidad que aplica esta directiva cuando está habilitada.

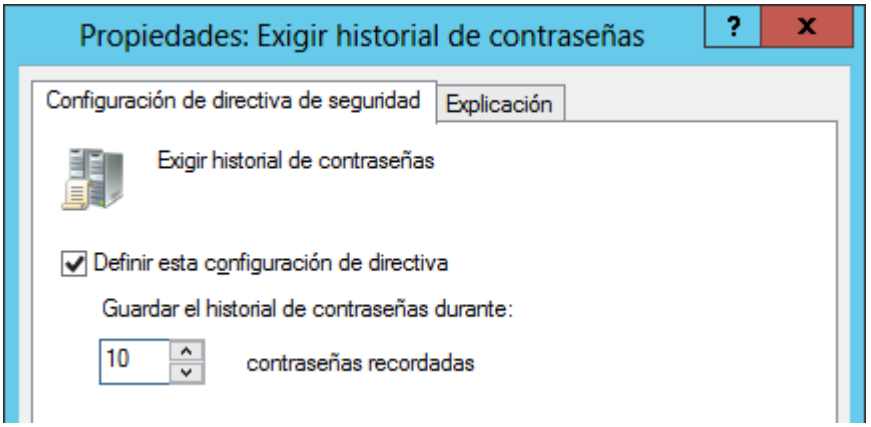


3.1.3. Historial de la contraseña

Editamos de nuevo el GPO 'Default Domain Policy' y accedemos a las directivas de contraseñas.

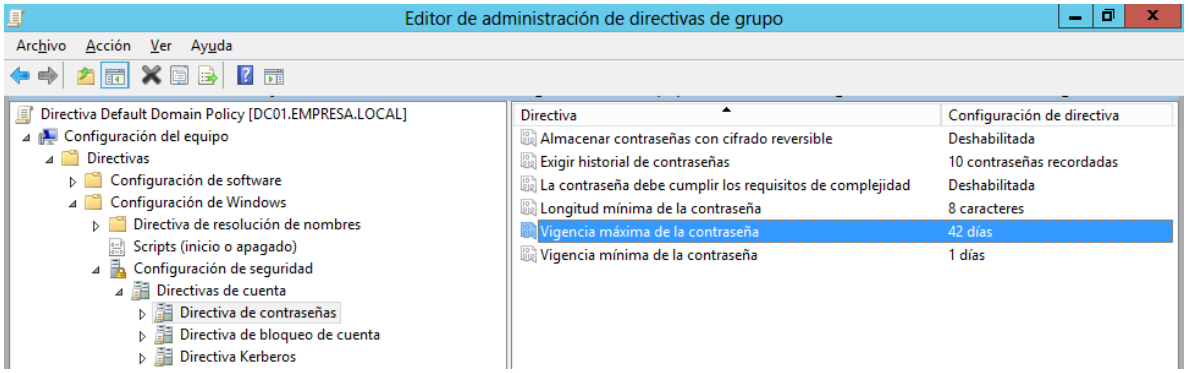


Y modificamos el número de contraseñas diferentes que deben utilizarse antes de poder repetir una contraseña.

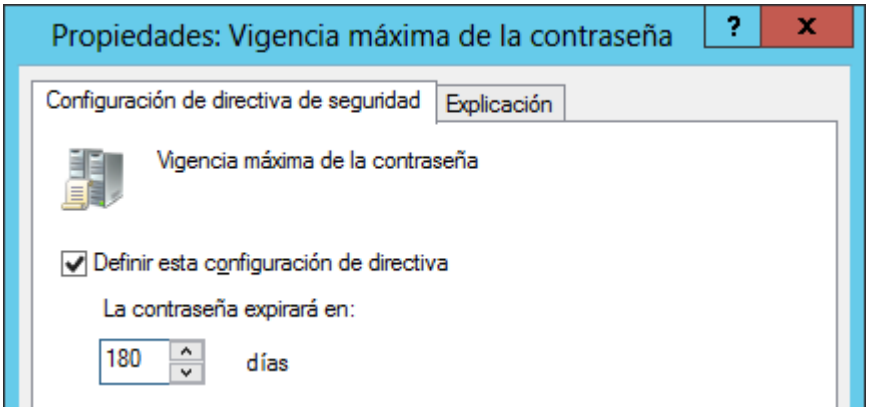


3.1.4. Vigencia de la contraseña

Como en casos anteriores accedemos a las directivas de contraseñas.



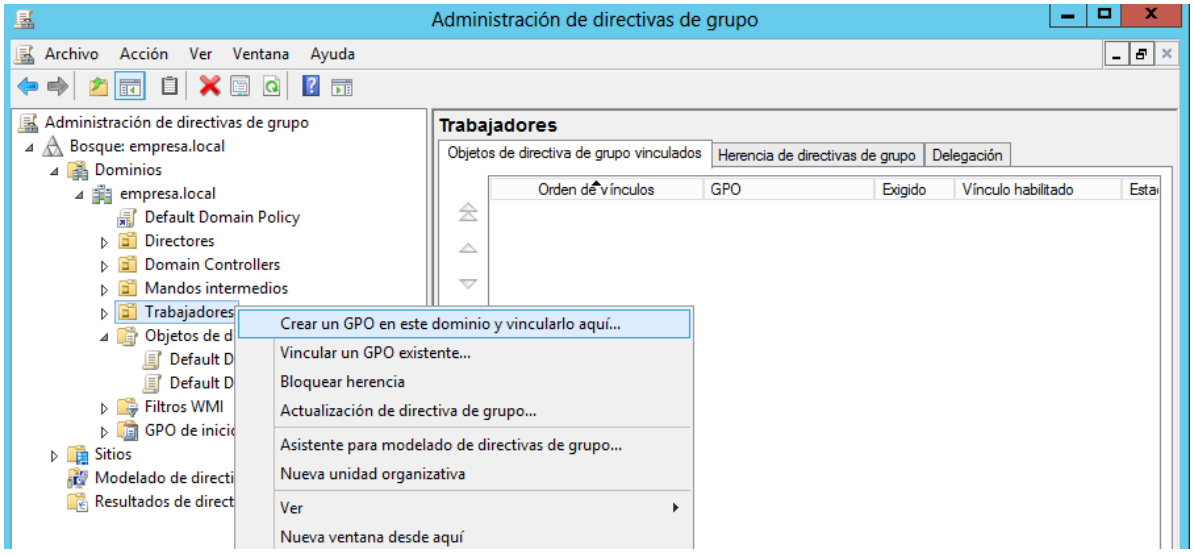
Cambiamos la duración máxima de las contraseñas a 180 días -6 meses- .



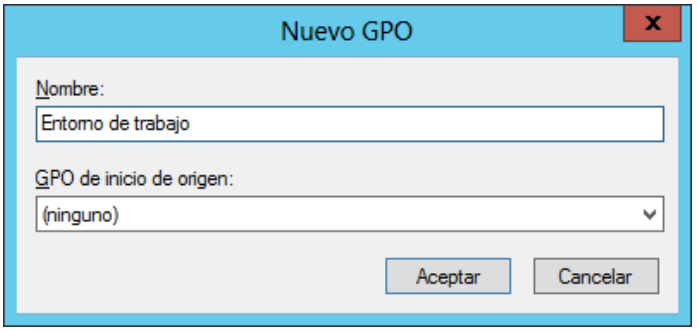
3.2. Creación de Directivas de Grupo

Para crear una directiva de grupo abriremos la consola de administración de directivas como en el punto anterior Administrador del servidor→Herramientas →Administración de directivas de grupo.

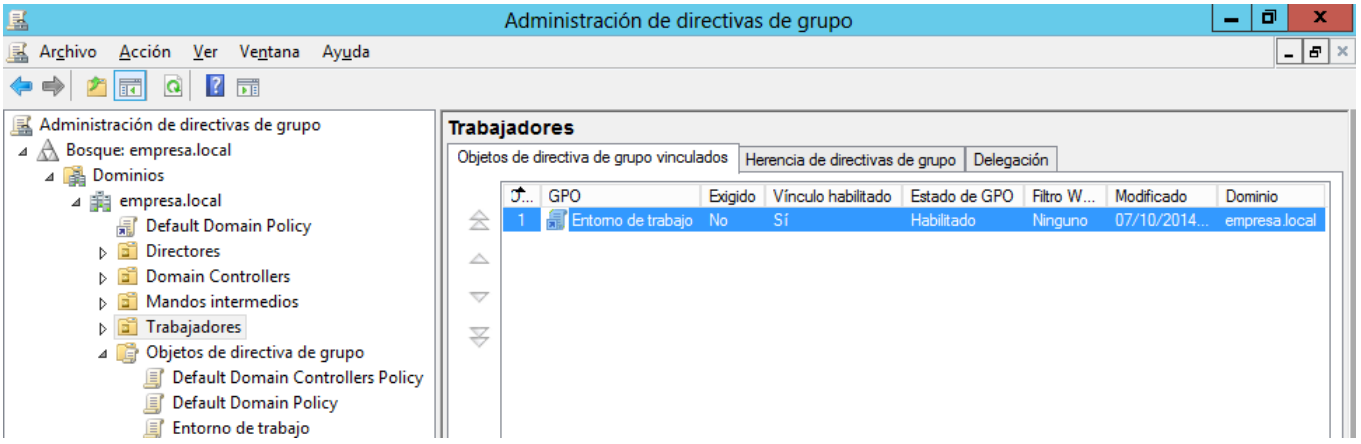
Supongamos que queremos crear una Directiva de Grupo sobre la unidad organizativa 'Trabajadores' que creamos en el tema anterior. Hacemos clic con el botón secundario y escogemos la opción 'Crear un GPO en este dominio y vincularlo aquí'.



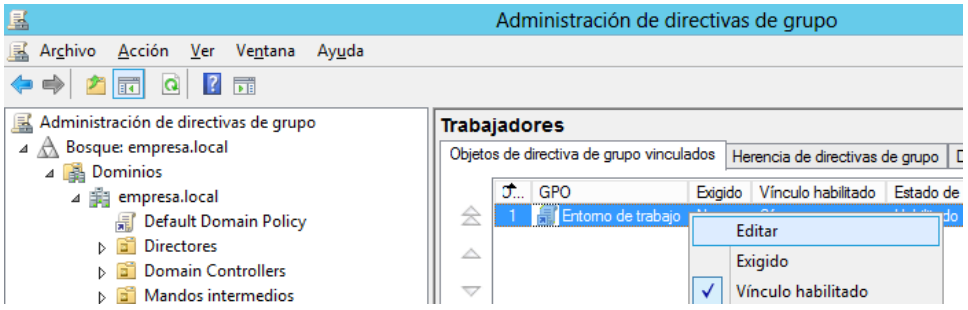
Aparecerá un cuadro de diálogo e introduciremos el nombre que le queremos dar, por ejemplo 'Entorno de trabajo', ya que posteriormente utilizaremos esta directiva para configurar un entorno de trabajo homogéneo en todos los usuarios que pertenecen a la Unidad Organizativa 'Trabajadores'.



La nueva directiva aparecerá en el panel de detalles.



Seleccionamos el GPO y hacemos clic con el botón derecho, escogiendo la opción 'Editar'.



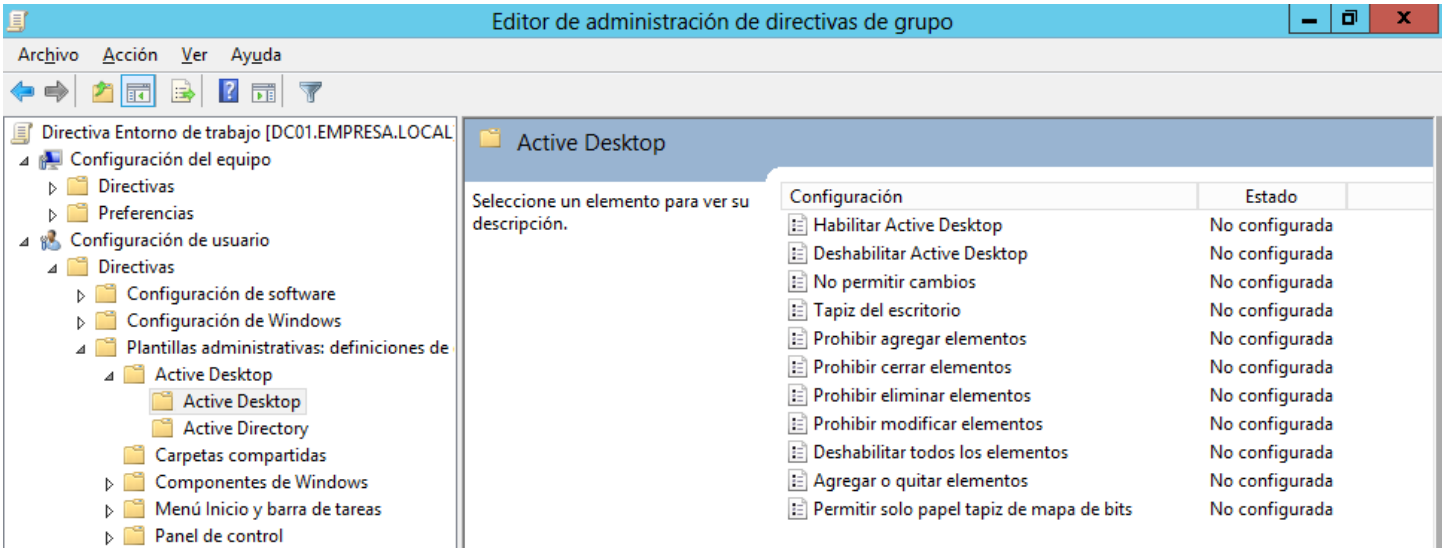
Con la nueva directiva vamos a establecer las siguientes configuraciones:

1. Todos los miembros de la unidad organizativa 'Trabajadores' tendrán un fondo de escritorio 'corporativo' que se instalará de manera automática y que no podrá ser modificado.
2. Los miembros de la unidad organizativa 'Trabajadores' no pueden abrir la consola de comandos.

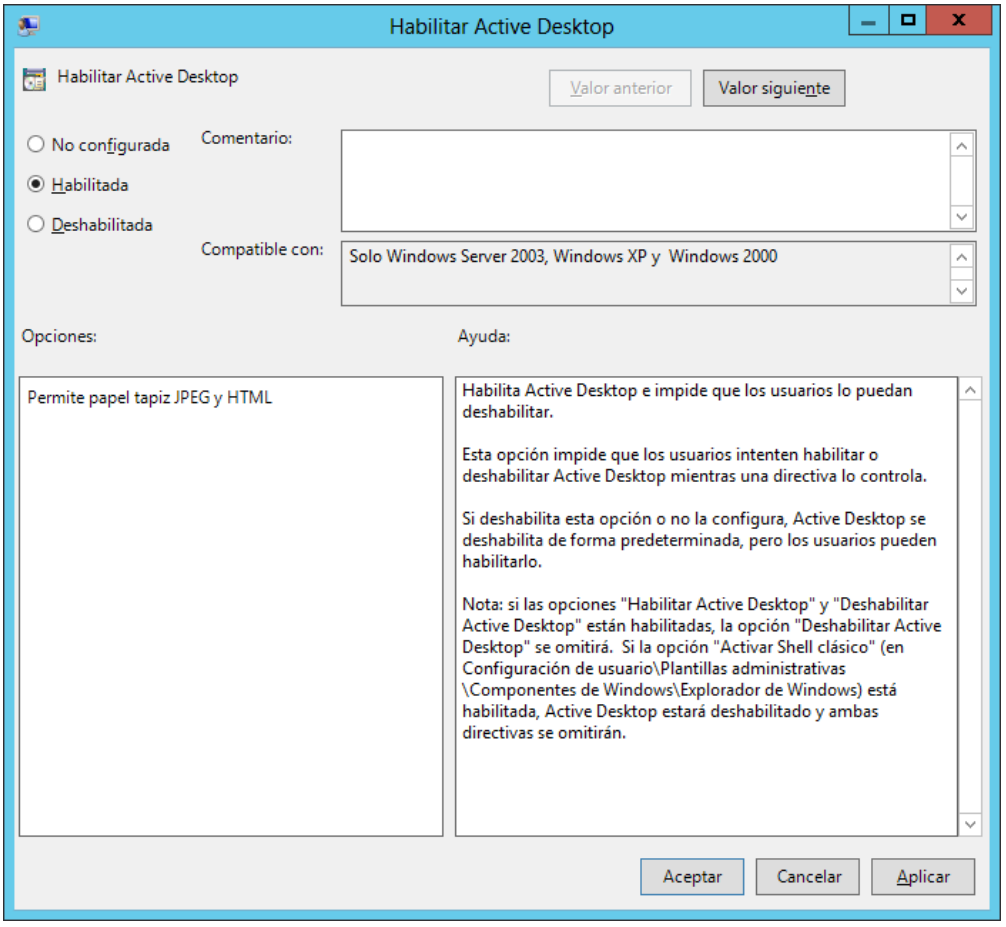
En las siguientes subsecciones se examina la manera de proceder para llevar a cabo estas configuraciones del sistema.

3.2.1. Fondo de escritorio obligatorio

Para modificar de una manera centralizada el fondo de escritorio de los usuarios de la unidad organizativa 'Trabajadores' debemos editar la directiva 'Entorno de Trabajo' y acceder a 'Configuración del usuario'→'Plantillas administrativas'→'Active Desktop'→'Active Desktop'.

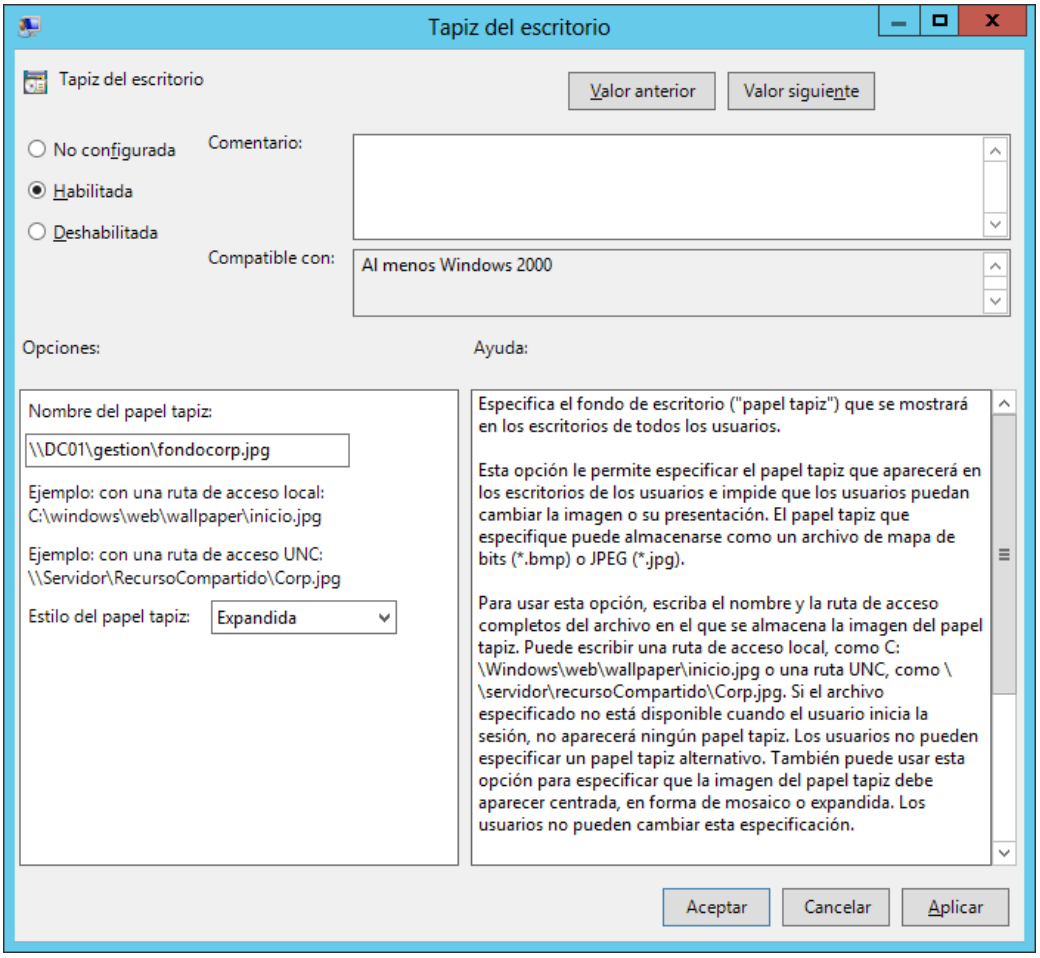


Habilitamos el Active Desktop, el cual permite poner como fondo de escritorio imágenes jpg o ficheros HTML.



Vamos a impedir también que los usuarios puedan modificar el fondo de escritorio.

Indicamos la ruta en la que se halla la imagen que queremos poner como fondo de escritorio. En este caso se llama fondocorp.jpg (podéis descargárosla aquí: Maple Leaf by Petr Kratochvil) y está en la carpeta compartida 'gestion' albergada en el servidor.



La imagen debe hallarse en una carpeta compartida en red (preferiblemente en el servidor por cuestiones de disponibilidad) donde todos los usuarios del dominio tengan permiso de lectura.

Además, se recomienda que la ruta se introduzca en formato UNC del tipo:

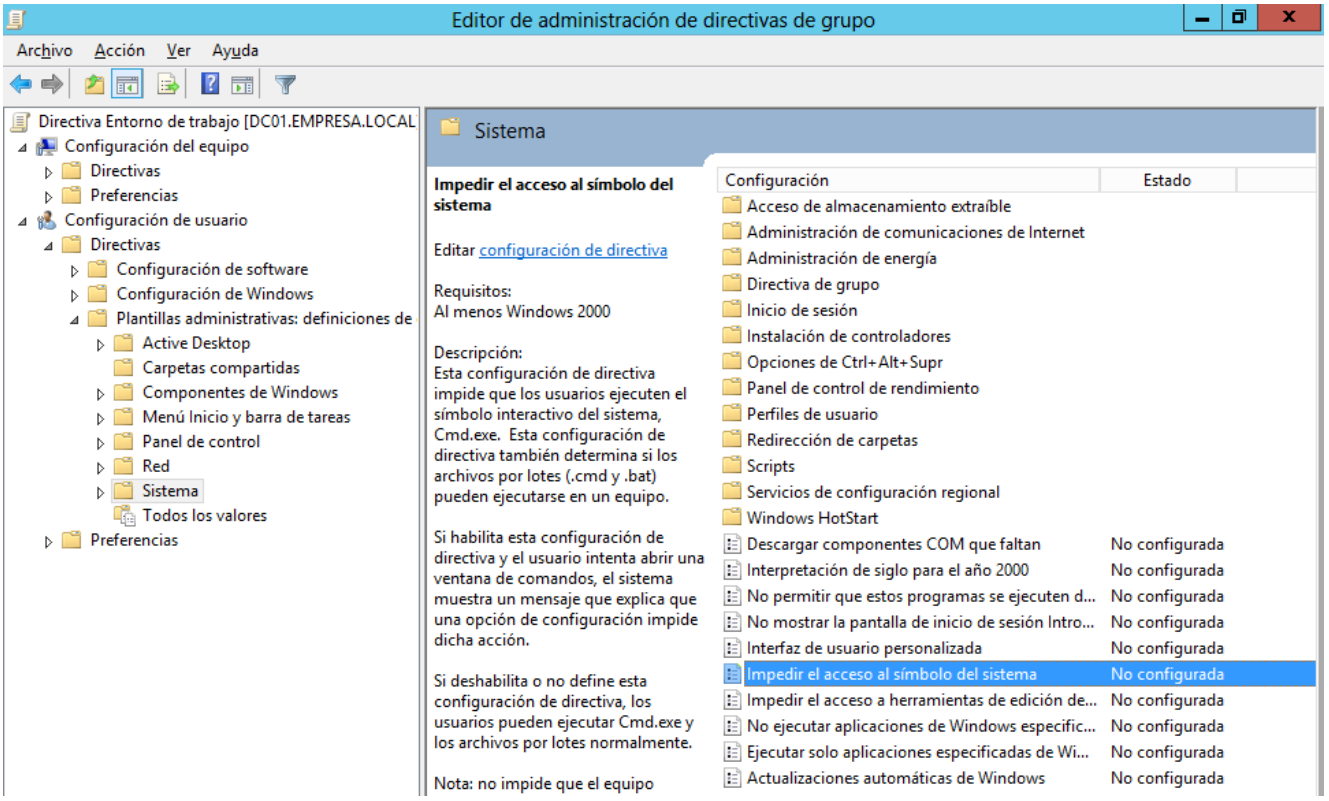
```
\\DC01\gestion\fondocorp.jpg
```

no en formato

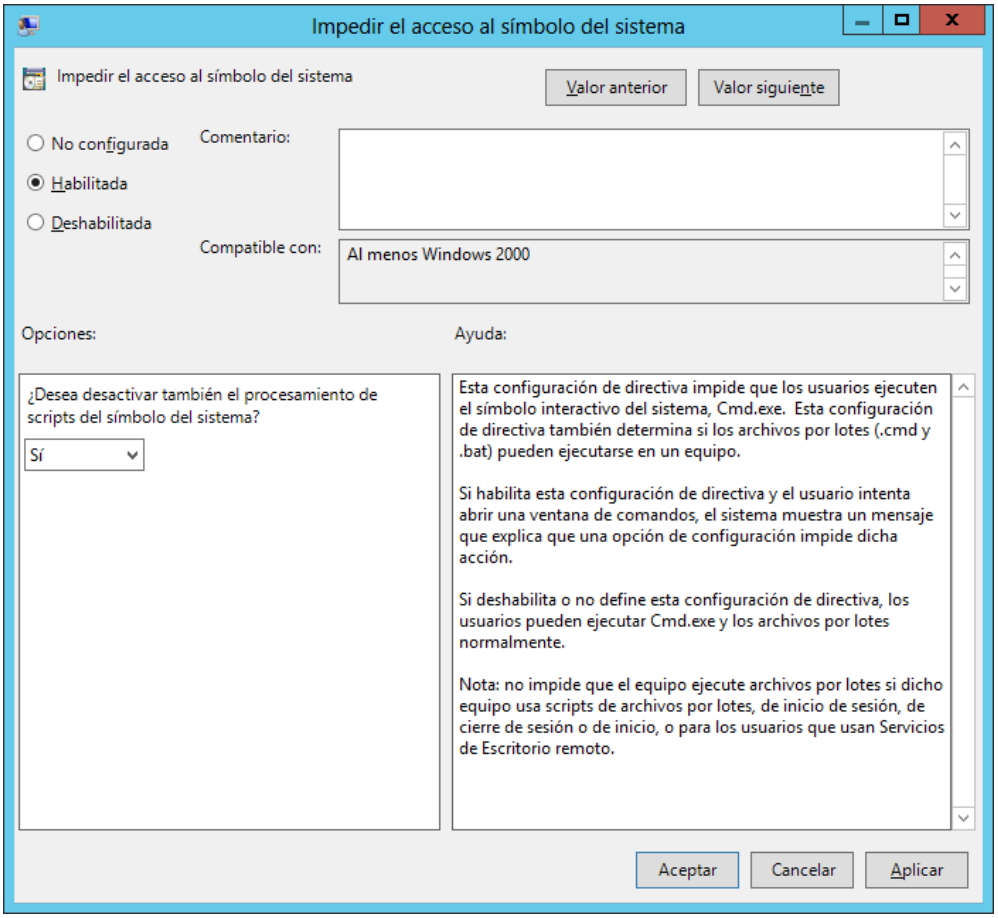
```
\\192.168.0.1\gestion\fondocorp.jpg
```

3.2.2. Bloqueo de la línea de comandos

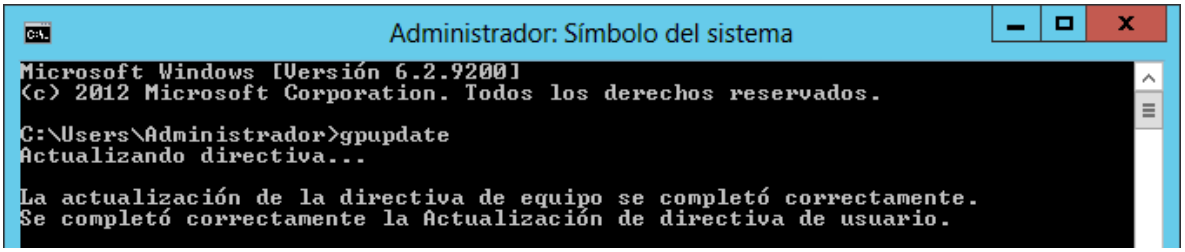
Para bloquear la línea de comandos editaremos el GPO correspondiente accediendo a 'Configuración del usuario'→'Directivas→Plantillas administrativas'→'Sistema'.



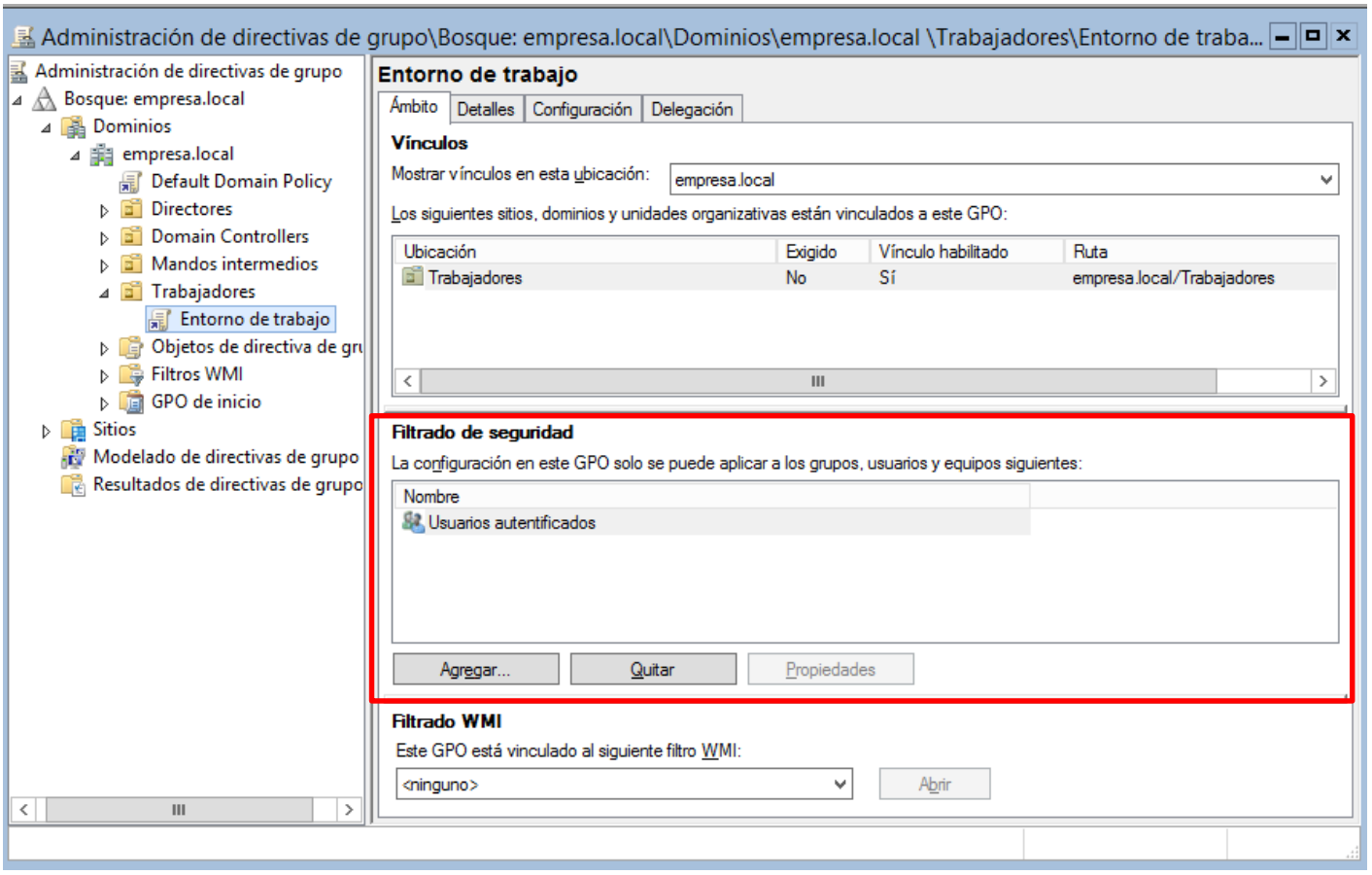
Habilitamos el bloqueo y el procesamiento de scripts del símbolo del sistema.



Finalmente ya solo queda actualizar mediante `gpupdate` las directivas modificadas en el GPO 'Trabajadores'.



Recordad que únicamente afectarán a los miembros de la unidad organizativa trabajadores independientemente del grupo al que pertenezcan, si no explicitamos lo contrario en el campo 'Filtrado de Seguridad'.

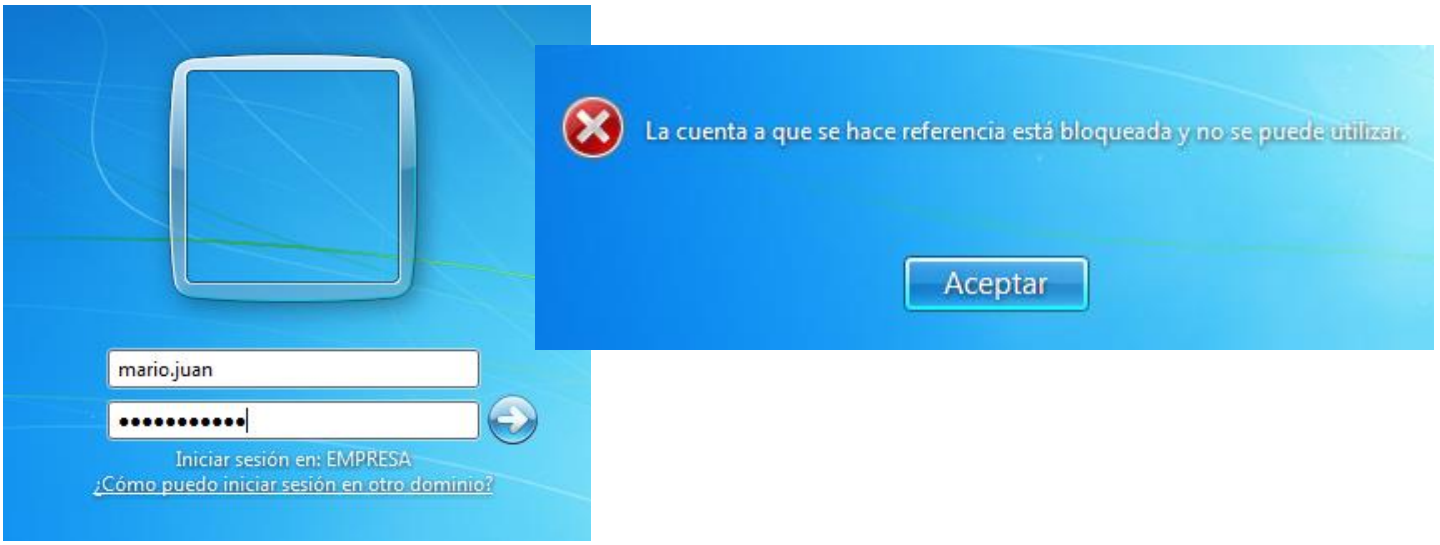


3.2.3. Comprobación de las directivas establecidas

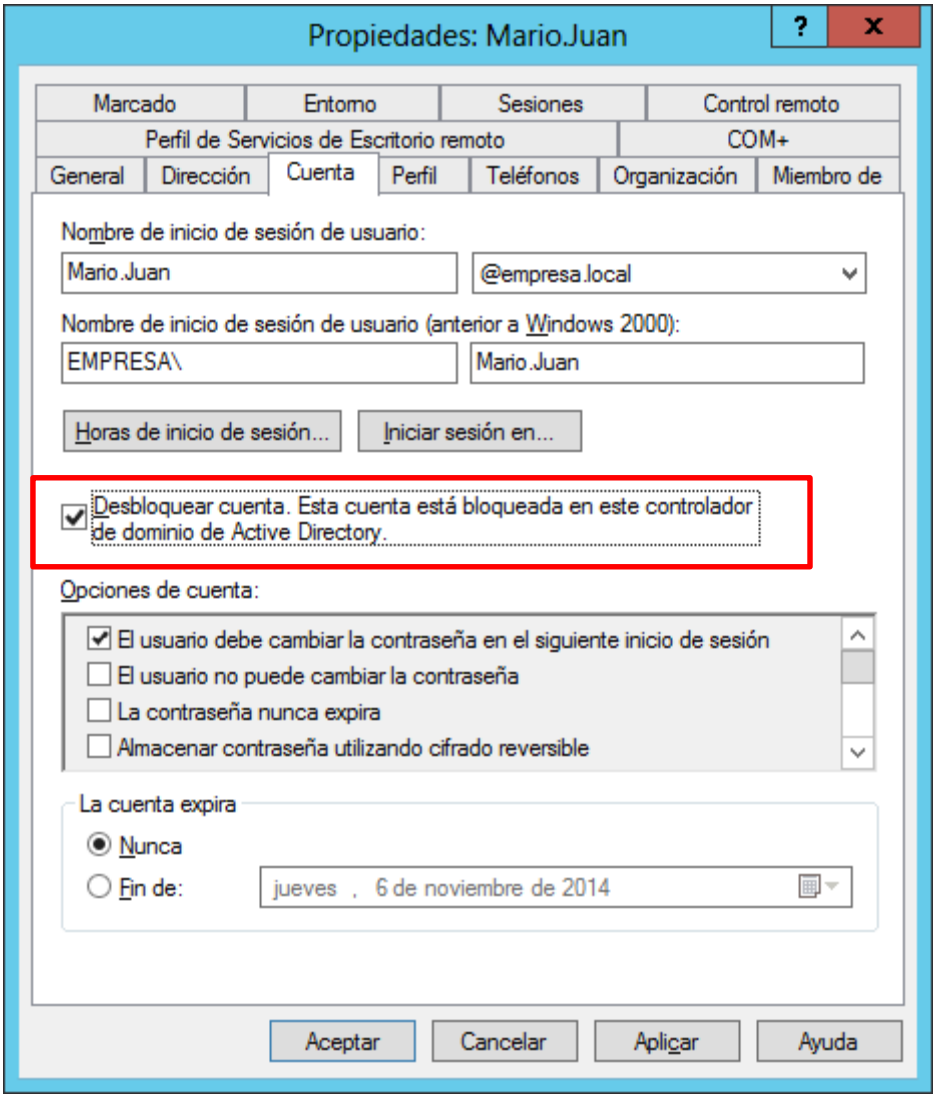
Ahora comprobaremos que las directivas se han aplicado correctamente. Para ello utilizaremos un usuario cualquiera dentro de la unidad organizativa 'Trabajadores' que es sobre la que se **aplican el GPO creado 'Entorno de Trabajo'**, y obviamente el GPO Default Domain Policy, que hemos editado. En este caso se harán las pruebas con el usuario `Mario.Juan` (su contraseña inicial la cual podemos consultar en el fichero usuarios.csv es ABC123!).

Bloqueo de cuenta

La primera directiva que hemos aplicado consistía en bloquear la cuenta indefinidamente al introducir en tres ocasiones la contraseña incorrectamente. Nos equivocamos voluntariamente al iniciar sesión en un equipo cliente y la cuenta se acaba bloqueando.

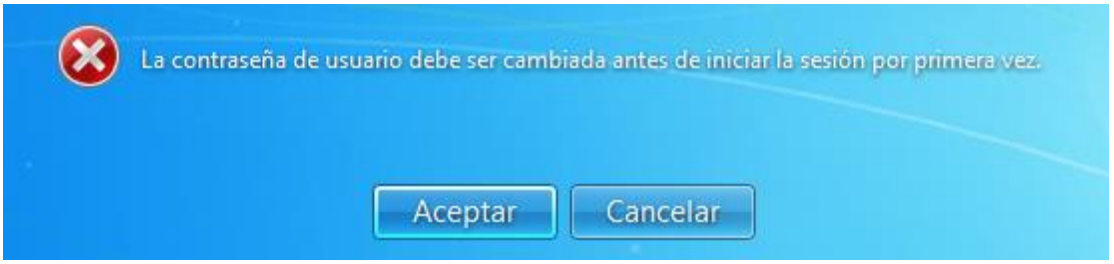


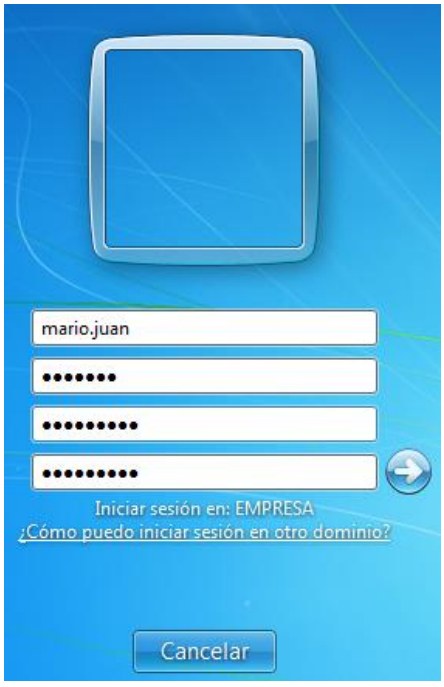
Comprobamos en el controlador de dominio que efectivamente está bloqueada y la desbloqueamos.



Longitud de contraseña

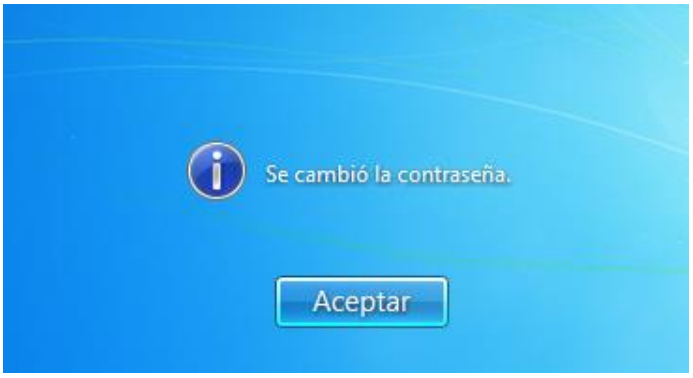
Una vez desbloqueada la cuenta, iniciamos sesión con este usuario y lo primero que se nos indica es que debemos cambiar la contraseña, tal y como se configuró en el tema anterior al crear los usuarios del dominio.





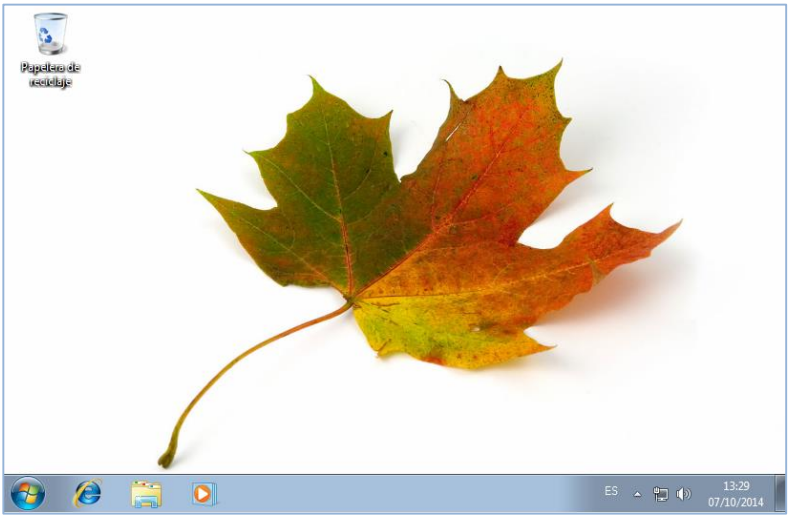
Introducimos una nueva contraseña (`mariojuan`) sin caracteres especiales ni números, y longitud al menos de 8 caracteres.

El sistema nos indica que la contraseña se cambió correctamente.



Fondo de escritorio obligatorio

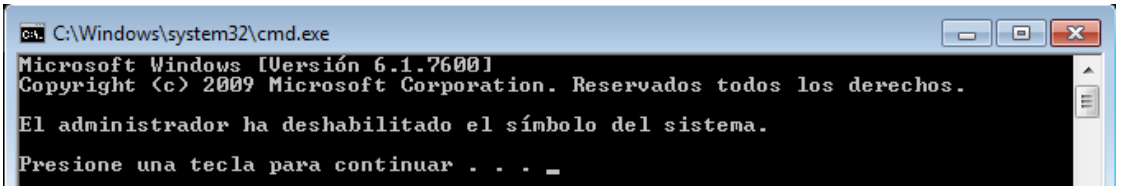
Al iniciar sesión se carga el fondo de escritorio definido con la directiva de grupo, y además el usuario no puede modificarlo.



Para que esta directiva funcione correctamente es **imprescindible** instalar en los equipos clientes Windows 7 un parche de Microsoft que resuelve el error que impide que se aplique esta directiva.

Bloqueo de la línea de comandos

Una vez iniciada la sesión, si se intenta ejecutar `cmd` aparece el siguiente mensaje.



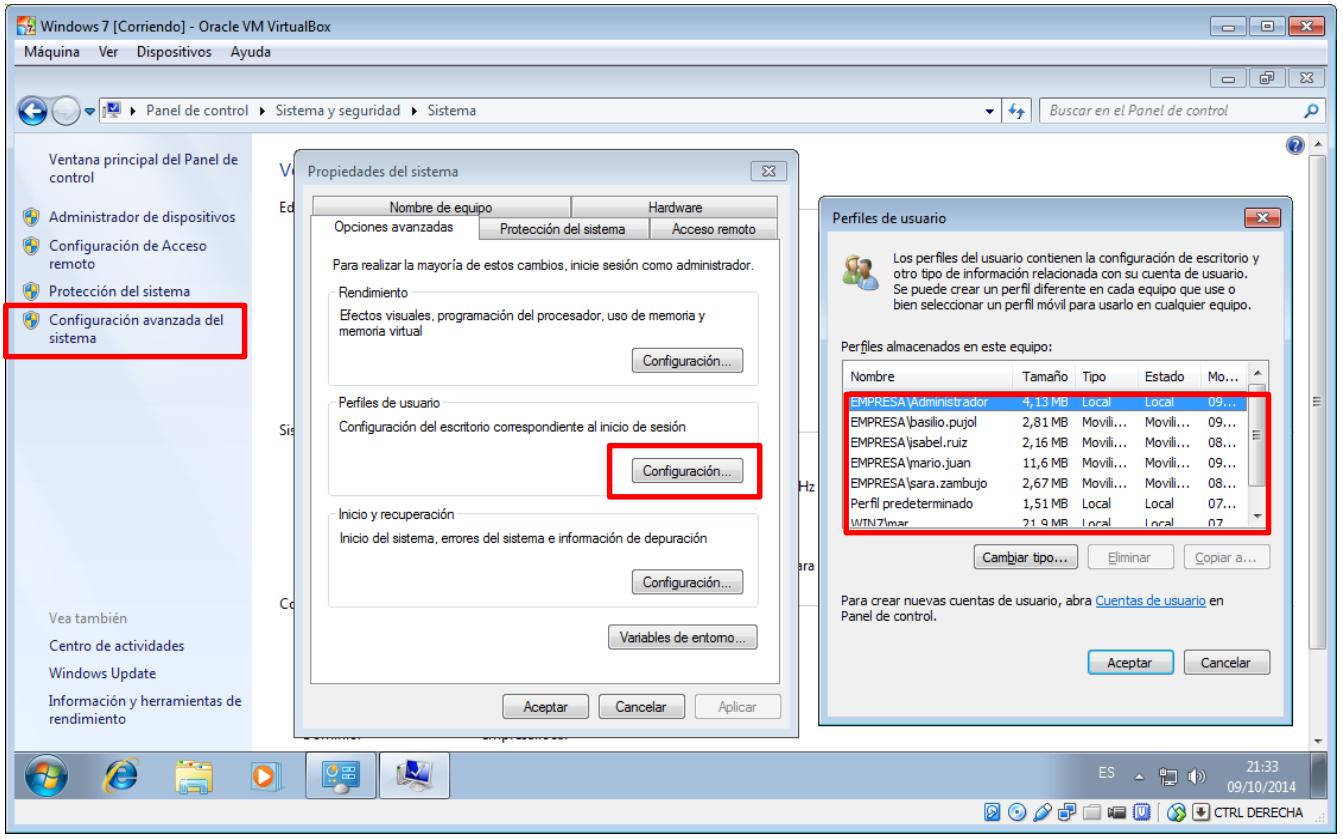
Podéis comprobar que las otras dos directivas establecidas también funcionan correctamente.

4. Perfiles

Podemos definir un perfil como aquellos aspectos de configuración del equipo y del entorno de trabajo propios del usuario y que además son exportables a otras máquinas de manera transparente al mismo. En otras palabras, mediante los perfiles conseguimos que el usuario **independientemente** del equipo en el que inicie la sesión disponga de un entorno de trabajo similar. Todo esto se entenderá mejor con los ejemplos preparados en las secciones siguientes.

Existen tres tipos de perfiles:

1. Perfiles locales: se almacenan en el equipo, y configuran el entorno de trabajo de cada usuario. No los abordaremos en este curso ya que lo que nos interesa es la gestión centralizada de recursos.



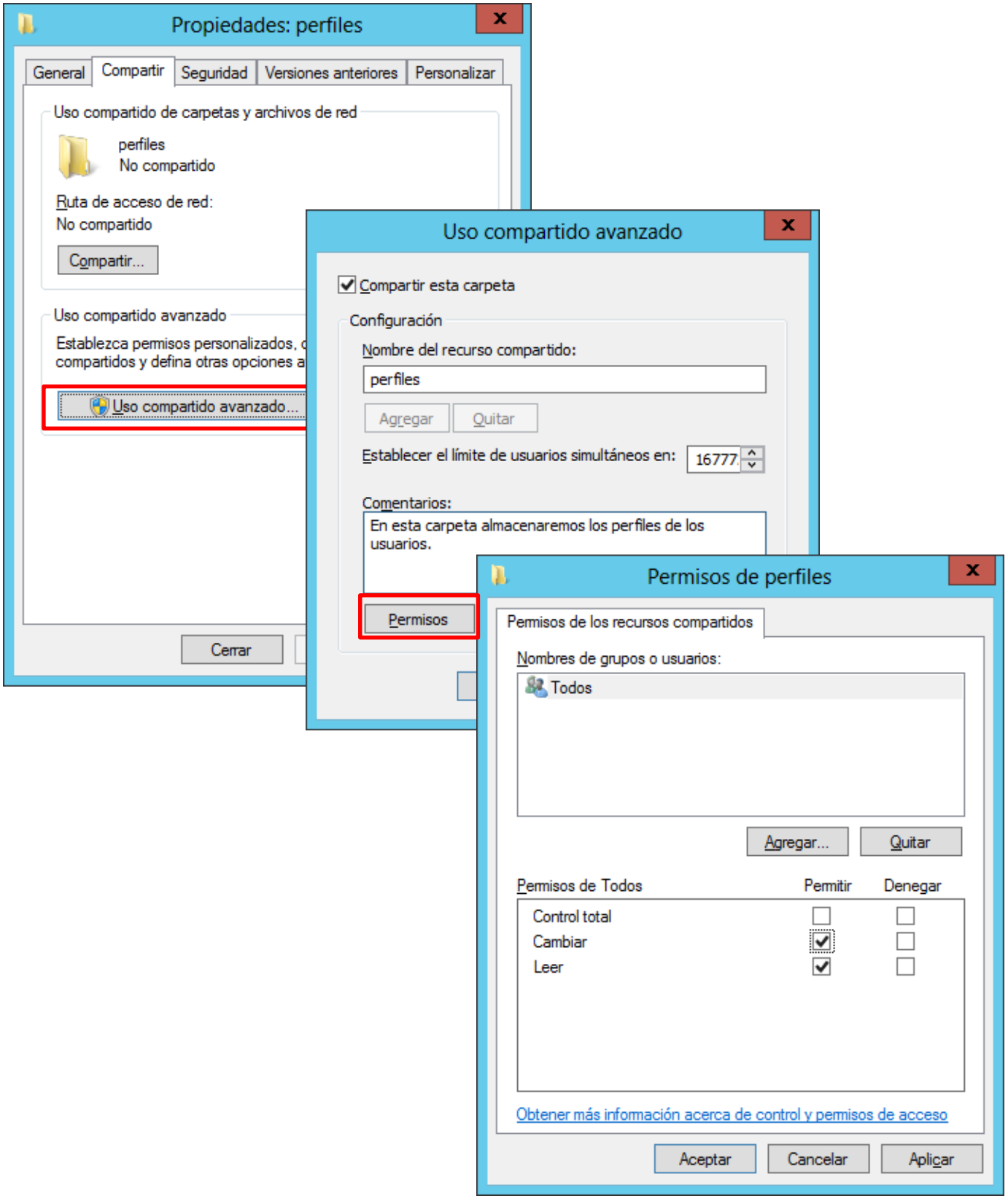
2. Perfiles móviles: el usuario configura el entorno de trabajo a su gusto en un equipo, y al iniciar sesión en cualquier otra estación de trabajo, la configuración se importa y aplica a ese nuevo equipo. Abordaremos este tipo de perfiles en el apartado 5.1

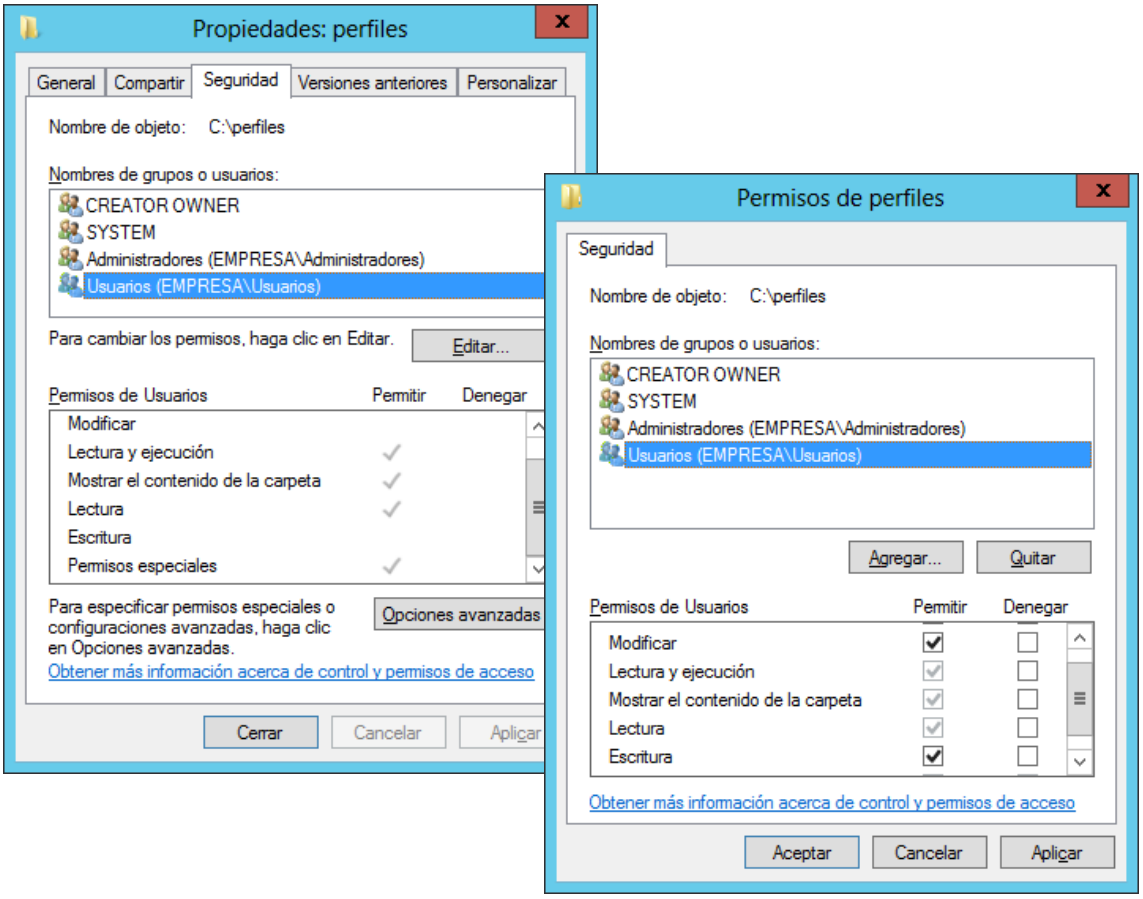
3. Perfiles obligatorios: un usuario con permisos de administración define la configuración del entorno de trabajo, y se aplica a los usuarios del dominio. Estos pueden modificarla durante la sesión, pero al iniciar otra sesión, se vuelve a cargar la configuración del perfil obligatorio. En lugar de trabajar con perfiles obligatorios, en el apartado anterior hemos visto cómo configurar entornos de trabajo definidos para los miembros de una unidad organizativa de una manera más cómoda y potente.

4.1. Perfiles móviles

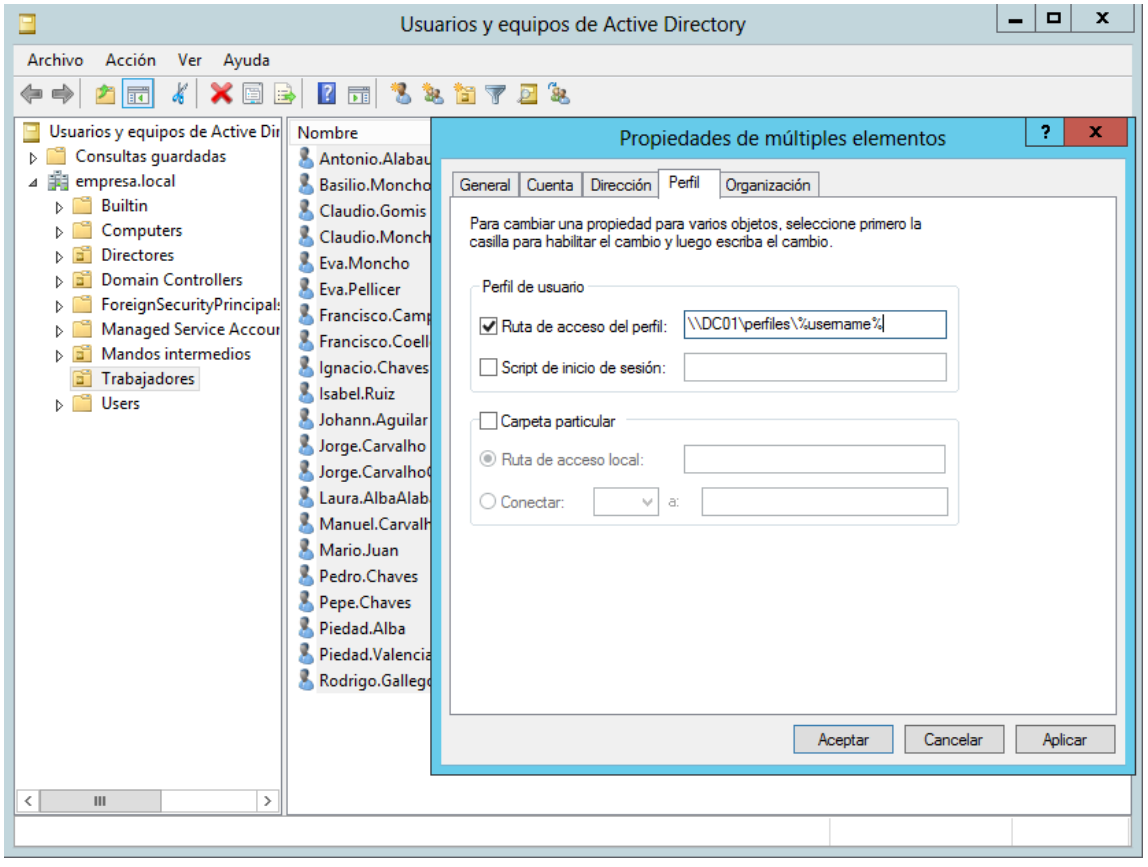
Como se ha comentado en el apartado anterior, los perfiles consisten en una serie de ficheros de configuración del entorno de trabajo, que se aplican a todos los equipos de la red desde donde pueda comenzar sesión el usuario. Estos ficheros de configuración deben almacenarse en una ubicación accesible por los equipos clientes, como por ejemplo el controlador de dominio.

Concretamente, almacenaremos los perfiles en una carpeta del servidor denominada 'Perfiles', y que tendremos que compartir en red con los permisos adecuados para que al iniciar sesión el sistema pueda cargar la configuración, y al cerrar sesión, en su caso, se guarden las modificaciones del perfil realizadas.



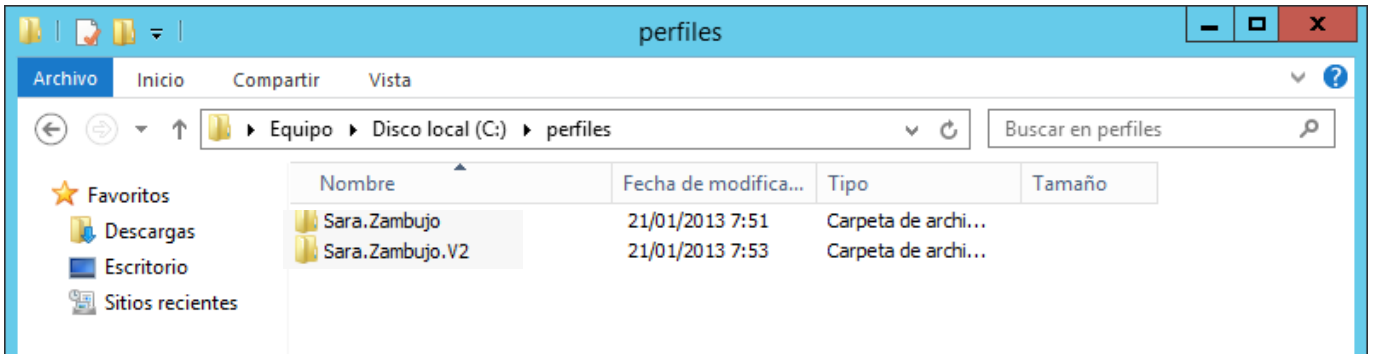


Ya disponemos de una ubicación en red con los permisos suficientes donde se almacenarán los perfiles. Ahora hay que indicar en las cuentas de usuario la ubicación de dicha carpeta. Para ello, iremos a cada una de las tres unidades organizativas que creamos en prácticas anteriores ('Directores', 'Mandos Intermedios' y 'Trabajadores') y seleccionaremos todos los usuarios. A continuación, con el botón secundario haremos clic en propiedades y accederemos a la ficha 'Perfil', la cual es de las pocas opciones comunes a todos los usuarios que podemos modificar de esta forma.



En la imagen anterior, observamos que se ha introducido como ruta del perfil `\\DC01\perfiles\%username%`. En lugar de introducirla manualmente para cada usuario. `%username%` es una variable del sistema que contiene el nombre del usuario, por tanto al aplicar `%username%` al perfil de, por ejemplo, `Sara.Zambujo`, se creará una carpeta en `\\DC01\perfiles` que se llamará `Sara.Zambujo.V2`.

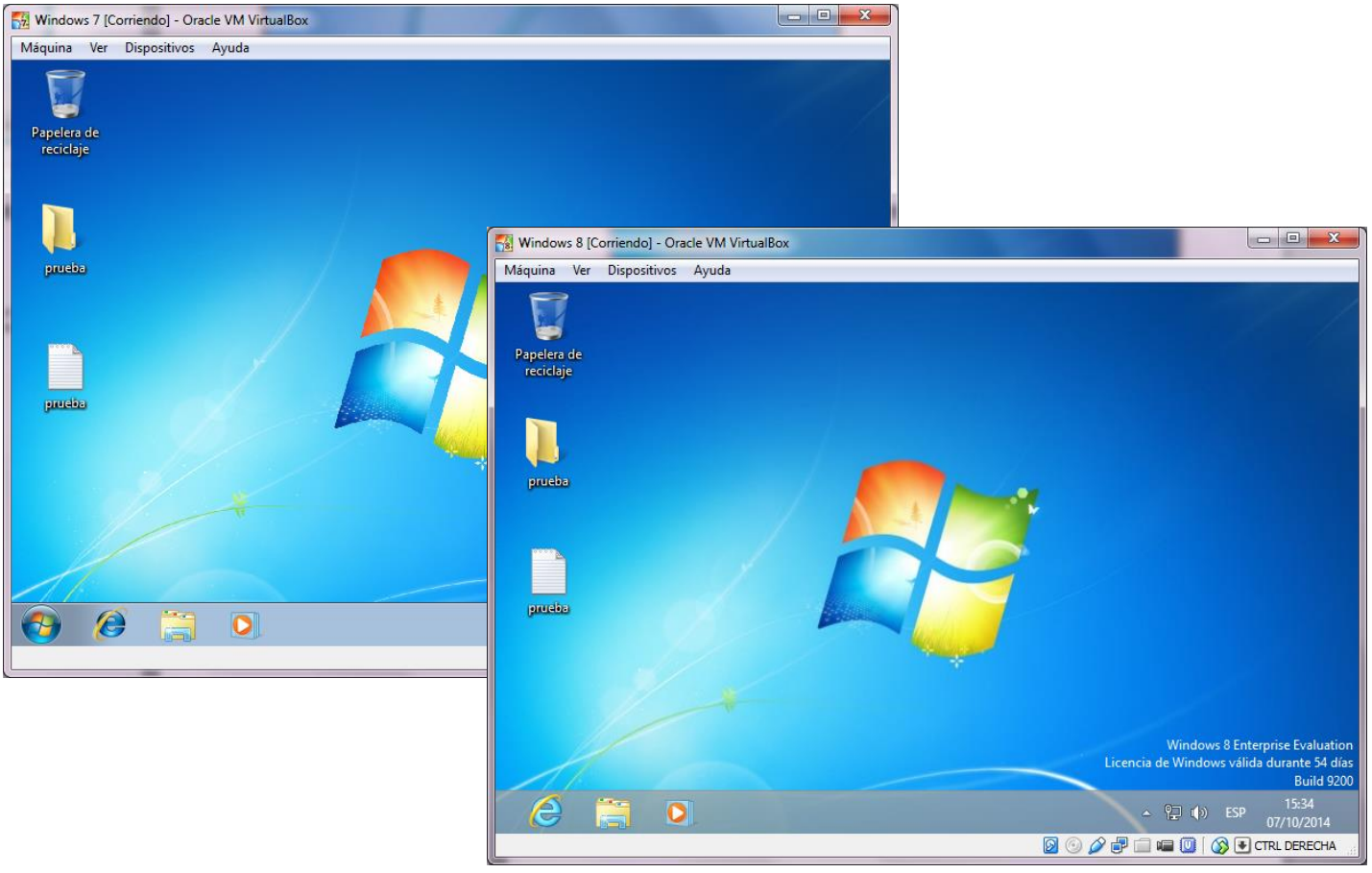
El motivo por el que la carpeta se llamará así y no simplemente `Sara.Zambujo` es porque los perfiles de Windows 7 se almacenan de manera diferente a los de Windows XP, por tanto, si el usuario inicia sesión desde un equipo XP se creará una carpeta con el nombre del usuario, si inicia sesión con Windows 7, se creará una carpeta con el nombre del usuario acabado en `.V2`.



Comprobemos que efectivamente funciona el perfil móvil establecido. Para ello el usuario `Sara.Zambujo` modificará el fondo de escritorio (recordad que los usuarios de la unidad organizativa 'Mandos Intermedios' sí tienen permiso para ello), y añadirá algún documento en el escritorio.

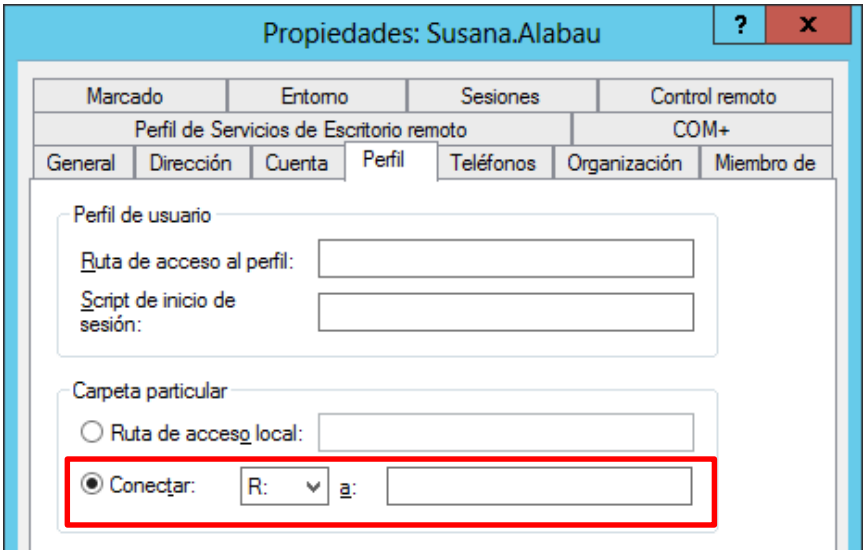
Iniciando sesión desde otra máquina Windows 7/8 la configuración modificada debe ser la misma.

Para que el nuevo fondo de escritorio se aplique a distintos equipos Windows 7/8 es necesario que la imagen de fondo sea accesible desde los equipos Windows 7/8 en los que se va a iniciar sesión y tener instalado en los equipos clientes el complemento que se utilizó en el apartado de directivas de grupo.

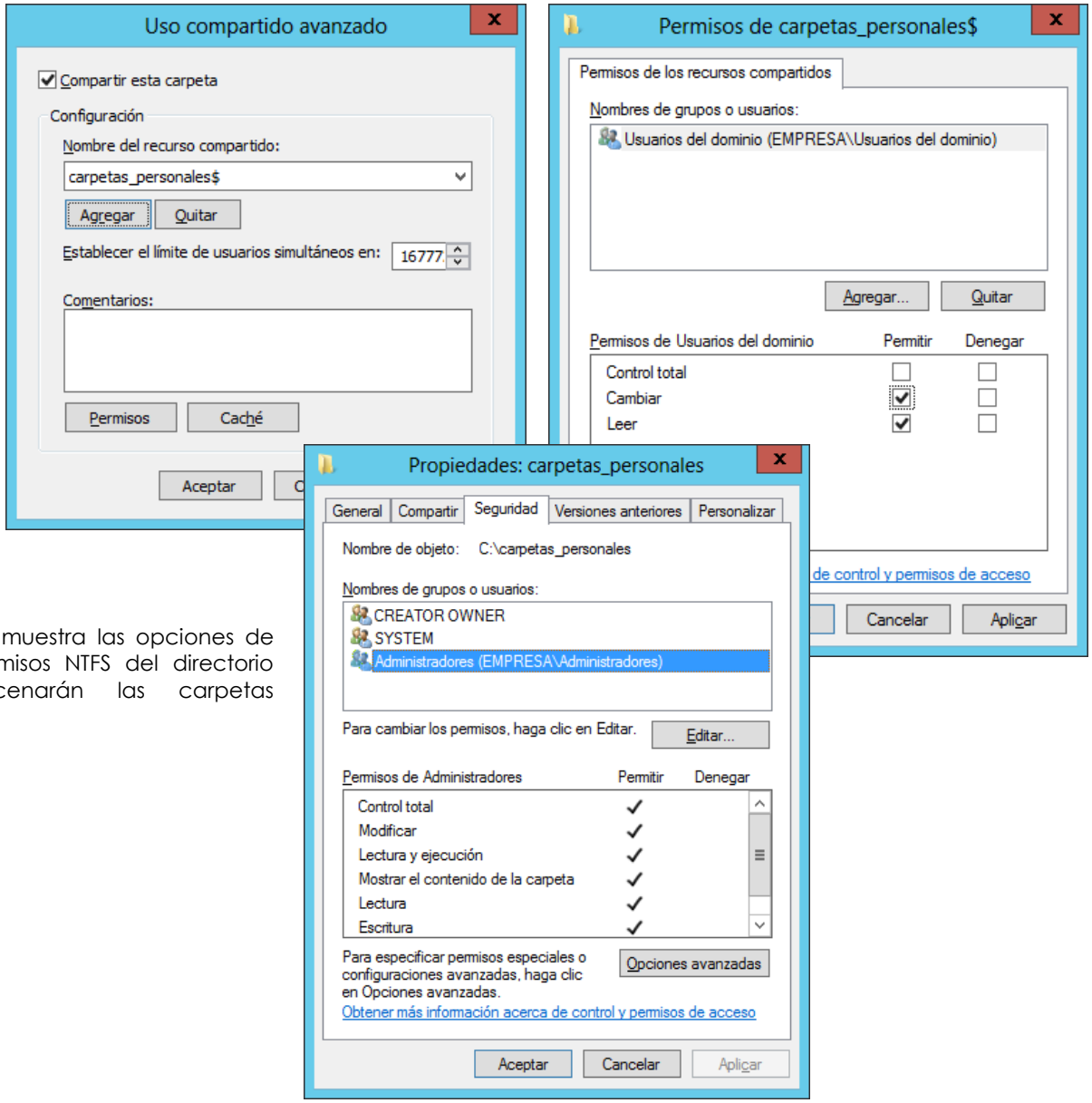


5. Carpetas personales

Otra de las opciones más utilizadas que puede configurarse en la ficha 'Perfiles' de las propiedades de la cuenta de usuario es el establecimiento de una unidad en red personal para cada usuario a la que únicamente él tiene acceso.



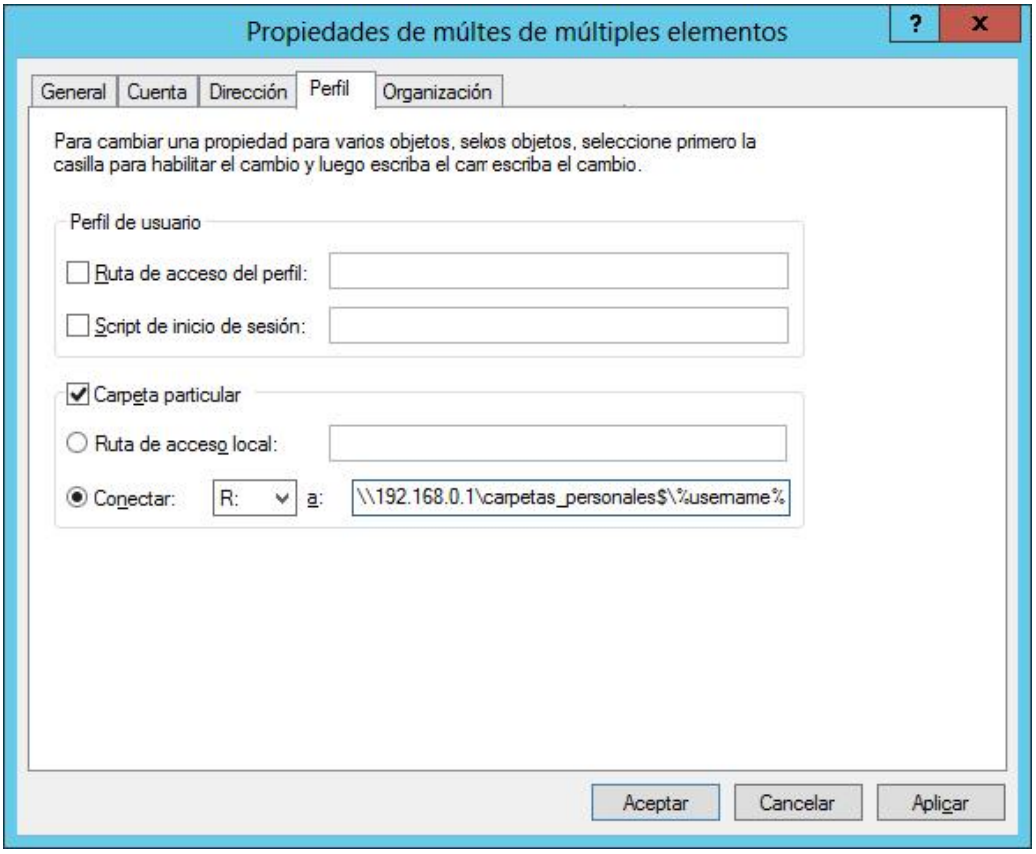
Para configurarla, basta crear una carpeta a la que se tenga acceso desde la red. En este caso la crearemos en el controlador de dominio (en casos reales podríamos ubicarla en un dispositivo de almacenamiento como un NAS).



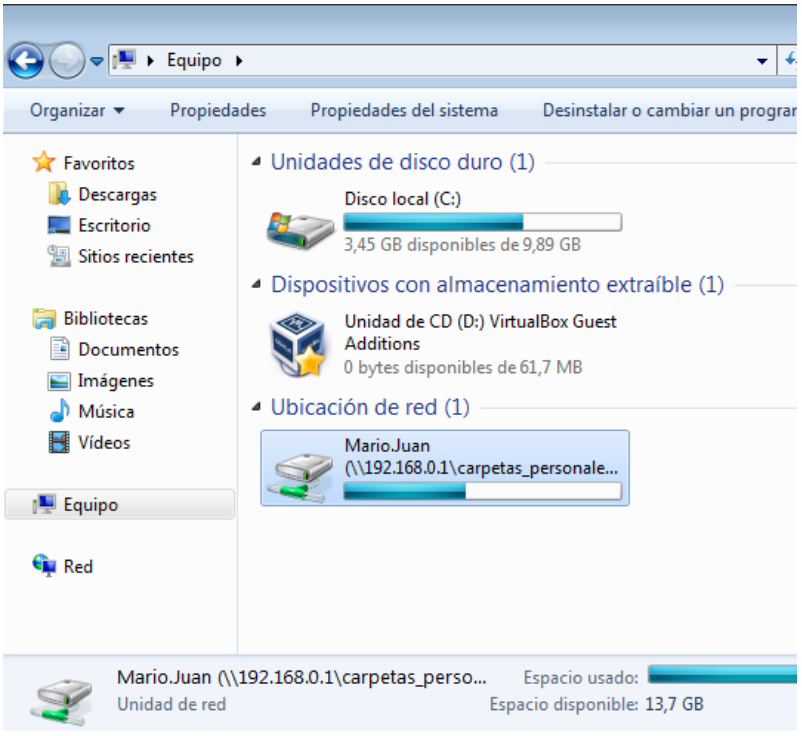
A continuación, se muestra las opciones de compartición y permisos NTFS del directorio donde se almacenarán las carpetas personales:

Ojo! Recuerda que para que los usuarios no puedan ver las carpetas de los otros debes quitar los permisos para el grupo 'Usuarios' y para ello necesitarás deshabilitar la herencia.

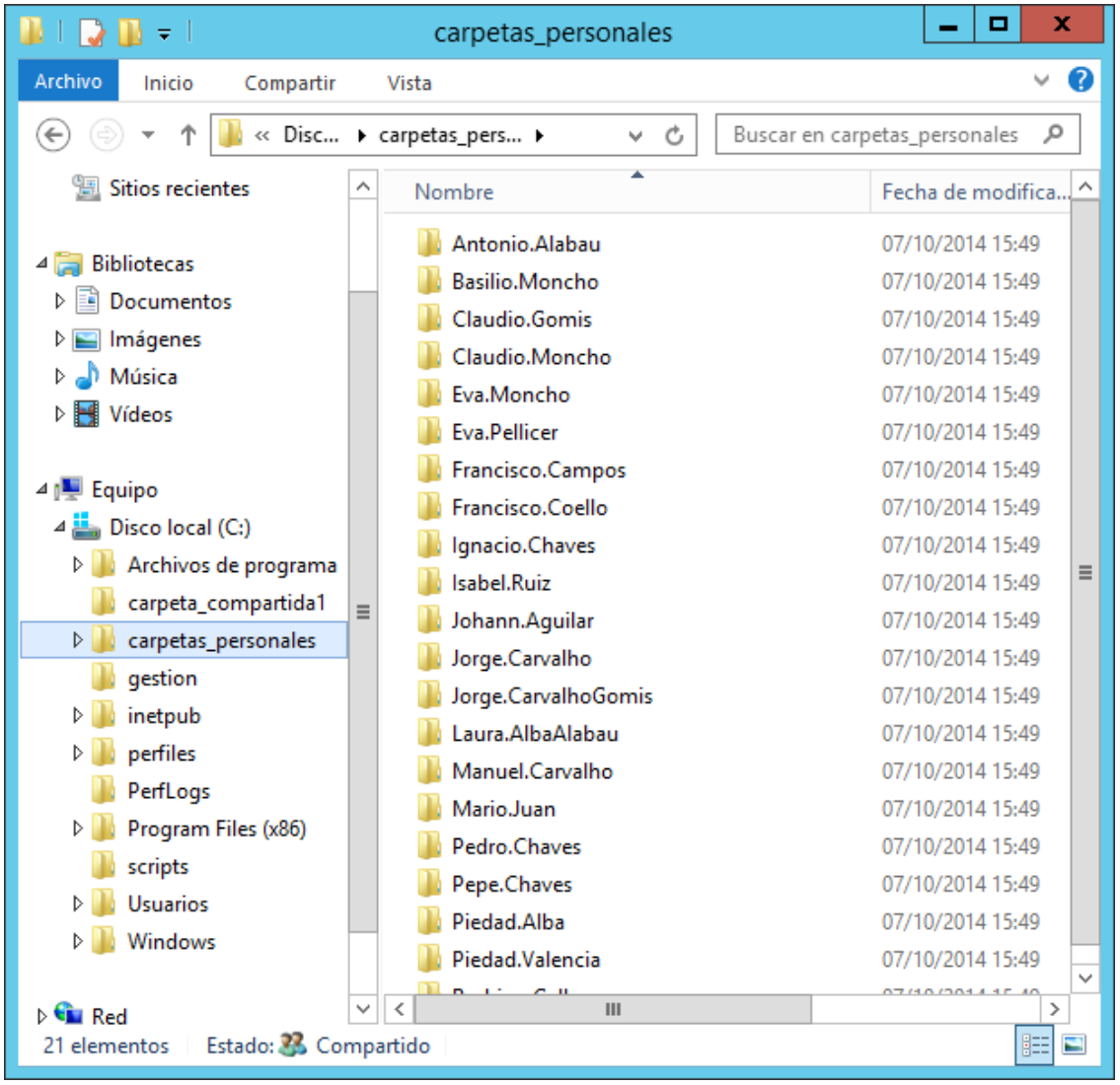
Para no tener que añadir manualmente la carpeta personal usuario por usuario utilizaremos de nuevo la variable `%username%` seleccionando a todos los usuarios y modificando la ficha perfil.



De esta manera se creará automáticamente en el controlador de dominio una carpeta con el nombre de cada usuario a la que únicamente él tendrá acceso, y que tendrá disponible (en este caso) en la unidad R:

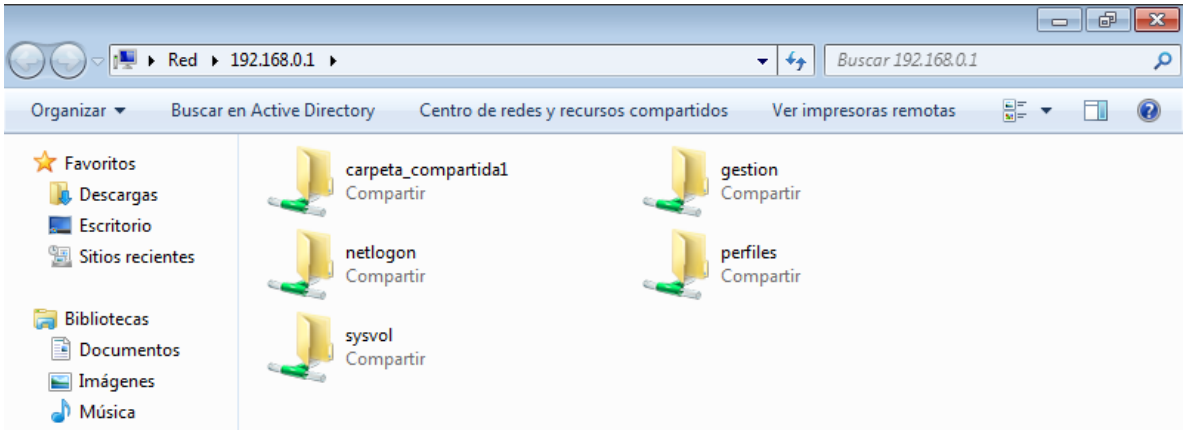


Si examinamos el lado del servidor, vemos que se han creado automáticamente las carpetas de todos los usuarios.



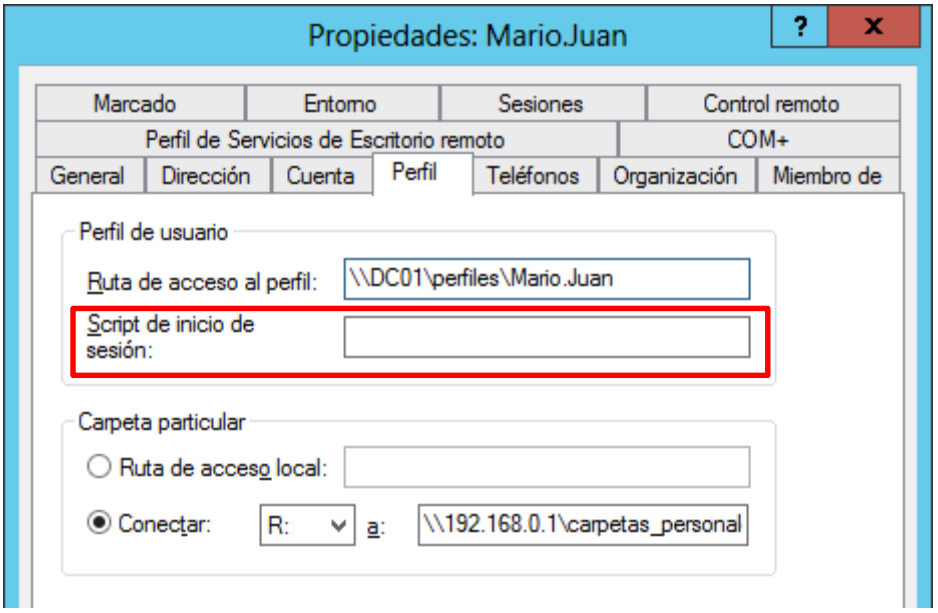
La dirección de la unidad montada es `\\192.168.0.1\carpetas_personales$\%username%`. En primer cabe destacar que se ha optado por poner la dirección IP del controlador de dominio en lugar del nombre del equipo porque de esta manera se reduce el tráfico en la red que supondría hacer la consulta al servidor DNS.

Por otra parte, al crear la carpeta compartida se le ha asignado como nombre `carpetas_personales$`. El símbolo `$` hace que las carpetas compartidas se hallen 'ocultas' en la red, en definitiva, si no se busca por su nombre, no aparecen en el listado de recursos compartidos accesibles vía red como se vio anteriormente.

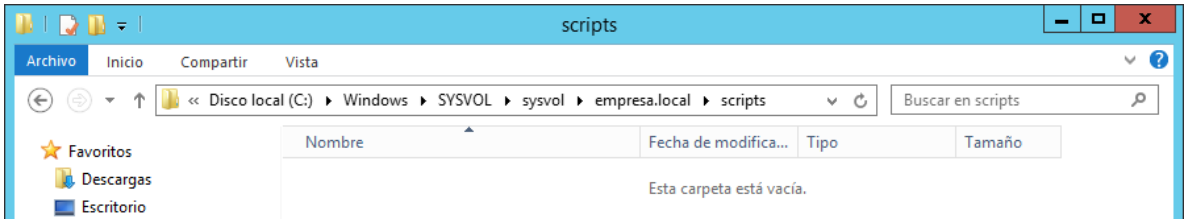


6. Comandos de inicio de sesión

Otra opción que podemos configurar dentro de la ficha perfil consiste en indicar un script que se ejecutará en cada inicio de sesión de manera automática y transparente al usuario.



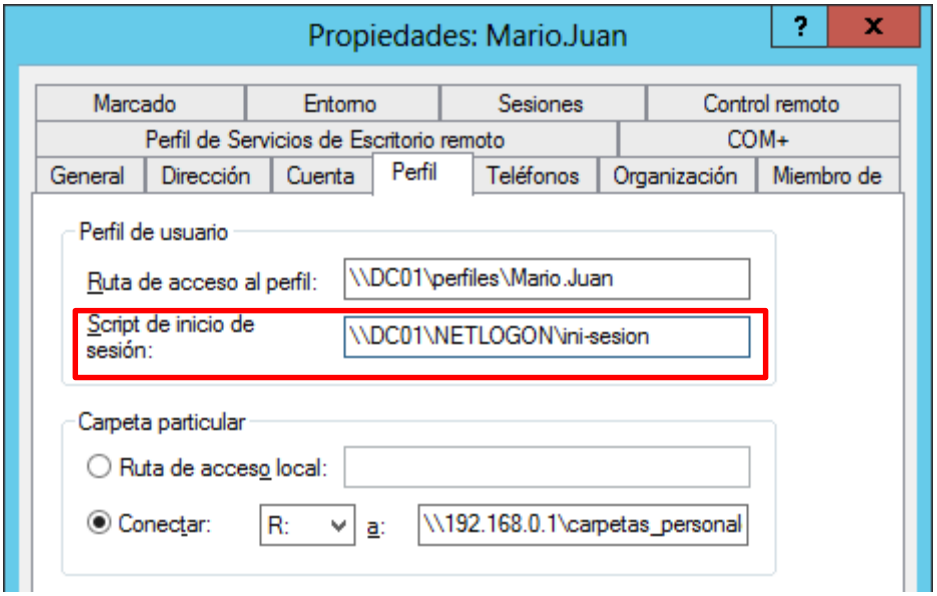
Estos scripts **deben** hallarse en la carpeta compartida `NETLOGON`, cuya dirección local en el controlador de dominio (puede cambiar dependiendo de versiones) es: `C:\Windows\SYSVOL\sysvol\[nombre dominio]\scripts`.



En este caso concreto, la dirección local y la dirección en red serían respectivamente:

- `C:\Windows\SYSVOL\sysvol\empresa.local\scripts`
- `\\DC01\NETLOGON`

Una vez que lo hayamos creado, indicaremos la ruta completa en la ficha 'Perfil' de las propiedades de la cuenta de usuario.



Cuando se introduzca en la ficha perfil la ruta del script de inicio de sesión **NO** se ha de añadir la extensión .bat del script.

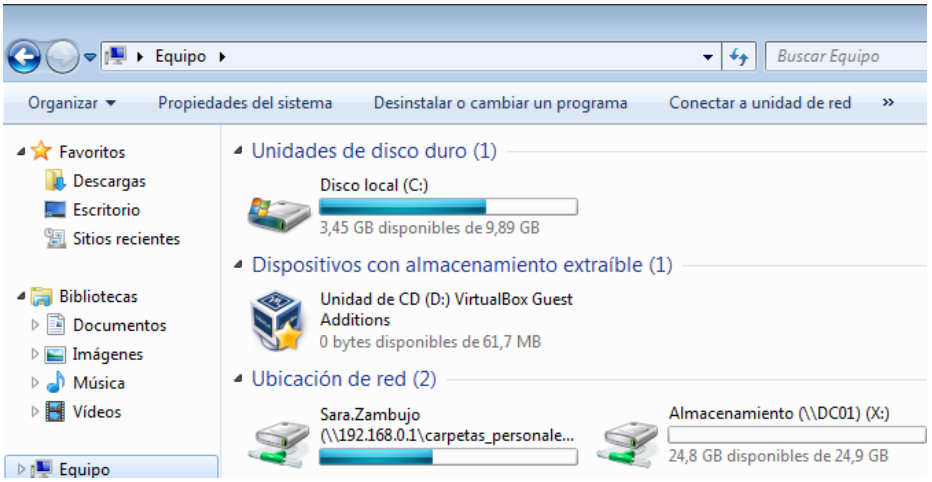
6.1. Ejemplos de scripts de inicio de sesión: Asignación de una nueva unidad de red

Supongamos que hemos dado de alta en el controlador de dominio una unidad nueva que vamos a destinar a almacenamiento compartido por parte de los usuarios del dominio. Queremos que este nuevo volumen de almacenamiento se halle disponible para **todos** los usuarios en la unidad X:. La manera más sencilla de hacerlo sería mediante la creación de un script de inicio de sesión que monte el recurso compartido en la unidad X:

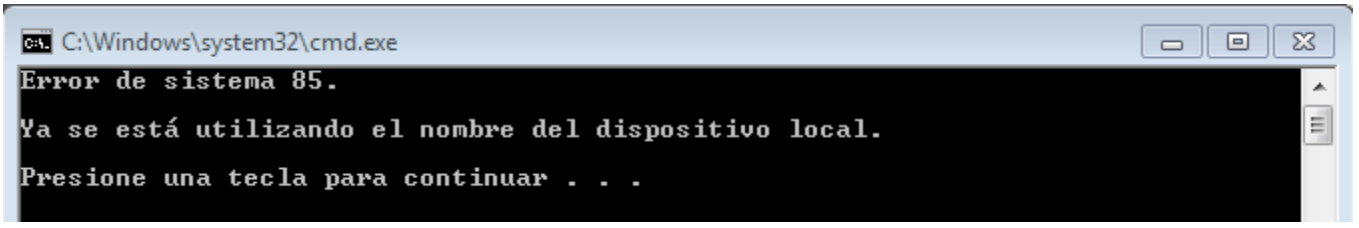
Una posible solución sería el siguiente script:

```
@echo off

net use X: \\DC01\Almacenamiento
```

Este script asigna el recurso compartido `\\DC01\Almacenamiento` a la unidad local `X:`. Si lo probamos, vemos que efectivamente cumple su cometido.



En algunos sistemas es posible que tras volver a iniciar sesión, observemos este error:



El problema radica en que estamos intentando asignar de nuevo un recurso que ya existe a la unidad X:. Para solucionar de manera sencilla esto, podemos poner un comando de control previo al montaje de la unidad.

```
@echo off

if NOT EXIST X: net use X: \\DC01\Almacenamiento
```

De esta manera lo que sucede es que si ya existe la unidad X:, no la montamos de nuevo, y si no existe, entonces efectivamente la montamos. Podemos comprobar que ahora no se produce el error que teníamos antes.

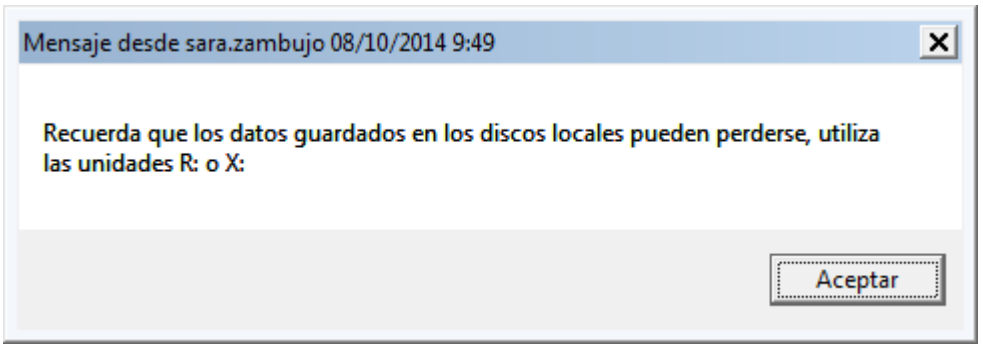
¿Por qué al iniciar sesión los miembros de la unidad organizativa 'Trabajadores' no les aparece en X: la carpeta `\\DC01\almacenamiento`?

6.2. Ejemplos de scripts de inicio de sesión: Mensaje a los usuarios

Supongamos que queremos enviar un mensaje a los usuarios cuando se conecten al sistema. Suele ser habitual enviar mensajes del tipo 'Guarda los datos en red' o 'No instales software sin permiso del administrador', o simplemente avisar de paradas planeadas en el sistema. Para enviar este tipo de mensajes automáticamente cuando el usuario inicia sesión podemos utilizar el comando `msg` dentro del fichero de comandos de inicio de sesión que hemos creado en el punto anterior:

```
@echo off

if NOT EXIST X: net use X: \\DC01\Almacenamiento

msg %username% Recuerda que los datos guardados en los discos locales pueden
perderse, utiliza las unidades R: o X:
```

El comando añadido envía al usuario que ha iniciado sesión `%username%` el mensaje escrito a continuación.



6.3. Ejemplos de scripts de inicio de sesión: Registro de conexiones

Aunque existen herramientas más específicas para realizar un registro de las conexiones, en este ejemplo añadiremos un comando al script de inicio de sesión para que almacene en un fichero que se halla en una carpeta en el controlador de dominio:

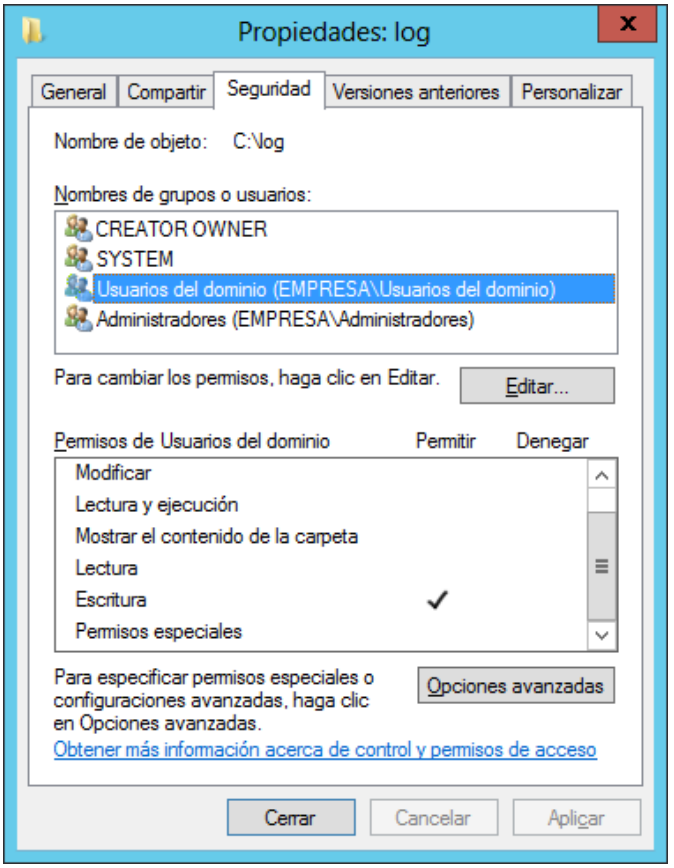
- el nombre del usuario que ha iniciado la sesión: `%username%`
- el día en que se ha realizado la conexión: `%date%`
- la hora a la que se ha iniciado la sesión: `%time%`
- el equipo desde el que se ha iniciado la sesión: `%computername%`

El script de inicio de sesión quedaría como sigue:

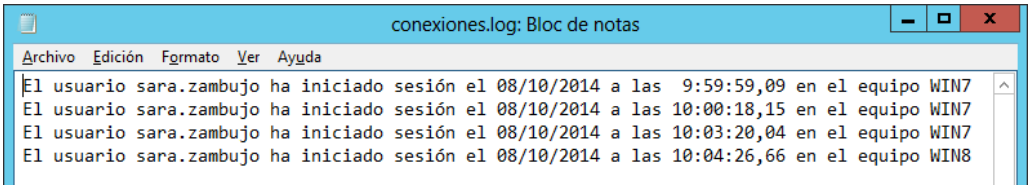
```
@echo off

if NOT EXIST X: net use X: \\DC01\Almacenamiento

msg %username% Recuerda que los datos guardados en los discos locales pueden
perderse, utiliza las unidades R: o X:

echo El usuario %username% ha iniciado sesión el %date% a las %time% en el
equipo %computername% >> \\DC01\log$\conexiones.log
```

La redirección de salida >> hace que la línea tras el `echo` se añada al final fichero `conexiones.log` sin borrar el contenido anterior.

La carpeta que hemos creado en el servidor (`log$`, recordad que el `$` evitaba la difusión del nombre a través de la red) otorga permisos de escritura a los usuarios del domino (se debe poder añadir la información de la conexión), pero se han eliminado los permisos de lectura, mostrar, etc., de manera que los miembros del grupo 'Usuarios del dominio' no pueden consultar el fichero.

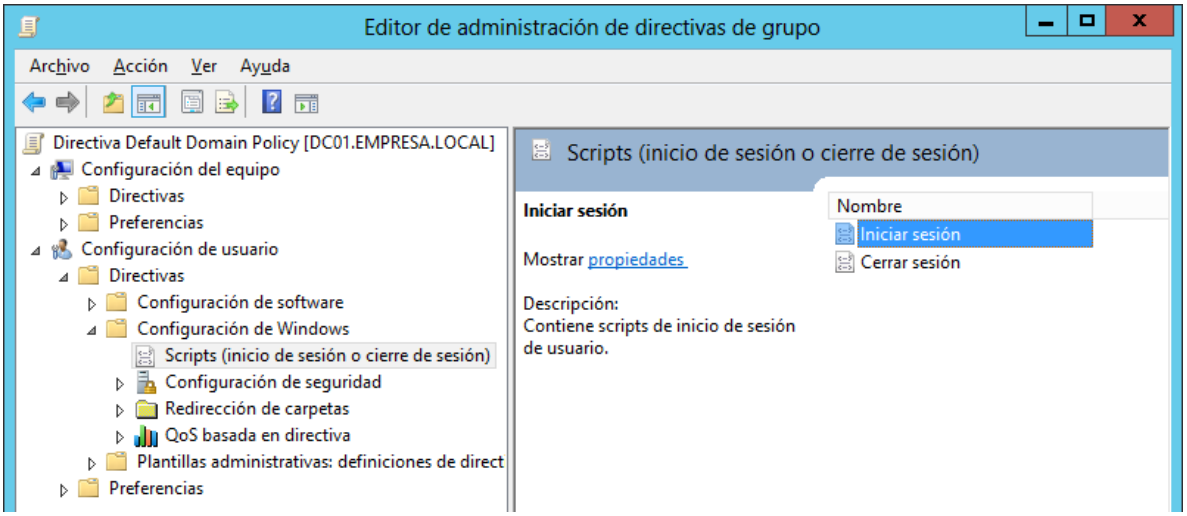


Si se revisa el fichero `conexiones.log`, se puede ver que efectivamente se va añadiendo la información de la conexión que se ha configurado en el script anterior.



6.4. Comandos de inicio de sesión con GPO

Además de lanzar los comandos de inicio de sesión mediante perfiles, también es posible hacerlo aplicando directivas de grupo. Para ello hay que editar el GPO en el que se quieren añadir los scripts, acceder a 'Configuración de usuario'→Directivas→'Configuración de Windows'→'Scripts (inicio de sesión o cierre de sesión' seleccionar el tipo de script (inicio o cierre) y añadir el archivo .bat correspondiente.



7. Bibliografía

- José Ramón Ruiz Rodríguez (2013). Curso Cefire Windows 2008 Server.
- José Ramón Ruiz Rodríguez (2013). Curso Cefire Windows Server 2012.
- SomeBooks.es (2014). Sistemas Operativos en Red. Disponible en http://somebooks.es/?p=4787
- Wikipedia. Sistema Operativo de red. Disponible en http://es.wikipedia.org/wiki/Sistema_operativo_de_red
- Blog de SoporteTI. Disponible en: http://blog.soporteti.net/