Permisos NTFS

El sistema de archivos NTFS permite la seguridad de los datos. La seguridad asociada al sistema de archivos NTFS permite:

- Conceder permisos a carpetas y archivos para controlar el nivel de acceso de los usuarios a los recursos.
- Usar el espacio del disco duro más eficazmente permitiéndonos comprimir datos y configurar cuotas de disco.
- Cifrar datos de archivos en el disco duro físico utilizando el Sistema de archivos Encriptado (Encrypting Fyle System, EFS).

Estrategia A G DL P

Para dar seguridad a archivos y carpetas en particiones NTFS, concedemos permisos NTFS para cada usuario utilizando la cuenta individual o utilizando grupos. En ell caso de un dominio, se recomienda utilizar grupos locales del dominio para conceder acceso a un recurso utilizando la estrategia A G DL P. Ésta estrategia consiste en ubicar cuentas de usuario (A) en grupos globales (G), ubicar los grupos globales en grupos locales del dominio (DL), y conceder permisos (P) al grupo local del dominio.
Explica qué son grupos globales, grupos locales y dominio

Lista de control de acceso

NTFS almacena una lista de control de acceso (Access Control List , ACL) con cada archivo y carpeta en una partición NTFS. La lista ACL contiene un listado de todas las cuentas de usuario, grupos y equipos a los que se ha concedido acceso al archivo o carpeta, y el tipo de acceso concedido.
Para que un usuario pueda acceder a un archivo o carpeta:

- La lista ACL debe contener una entrada, denominada entrada de control de acceso (Access Control Entry, ACE), para la cuenta de usuario, grupo o equipo al que pertenece el usuario.
- La entrada debe permitir específicamente el tipo de acceso solicitado por el usuario para que éste pueda tener acceso al archivo o carpeta.
- Si no existe ninguna entrada ACE en la lista ACL, Windows denegará al usuario el acceso al recurso.

Permisos NTFS

Utilizamos los permisos de NTFS para especificar qué usuarios, grupos y equipos pueden acceder a archivos y carpetas. Los permisos de NTFS también determinan qué pueden hacer los usuarios, grupos y equipos con el contenido del archivo o carpeta.

- Permisos de carpetas en NTFS: Podemos conceder permisos a carpetas para controlar el acceso a las carpetas y a los archivos y subcarpetas que contienen. La siguiente tabla muestra una lista de los permisos estándares de NTFS que podemos otorgar a carpetas y el tipo de acceso que proporciona cada permiso.

Permiso carpeta NTFS	Permite hacer al usuario
Lectura	Ver los archivos y subcarpetas y los atributos, propiedades y permisos de la carpeta.
Escritura	Crear nuevos archivos y subcarpetas, cambiar los atributos de la carpeta y ver sus propiedades y permisos.
Listar contenido en la carpeta	Ver los nombres de los archivos y subcarpetas.
Leer y Ejecutar	Cruzar carpetas, además de realizar las acciones permitidas por el permiso de Lectura y el permiso de Listar contenidos de la carpeta.
Modificar	Borrar la carpeta y realizar acciones permitidas por el permiso de Escritura y el permiso Leer y ejecutar.
Control total	Cambiar los permisos, tomar posesión, eliminar subcarpetas y archivos y realizar las acciones permitidas por el resto de permisos de NTFS.

Permisos NTFS de carpetas

- Permisos de archivos en NTFS: Podemos conceder permisos a archivos para controlar el acceso a ellos. La siguiente tabla muestra una lista de los permisos de archivos estándares de NTFS que podemos otorgar y el tipo de acceso que cada uno de ellos proporciona a los usuarios.

Permiso archivo NTFS	Permite hacer al usuario
Lectura	Leer el archivo y ver sus atributos, propiedades y permisos.
Escritura	Sobrescribir el archivo, cambiar sus atributos y visualizar sus propiedades y permisos.
Leer y Ejecutar	Ejecutar aplicaciones y realizar las acciones permitidas por el permiso de Lectura.
Modificar	Modificar y eliminar el archivo y realizar las acciones permitidas por el permiso de Escritura y el permiso Leer y ejecutar.
Control total	Modificar permisos, tomar posesión y realizar las acciones permitidas por el resto de permisos de archivo de NTFS.

Permisos NTFS de archivos

Nota: Cuando se formatea una partición NTFS, Windows concede automáticamente el permiso de "**Lectura y ejecución**" (en forma de permisos especiales) sobre la raíz al grupo **Todos**. Por defecto, el grupo Todos tendrá acceso sobre todas las carpetas y archivos creados en la carpeta raíz. Para restringir el acceso a usuarios autorizados, deberíamos cambiar los permisos predeterminados sobre las carpetas y archivos que creemos.

Aplicación de Permisos NTFS

Por defecto, cuando concedemos permisos a usuarios y grupos sobre una carpeta, los usuarios o grupos tienen acceso a las subcarpetas y archivos que ésta contiene. Es importante entender el modo en que las subcarpetas y los archivos heredan los permisos de NTFS desde las carpetas padre para poder utilizar la herencia en la propagación de permisos a archivos y carpetas.
Si concedemos permisos sobre un archivo o carpeta a una cuenta de usuario individual o a un grupo al que pertenezca el usuario, el usuario obtendrá varios permisos sobre el mismo recurso. Existen reglas y prioridades asociadas al modo en que NTFS combina múltiples permisos. Además, también es posible afectar a los permisos cuando copiamos o movemos archivos y carpetas.

Nota: Se recomienda asignar permisos a un recurso utilizando A G DL P. En otras palabras, asignar permisos a un recurso utilizando grupos locales del dominio en lugar de cuentas de usuario individuales.

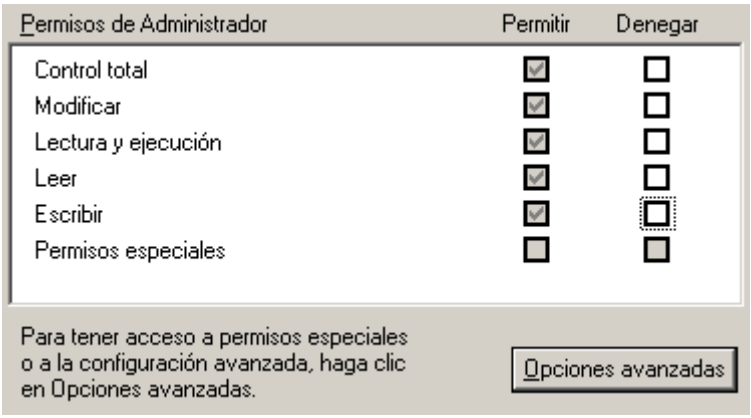
1. Múltiples Permisos NTFS

Si concedemos permisos de NTFS a una cuenta de usuario individual además de a un grupo al que pertenezca el usuario, estaremos concediendo múltiples permisos a dicho usuario. Existen reglas en la forma en que NTFS combina estos permisos múltiples para generar permisos eficaces para el usuario.

- Los permisos son **acumulativos**: Los permisos efectivos de un usuario sobre un recurso son la combinación de los permisos de NTFS concedidos a la cuenta de usuario individual y los concedidos a los grupos a los que pertenece el usuario. Por ejemplo, si un usuario tiene permiso de “Lectura” sobre una carpeta y pertenece a un grupo con permiso de “Escritura” sobre la misma carpeta, el usuario tendrá ambos permisos, “Lectura” y “Escritura”, sobre esa carpeta.
- Los permisos de archivo son independientes de los permisos de carpeta. Los permisos de archivo de NTFS tienen **prioridad** respecto a los permisos de carpetas de NTFS. Por ejemplo, un usuario con el permiso “Modificar” para un archivo podrá modificar el archivo aunque únicamente disponga del permiso de Lectura sobre la carpeta que contiene dicho archivo.
- Denegar invalida otros permisos. Se puede denegar el acceso a un determinado archivo o carpeta aplicando la denegación del permiso a la cuenta de usuario o grupo. Aunque un usuario tenga permiso para acceder al archivo o carpeta como miembro de un grupo, denegar el permiso al usuario bloquea cualquier otro permiso de que éste disponga. Por tanto, la denegación de permiso es una excepción a la regla acumulativa. Es aconsejable evitar la denegación de permiso ya que es más fácil permitir el acceso a usuarios y grupos que denegar el acceso específicamente. Ese preferible estructurar grupos y organizar recursos en carpetas de forma que otorgar permisos sea suficiente.

2. Herencia de permisos NTFS

Por defecto, los permisos concedidos a una carpeta padre se heredan y propagan a las subcarpetas y archivos contenidos en dicha carpeta padre. Sin embargo, podemos evitar que esto ocurra si deseamos que las carpetas o archivos tengan permisos diferentes a los de su carpeta padre.

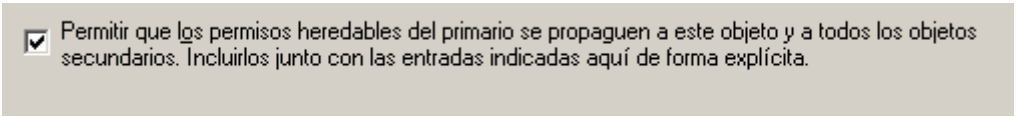


Permisos heredados

Los permisos concedidos a una carpeta padre son aplicables también a las subcarpetas y archivos que contiene. Cuando concedemos permisos de NTFS para dar acceso a una carpeta, estamos concediendo permisos sobre la carpeta, sobre cualquier archivo y subcarpeta existentes, y sobre cualquier nuevo archivo o subcarpeta que se cree en la carpeta.

2.1 Evitar la herencia de permisos

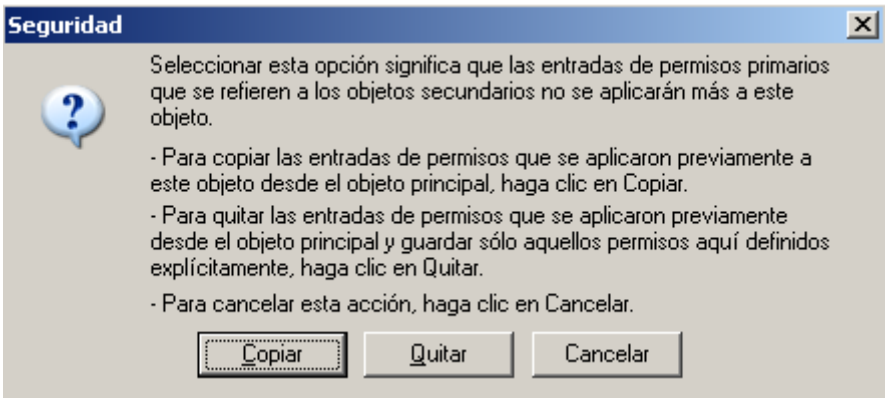
En general, deberíamos permitir que el SO propague los permisos de una carpeta padre a las subcarpetas y archivos que contiene. La propagación de permisos simplifica la asignación de permisos a recursos. Sin embargo, es posible que en ocasiones deseemos evitar la herencia de permisos. Por ejemplo, es posible que necesitemos guardar todos los archivos del departamento de ventas en una carpeta Ventas para la que todos los miembros de dicho departamento tengan permiso de Escritura. Sin embargo, debemos limitar los permisos sobre algunos archivos de la carpeta con el permiso de Lectura únicamente. Por tanto, deberíamos evitar la herencia para que el permiso de Escritura no se propague a los archivos contenidos en la carpeta. Por defecto, las subcarpetas y archivos heredan los permisos concedidos sobre sus carpetas padre, como se muestra en las **Opciones avanzadas** de la ficha **Seguridad** del cuadro de texto **Propiedades** cuando está seleccionada la casilla de verificación siguiente:



Casilla de verificación para permitir o impedir la herencia

Para evitar que una subcarpeta o archivo herede permisos de una carpeta

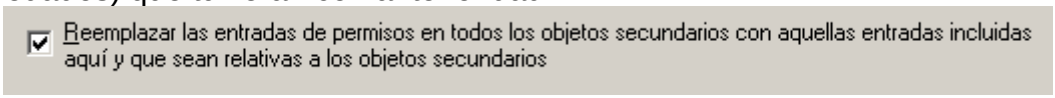
padre, debemos desmarcar dicha casilla y seleccionar una de las siguientes opciones:



Opciones si desmarcamos las casilla de propagar la herencia

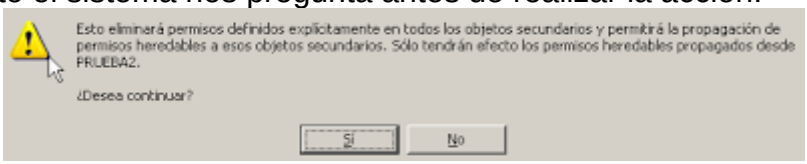
- **Copiar**: Copia permisos previamente heredados desde la carpeta padre a la subcarpeta o archivo y deniega la posterior herencia de permisos desde la carpeta padre.
- **Quitar**: Elimina los permisos heredados concedidos sobre la carpeta padre desde la subcarpeta o archivo y conserva únicamente los permisos explícitamente concedidos sobre la subcarpeta o archivo.

Existe la opción también de propagar los permisos desde una carpeta a los objetos de su interior, eliminando todos aquellos permisos explícitos (no heredados) que tuvieran con anterioridad.



Casilla de verificación para forzar la propagación de permisos heredables

Por supuesto el sistema nos pregunta antes de realizar la acción:



2.2 Copiar archivos y carpetas

Cuando copiamos o movemos un archivo o carpeta, los permisos pueden cambiar dependiendo del lugar dónde movemos el archivo o carpeta. Es importante entender los cambios sufridos por los permisos cuando se mueven o copian.

Copiar un archivo o carpeta tiene los siguientes efectos en los permisos de NTFS:

- Cuando copiamos una carpeta o archivo dentro de una única partición NTFS, la copia de la carpeta o archivo hereda los permisos de la carpeta de destino.
- Cuando copiamos una carpeta o archivo entre particiones NTFS, la copia de la carpeta o archivo hereda los permisos de la carpeta de destino.

- Cuando copiamos archivos o carpetas a particiones que no son NTFS, como FAT, las carpetas y archivos pierden sus permisos de NTFS, porque las particiones que no son NTFS no soportan los permisos de NTFS.

Nota: Para copiar archivos y carpetas dentro de una única partición NTFS o entre particiones NTFS, debemos disponer del permiso de “Lectura” sobre la carpeta original y permiso de “Escritura” sobre la carpeta de destino.

2.3 Mover archivos y carpetas

Cuando movemos un archivo o carpeta, los permisos pueden cambiar dependiendo de los permisos de la carpeta de destino. Mover un archivo o carpeta tiene los siguientes efectos en los permisos de NTFS:

- Cuando movemos una carpeta o archivo dentro una partición NTFS, la carpeta o archivo conserva sus permisos originales.
- Cuando movemos una carpeta o archivo entre particiones NTFS, la carpeta o archivo hereda los permisos de la carpeta de destino. Si lo pensamos bien mover una carpeta o archivo entre particiones es copiar la carpeta o archivo a la nueva ubicación y eliminarlo de su antigua ubicación.
- Cuando movemos archivos o carpetas a particiones que no son NTFS, las carpetas y archivos pierden sus permisos de NTFS, porque las particiones que no son NTFS no soportan los permisos de NTFS.

Nota: Para mover archivos y carpetas dentro de una partición NTFS o entre particiones NTFS, debemos tener el permiso de Escritura sobre la carpeta de destino y el permiso de “Modificación” sobre la carpeta o archivo original. El permiso de “Modificación” es necesario para mover una carpeta o archivo, ya que Windows elimina la carpeta o archivo de la carpeta original después de copiarla a la carpeta de destino.

Recomendaciones para conceder permisos de NTFS

Consideraciones prácticas recomendadas cuando conceda permisos NTFS:

1. Conceder permisos a grupos locales (del dominio) en lugar de a usuarios.
2. Agrupar recursos para simplificar la administración.
3. Crear grupos de acuerdo con el acceso que sus miembros requieren.
4. Otorgar a los usuarios únicamente el nivel de acceso que necesiten.
5. Conceder permisos de “Leer y ejecutar” y “Escritura” para carpetas de datos.
6. Conceder permisos de “Leer y ejecutar” para carpetas de aplicaciones.

Conceder permisos a grupos locales del dominio en lugar de a usuarios, ya que es más fácil administrar grupos que usuarios. De este modo se mantiene la lista más corta, mejorando el rendimiento.
Para simplificar la administración, agrupa archivos en carpetas, carpetas de aplicación donde se guarden las aplicaciones más utilizadas, carpetas de datos que contienen archivos de datos compartidos por múltiples usuarios, y carpetas de usuarios que contengan los archivos de cada usuario individual. Centraliza las carpetas de usuario y las carpetas de datos en una partición distinta.
Otorga a los usuarios únicamente el nivel de acceso que requieran, si un usuario únicamente necesita leer un archivo, conceda al usuario, o grupo al que pertenezca, el permiso de “Lectura” sobre el archivo.
Crea grupos según los requerimientos de acceso a los recursos que necesitan sus miembros, y concede los permisos adecuados a los grupos. Cuando concedas permisos sobre carpetas de aplicaciones, concede el permiso “Leer y Ejecutar” a los grupos Usuarios y Administradores. De este modo, se evita que archivos de datos y aplicaciones se eliminen o se dañen accidentalmente por usuarios o virus. Cuando concedas permisos sobre carpetas de datos, concede los permisos “Leer y Ejecutar” y “Escritura” al grupo Usuarios y el permiso de “Modificación” al grupo Propietario Creador. De este modo, los usuarios tendrán la capacidad de leer y modificar documentos creados por otros usuarios, y la capacidad de leer, modificar y eliminar los archivos y carpetas que ellos mismos creen.
Nota: Deberíamos utilizar la denegación de permisos únicamente cuando sea imprescindible para denegar el acceso a una cuenta de usuario o grupo específico. Se recomienda también el uso de grupos locales del dominio para asignar permisos en vez de asignar permisos a cuentas individuales.

Permisos especiales NTFS

Generalmente, los permisos estándar de NTFS proporcionan todo el control de acceso que necesitamos para asignar seguridad a nuestros recursos. Sin embargo, en ocasiones los permisos estándares de NTFS no proporcionan el nivel especifico de acceso que deseamos conceder a los usuarios. Para crear un nivel específico de acceso, concedemos permisos de acceso especiales de NTFS.

Los permisos de acceso especiales nos proporcionan un mayor grado de control para conceder acceso a recursos. Los 13 (o 14) permisos de acceso especiales, cuando se combinan, constituyen los permisos estándares de NTFS.

Por ejemplo, el permiso estándar de “Lectura” consta de los permisos de acceso especiales “Leer datos”, “Leer atributos”, “Permisos de lectura” y “Leer atributos extendidos”.

Dos de los permisos de acceso especiales son especialmente útiles para la administración del acceso a archivos y carpetas:

- Cambiar permisos. Con este permiso, el usuario tiene la capacidad de cambiar permisos sobre un archivo o carpeta.
- Tomar posesión. Con este permiso, el usuario tiene la capacidad de tomar posesión de archivos y carpetas.

Cambiar permisos

Podemos dar a otros administradores y usuarios la capacidad de cambiar permisos sobre un archivo o carpeta sin necesidad de concederles el permiso “Control total” sobre el archivo o carpeta. De esta forma, el administrador o usuario no puede borrar o escribir en el archivo o carpeta, pero puede conceder permisos al archivo o carpeta. Para dar a los administradores la capacidad de cambiar permisos, concede el permiso de “Modificación” sobre archivo o carpeta al grupo Administradores.

Tomar posesión

Podemos dar a un usuario la capacidad de tomar posesión o, como administrador, podemos tomar posesión de un archivo o carpeta. Las siguientes normas son aplicables a tomar posesión de un archivo o carpeta:

- El propietario actual o cualquier usuario con permiso ***Control total*** puede conceder el permiso estándar ***Control total*** o el permiso de acceso especial ***Tomar posesión*** a otra cuenta de usuario o grupo. Esto permite a la cuenta de usuario o a un miembro del grupo tomar posesión.
- Un miembro del grupo de administradores puede tomar posesión de una carpeta o archivo, con independencia de los permisos concedidos sobre esa carpeta o archivo. Si un administrador toma posesión, el grupo de administradores se convierte en el propietario, y cualquier miembro del grupo de administradores puede modificar los permisos sobre el archivo o carpeta y conceder el permiso “Tomar posesión” a otra cuenta de usuario o grupo.

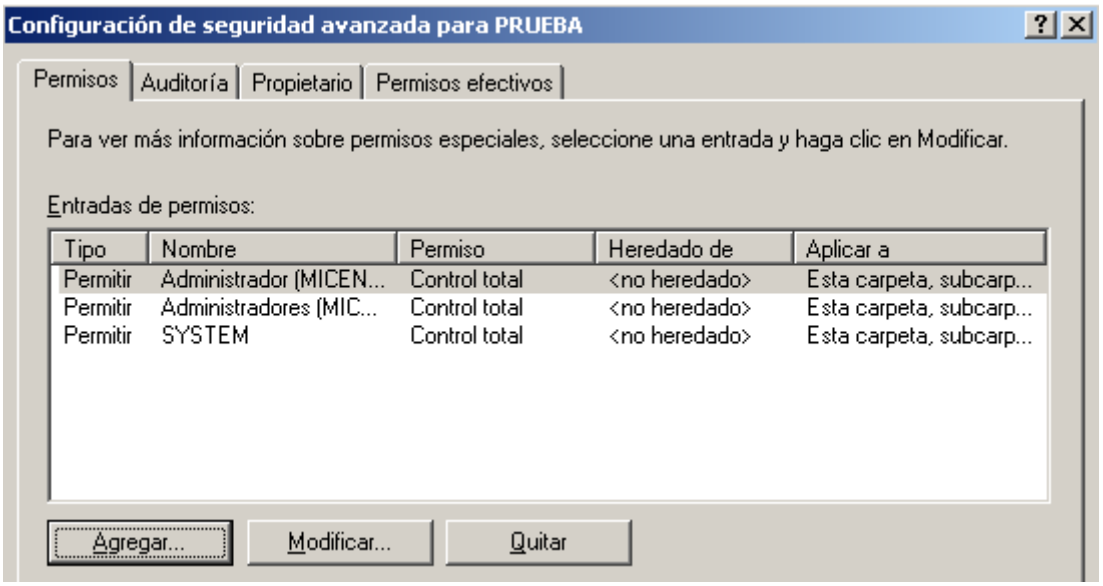
Por ejemplo, si un empleado deja la compañía, un administrador puede tomar posesión de los archivos del empleado y conceder el permiso “Tomar posesión” a otro empleado, y ese empleado puede tomar posesión de los archivos del primero.

Nota: Para convertirse en el propietario de un archivo o carpeta, un usuario o miembro de un grupo con el permiso “Tomar posesión” debe explícitamente tomar posesión del archivo o carpeta. No podemos conceder automáticamente a ninguna persona la propiedad de un archivo o carpeta.

Concesión de permisos especiales de NTFS

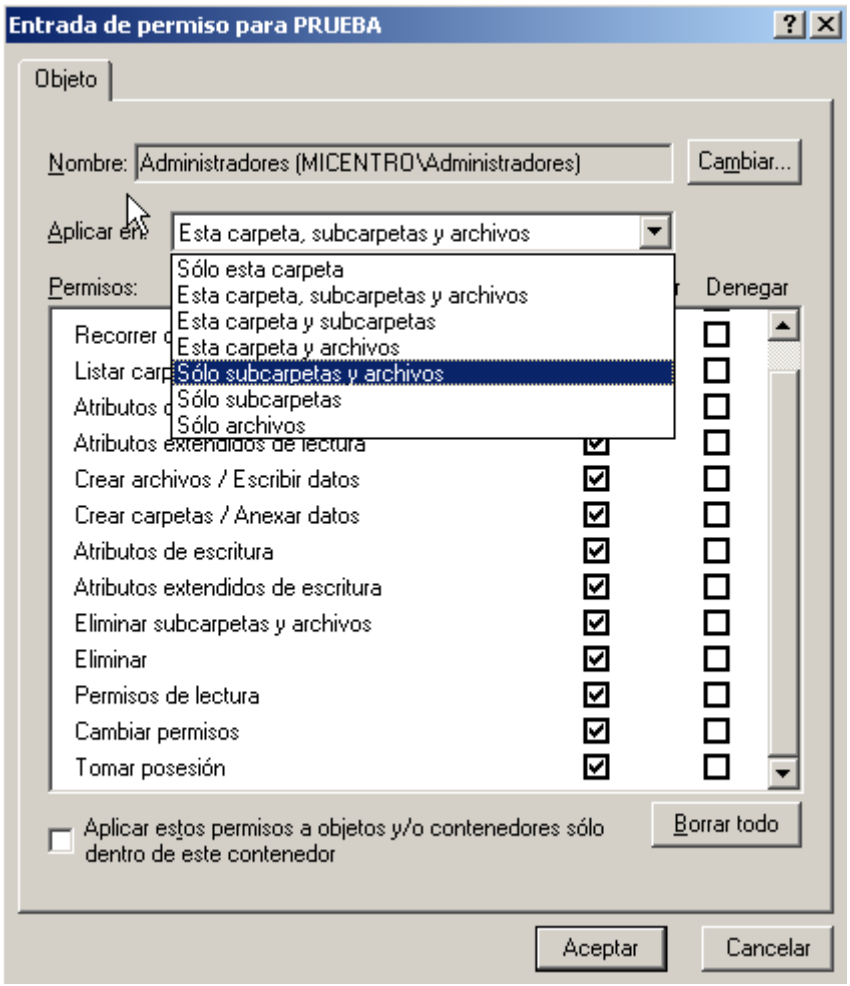
Para conceder permisos de acceso especiales a usuarios y grupos:

- En el cuadro de diálogo Propiedades de un archivo o carpeta, en la ficha Seguridad, haz clic en el botón opciones avanzadas.
- En el cuadro de diálogo Configuración de seguridad avanzada del archivo o carpeta, en la ficha Permisos, selecciona la cuenta de usuario o grupo para el que desea aplicar permisos de acceso especiales de NTFS, y haz clic en Modificar



Permisos especiales Paso 1

- En el cuadro de diálogo de Entrada de permiso del archivo o carpeta, configura la cuenta de usuario o nombre del grupo con el botón Cambiar, el nivel de la jerarquía de carpetas desde el que se heredan los permisos especiales de NTFS desde la lista desplegable Aplicar en:



Permisos especiales Paso2

- Para permitir los permisos “Cambiar permisos” o “Tomar posesión”, selecciona la casilla de verificación de Permitir junto a cada uno de ellos. Aplica estos permisos a objetos y/o contenedores dentro de este contenedor únicamente Especifica si las subcarpetas y archivos de una carpeta heredan los permisos de acceso especiales de dicha carpeta. Deshabilita esta casilla de verificación para evitar la herencia de permisos. Selecciónala para propagar los permisos de acceso especiales a archivos y subcarpetas. Borra todo sirve para deseleccionar todos los seleccionados.

Resumen final:

- Para asignar permisos se debe utilizar la estrategia AGDLP.
- Existen dos tipos de permisos independientes: de carpeta y de archivo.
- Los permisos NTFS son acumulativos.
- La denegación sobre el objeto invalida cualquier otro permiso que tenga.
- Por defecto asignar permisos a un objeto propaga esos permisos a todos sus descendientes.
- Por defecto crear un objeto implica heredar los permisos del contenedor padre.
- La herencia se puede bloquear transformándola en permisos efectivos o eliminándola por completo. Una vez eliminada es posible recuperarla forzando su propagación desde el contenedor padre.
- Cuando se copia el objeto entre particiones NTFS o en la misma partición se heredan los permisos del contenedor de destino.
- Cuando se mueve un objeto entre particiones NTFS se heredan los permisos del contenedor pero si se mueve en la misma partición los permisos se conservan.
- Los permisos mas granulares que existen son 13 y se denominan permisos especiales. La combinación de estos permisos da lugar a los permisos estándar y a los de compartir.
- El permiso de tomar posesión es un permiso especial que permite a quién lo tiene tomar la propiedad del objeto. No se puede dar la propiedad de un objeto así sin más, hay que querer tomar posesión (y poder claro).
- El Administrador y por tanto el grupo de Administradores puede tomar posesión de cualquier objeto independientemente de los permisos que tenga.
- Los permisos de compartir solo afectan cuando se accede por la red al recurso, los permisos NTFS afectan siempre.
- Los permisos de compartir son acumulativos
- Entre los permisos de compartir y los permisos NTFS mandan los más restrictivos a la hora de acceder por la red. Como es lógico si no estamos accediendo por la red los permisos de compartir no cuentan.
- Solo se permite compartir carpetas, no ficheros y además puede haber múltiples comparticiones para la misma carpeta.
- Existen una serie de carpetas denominadas carpetas administrativas que el sistema comparte automáticamente.
- El símbolo $ permite compartir un recurso sin que este sea visible.

CONCLUSIONES FINALES

- Se debe conceder permisos a grupos y no a cuentas individuales.

No es efectivo el mantenimiento de cuentas de forma individual

- Se usará la denegación solo para excluir de un grupo a un elemento o subconjunto que no deseamos que tengan los permisos del grupo.

El uso de la denegación deber ser muy cuidadoso ya que se superpone a cualquier otro permiso que pueda tener un usuario por pertenencia a varios grupos

- No se usará la denegación para impedir el acceso al grupo Todos.

Porque estaríamos negando el acceso también a los administradores, lo correcto es quitar al grupo todos y añadir los usuarios, grupos o equipos que se desee.

- No se deben cambiar los permisos predefinidos de carpetas del sistema o de la raíz.

Podrías causar problemas en el sistema o disminuir la seguridad de dichos elementos.

- Aplicar permisos al nivel mas superior que se pueda implica la propagación a todos los contenidos de niveles inferiores.

Es una forma fácil y efectiva de conceder permisos a un árbol

- Conceder permisos de lectura y ejecución a carpetas de Aplicaciones a usuarios y administradores.

Es una forma de impedir borrados accidentales de datos y aplicaciones.

- Conceder permisos de lectura, ejecución y escritura a usuarios y modificación a creadores propietarios a carpetas de Datos.

Así, los usuarios podrán leer y modificar archivos de otros usuarios y leer, modificar y borrar los archivos propios.