

GESTIÓN DE RECURSOS COMPARTIDOS EN WINDOWS SERVER.

CASO PRÁCTICO

En el Pregonero del Norte, diario de ámbito regional, están muy preocupados. La productividad de los trabajadores ha descendido notablemente desde que se incorporaron nuevas personas al equipo, a pesar de tratarse de una plantilla muy experimentada y profesional.

En la dirección del periódico analizan las causas de este deterioro de la eficacia y al entrevistar a los trabajadores y trabajadoras encuentran el motivo principal: la utilización que se está haciendo de los **recursos** informáticos está provocando situaciones de caos. Entre los problemas detectados se encuentran los siguientes:

- Cuando dos o más redactores trabajan en un mismo artículo, se van pasando las versiones unos a otros mediante **discos USB** o correos electrónicos. Esto ha provocado, más de una vez, que la versión publicada de un artículo no sea la versión definitiva, sino una intermedia.
- Las imágenes utilizadas para ilustrar los artículos deben residir en un ordenador central. Cuando un maquetador necesita imágenes ya existentes, debe acudir, físicamente, a dicho ordenador para coger los archivos. Sin embargo, el ordenador muchas veces está ocupado o apagado, por lo que los maquetadores terminan por tener sus propios bancos de imágenes, que no residen en un repositorio central.
- El diario cuenta con dos impresoras: una destinada a las impresiones habituales de la oficina y otra, de mayor calidad, que sólo utilizan los maquetadores y los jefes de redacción, para las pruebas finales de impresión, antes de dar el visto bueno y que el diario se envíe a la imprenta. Para imprimir en la impresora normal, hay que iniciar sesión localmente en el equipo al que está conectada, lo que implica “atascos” cuando varias personas quieren imprimir a la vez. La impresora de alta calidad está conectada a la red y actualmente cualquier trabajador puede imprimir en ella desde su ordenador. El resultado es que muchas veces los empleados y empleadas utilizan la impresora de alta calidad (cuyo tóner es mucho más caro) sin necesidad, con el objetivo de evitarse esperas e incomodidades.

Todos estos factores han llevado a la Dirección del Pregonero del Norte a contratar a CARMINFO S. L. para reorganizar la estructura informática de forma que se puedan solucionar todos estos problemas. Carmen, propietaria de CARMINFO S. L. y Laura, su más antigua empleada, debaten acerca de cómo abordar el problema:

-Tendremos que analizar los problemas uno a uno, pero está claro que la solución pasa por la utilización de carpetas compartidas y de impresoras compartidas -dice Laura.

-Tienes razón, Laura. También convendría instalar **Active Directory** y asignar a cada trabajador y a cada trabajadora una **cuenta de usuario** -responde Carmen.

-Sí. Así podremos asignar permisos de acceso a las carpetas y a las impresoras.

-Por supuesto -corroboró Carmen-. Ya sabes que una de las cosas que nos han pedido es que en la impresora de alta calidad sólo puedan imprimir determinadas personas.

-Y también nos han pedido que se controle quién puede hacer cambios en los archivos del periódico, para que no se borren artículos e imágenes “accidentalmente” -recuerda Laura.

-Bien, pues... ¡manos a la obra!

1.- Cómo compartir carpetas y archivos.

CASO PRÁCTICO

Carmen ha encargado a Alberto y a Marisa, trabajadores de CARMINFO S.L., las primeras tareas para poner en orden el caos informático en el que se ha convertido la redacción del Pregonero del Norte. Ambos se han esforzado mucho para configurar un dominio en Active Directory y para hacer miembros de dicho dominio a todos los equipos de la oficina.

Una vez hecho esto, Carmen planifica el siguiente paso:

-Alberto, Marisa, ha llegado el momento de empezar a solucionar punto por punto los problemas más acuciantes que tienen en este periódico. Propongo abordar en primer lugar el asunto de los artículos sobre los que trabajan varios redactores a la vez -dice Carmen.

-Sí, Carmen -responde Marisa-, ahora mismo es un desastre: se van pasando la última versión que han escrito los unos a los otros mediante discos USB y correos electrónicos.

-A mí me han dicho que muchas veces acaban publicando una versión que no es la buena -interviene Alberto.

-La solución pasa por poner todos los artículos en un lugar en el que puedan acceder todos simultáneamente, ¿no creéis? -dice Carmen.

-Sí. O sea, una carpeta compartida, ¿verdad?

-Sí, Marisa. Tenéis que configurar un servidor de archivos, es decir, un equipo que estará siempre encendido y que albergará las carpetas compartidas.

Alberto recuerda las limitaciones de presupuesto que les ha impuesto la dirección del periódico y propone:

-Como no podemos adquirir un equipo exclusivamente para eso, ¿qué os parece utilizar el **controlador de dominio**? Ya he comprobado que tiene espacio suficiente en el disco.

-Muy bien -responde Carmen-. Empezaremos por ahí.

1.1 Dos modelos de compartición: estándar y carpeta pública.

¿Qué queremos decir cuando hablamos de “**recursos compartidos**”? Esta expresión hace referencia, normalmente, a archivos, carpetas e impresoras, que se comparten en red. El hecho de que estén “compartidos en red” significa que se puede acceder a esos recursos desde un equipo diferente a aquél en el que se encuentran físicamente ubicados. Para que eso sea posible, los equipos deben estar conectados en red. Dicho de otra forma: si Carmen crea una carpeta compartida en el ordenador A, podrá acceder a dicha carpeta desde el ordenador B y desde el ordenador C, que están conectados en red al primero.

Antes de que empieces a compartir recursos en la red, es necesario que aprendas las diferentes posibilidades que Windows Server ofrece para ello. Dependiendo de las necesidades que tengas, elegirás una forma u otra de hacerlo. En concreto, Windows Server soporta dos modelos de compartición de archivos: la compartición **estándar** y la compartición **mediante la carpeta pública**.

1) En la compartición estándar, permitimos a los usuarios de la red acceder a carpetas, archivos y unidades. En este modelo, cuando se comparte una carpeta o una unidad, todos los archivos y subcarpetas quedan disponibles para un determinado grupo de usuarios. Para utilizar la compartición estándar no es necesario mover lo que se desea compartir a otro lugar.

2) Compartición mediante la carpeta pública, sin embargo, cuando utilices este modelo tendrás que copiar o mover aquello que quieras compartir, a la carpeta: `%SystemDrive%\Users\Public`. Ten en cuenta que, en la ruta anterior, `%SystemDrive%` representa una **variable de entorno**, cuyo valor se sustituye por la letra de la partición en la que está instalado el sistema operativo (normalmente C:).

Existe otra diferencia importante entre ambos modelos:

- ⤴ Cuando se utiliza el modelo estándar de compartición, se puede determinar claramente **qué grupos** y **qué usuarios** podrán acceder al recurso y de qué manera. Por ejemplo, si decides compartir una carpeta llamada *Artículos*, podrás establecer que el grupo *LecturaArticulos* tenga acceso de lectura al contenido; y que el grupo *EscrituraArticulos* tenga acceso de lectura y también de escritura.
- ⤴ Por el contrario, con el modelo de carpeta pública, sólo se puede controlar si el acceso a través de la red es de lectura o de lectura y escritura, pero esto se aplicará a todos los usuarios. Es decir, no se puede distinguir entre lo que pueden hacer unos usuarios y lo que pueden hacer otros.

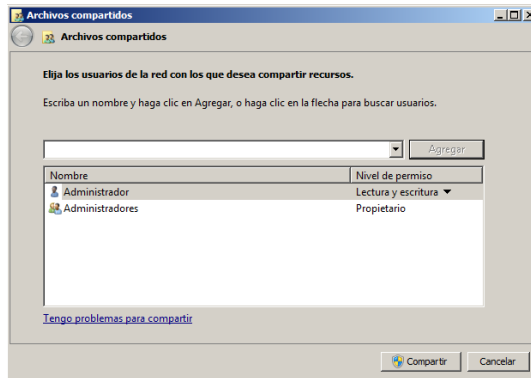
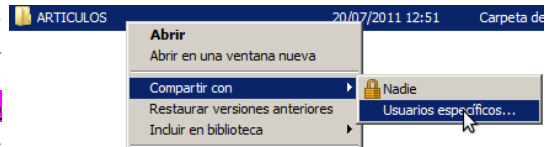
Por todo lo anterior, suele ser más recomendable utilizar el modelo estándar de compartición en lugar del modelo de carpeta pública. En el resto de los capítulos, nos centraremos en el modelo estándar.

1.2 Compartir carpetas mediante el explorador de Windows.

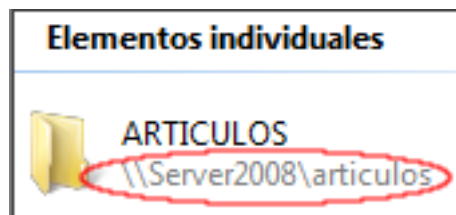
En esta sección vas a aprender la forma más utilizada para compartir carpetas. Sin embargo, no es la única, como verás más adelante. Al ser la más intuitiva, es la que más utilizan los usuarios y usuarias no familiarizados con las tareas de administración del sistema.

Para compartir recursos en red, tu cuenta de usuario debe ser miembro del grupo **Administradores** (o de un grupo que a su vez pertenezca a **Administradores**).

Para compartir una carpeta mediante el explorador de Windows, haz clic con el botón secundario del ratón sobre la carpeta que deseas compartir y elige “Compartir con → Usuarios específicos”. Así, accederás al **cuadro de diálogo** “Archivos compartidos”. En esta ventana aparece una lista de los usuarios y grupos que tendrán acceso a la carpeta. Al lado de cada usuario o grupo, puedes ver el tipo de acceso que tienen (Lectura, Escritura...).



Aprenderás a establecer correctamente estos permisos un poco más adelante. De momento, los dejaremos como vienen por defecto. Pulsa el botón “**Compartir**” de este cuadro de diálogo y fíjate bien en la ruta de red que aparece bajo el nombre de la carpeta. Este es el nombre que tendrá la carpeta en la red. Es decir, cuando se acceda a la carpeta desde otro equipo, se utilizará este nombre, que no tiene por qué coincidir con el nombre que tenga esta carpeta en el sistema de archivos en el que se encuentre ubicada.



Ya está. La carpeta está compartida en red, por lo que será accesible desde equipos remotos. Como has podido comprobar, este método es muy sencillo de usar, pero presenta algunos inconvenientes:

- ⤴ Sólo te permite compartir recursos en el equipo local en el que se ha iniciado sesión.
- ⤴ Utilizando este método, no tienes una visión global de todos los recursos compartidos que hay en el equipo.
- ⤴ El nombre de red del recurso compartido se ha asignado automáticamente, es decir, no has tenido control sobre él.

Por todo ello, puede ser más deseable utilizar la herramienta “Administración de equipos” para compartir recursos.

Para dejar de compartir un recurso, en el menú contextual, elige “Compartir con” → **Nadie**.

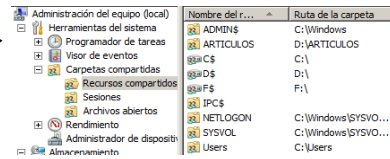
1.1.- Compartir carpetas mediante Administración de Equipos.

En esta sección vas a aprender un método para compartir recursos que soluciona los problemas presentados en la sección anterior:

- ⚡ La imposibilidad de compartir recursos en equipos remotos.
- ⚡ La falta de una visión global de los recursos compartidos.
- ⚡ La asignación automática del nombre del recurso compartido.

Para **compartir una carpeta** de esta forma:

1. Abre la herramienta “Administración de Equipos” en “Inicio” → “Herramientas Administrativas”.
2. Selecciona “Carpetas compartidas”.
3. Selecciona “Recursos compartidos”.



En este punto puedes comprobar qué recursos están compartidos en tu equipo. De esta forma consigues tener una visión centralizada de todo lo que has compartido. Muchas veces, hay recursos compartidos antiguos, que ya no deberían existir. Esta herramienta te permite llevar un control sobre ello.

Sigue con el proceso:

4. En el menú “Acción”, elige “Recurso compartido nuevo”. Te aparece un asistente.
5. El primer paso del asistente consiste en especificar la ruta de la carpeta, es decir, debes decirle al servidor qué carpeta deseas compartir.
6. El siguiente paso consiste en establecer el nombre del recurso compartido, es decir, el nombre que tendrá en la red. Opcionalmente, puedes adjuntar una descripción.
7. Finalmente, se seleccionan unos permisos básicos de acceso. Como te hablaremos de los permisos más adelante, por el momento debes preocuparte de este asunto.

Cuando trabajas en un dominio, es interesante publicar los recursos compartidos en Active Directory. Esto hace que sean mucho más fáciles de encontrar cuando se desea acceder a ellos. Para **publicar un recurso compartido en Active Directory**, en la herramienta Administración de equipos → “Carpetas compartidas” → “Recursos compartidos”, haz clic con el botón secundario sobre el recurso que quieras publicar y elige “Propiedades”. En la pestaña “Publicar”, marca la casilla “Publicar este recurso compartido en ‘Active Directory’”.

Por último, para **dejar de compartir un recurso**, en el mismo entorno en el que estamos trabajando, haz clic con el botón secundario sobre el recurso y elige “Dejar de compartir”.

Si lo que quieres es **manejar recursos compartidos que se encuentran en un equipo remoto**, en la misma herramienta, Administración de Equipos, haz clic con el botón secundario en “Administración del equipo (local)” y elige “Conectar con otro equipo”. En el cuadro de diálogo que aparece, podrás seleccionar un equipo remoto y gestionar sus recursos compartidos.

2.- Acceder a recursos compartidos.

CASO PRÁCTICO

La labor que el diario Pregonero del Norte ha encargado a CARMINFO S. L. consiste en reorganizar los recursos informáticos de la empresa. Por el momento, han instalado Active Directory, han unido todos los equipos al dominio y han creado dos carpetas compartidas: una para almacenar las imágenes y otra para los textos de los artículos.

El nuevo sistema se pone en funcionamiento y al cabo de una semana, la dirección del periódico analiza los resultados. Ha encontrando, para su gran sorpresa, que los maquettadores y los redactores seguían utilizando los antiguos métodos de trabajo, es decir, almacenaban los archivos localmente, en lugar de utilizar el servidor de archivos, con las carpetas compartidas.

La directora del periódico se pone en contacto con Carmen, propietaria de CARMINFO S. L.

-Carmen, los empleados rechazan el nuevo sistema. Siguen empleando los mismos métodos de trabajo, a pesar de que usted nos dijo que la nueva forma de trabajo sería fácil de adoptar.

-El problema es que sus empleados y empleadas no han recibido ningún tipo de formación y no saben cómo acceder a los recursos compartidos -responde Carmen-. Ya le advertí que sería necesario impartirles una o dos clases para que aprendan a utilizar el nuevo sistema.

-Es posible que nos equivocáramos rechazando esa formación -reconoce la directora-. ¿Podrían ustedes organizar esas clases?

-Por supuesto. No se preocupe, se adaptarán perfectamente al nuevo método de trabajo.

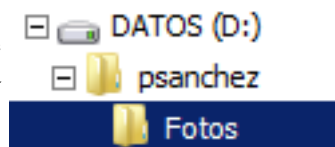
Cuando se crean recursos compartidos, lógicamente, es porque existe la necesidad de utilizarlos. Hemos empezado enseñándote a crearlos, pero para que esto tenga sentido, tendrás que aprender a acceder a ellos. Verás que es un proceso tremendamente sencillo, pero conviene tenerlo muy claro, sobre todo en lo referente a las rutas de red.

2.1 Conectar una unidad de red.

Existe una forma de acceder a las carpetas compartidas que te resultará muy cómoda: en el equipo cliente, es decir, en el equipo desde el que se accede a la carpeta compartida, se **asocia una letra de unidad al nombre de recurso** compartido de la carpeta, por ejemplo la **Z**. Esto hace que en “Mi Pc” o “Mi Equipo” aparezca una nueva unidad, Z:, como si fuera una de las particiones del disco duro, o una unidad de CD/DVD. Al entrar en Z:, realmente se accede a través de la red al recurso compartido.

Las carpetas compartidas tienen asociadas dos importantes características: el **nombre de recurso compartido** y la **ruta de carpeta**.

La ruta de carpeta es el camino para localizar la carpeta en el sistema de archivos. Por ejemplo, una carpeta llamada *Fotos*, que se encuentra en la carpeta *psanchez*, que a su vez se encuentra en la unidad D:, tiene como ruta de carpeta: **D:\psanchez\Fotos**.

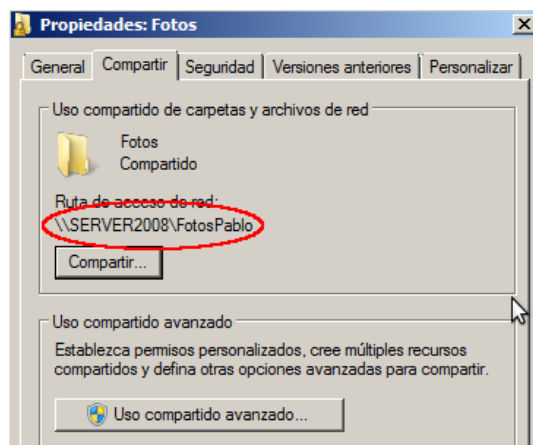


Ya te hemos hablado del nombre de recurso compartido en apartados anteriores: se trata del nombre que va a tener el recurso cuando se acceda a él a través de la red. Es muy importante que tengas en cuenta que este nombre **no tiene nada que ver con la ruta de carpeta**.

Para poder asociar una letra de unidad a la carpeta compartida, debes conocer:

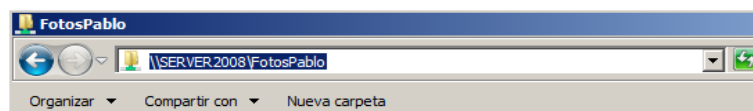
- ⤴ El nombre del **equipo** en el que reside la carpeta.
- ⤴ El nombre de **recurso compartido** de la misma.

Imagina que la carpeta Fotos del ejemplo anterior reside en un equipo cuyo nombre se ha establecido como *SERVER2008*. Además, supón que el nombre de recurso compartido es *FotosPablo*. En ese caso, el nombre completo del recurso compartido, que incluye el nombre del equipo sería: **\\SERVER2008\FotosPablo**. Observa las dos barras invertidas (\) al principio del nombre.



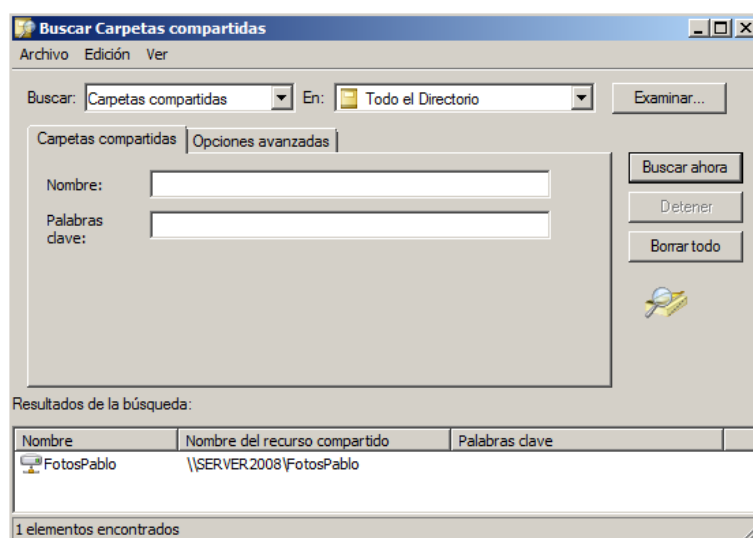
2.2 Otras formas de acceder a una carpeta compartida.

Muchas veces necesitarás acceder a una carpeta compartida para un uso puntual. En ese caso, puede no ser conveniente que utilices una unidad de red, ya el verdadero motivo de utilizar estas unidades es la continuidad en su uso. Para estos casos debes saber que también es posible abrir directamente una carpeta compartida sin necesidad de asociarla a una unidad de red. Para ello, simplemente introduce el nombre completo del recurso (por ejemplo, \\SERVER2008\FotosPablo) en la barra de navegación del explorador de Windows. Si en la barra de navegación escribes sólo la ruta al equipo (por ejemplo, \\SERVER2008) podrás ver un listado de todos sus recursos compartidos.



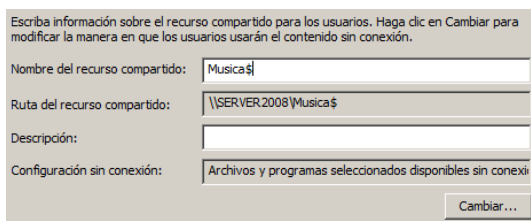
Otra forma muy habitual de acceder a carpetas compartidas es utilizar la herramienta “Mis sitios de red” o “Red”. Accediendo a ella podemos explorar la red en busca de carpetas compartidas en la misma. Sin embargo, este método cada vez se utiliza menos porque, a veces, el listado de los equipos conectados en la red tarda mucho en aparecer o no aparece.

En el caso de trabajar con Active Directory, existe una forma muy eficiente de buscar carpetas compartidas. En el capítulo anterior aprendiste a publicar recursos compartidos en Active Directory. Si has compartido una carpeta y las has publicado en Active Directory, el usuario que desee entrar en ella a través de la red, puede buscarla en el servicio de directorio. ¿Cómo? Accediendo a Red y pulsando “Buscar en Active Directory”. Aparecerá un cuadro de diálogo en el que habrá que seleccionar “Carpetas compartidas” en el cuadro desplegable de “Buscar:” y pulsar el botón “Buscar ahora”. Esto hace que aparezca un listado con todas las carpetas compartidas publicadas en Active Directory.

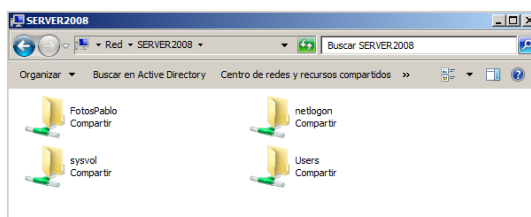


2.1.- Recursos compartidos ocultos y administrativos.

Recuerda que te hemos contado en el apartado anterior que si escribes en la barra de navegación \\SERVER2008, puedes ver los recursos compartidos de dicho equipo. A veces puede interesarte compartir un recurso en red, pero que no lo pueda ver cualquiera con sólo acceder al equipo. ¿Cómo lograr esto? Nada más fácil: al compartir el recurso, cuando establezcas el nombre de recurso compartido, añade un símbolo de dólar (\$) al final del mismo.



En el ejemplo de la imagen, para acceder al recurso, habrá que introducir en la barra de navegación del explorador de Windows la ruta “\\SERVER2008\Musica\$”. Observa que el símbolo de dólar forma parte del nombre. También es posible conectar una unidad de red al recurso, como con cualquier otro. La diferencia es que esta carpeta no aparecerá al explorar “Mis sitios de red”, ni “Red”, ni al introducir el nombre de red **del equipo** en la barra de navegación.



Como puedes ver en la imagen, la carpeta compartida “Musica\$” no aparece en la lista de recursos compartidos del equipo, aunque sí aparece “FotosPablo”, que fue configurada en su momento sin añadir el símbolo de \$ a su nombre de recurso compartido.

¡Cuidado! El hecho de ocultar un recurso compartido no impide que se pueda acceder a él. Basta con saber el nombre, escribirlo en la barra de navegación y ya está. Lo que realmente controla el acceso los recursos son los **permisos**, de lo que tratan los siguientes capítulos.

Cuando accedes a la herramienta “Administración de equipos” → “Carpetas compartidas” → “Recursos compartidos”, puedes notar que en el listado aparecen elementos que tú no has compartido en red. Además, si te fijas bien, verás que muchos de esos elementos llevan el símbolo de dólar al final del nombre, por lo que son recursos compartidos ocultos. Estos elementos que aparecen sin que tú los hayas manipulado son **recursos compartidos administrativos** y están ahí para cumplir funciones del sistema operativo. En concreto, suelen ser: **ADMIN\$, IPC\$, NETLOGON, SYSVOL, Users** y **C\$, D\$, etc.** Como puedes observar, cada unidad lógica que haya en tu equipo tiene un correspondiente recurso compartido oculto: C\$, D\$, etc. Esto no debe preocuparte, ya que los permisos por defecto están establecidos para que sólo los usuarios con credenciales administrativas puedan escribir en ellos, tanto localmente como a través de la red. Sin embargo, debes tener muchísimo cuidado con asignar usuarios a grupos administrativos, como ya te hemos insistido en otras unidades.

PARA SABER MÁS

En el siguiente enlace encontrarás una pequeña introducción sobre los recursos compartidos administrativos:

Texto enlace: Recursos compartidos administrativos.

URL: <http://support.microsoft.com/kb/954422/es>

3.- Permisos de compartición.

CASO PRÁCTICO

Marisa, empleada de CARMINFO S. L., ha sido elegida para impartir una pequeña clase en el Pregonero del Norte, con el objetivo de enseñar a los trabajadores y trabajadoras del periódico a utilizar el nuevo sistema basado en Active Directory y en recursos compartidos.

Los trabajadores, sentados en la sala de reuniones, observan los diagramas que Marisa ha representado en la pizarra.

-Como podéis ver -explica Marisa- hemos creado dos carpetas compartidas: una es para los artículos y la otra para las imágenes.

Uno de los redactores levanta la mano:

-Eso está muy bien, pero... ¿Eso quiere decir que todos los los del periódico pueden acceder a la carpeta? ¿Y si alguien mete la pata y lo borra todo?

-Evidentemente -responde Marisa-, hay que programar copias de seguridad de todos los datos importantes. Pero vamos a hacer que sólo puedan escribir en esa carpeta los redactores.

Una trabajadora interviene:

-Pero los de maquetación necesitamos acceder a lo que han escrito los redactores para introducir los textos en la maqueta final del periódico. Así que los maquetadores y maquetadoras también tenemos que poder entrar a esa carpeta.

-El problema -interviene un redactor- es que podríais borrar algo “accidentalmente”. No sería la primera vez que desaparece un artículo y hay que volverlo a escribir.

Ante el conflicto que se está generando, Marisa intenta mediar:

-Señoras y señores, un poco de calma. No se preocupen por eso. Cada uno de ustedes podrá acceder a las carpetas de forma adecuada. Aquellas personas que no deban tener el poder de borrar nada, no lo tendrán. Aquellas que deban poder ver el contenido de la carpeta lo podrán hacer.

-¿Eso es posible? -pregunta el redactor que ha hablado.

-Por supuesto. Es una parte imprescindible de esta forma de trabajo: se trata de configurar permisos. Y es algo que nuestra empresa va a hacer por ustedes.

Como habrás podido deducir por el título del capítulo y por la conversación entre Marisa y los trabajadores y trabajadoras del Pregonero del Norte, vamos a hablarte de permisos. Los permisos sirven para controlar el acceso que los usuarios tienen a los recursos.

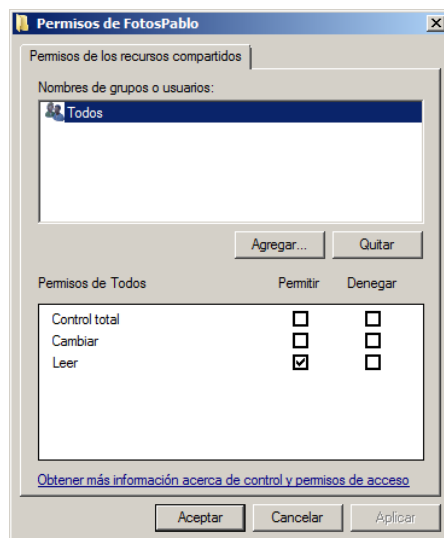
En este capítulo nos vamos a ocupar de los permisos de compartición, pero debes saber que existe otro conjunto de permisos, los permisos locales, de los que hablaremos en el capítulo siguiente.

3.1.- Significado de los permisos de compartición.

Los permisos de compartición que establezcas sólo se tendrán en cuenta cuando accedas a los archivos **a través de la red**, pero nunca cuando accedas **de forma local**. Sirven para establecer el máximo nivel de acceso que tendrá un usuario sobre el recurso compartido cuando acceda de forma remota.

Existen tres permisos de compartición que se pueden asignar sobre una carpeta compartida:

- ⤴ **Leer:** si concedes este permiso a un usuario o grupo, éste podrá ver los nombres de los archivos y subcarpetas contenidos en la carpeta compartida. También podrá entrar en las subcarpetas, leer la información contenida en los archivos (por ejemplo, leer un documento de texto), leer los **atributos** de los archivos y carpetas y ejecutar programas contenidos en la carpeta.
- ⤴ **Cambiar:** si concedes este permiso a un usuario o grupo, éste podrá realizar las mismas acciones que si se le concede “Leer” y además podrá crear y eliminar archivos y subcarpetas, así como modificar sus atributos .
- ⤴ **Control total:** si concedes este permiso a un usuario o grupo, éste podrá realizar las mismas acciones que si se le conceden “Leer” y “Cambiar”, además de cambiar permisos y establecer el propietario de los objetos que contenga la carpeta (y de la propia carpeta).

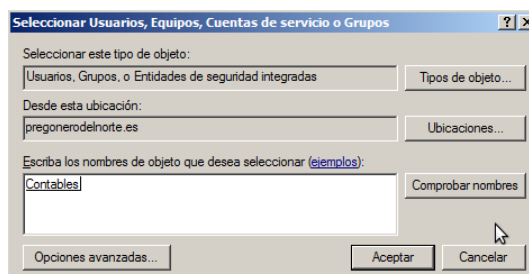
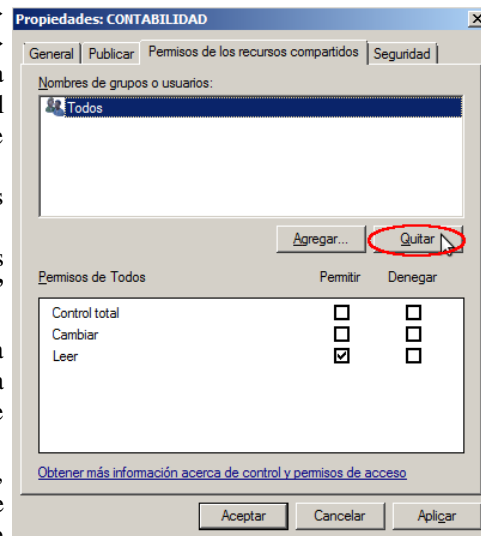


¡Cuidado! Cuando creas una carpeta y la compartes, los permisos por defecto pueden ser más permisivos de lo deseado. En concreto, a veces se le asigna el permiso “Leer” al grupo “Todos”, lo que implica que cualquiera que acceda a la carpeta compartida podrá ver su contenido (incluyendo al grupo “Invitados”, que pertenece a “Todos”). Generalmente, cuando se comparte un recurso, no se dejan los permisos por defecto, ya que estos son demasiado permisivos.

3.2.- Cómo establecer los permisos de compartición.

Puedes establecer los permisos de compartición desde dos lugares: desde el explorador de Windows y desde la herramienta “Administración de equipos”. Como puedes observar, se trata de los mismos lugares desde los que se puede compartir una carpeta. La herramienta “Administración de equipos” ofrece un entorno más potente y profesional, por lo que te vamos a enseñar los pasos para manejar los permisos utilizando este método.

1. En primer lugar, abre la herramienta en “Inicio” → “Panel de control” → “Herramientas administrativas” → “**Administración de equipos**”. Si deseas conectarte a otro equipo para manejar sus recursos compartidos, es el momento de hacerlo, siguiendo el procedimiento que te explicamos en la sección.
2. Dentro de la herramienta, accede a “Carpetas compartidas” → “**Recursos compartidos**”.
3. Haz clic con el botón secundario sobre el recurso cuyos permisos deseas configurar y selecciona “**Propiedades**” en el menú emergente.
4. En el cuadro que aparece, selecciona la pestaña “**Permisos de los recursos compartidos**”. Aparece una lista con los grupos y usuarios que tienen permisos sobre ese recurso.
5. Si deseas eliminar a algún usuario o grupo de la lista, selecciónalo y pulsa el botón “**Quitar**”. Esto hace que ese usuario o grupo deje de tener permisos (ojo, puede que siga accediendo al recurso si pertenece a algún grupo que sí tenga permisos).
6. Para añadir un usuario o grupo nuevo a la lista de los que tienen permisos, haz clic en el botón “**Agregar**”. Aparece un nuevo cuadro de diálogo.
7. Si sabes el nombre del usuario o del grupo que deseas agregar, escríbelo y pulsa “**Comprobar nombres**” y, si el nombre es correcto, pulsa “**Aceptar**”. Puedes introducir varios nombres separándoles por un punto y coma (;). Si no sabes el nombre, pulsa “**Opciones avanzadas**” y a continuación “**Buscar ahora**”. Aparece una lista de los grupos y usuarios del dominio. Elige los que desees y pulsa “**Aceptar**”.
8. Una vez que el grupo o usuario está en la lista, selecciónalo y, en la parte baja del cuadro de diálogo, **elige los permisos** que desees que tenga.
9. Pulsa aceptar y ya está.



Habrás observado que existen dos casillas para cada permiso: “**Permitir**” y “**Denegar**”. Las posibilidades, entonces se reducen a:

- ⚡ Marcar “Permitir”. Esto concede el permiso al grupo o usuario.
- ⚡ No marcar nada. El usuario o grupo no disfruta de ese permiso.
- ⚡ Marcar “Denegar”. El usuario o grupo no disfruta de ese permiso.

Existe una diferencia muy importante entre **denegar** un permiso y **no marcar nada**. Pero vas a tener que esperar a la sección siguiente para descubrirla.

3.3.- Cómo se combinan los permisos de compartición.

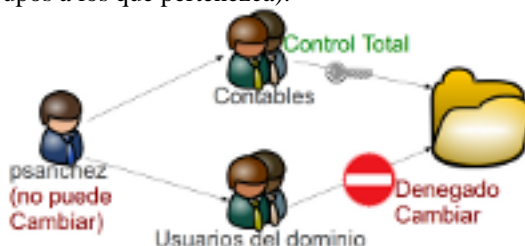
Ya sabes la mecánica para conceder permisos de compartición a usuarios y grupos. Pero es posible que te hayas preguntado lo siguiente: ¿qué pasa si concedo diferentes permisos a dos o más grupos y hay un usuario que pertenece a varios de esos grupos? ¿Qué permisos tendrá ese usuario? La respuesta se resume en los siguientes puntos:

1. Cuando concedes permisos a un grupo, todos los usuarios que pertenezcan a dicho grupo tendrán esos permisos.
2. Los permisos son **acumulativos**. ¿Qué significa esto? Supón que el usuario *psanchez* pertenece a los grupos *Contables* y también a *Usuarios del dominio*. Además, existe una carpeta llamada *CONTABILIDAD* con los siguientes permisos:

GRUPO	PERMISOS DE COMPARTICIÓN
Contables	Control Total
Usuarios del dominio	Leer

Como los permisos son acumulativos, el usuario *psanchez* tiene permisos Control Total + Leer, es decir, **Control Total** (que ya incluye a Leer).

3. Denegar invalida a otros permisos. En el ejemplo anterior, si *Usuarios del dominio* tuviera marcada la casilla “denegar” en “Cambiar”, el usuario *psanchez* no podría realizar cambios en la carpeta, porque pertenece a un grupo que lo tiene denegado. Debido a este comportamiento, no se recomienda abusar de la opción “Denegar”. Si no deseas que un grupo tenga un determinado permiso, simplemente no marques ni “Permitir” ni “Denegar” (y asegúrate de que no pertenezca a otro grupo que sí tenga ese permiso). Utiliza “Denegar” sólo para casos muy concretos (por ejemplo, para evitar que un usuario concreto que ha abusado del espacio de almacenamiento pueda crear archivos nuevos, independientemente de los grupos a los que pertenezca).



Siempre que desees compartir un recurso, debes configurar los permisos para que sólo puedan acceder aquellos grupos y usuarios que deban hacerlo. **Nunca** dejes los **permisos por defecto**. Y procura, siempre, dar a los usuarios **el mínimo acceso que necesiten** y, además, procurando no utilizar las casillas de “Denegar”. Si un grupo o usuario sólo necesita leer una carpeta, no le concedas Leer y Cambiar, porque eso puede provocar pérdidas de datos y otros inconvenientes, pero tampoco hace falta que le deniegues el permiso Cambiar. Bastaría con no marcar nada.

4.- Permisos locales o NTFS.

CASO PRÁCTICO

Laura llega a la oficina de CARMINFO S. L. un lunes por la mañana. Al sentarse en su mesa exclama:

-¡En casa del herrero, cuchillo de palo!

Todos la miran extrañados:

-¿Qué pasa, Laura? -pregunta Marisa.

-Pasa que mis padres me están volviendo loca con su ordenador ya que mi hermana pequeña les ha borrado todas las fotos.

-¿Y eso? -pregunta Alberto.

-Tienen Windows 7. Les hice una cuenta de usuario a cada uno, incluyendo a mi hermana. Pues bien, ha seleccionado todo el contenido de la carpeta en la que mis padres tenían todas las fotos familiares y lo ha borrado. Y no lo ha mandado a la papelera, no, no. ¡Lo ha borrado del todo! Anoche me llamaron mis padres desesperados para ver si puedo recuperar los datos.

-Pero... ¿no modificaste los permisos locales para que tu hermana no pudiera hacer eso? -pregunta Carmen.

-Pues... no -responde Laura, apurada-. No pensé que fuera a pasar nada.

-Error, y de los grandes. Seguro que ya no te vuelve a pasar. -dice Marisa.

Esa misma tarde, Laura fue a casa de sus padres y recuperó la mayoría de las fotos, utilizando un software de recuperación de datos. Inmediatamente después, configuró los permisos locales de todas las carpetas con datos “sensibles” para que la cuenta de usuario de su hermanita no pudiera eliminar ni cambiar nada.

Los permisos locales son los que controlan el acceso a los recursos en el nivel más bajo. Dicho de otra forma: un usuario nunca podrá acceder a un recurso con más privilegios que los indicados en los permisos locales. En sistemas Windows, sólo puedes utilizar permisos locales cuando los recursos están ubicados en **particiones NTFS** (NTFS significa NT File System). Por eso, en el título de este capítulo aparecen estas siglas. Si el recurso se encuentra en una **partición FAT** (FAT significa File Allocation Table), no se le aplican permisos locales. Es decir, cuando un usuario inicie sesión en ese equipo, siempre podrá acceder a los recursos ubicados en una partición FAT, pues no hay permisos aplicables. Esto es así porque la estructura de archivos FAT no soporta la definición de permisos.

Si el acceso se hace a través de la red, mediante la compartición de carpetas, entran en juego también los permisos de recursos compartidos. Aprenderás cómo se combinan los permisos locales y los permisos de compartición en la sección siguiente. En este capítulo también aprenderás cómo establecer el propietario de una carpeta o de un archivo, cómo se heredan los permisos y, por supuesto, cómo establecerlos.

4.1.- Relación entre los permisos de compartición y los permisos locales.

Los permisos de compartición y los permisos locales se relacionan entre sí dependiendo de cómo se acceda a la carpeta o el archivo. Y es que existen dos formas de acceder a una carpeta o archivo:

- ✦ **A través de la red:** existe una carpeta compartida y accedemos a ella utilizando su ruta de red, como has aprendido en el capítulo anterior. Como ejemplo, hemos utilizado la ruta `\\SERVER2008\FotosPablo`.
- ✦ **De forma local:** independientemente de si la carpeta está compartida o no, puedes acceder a ella iniciando sesión en el equipo en el que está ubicada y recorriendo el sistema de archivos. Como ejemplo, en el capítulo anterior, hemos utilizado `D:\psanchez\Fotos`.



La correspondencia entre los tipos de acceso y los permisos es la siguiente:

TIPO DE ACCESO	CONJUNTO DE PERMISOS QUE SE APLICA
Local.	Permisos locales (si el recurso está en una partición NTFS).
A través de la red.	Permisos de compartición. + Permisos locales (si el recurso está en una partición NTFS). El S. O. compara los dos conjuntos de permisos y aplica la combinación más restrictiva .

Veámoslo con un ejemplo. Imagina que el usuario *psanchez* tiene los siguientes conjuntos de permisos sobre la carpeta `D:\psanchez\Fotos`, ubicada en una partición formateada con NTFS. Recuerda que si el recurso está en una partición FAT, no se tienen en cuenta los permisos locales, ¡porque no existen!

PERMISOS DE COMPARTICIÓN	PERMISOS LOCALES (NTFS)
Sólo leer.	Control total.

Cuando el usuario acceda de forma local, podrá hacer lo que quiera en la carpeta, como borrar archivos, porque tiene “Control total”. Sin embargo, cuando acceda a través de la red, **se aplica la combinación más restrictiva** entre ambos permisos, por lo que sólo podrá leer los archivos contenidos en la carpeta. Otro ejemplo sería el siguiente:

PERMISOS DE COMPARTICIÓN	PERMISOS LOCALES (NTFS)
Control total.	Sólo leer.

En este caso, cuando el usuario acceda de forma local, sólo podrá realizar acciones de lectura. Cuando acceda a través de la red, se combinan ambos permisos y se aplica lo más restrictivo, resultando que... ¡sólo puede realizar acciones de lectura, a pesar de haber asignado “Control total” en los permisos de compartición!

A veces es interesante que el nivel de acceso a un recurso sea idéntico cuando se accede a través de la red y cuando se accede en modo local. Dicho de otra forma, a veces nos interesa que tanto a través de la red como en modo local, los permisos que intervengan sean los permisos locales o NTFS. En tal caso, lo que debes hacer es asignar control total al **grupo Todos** en los permisos de compartición. De esa forma, todo el control de acceso recae en los permisos locales o NTFS. Ten cuidado con esto: a través de la red se podrá hacer lo mismo que en modo local, y eso no siempre es deseable.

4.2.- Establecer el propietario de archivos y carpetas.

Antes de que aprendas a establecer los permisos locales, es necesario que asimiles dos importantes conceptos:

- 1) La propiedad sobre carpetas y archivos .
- 2) La herencia de permisos.

En esta sección nos ocupamos del primero de estos dos conceptos y en la sección siguiente, aprenderás en qué consiste el segundo.

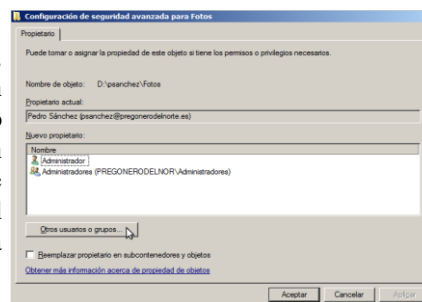
Cada **carpeta y archivo** en una partición NTFS **tiene un propietario**. El propietario puede ser un grupo o un usuario. Normalmente, el propietario de un elemento es el usuario que lo crea. Sin embargo, el propietario se puede cambiar con posterioridad y, además, las carpetas y los archivos del sistema tienen diferentes propietarios en función de las necesidades.

Ser el propietario de un elemento significa tener **SIEMPRE** la posibilidad de **cambiar sus permisos**. Por ejemplo, supón el usuario *psanchez* es el propietario de la carpeta *Fotos*. Ahora, imagina que en la lista de permisos, el usuario *psanchez* no tuviera ningún permiso asignado o, incluso, que los tuviera TODOS denegados. Pues bien, aún así, al ser el usuario *psanchez* el propietario de la carpeta *Fotos*, podría cambiar los permisos y recuperar el control sobre la carpeta.

Existe la posibilidad de “tomar posesión” de un elemento, es decir, de **que un usuario se convierta en el propietario** de una carpeta o archivo que no le pertenece previamente. ¿Qué usuarios pueden hacer esto? La respuesta es: los miembros del grupo *Administradores*, que lo pueden hacer siempre, y cualquier usuario que tenga asignado el permiso local “Tomar posesión”. El usuario propietario de una carpeta o archivo también puede “transferir la propiedad” a otro usuario.

Para ver el propietario de un archivo y para tomar posesión o transferir la propiedad de un elemento, haz clic con el botón secundario y elige “Propiedades” en el menú emergente. Después, selecciona la pestaña “Seguridad” y pulsa el botón “Opciones avanzadas”. Aparece un nuevo cuadro de diálogo llamado “Configuración de seguridad avanzada”. En él, selecciona la pestaña “Propietario”.

Se muestra el propietario actual (en la imagen, Pablo Sánchez, *psanchez*). Para cambiar el propietario, hay que pulsar el botón “Editar”. Se puede seleccionar el usuario *Administrador*, el grupo *Administradores* o cualquier otro usuario o grupo, pulsando el botón correspondiente. Una vez seleccionado el usuario o grupo deseado, se pulsa “Aceptar”. Si el elemento es una carpeta, y deseas cambiar el propietario en los elementos contenidos en ella, marca la casilla “Reemplazar propietario en subcontenedores y objetos”.



El grupo *Administradores* SIEMPRE puede convertirse en el propietario de una carpeta o archivo. Consecuencia: como los propietarios de los archivos y las carpetas SIEMPRE pueden cambiar los permisos, y los *Administradores* SIEMPRE pueden convertirse en propietarios, entonces, indirectamente, nunca se puede evitar que un *Administrador* asigne los permisos que desee, previa toma de posesión del elemento.

4.3.- Herencia de permisos NTFS.

Como es lógico y has podido comprobar, cuando un nuevo elemento (archivo o carpeta) es creado, cuenta con ciertos permisos “**por defecto**”. ¿De dónde salen estos permisos? ¿Cuáles son? La respuesta a estas preguntas la encontrarás en la herencia.

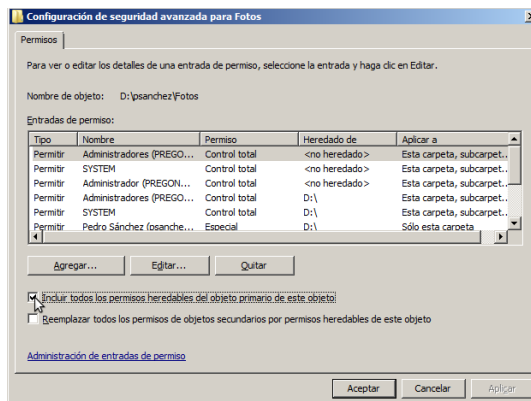
Cada vez que creas una carpeta o un archivo, este elemento **hereda** los permisos de la carpeta dentro de la cual lo has creado. Así de simple. Por ejemplo, si el grupo *Usuarios del dominio* tiene permiso para leer en la carpeta “Fotos”, y *psanchez* crea una subcarpeta llamada “Cena de diciembre”, el grupo *Usuarios del dominio* podrá leer en la nueva subcarpeta.

Al asignar un permiso nuevo sobre una carpeta, éste se propaga hacia abajo en la jerarquía de archivos y carpetas, gracias al mecanismo de **herencia**. Por ejemplo, si se le concede permiso de escritura al grupo *Usuarios del dominio* sobre la carpeta “Fotos”, automáticamente ese grupo también podrá escribir sobre la carpeta “Cena de diciembre”.

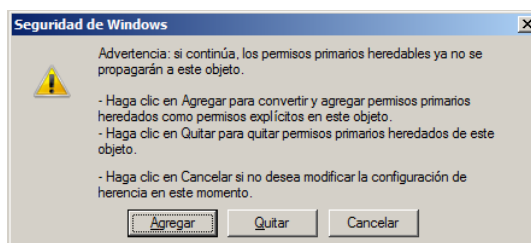
Cuando un elemento tiene un permiso heredado, dicho permiso no se puede eliminar, a no ser que se **rompa la línea de herencia**. Es decir, no podrías quitar el permiso de escritura al grupo *Usuarios del dominio* sobre la carpeta “Cena de diciembre”, hasta que no rompieses la herencia, ya que ese permiso se está heredando desde la carpeta superior llamada “Fotos”.

¿Qué es eso de “romper la herencia”? La herencia es automática, viene establecida por defecto, pero no es inevitable. Si no deseas que una determinada carpeta (o un determinado archivo) herede los permisos de su “carpeta madre” debes hacer lo siguiente:

1. Haz clic sobre el elemento con el botón secundario y elige “**Propiedades**”.
2. Selecciona la pestaña “**Seguridad**”.
3. Pulsa el botón “**Opciones avanzadas**”.
4. En la pestaña “Permisos” pulsa el botón “**Cambiar permisos**”.



5. En la parte de abajo existe una casilla de verificación con la leyenda “Incluir todos los permisos heredables del objeto primario de este objeto”. Por defecto estará marcada. Para romper la herencia, desmárcala. En ese momento, aparece una ventana con tres opciones:
 - **Agregar:** la herencia se romperá, pero se hará una copia de todos los permisos heredables de la carpeta madre en los permisos del elemento con el que estamos trabajando.
 - **Quitar:** se rompe la herencia y se deja la lista de permisos en blanco, con lo que nadie podrá acceder hasta que no asignemos algún permiso.
 - **Cancelar:** detiene la acción.



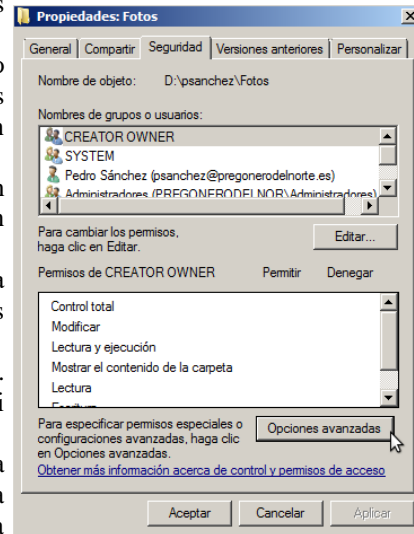
6. Pulsa “Aceptar” hasta cerrar todos los cuadros de diálogo.

4.4.- Significado de los permisos locales o NTFS.

Antes de que te lances a asignar permisos locales sin parar, conviene que sepas exactamente qué se puede hacer y qué no con cada permiso. En primer lugar, debes saber que los permisos NTFS se pueden asignar desde dos cuadros de diálogo diferentes: el de los permisos básicos y el de los permisos avanzados. En realidad, los permisos **básicos** son una especie de resumen de los permisos **avanzados**. Dicho de otra manera: un permiso básico puede equivaler a dos o tres permisos avanzados.

A continuación puedes encontrar la lista y significado de los permisos avanzados:

- ✦ **Recorrer carpeta / ejecutar archivo:** si tienes este permiso puedes entrar en la carpeta. Si se trata de un archivo, podrás ejecutarlo (sólo tiene sentido para archivos que contengan algún tipo de programa o guión).
- ✦ **Listar carpeta / leer datos:** si el elemento es una carpeta, con este permiso puedes ver su contenido. Si es un archivo, con este permiso puedes ver los datos que contiene.
- ✦ **Atributos de lectura:** está mal traducido. Debería ser “lectura de atributos” y, si tienes este permiso, puedes ver los atributos del elemento.
- ✦ **Atributos extendidos de lectura:** también está mal traducido. Debería ser “lectura de atributos extendidos” y lógicamente, si disfrutas de este permiso podrás ver dichos datos.
- ✦ **Crear archivos / escribir datos:** si el elemento es una carpeta y posees este permiso, podrás crear archivos dentro de la misma. Si el elemento es un archivo, este permiso te concede la capacidad de escribir información dentro del mismo.
- ✦ **Crear carpetas / anexar datos:** si el elemento es una carpeta, este permiso te concede la capacidad de crear subcarpetas en ella. Si se trata de un archivo, podrás añadir información al final del archivo.
- ✦ **Atributos de escritura:** está mal traducido. Debería ser “escritura de atributos” y te permite modificar los mismos.
- ✦ **Atributos extendidos de escritura:** al igual que en el caso anterior, está mal traducido y debería ser “escritura de atributos extendidos”.
- ✦ **Eliminar subcarpetas y archivos:** te permite eliminar, como su propio nombre indica, el contenido de la carpeta sobre la que se concede el permiso.
- ✦ **Eliminar:** te permite eliminar el elemento en sí.
- ✦ **Permisos de lectura:** también está mal traducido. Debería ser “lectura de permisos” y te permite ver los permisos de la carpeta o archivo, pero no cambiarlos.
- ✦ **Cambiar permisos:** con este permiso podrás alterar los permisos del elemento.
- ✦ **Tomar posesión:** con este permiso podrás convertirte en propietario del elemento.



Como ves, es una lista bastante larga, pero que permite un ajuste muy fino del acceso a las carpetas y archivos.

DEBES CONOCER

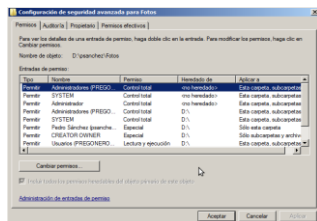
En cuanto a los permisos básicos, puedes encontrar su equivalencia con los permisos avanzados en el siguiente enlace:

Texto enlace: Correspondencia entre los permisos básicos y los avanzados.

URL: <http://technet.microsoft.com/es-es/library/cc732880.aspx>

Ahora que ya tienes claro qué significa ser el propietario de una carpeta o archivo, cómo funciona la herencia de permisos y qué representa cada permiso, ha llegado el momento de que aprendas a establecerlos.

En este cuadro de diálogo, cuando seleccionas un usuario o un grupo de la lista, en la parte de abajo se pueden ver los permisos que tiene asignados. Los permisos que ves en este cuadro de diálogo son los permisos básicos, pero si haces clic en el botón “Opciones avanzadas”, accederás a otro cuadro de diálogo, llamado **“Configuración de seguridad avanzada”** en el que puedes configurar los permisos avanzados, que permiten mayor nivel de control que los básicos.



Cuando aprendiste el comportamiento de los permisos de compartición, te dijimos que cuando concedes permisos a un grupo:

- ✓ Todos los usuarios que pertenezcan a dicho grupo tendrán esos permisos.
- ✓ Los permisos son acumulativos.
- ✓ Denegar invalida a otros permisos.

- ✓ Asignar siempre el mínimo nivel de acceso necesario.
- ✓ No utilizar la opción de denegar a menos que sea estrictamente necesario.

Puedes profundizar en todo lo relacionado con los permisos en este enlace:

Texto enlace: Permisos locales o NTFS.

URL: <http://technet.microsoft.com/es-es/library/cc770962.aspx>

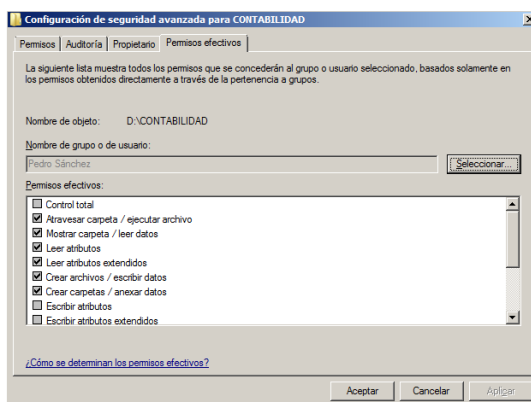
4.6.- Permisos efectivos.

¿Te has parado a pensar en **cómo saber exactamente** que es lo que puede hacer o no un usuario sobre un determinado archivo o carpeta? Una respuesta irreflexiva a este interrogante podría ser: “fácil, sólo hay que mirar los permisos que tiene asignado dicho usuario en la ACL correspondiente”. Esta afirmación no es del todo cierta. Imagina que el usuario *psanchez* pertenece a los grupos *Contables* y *Usuarios del dominio*. Sobre la carpeta “CONTABILIDAD”, *Contables* tiene permiso de control total y *Usuarios del dominio* tiene permiso de Lectura. Está claro que en este caso, *psanchez* no aparece en la lista de usuarios y grupos con permisos sobre la carpeta. Sin embargo, tiene control total sobre la misma, por el hecho de pertenecer a *Contables*. De modo que esa no es la forma de conocer lo que un usuario puede o no puede hacer.

Evidentemente, existe la posibilidad de **explorar** la estructura de usuarios y grupos para determinar a qué grupos pertenece un usuario y después comprobar la ACL del archivo o la carpeta. Pero no olvidemos que **unos grupos pueden pertenecer también a otros**, lo que puede convertir este proceso en interminable y con tendencia a errores.

Tiene que existir una forma más directa y sencilla de saber qué permisos tiene **realmente** un grupo o un usuario sobre un determinado elemento. Y así es: **se trata de los permisos efectivos**.

Si deseas saber qué permisos tiene el usuario *psanchez* sobre la carpeta “CONTABILIDAD”, haz clic con el botón secundario del ratón sobre ella, elige “Propiedades” y la pestaña “Seguridad”. En este punto, pulsa el botón “Opciones avanzadas”. A continuación, elige la pestaña “Permisos efectivos”. En esta pestaña, pulsando el botón “Seleccionar”, puedes elegir el usuario o grupo cuyos permisos reales o efectivos desees conocer. En el ejemplo, elegirías *psanchez*. Al elegir un usuario o grupo puedes ver, en la parte de abajo, los permisos de los que dicho usuario disfruta. Se muestra la lista de acciones con una casilla de verificación a su izquierda. Si la casilla está marcada, el usuario puede realizar dicha acción. Si la casilla no está marcada, no pueda.



De esta forma, los administradores y administradoras pueden asegurarse de que los permisos que están asignando funcionan tal y como quieren.

4.7.- Estrategias A G U DL P y A G DL P.

Asignar permisos es fácil. Lo realmente **difícil es decidir qué permisos se asignan y a quién**. En este sentido, existen diferentes pautas que un buen administrador o administradora debe seguir. Ya te hemos dicho algunas: **asignar siempre el mínimo nivel de acceso y no abusar de la opción denegar**. Hay otra recomendación que siempre debes seguir: **asigna permisos a grupos antes que a usuarios individuales**. Esto facilita muchísimo la administración de los permisos. Es muy fácil verlo: es mucho más fácil agrupar a cincuenta usuarios con requerimientos de acceso similares y asignar permisos a ese grupo, que asignar permisos a cincuenta usuarios individualmente. Haciendo esto te ahorrarás tiempo y, sobre todo, errores.

Ahora bien, no es lo mismo asignar permisos dentro de un dominio solitario que dentro de un bosque con varios dominios. Si alguna vez tienes que decidir los permisos que se van a asignar a los recursos de un dominio completamente aislado y que nunca se va a unir a otros dominios, puedes utilizar **grupos globales** para agrupar a los usuarios y asignar permisos sobre los recursos a dichos grupos globales.

Sin embargo, si tu dominio pertenece a un bosque con más dominios, o es previsible que así sea en un futuro, debes planificar mejor tu estrategia de asignación. Y de ahí vienen las siglas del título de este apartado.

- ⚡ **A** (Account): representa las cuentas de usuario y de equipo.
- ⚡ **G** (Global): representa los grupos globales.
- ⚡ **U** (Universal): representa los **grupos universales**.
- ⚡ **DL** (Domain Local): representa los **grupos locales de dominio**.
- ⚡ **P** (Permission): representa los permisos.

La estrategia consiste en lo siguiente: se agrupan las cuentas de usuario y de equipo (A) en grupos globales (G). A su vez, a los grupos globales se les hace miembros de grupos universales (U). Estos grupos universales serán miembros de grupos locales de dominio (DL) que serán a los que finalmente se les asignen los permisos (P).

¿Recuerdas el bosque *garabato.es*, que fue uno de los ejemplos que desarrollamos en la unidad anterior? Si un usuario del dominio *valencia.garabato.es* debe tener permiso para imprimir en la impresora *láser* del dominio *santander.garabato.es*, lo que se hace es seguir esta estrategia, de modo que el usuario tendrá dicho permiso a través de las pertenencias a distintos grupos. En la figura puedes ver la cadena de pertenencias que se produce.

Hemos utilizado como ejemplo un permiso sobre una impresora. Hablaremos de los permisos de impresión en la sección siguiente. Pero ten en cuenta que se seguiría exactamente el mismo proceso en el caso de tratarse de carpetas o archivos.

En escenarios de bosques con uno o más dominios también se utiliza ampliamente la estrategia **A G DL P**, que es similar a la anterior, pero se diferencia en que **no se utilizan grupos universales**. Es decir, las cuentas de usuario y de equipo (A) se agrupan en grupos globales (G). Por otro lado, se crean grupos locales de dominio (DL) y se les conceden permisos (P) sobre los recursos. Según qué permisos sean necesarios, se hace a los grupos globales miembros de los grupos locales de dominio. Esta estrategia se utiliza cuando no se requiere una administración centralizada de los grupos globales (que es el motivo de agruparlos en grupos universales).

En resumen, si el bosque en el que trabajas tiene un único dominio con pocos usuarios y no se prevé que vaya a crecer, entonces utiliza grupos globales. Si tu bosque tiene uno o más dominios, pero la estructura de grupos no aconseja utilizar grupos universales, entonces emplea A G DL P. Sin embargo, en un ejemplo como el de la imagen, en el que sí tiene sentido aglutinar los grupos globales en grupos universales, entonces utiliza la estrategia A G U DL P.



5.- Configurar una impresora compartida en red.

CASO PRÁCTICO

Uno de los grandes problemas con los que tienen que luchar en el Pregonero del Norte es con la utilización de las impresoras. Actualmente utilizan dos:

- La destinada a las impresiones habituales de oficina: para poder imprimir en ella hay que iniciar sesión localmente en el ordenador al que está conectada, ya que no es una impresora de red, ni tampoco se encuentra compartida.
- La de mayor calidad, que se utiliza para las pruebas finales de impresión. Esa sí es una impresora de red y su tóner es muy caro. Los empleados y empleadas abusan de su utilización, porque es más accesible que la otra.

En CARMINFO S. L. discuten sobre cómo solucionar el problema. Laura sugiere:

-Creo que lo más lógico sería utilizar el equipo con Windows Server para conectar las impresoras y compartirlas en red.

-Sí, es lo que vamos a hacer -interviene Carmen-. Así podremos asignar permisos a cada impresora, de modo que sólo puedan imprimir en la impresora de alta calidad los de maquetación y los responsables de redacción, que es lo que nos han pedido.

-También hay que facilitar el acceso a la impresora común. De esa forma el trabajo del resto de los componentes del periódico no se verá afectado -apunta Laura.

-Efectivamente -responde Carmen-, ambas impresoras estarán disponibles a través del servidor.

-Déjame que lo configure yo -dice Laura-. Tengo ganas de ver cómo es el proceso en la última versión de Server.

5.1.- Compartición de impresora y asignación de permisos.

Para compartir una impresora, primero debes configurarla en el equipo en que está conectada. Para hacer esto, entra en el panel de control, selecciona “iconos grandes” o “iconos pequeños” en el desplegable “ver por:” y accede a “dispositivos e impresoras”. En esta ventana, elige agregar una impresora y sigue los pasos del asistente que a continuación te detallamos. (Ten en cuenta que puedes realizar este proceso aún sin contar físicamente con una impresora, ya que la configuración de la misma, de sus permisos y la conexión a la impresora compartida desde un cliente, pueden realizarse con fines didácticos sin trabajar con un equipo real).

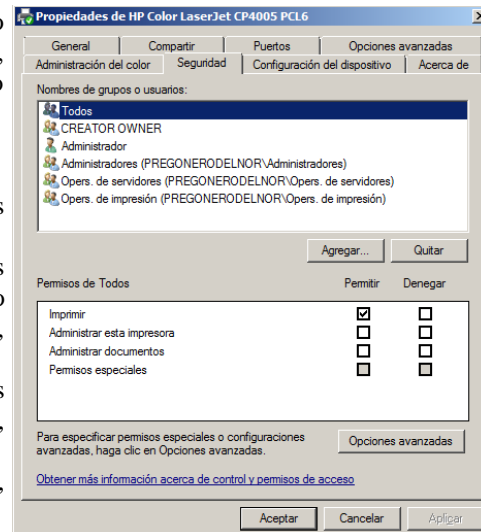
1. Elige si la impresora es **local** (se conecta físicamente al equipo en el que la estás configurando) o de **red** (se comunica con el equipo que estás configurando mediante red, tanto de cable como inalámbrica. En este caso, **elegirías “impresora local”**, porque estamos suponiendo que está físicamente conectada al equipo en el que estás ejecutando este asistente.
2. Elige el puerto por el que se conecta la impresora. Lo habitual será que el equipo haya **detectado automáticamente** el puerto.
3. Selecciona la marca y el modelo de la impresora. **Si no aparece en la lista**, tendrás que pulsar el botón **“utilizar disco”** y seleccionar los controladores de tu modelo de impresora, que tendrás en un disco o habrás descargado de Internet previamente.
4. Escribe un nombre para la impresora. Este será el **nombre con el que identificarás la impresora** en el equipo local. Más adelante, cuando la compartas en red, puedes elegir otro nombre, como sucede con las carpetas compartidas.
5. El propio asistente te da la opción de compartir la impresora si lo deseas. En ese caso, puedes elegir un nombre en el cuadro de texto **“Recurso compartido:”**. Por ejemplo, en el Pregonero del Norte, pueden llamar a una de sus impresoras “AltaCalidad” y a la otra “Normal”, para distinguirlas. Opcionalmente, puedes escribir la ubicación de la impresora y un comentario.
6. Pulsa el botón “Finalizar”.

Siguiendo estos pasos, la impresora queda instalada y compartida en red. Como has podido comprobar es un proceso muy sencillo. Lo verdaderamente interesante de compartir una impresora en red es configurar los **permisos de impresión**. De modo que, una vez que has finalizado el asistente y, por lo tanto, aparece el icono de la impresora en la ventana “dispositivos e impresoras”, haz clic con el botón secundario del ratón en dicho icono y selecciona **“propiedades de impresora”**. En el cuadro de diálogo que aparece tienes dos pestañas que te resultarán familiares: “compartir” y “seguridad”. En la primera puedes configurar opciones relacionadas con la compartición. En la pestaña “seguridad” puedes configurar los permisos sobre la impresora.

Como puedes ver, los permisos por defecto incluyen al grupo “Todos” con permiso de imprimir. Esto significa que, por defecto, todos los usuarios pueden imprimir en el dispositivo. Esto no es lo que se pretende, por ejemplo, en el Pregonero del Norte.

Veamos qué posibilidades te ofrecen estos permisos:

- **Imprimir:** Si tienes asignado este permiso, como podrás adivinar, puedes imprimir trabajos en la impresora.
- **Administrar esta impresora:** Con este permiso puedes realizar tareas de administración de la impresora, como por ejemplo, compartirla en red, cambiar su nombre, asignarle otros controladores, etc.
- **Administrar documentos:** esto te permite gestionar los documentos de la cola de impresión: parar trabajos, reanudarlos, eliminarlos...
- **Permisos especiales:** estos incluyen leer los permisos, cambiarlos y tomar posesión de la impresora.



El mecanismo de asignación de permisos es igual al de las carpetas, salvo que en este caso no existe el concepto de herencia, aunque sí el de propietario.

No olvides que las recomendaciones para asignar los permisos de impresión son similares a las de los permisos de las carpetas: concede siempre el mínimo nivel de acceso necesario, no abuses de la opción “denegar” y utiliza siempre que puedas la estrategia A G U D L P.

5.2.- Conectarse a la impresora compartida.

A estas alturas, ya sabes cómo configurar una impresora en red. Ahora ha llegado el momento de utilizarla. Para ello, vamos a mostrarte el proceso para utilizar la impresora desde un equipo cliente, que pertenece al mismo dominio que el equipo en el que se ha configurado y compartido la impresora.

En el equipo cliente, los usuarios podrán acceder a la impresora a través de su nombre completo de recurso compartido, como si fuera una carpeta. En el ejemplo de la figura, este nombre de recurso compartido será `\\Server2008\Normal`. Sólo podrán conectarse a la impresora (y por lo tanto, utilizarla) aquellos usuarios que cuenten, al menos, con permiso para imprimir en la ACL de la impresora.

