Tema 8: La administración del acceso al dominio

Contenido

1.- LOS PERMISOS Y LOS DERECHOS

El modelo de protección de Windows establece la forma en que el sistema lleva a cabo el control de acceso de cada usuario o grupo de usuarios. Es el modelo que sigue el sistema para establecer las acciones que un usuario o grupo está autorizado a llevar a cabo. Este modelo está basado en la definición de ciertos atributos de protección que se asignan a los procesos de usuarios y al sistema y sus recursos por otro. En el caso del sistema y sus recursos, Windows define dos conceptos distintos y complementarios: el concepto de derecho y el concepto de permiso, respectivamente.

Un **derecho** es un atributo de un usuario (o grupo) que le permite realizar una acción que afecta al sistema en su conjunto (y no a un objeto o recurso en concreto).

- Existe un conjunto fijo y predefinido de derechos en Windows.
- ¿Cómo saber qué usuarios poseen qué derechos? Cada derecho posee una lista donde se especifican los grupos o usuarios que tienen concedido ese derecho.

Un **permiso** es una característica de cada recurso (carpeta, archivo, impresora, etc.) del sistema que concede o deniega el acceso al mismo a un usuario o grupo concreto.

- Cada recurso del sistema posee una lista en la que se establece qué usuarios o grupos pueden acceder a dicho recurso y qué tipo de acceso puede hacer cada uno (lectura, modificación, ejecución, borrado, etc.)

1.1 La acreditación de los usuarios.

Cuando se autoriza a un usuario para conectarse a Windows, el sistema construye para él una acreditación denominada **Security Access Token (SAT)**.

SAT contiene los siguientes atributos de protección:

- El **SID** que identifica unívocamente al usuario.
- La **lista de los SID** de los grupos a los que pertenece dicho usuario.
- La **lista de los derechos** que el usuario tiene otorgados por sí mismo o por los grupos a los que pertenece.

1.2 Los derechos de usuario.

Windows distingue dos tipos de derechos:

- Los derechos **de conexión**, que establecen las diferentes formas en que un usuario puede conectarse al sistema (de forma interactiva, a través de la red, etc.). Entre ellos se encuentran:
    - **Denegar el acceso desde la red a este equipo**: que permite al usuario conectar con el ordenador desde otro equipo a través de la red.
    - **Permitir el inicio de sesión local**: que permite al usuario iniciar una sesión local en el ordenador.
- Los **privilegios**, que hacen referencia a ciertas acciones predefinidas que el usuario puede realizar una vez conectado el sistema. Entre ellos se encuentran:
    - **Agregar estaciones de trabajo al dominio.**
    - **Hacer copias de seguridad de archivos y directorios.**
    - **Restaurar archivos y directorios.**
    - **Cambiar la hora del sistema.**
    - **Dispositivos**: impedir que los usuarios instalen controladores de impresora.
    - **Apagar el sistema**.

Es importante destacar lo siguiente: cuando existe un conflicto entre lo que concede o deniega un **permiso** y lo que concede o deniega un **derecho**, este último tiene **prioridad**.

- Por ejemplo, los miembros del grupo Operadores de Copia poseen el derecho de realizar una copia de seguridad de todos los archivos del sistema.

Es muy probable que existan archivos sobre los que no tengan ningún tipo de permiso. Sin embargo, al ser el derecho más prioritario, podrán realizar la copia sin problemas.

1.3 Las directivas de seguridad.

En Windows, los **derechos** se han agrupado en un conjunto de **reglas de seguridad** y se han incorporado en unas consolas de administración denominadas **directivas de seguridad** que definen el comportamiento del sistema en temas de seguridad. Pueden ser de tres tipos:

- **Directiva de seguridad local**: es la que se debe utilizar si se desea modificar la configuración de seguridad y el equipo es una estación de trabajo o no tiene instalado el AD.
- **Directiva de seguridad de dominio**. Es la que se debe utilizar si el servidor Windows es un controlador de dominio y se desea modificar la configuración de seguridad para todos los miembros del dominio.

- **Directiva de seguridad del controlador de dominio.** Es la que se debe utilizar si el servidor Windows es un controlador de dominio y se desea modificar la configuración de seguridad para todos los controladores de dominio.

Desde estas herramientas de administración se pueden establecer, entre otras, las siguientes directivas:

- **Directivas de cuentas.** En este apartado se puede establecer cuál es la política de cuentas o de contraseñas que se seguirá. Dentro de este apartado se pueden distinguir reglas en tres grupos: Contraseñas, Bloqueo y Kerberos. Entre ellas, las dos primeras hacen referencia a cómo deben ser las contraseñas en el equipo (longitud mínima, vigencia máxima, historial, etc.) y cómo se debe bloquear una cuenta que haya alcanzado un cierto máximo de intentos fallidos de conexión.
- **Directiva local.** En este apartado se encuentran: la Auditoría del equipo, que permite registrar en el visor de sucesos ciertos eventos que sean interesantes, a criterio del administrador (por ejemplo, los inicios de sesión local), y los derechos y privilegios que se han indicado en el epígrafe anterior (además de otros muchos) .
- **Directivas de clave pública.** En este apartado se pueden administrar las opciones de seguridad de las claves públicas emitidas por el equipo.

1.4. Atributos de protección de los recursos

En un sistema de archivos NTFS de Windows cada carpeta o archivo posee los siguientes atributos de protección:

- **El SID del propietario**. Inicialmente, el propietario es siempre el usuario que ha creado el archivo o carpeta, aunque este atributo puede ser modificado posteriormente.
- **La lista de control de acceso de protección** (ACL), que incluye los permisos que los usuarios tienen sobre el archivo o carpeta. La lista puede contener un número indefinido de entradas, de forma que cada una de ellas concede o deniega un conjunto concreto de permisos a un usuario o grupo del sistema.
- **La lista de control de acceso de seguridad** (SACL), que se utiliza para definir qué acciones sobre un archivo o carpeta tiene que auditar el sistema (el proceso de auditoría supone la anotación en el registro del sistema de las acciones que los usuarios realizan sobre los archivos o carpetas).

  El sistema sólo audita las acciones especificadas (de los usuarios o grupos especificados) en la lista de seguridad de cada archivo o carpeta. Esta lista está inicialmente vacía en todos los objetos del sistema de archivos.

La lista de control de acceso de protección se divide realmente en dos listas, cada una de ellas denominada Lista de Control de Acceso Discrecional (DACL). Cada elemento de una DACL se denomina Entrada de Control de (ACE) y se utiliza para unir un SID de usuario o grupo con la concesión o denegación de un permiso concreto (o un conjunto de permisos).

El hecho de que cada archivo o carpeta tenga dos DACL en vez de una tiene que ver con el mecanismo de la herencia de permisos que incorpora Windows: cada archivo o carpeta puede heredar implícitamente los permisos establecidos para la carpeta que lo contiene y puede,

además, definir permisos propios (denominados explícitos). Es decir, que cada archivo o carpeta puede poseer una DACL heredada y una DACL explicita. De esta forma, si una cierta carpeta define permisos explícitos, éstos (junto con sus permisos heredado) serán a su vez los permisos heredados de sus subcarpetas y archivos (y así sucesivamente). El mecanismo de herencia de permisos es dinámico, es decir, la modificación de un permiso explícito de una carpeta se refleja en el correspondiente permiso heredado de sus subcarpetas y archivos.

1.5. La asociación de los permisos a los recursos

La asociación de los permisos a los archivos y carpetas sigue una serie de reglas:

- Cuando se crea un nuevo archivo o carpeta, éste posee por defecto permisos heredados de la carpeta o unidad donde se ubica y ningún permiso explícito.
- Cualquier usuario que posea control total sobre el archivo o (por defecto, su propietario) podrá incluir nuevos permisos (positivos o negativos) en la lista de permisos explícita.
- El control sobre la herencia de permisos (por ejemplo, qué objetos heredan y qué permisos se heredan) se realiza a dos niveles:
    - En cada objeto (archivo o carpeta) se puede decidir si se desea o no heredar los permisos de su carpeta padre.
    - Cuando se define un permiso explícito en una carpeta, se puede también decidir Qué objetos van a heredarlo. En este caso, se puede decidir entre cualquier combinación de la propia carpeta, las subcarpetas y los archivos.
- El copiar un archivo o carpeta a otra ubicación se considera una creación, y, por tanto, el archivo copiado recibirá una lista de permisos explícitos vacía y se activará la herencia de la carpeta padre correspondiente a la nueva ubicación.
- En el proceso de mover un archivo se distinguen dos casos:
    - Si se mueve una carpeta o archivo a otra ubicación dentro del mismo volumen (o partición) NTFS, se desactivará la herencia y se mantendrán los permisos que tuviera como explícitos en la nueva ubicación.
    - Si el volumen destino es distinto, entonces se actuará como en una copia (sólo se tendrán los permisos heredados de la carpeta padre correspondiente a la nueva ubicación).

1.6. Los permisos NTFS estándar y especiales

Windows distingue entre:

- **Los permisos NTFS especiales, que** son los que controlan cada una de las acciones que se pueden realizar sobre las carpetas o los archivos.
- **Los permisos NTFS estándar,** que son combinaciones de los permisos NTFS especiales que están predefinidas en el sistema.

La existencia de estas combinaciones predefinidas facilita la labor del Administrador

Las principales reglas que controlan la aplicación de los permisos a las carpetas y archivos son las siguientes:

- Una única acción de un proceso puede involucrar varias acciones individuales sobre varios archivos o carpetas. En este caso, el sistema verificará si el proceso tiene o no permisos para todas ellas. Si le falta algún permiso, la acción se rechazará con un mensaje de error genérico de falta de permisos.
- Los permisos en Windows son acumulativos: un proceso de usuario posee implícitamente todos los permisos correspondientes a los SID de su acreditación, es decir, poseerá todos los permisos del usuario y de los grupos a los que pertenezca.
- La ausencia de un determinado permiso sobre un objeto supone implícitamente la imposibilidad de realizar la acción correspondiente sobre el objeto.
- Si se produce un conflicto en la comprobación de los permisos, los permisos negativos tendrán prioridad sobre los positivos y los permisos explícitos tendrán prioridad sobre los heredados.

1.7. Los permisos de los recursos *compartidos*

Cuando se establecen los permisos de un directorio compartido, únicamente son efectivos cuando se tiene acceso a dicho directorio a través de la red es decir, no protegen a los directorios cuando se abren localmente en el servidor.

Para los directorios locales se deben utilizar los permisos NTFS, indicados en el epígrafe anterior.

Los permisos de recurso compartido se aplican a todos los archivos y subdirectorios del directorio compartido y se puede especificar, además, el número máximo de usuarios que pueden acceder al directorio a través de la red.

Se puede controlar el acceso a los recursos compartidos mediante tres métodos:

- ✓ Utilizando los permisos de recurso compartido que son sencillos de aplicar y administrar.
- ✓ Utilizando los permisos NTFS que proporcionan un control más detallado del recurso compartido y su contenido .
- ✓ Utilizando una combinación de los dos métodos anteriores.

Si utiliza una combinación de los métodos primeros, siempre se aplicará el permiso más restrictivo. Por ejemplo, si el permiso de un recurso compartido está definido como Todos = Lectura (que es el valor predeterminado) y el permiso NTFS permite que los usuarios realicen cambios en un archivo compartido, se aplicará el permiso de recurso compartido y el usuario no podrá realizar cambios en el archivo.

Nota: Si un usuario tiene habilitado el derecho de conexión **Denegar el acceso desde la red a este equipo**, no podrá acceder al recurso independientemente de los permisos que tenga sobre él.

2.- ADMINISTRADOR DE ARCHIVOS

Windows Server presenta avances técnicos para la administración de archivos. Aparte de los recursos compartidos, Windows Server ofrece la posibilidad de la publicación de esos ficheros en el servicio de directorios del Directorio Activo. Publicar los ficheros en el Directorio Activo hace más fácil su localización. La ventaja del sistema de ficheros distribuidos (Dfs) permite una mejor administración de los directorios compartidos. La mejor administración del espacio de disco está disponible para volúmenes NTFS asignando cuotas de disco a los usuarios. La encriptación del sistema de ficheros (EFS) ayuda a incrementar la seguridad de los directorios y de los archivos. Así, el personal autorizado podrá restaurar los ficheros encriptados cuando el propietario de los recursos no esté disponible. Finalmente, la utilidad de desfragmentación de disco de Windows Server desfragmentará el disco sólo cuando se requiera. Esto significa que la utilidad analizará primero el disco para determinar si se le debe desfragmentar. Basado en el informe de análisis, se puede elegir entre continuar o salir de la fragmentación.

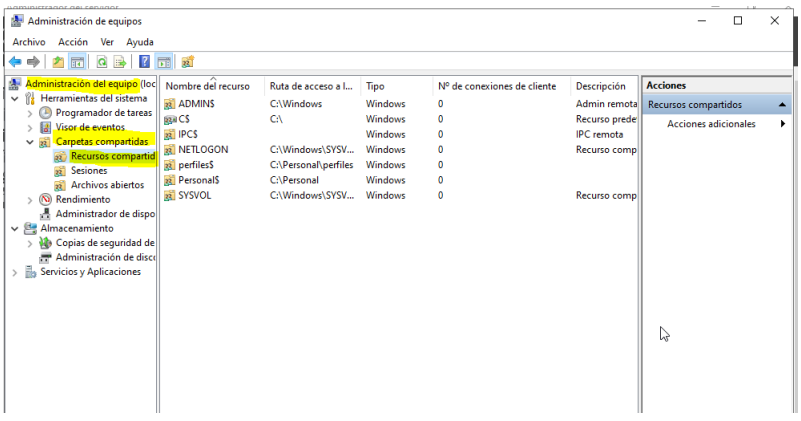
Windows Server permite que los recursos de ficheros sean administrados y publicados en el Directorio Activo. Esto hace más fácil su localización ya que se accede de forma central a ellos.

Para administrar los recursos a través de la red, primero se deben compartir dichos recursos.

Se utilizará la **Recursos Compartidos** para compartir los directorios. Se diseñó para trabajar con un equipo sólo y la totalidad de sus características se pueden utilizar desde un ordenador remoto, permitiendo resolver problemas desde cualquier otro ordenador de la red.

Proporciona acceso a la herramienta de Windows Server para acceder y visualizar los recursos compartidos de un ordenador, así como los dispositivos de almacenamiento de que dispone.

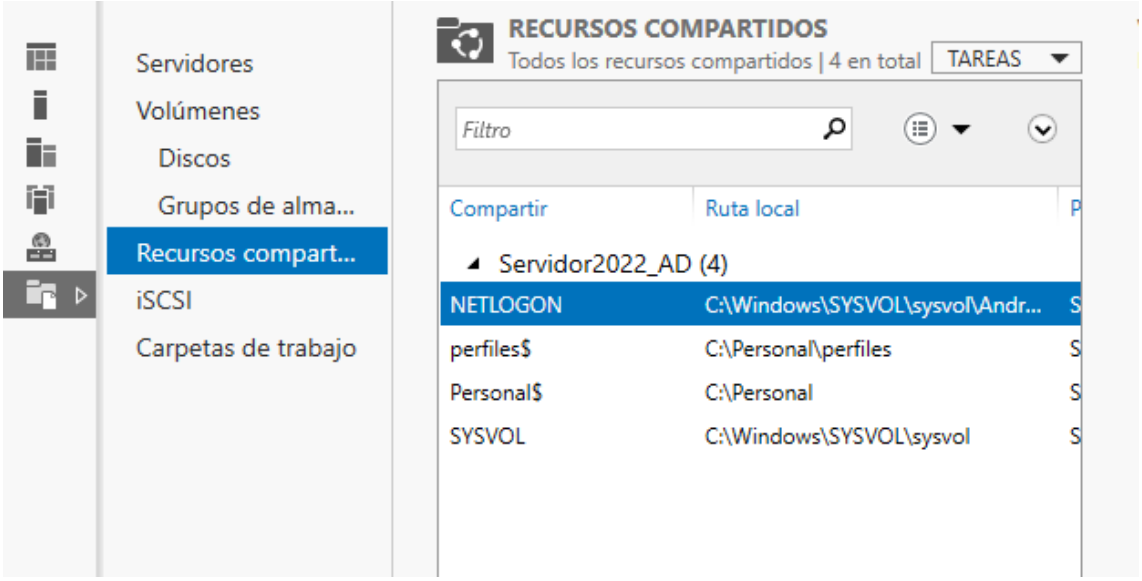
Recursos Compartidos se inicia seleccionando Inicio -> Herramientas administrativas -> Administrador del equipo. Se mostrará una consola desde donde puede acceder a los servicios que tiene instalado dicho servidor. Pulse en Carpetas Compartidas y dentro en Recursos compartidos y se mostrará una consola como la siguiente:



3.- COMPARTIR RECURSOS

3.1. Recursos compartidos especiales

Además de los recursos compartidos creados por los usuarios o por los administradores, el sistema crea varios recursos compartidos especiales para uso administrativo y del sistema que no se deben modificar ni eliminar. Estos recursos compartidos no se pueden ver en Mi PC, pero se pueden ver mediante Recursos compartidos.



Puede ocultar otros recursos compartidos a los usuarios si escribe $ como último carácter del nombre del recurso compartido (el signo $ pasa a formar parte del nombre del recurso. Los recursos compartidos especiales existen como parte de la instalación del sistema operativo.

Dichos recursos son los siguientes:

- **letra de unidad$**: Recurso compartido que permite a los administradores conectar al directorio raíz de una unidad.
- **ADMIN$:** Recurso que se utiliza durante la administración remota de un equipo. La ruta de acceso a este recurso es siempre la raíz del sistema (el directorio en el que está instalado el sistema operativo, por ejemplo, C:\Windows).
- **IPC$** : Recurso que comparte canalizaciones con nombre fundamentales para la comunicación entre programas. IPC$ se utiliza durante la administración remota de un equipo y ver sus recursos compartidos. Este recurso no se puede eliminar.
- **NETLOGON:** Recurso necesario que se utiliza en los controladores de dominio. Si se elimina este recurso compartido, se produce una pérdida de funcionalidad en todos los equipos cliente a los que da servicio el controlador de dominio.
- **SYSVOL:** Recurso necesario que se utiliza en los controladores de dominio. Si se elimina este recurso compartido, se produce una pérdida de funcionalidad en todos los equipos cliente a los que da servicio el controlador de dominio.
- **PRINT$:** Recurso que se utiliza para la administración remota de impresoras.

3.2. Permisos de un recurso compartido

Los permisos de los recursos compartidos establecen el máximo acceso disponible. La tabla 7.2 resume los tres tipos de acceso, desde el más restrictivo al menos restrictivo.

Permiso del recurso compartido	Tipo de acceso
Lectura	Permite ver los nombres de archivos y de subcarpetas, ver los datos de los archivos y ejecutar archivos de programa.
Modificar	Permite el mismo acceso que Lectura y, además, agregar archivos y subcarpetas, cambiar datos en archivos, eliminar subcarpetas y archivos.
Control total	Permite el mismo acceso que Modificar y, además, modificar permisos (sólo en volúmenes NTFS) y tomar posesión (sólo en volúmenes NTFS).

Tabla 7.2: Permisos sobre recursos compartidos

3.3. Compartir un directorio

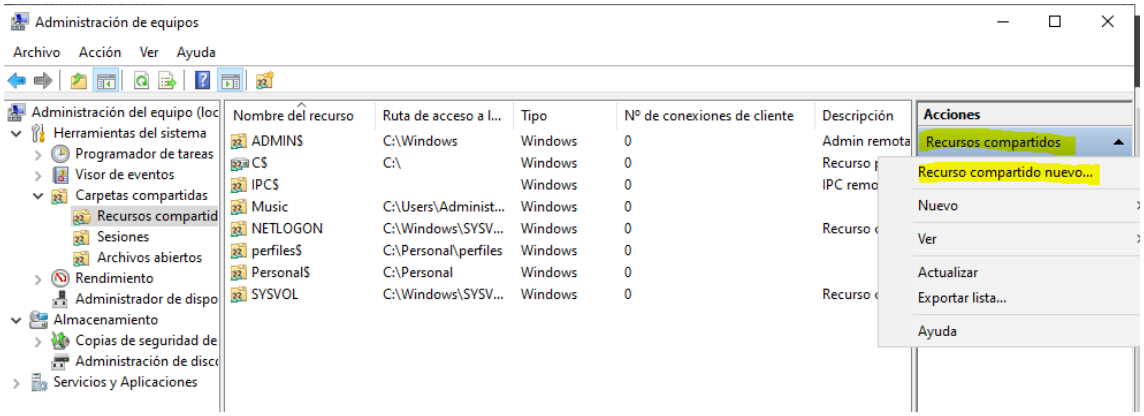
Para compartir directorios en e l administrador de equipos, siga los siguientes pasos:

1. Abra el Administrador de equipos desde el menú Herramientas administrativas.

2. En el árbol de consola Administracion de equipo , haga clic en Carpetas compartidas -> recursos compartidos.

3. En el menú Acciones -> Acciones adicionales, Haga clic en Nuevo Recurso Compartido.

4. Siga las instrucciones del asistente para compartir ficheros / carpetas.



3.4. Publicar un directorio desde Equipos y usuarios del Directorio Activo

Una de las claves de la administración de la red es cómo proporcionar publicación de seguridad de recursos de red a los usuarios de la red. Otro cambio es el de hacer más fácil el encontrar la información de la red. El Directorio Activo se diseñó para ello ya que guarda

objetos y la información de ellos para ofrecer un mecanismo de control rápido y eficaz de acceso.

Los recursos que se pueden publicar son objetos como usuarios, equipos, impresoras, archivos, directorios y servicios de red. La publicación de esta información hace más fácil a los usuarios encontrar a los recursos por la red.

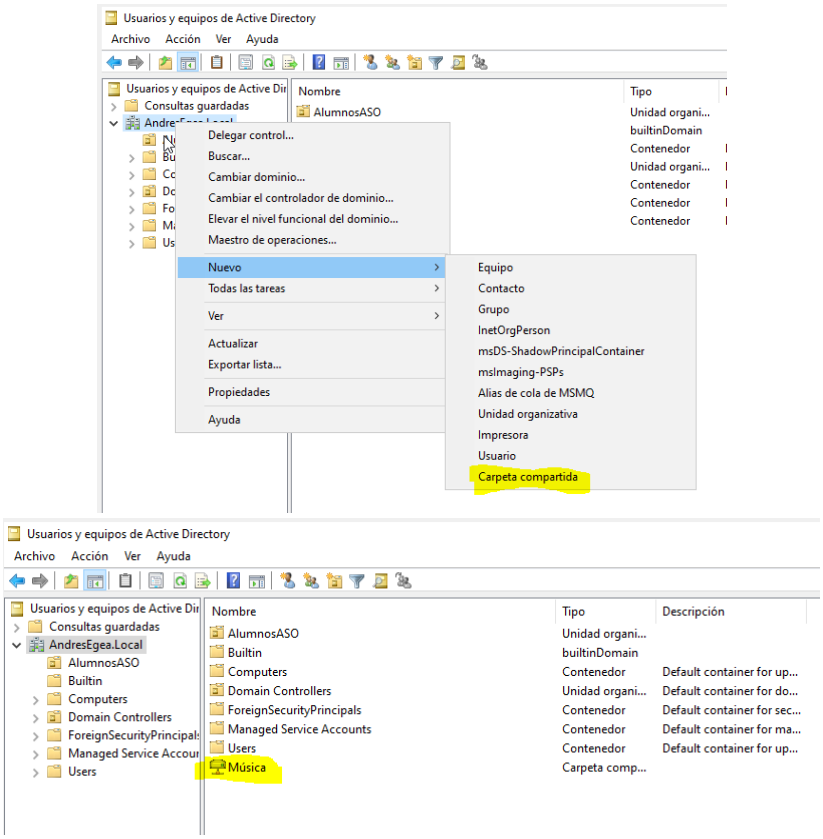
En Windows Server se puede publicar información sobre impresoras y directorios compartidos en el Directorio Activo desde la consola de Usuarios y equipos del Directorio Activo. Para publicar un directorio, siga los siguientes pasos:

1. Abra Usuarios y equipos del Directorio Activo desde las Herramientas Administrativas.

2. En el árbol de consola de esta herramienta, haga clic con el botón derecho del ratón en el dominio en el que se quiere publicar el directorio, marque Nuevo y después haga clic en Carpeta Compartida.

3. Escriba el nombre que quiera que aparezca como recurso compartido en el Directorio Activo.

4. En la ruta de red escriba la ruta hacia el recurso compartido y después haga clic en OK. El directorio compartido aparecerá en el dominio.



4.- PERMISOS NTFS

4.1. Introducción

Un permiso es una regla asociada a un objeto para regular los usuarios que pueden tener acceso al objeto y de qué forma.

Cuando se configuran permisos, se especifica el tipo de acceso de los grupos y usuarios. Por ejemplo, puede permitir a un usuario leer el contenido de un archivo, dejar a otro usuario realizar cambios en el archivo y evitar a los demás usuarios el acceso al archivo. Puede establecer permisos similares en impresoras para que determinados usuarios puedan configurarlas y otros usuarios puedan imprimir sólo desde una de ellas.

4.2. Tipos de permisos

Existen dos tipos de permisos diferentes específicos para NTFS: permisos de carpeta NTFS y permisos de archivo NTFS.

Los permisos de los archivos y de las carpetas controlan un grupo de permisos especiales. Si se desea se pueden ajustar aún más los permisos dados a un archivo o carpeta haciendo uso de los permisos especiales para archivos o carpetas respectivamente

4.2.1. Permisos de carpeta NTFS

Los permisos de carpeta permiten el control del acceso que los usuarios o los grupos pueden realizar a las carpetas, los archivos y a las subcarpetas que contenga la carpeta.

Los tipos de permisos de **carpeta** NTFS son los siguientes:

- **Lectura:** permite que el usuario o el grupo pueda leer archivos y subcarpetas de la carpeta y visualizar quien es el propietario, qué permisos y qué atributos posee.
- **Escritura:** este permiso habilita al usuario o al grupo a crear archivos y subcarpetas dentro de la carpeta, modificar los atributos de la carpeta y visualizar quien es el propietario y qué permisos posee.
- **Listar el contenido de la carpeta:** este permiso habilita al usuario o al grupo a visualizar los nombres de los archivos y de las subcarpetas que haya dentro de la carpeta.
- **Lectura y ejecución:** permite que los usuarios y grupos puedan pasar por las carpetas y ejecutar archivos. Incluye el permiso para listar el contenido de las carpetas.
- **Modificación**: permite eliminar la carpeta y realizar acciones permitidas por el permiso de escritura y el permiso de lectura y ejecución.
- **Control Total**: habilita a todas las acciones posibles.

4.2.2. Permisos sobre archivos NTFS

Para habilitar el acceso de un usuario o de un grupo a un archivo se asignan permisos de archivo, en el que se indica el tipo de acceso permitido. Los tipos de **permiso de archivo** son los siguientes:

- **Lectura:** permite que el usuario o el grupo pueda leer archivos y visualizar quien es el propietario, qué permisos y qué atributos posee.

- **Escritura**: este permiso habilita al usuario o al grupo a crear archivos y modificar los atributos del archivo y visualizar quien es el propietario y qué permisos posee.
- **Lectura y ejecución**: permite que los usuarios y grupos puedan leer y ejecutar archivos.
- **Modificación**: permite eliminar el archivo y realizar acciones permitidas por el permiso de escritura y el permiso de lectura y ejecución.
- **Control Total**: habilita a todas las acciones posibles

4.2.3. Permisos especiales NTFS

Los permisos especiales NTFS proporcionan un control de acceso a los recursos más fino. Es posible definir cualquier o todos los permisos especiales siguientes para las unidades:

- **Recorrer carpeta o ejecutar archivo**.

  Recorrer carpeta permite o deniega el movimiento por las carpetas para las que el usuario no tiene permiso de acceso con el fin de que pueda llegar a los archivos o las carpetas para los que sí tiene permiso de acceso (sólo se aplica a las carpetas).

  Al configurar el permiso Recorrer carpeta en una carpeta no se define de manera automática el permiso Ejecutar archivo en todos los archivos de esa carpeta. El permiso Ejecutar archivo permite o deniega la ejecución de archivos de programa (sólo afecta a archivos).

- **Listar carpeta o leer datos**

  El permiso Listar carpeta permite o deniega la vista de nombres de archivos y subcarpetas de la carpeta (sólo afecta a las carpetas)

  El permiso Leer datos permite o deniega la vista de datos en archivos (sólo afecta a archivos).

- ✓ **Atributos de lectura**

  Permite o deniega la vista de los atributos de un archivo o carpeta, como sólo lectura y oculto.

- ✓ **Atributos extendidos de lectura**

  Permite o deniega la vista de atributos extendidos de un archivo o carpeta.

- ✓ **Crear archivos o escribir datos**

  El permiso Crear archivos permite o deniega la creación de archivos dentro de la carpeta (sólo afecta a las carpetas).

  El permiso Escribir datos permite o deniega la realización de cambios en el archivo y la sobreescritura del contenido existente (sólo afecta a los archivos).

- ✓ **Crear carpetas o anexar datos**

El permiso Crear carpetas permite o deniega la creación de carpetas dentro de una carpeta (sólo afecta a las carpetas).

El permiso Agregar datos permite o deniega la realización de cambios al final del archivo, pero no el cambio, eliminación ni sobreescritura de los datos existentes (sólo afecta a los archivos).

- ✓ **Atributos de escritura**

  Permite o deniega el cambio de los atributos de un archivo o de una carpeta, como sólo lectura y oculto.

- ✓ **Atributos extendidos de escritura**

  Permite o deniega el cambio de los atributos extendidos de un archivo o carpeta.

- ✓ **Eliminar subcarpetas y archivos**

  Permite o deniega la eliminación de subcarpetas y archivos, incluso si no se ha otorgado el permiso Eliminar en la subcarpeta o archivo.

- ✓ **Eliminar**

  Permite o deniega la supresión del archivo o de la carpeta. Aun en el caso de que no tenga el permiso Eliminar para un archivo o una carpeta, podrá eliminarlo si se le ha otorgado el permiso Eliminar subcarpetas y archivos e n la carpeta principal.

- ✓ **Permisos de lectura**

  Permite o deniega la lectura de los permisos para el archivo o la carpeta, como Control total, Leer y Escribir.

- ✓ **Cambiar permisos**

  Permite o deniega el cambio de los permisos para el archivo o la carpeta, como Control total, Leer y Escribir.

- ✓ **Tomar posesión**

  Permite o deniega la toma de posesión del archivo o de la carpeta. El propietario de un archivo o de una carpeta siempre puede cambiar los permisos que protegen al archivo o a la carpeta.

- ✓ **Control total**

  Permite todos los permisos anteriores sobre un fichero o carpeta.

Las tablas 7.3 y 7.4 detallan los permisos especiales que abarcan los permisos de los archivos y de las carpetas respectivamente.

Permiso Especial	Control Total	Modificar	Lectura y Ejecución	Leer	Escribir
Recorrer Carpeta / Ejecutar Archivo	Sí	Sí	Sí	No	No
Listar Carpeta / Leer datos	Sí	Sí	Sí	Sí	No
Atributos de Lectura	Sí	Sí	Sí	Sí	No
Atributos Extendidos de Lectura	Sí	Sí	Sí	Sí	No
Crear Archivos / Escribir Datos	Sí	Sí	No	No	Sí
Crear Carpetas / Anexar Datos	Sí	Sí	No	No	Sí
Atributos de Escritura	Sí	Sí	No	No	Sí
Atributos Extendidos de Escritura	Sí	Sí	No	No	Sí
Eliminar Subcarpetas y Archivos	Sí	No	No	No	No
Eliminar	Sí	Sí	No	No	No
Permisos de Lectura	Sí	Sí	Sí	Sí	Sí
Cambiar Permisos	Sí	No	No	No	No
Tomar Posesión	Sí	No	No	No	No
Control Total	Sí	Sí	Sí	Sí	Sí

Tabla 7.3: Permisos especiales para los archivos

Permiso Especial	Control Total	Modificar	Lectura y Ejecución	Listar el contenido de la carpeta	Leer	Escribir
Recorrer Carpeta / Ejecutar Archivo	Sí	Sí	Sí	Sí	No	No
Listar Carpeta / Leer datos	Sí	Sí	Sí	Sí	Sí	No
Atributos de Lectura	Sí	Sí	Sí	Sí	Sí	No
Atributos Extendidos de Lectura	Sí	Sí	Sí	Sí	Sí	No
Crear Archivos / Escribir Datos	Sí	Sí	No	No	No	Sí
Crear Carpetas / Anexar Datos	Sí	Sí	No	No	No	Sí
Atributos de Escritura	Sí	Sí	No	No	No	Sí
Atributos Extendidos de Escritura	Sí	Sí	No	No	No	Sí
Eliminar Subcarpetas y Archivos	Sí	No	No	No	No	No
Eliminar	Sí	Sí	No	No	No	No
Permisos de Lectura	Sí	Sí	Sí	Sí	Sí	Sí
Cambiar Permisos	Sí	No	No	No	No	No
Tomar Posesión	Sí	No	No	No	No	No
Control Total	Sí	Sí	Sí	Sí	Sí	Sí

Tabla 7.4: Permisos especiales para las carpetas

4.3. Lista de control de acceso

NTFS almacena una lista de control de acceso con cada archivo y carpeta en un volumen NTFS. La lista de control de acceso contiene una lista de todas las cuentas de usuarios y grupos que han recibido acceso a la carpeta o al archivo, así como también el tipo de acceso concedido. Cuando un usuario intenta acceder al recurso, la lista de control de acceso debe contener una entrada para la cuenta del usuario o para la cuenta del grupo al cual pertenece el usuario. Para que el usuario pueda acceder al archivo o carpeta, la entrada debe habilitar al tipo de acceso que el usuario está requiriendo. Si no existe una

entrada en el control de acceso, o el tipo de acceso requerido no está permitido, el usuario no puede obtener el acceso al recurso.

4.4. Consideraciones sobre permisos

Una cuenta de usuario o un grupo puede ser asignado con múltiples permisos y además existen permisos que se heredan de manera automática. Por lo tanto, antes de decidir la estructura de seguridad es necesario conocer ciertas condiciones y prioridades en el otorgamiento de permisos para no provocar situaciones de incoherencia o agujeros de seguridad.

4.4.1. Acumulación de permisos

El permiso final para la utilización de un recurso que recibe un usuario es el resultado de la suma de los permisos NTFS que recibe el usuario y los permisos NTFS que recibe como miembro de los grupos a los que pertenece. Por lo tanto, si el usuario tiene permiso de lectura sobre un recurso y pertenece a un grupo que tiene permiso de modificación sobre ese recurso, cuando el usuario intente utilizar el recurso tendrá permiso de lectura y modificación.

4.4.2. Prioridad de permisos

Los permisos NTFS sobre un fichero tienen prioridad sobre los permisos de carpeta NTFS. Un usuario puede no tener ningún tipo de permiso sobre una carpeta NTFS determinada pero si tiene permiso sobre un archivo de esa carpeta podrá acceder al archivo sin inconvenientes.

Obviamente, al no tener acceso a la carpeta, el usuario no verá la carpeta al navegar por la unidad, por lo tanto para utilizar el archivo debería conocer la trayectoria completa de acceso al archivo para poder llegar al archivo desde cualquier programa.

4.4.3. Denegación de permisos

Cuando se revisa la seguridad de un recurso puede otorgar un recurso, denegar o no definir nada. Si se deniega un permiso, esta denegación tiene prioridad sobre cualquier otro permiso otorgado al usuario o a un grupo al que el usuario pertenezca.

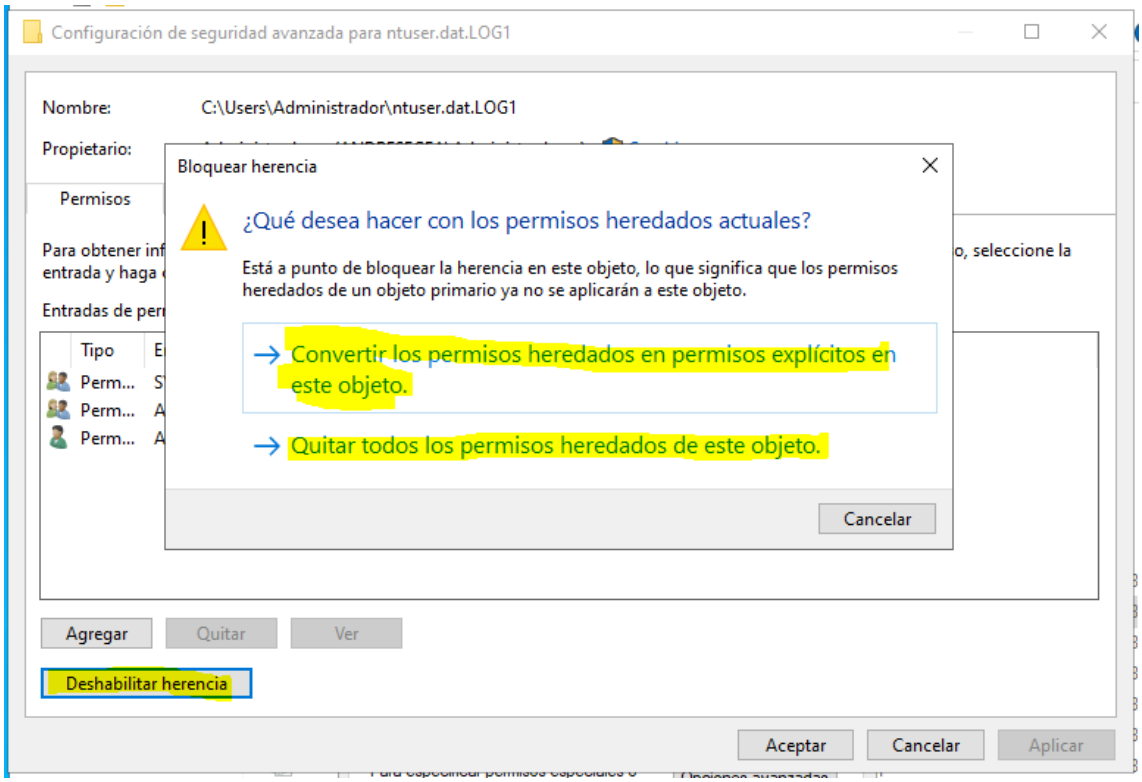
Por ejemplo, el usuario puede pertenecer a dos grupos. Por medio de un grupo tiene acceso de lectura sobre un recurso y desde el segundo grupo tiene denegado el permiso de lectura, el resultado finales que el usuario no podrá leer el archivo.

4.4.4. Herencia de permisos NTFS

Por defecto, los permisos de la carpeta principal se heredarán a los archivos y subcarpetas, aunque también se puede evitar que dichos permisos se hereden.

Cuando se dan permisos NTFS para acceder a una carpeta, esos permisos se aplican automáticamente a cualquier subcarpeta o archivo que se halle dentro del directorio padre y en suma, a cualquier archivo o subcarpeta nueva que se añada al nuevo directorio.

Las carpetas a las que se quiere evitar la herencia llegan a convertirse en nuevas carpetas padre y los permisos que se den sobre ellos se heredarán a las subcarpetas y archivos que contenga.



4.4.5. Planificación de permisos NTFS

La administración de los permisos requiere organización pero no es una tarea compleja. Antes que nada cabe señalar que ésta es una tarea que normalmente define la empresa y que asume funcionalmente un administrador, pero las tareas de protección llegan también a todos los usuarios. Los usuarios deben conocer también cómo proteger los archivos que ellos crean y es conveniente que la seguridad se extienda hasta el último nivel.

Como regla general, es conveniente catalogar a la información en dos grupos básicos: datos y programas. Los datos suelen ser menos estáticos que los programas y de más difícil recuperación ante un evento tipo catástrofe. Los programas, aún cuando son importantes, suelen ser mucho más estáticos (reciben menos modificaciones) y su recuperación es mucho más simple (muchas veces basta con reinstalar la aplicación).

Cuando se trata el problema de la seguridad también se debe considerar la tarea de generación de las copias de seguridad como una parte integrante de este problema. Si bien la organización de la asignación de los permisos es una tarea que difiere bastante dependiendo de cada empresa, existen unas recomendaciones generales que normalmente son adecuadas para todo tipo de solución:

- Los grupos se deben crear en base a una serie de requerimientos comunes de acceso a recursos. Evitar en lo posible los permisos individuales.
- Después de considerar los grupos necesarios se debe revisar qué grupos ya han sido incorporados de manera predeterminada por Windows Server. Esos grupos no es necesario crearlos, simplemente se utilizan.

- Asignar sólo el nivel de acceso requerido para un recurso. Si un grupo necesita nivel de lectura a un archivo se debe conceder exactamente ese nivel de acceso. Dar un nivel de acceso mayor al requerido sólo puede ocasionar problemas o destrucciones indeseadas.
- Agrupar en carpetas los datos de una aplicación, esto permite que se asignen los permisos a nivel de carpeta en lugar de hacerlo a nivel de archivo, con una menor carga administrativa. La agrupación de los datos de una aplicación en carpetas simplifica las tareas de las copias de seguridad.
- Evitar que los archivos de la propia aplicación se encuentren en la misma carpeta de los datos de la aplicación, ya que en cada copia de seguridad (si se hace a nivel de carpeta) estaría copiando una y otra vez la misma información estática. Además, las carpetas en donde se encuentra la aplicación requieren otro nivel de acceso que los datos de la aplicación (normalmente, el usuario normal sólo lee y ejecuta el archivo de la aplicación).
- Asignar permisos de lectura y ejecución de los archivos de la aplicación a los usuarios del grupo. Esto impide la destrucción accidental de la aplicación y evita la inserción de cierta clase de virus.
- La denegación de acceso es una herramienta poderosa para evitar el acceso a los recursos, pero debe usarse con mesura. Es mejor organizar la seguridad en base a permisos bien pensados y administrados en el nivel adecuado que usar indiscriminadamente la opción de asignar
- Revisar la utilización del mecanismo de herencia de los permisos.

4.4.6. Permisos NTFS en la copia de archivos y carpetas

Un usuario o un grupo pueden tener un subconjunto determinado de permisos sobre un archivo o sobre una carpeta y sus subcarpetas. Cuando este usuario o grupo copia un archivo sobre el que tiene permisos de lectura (al menos) y lo coloca en una nueva carpeta o incluso en otro volumen, los permisos de este nuevo archivo son nuevos. Es decir, la copia de un archivo o de una carpeta **no** trae aparejada la copia de los permisos.

Windows Server trata al nuevo archivo como lo que es: un archivo nuevo y, por lo tanto, toma los permisos de la carpeta de destino. El nuevo propietario del archivo es el usuario que realiza la copia. Obviamente, el usuario que realiza esa operación debe tener permiso de escritura sobre la carpeta de destino.

4.4.7. Permisos NTFS en el movimiento de archivos y carpetas

Cuando se mueve un archivo o carpeta a un nuevo destino los permisos se mantienen, siempre y cuando el destino sea un volumen NTFS.

El usuario que realice la operación debe tener permiso para escribir en la carpeta de destino y para modificar en la carpeta de origen. Esta operación implica la destrucción del archivo o carpeta de origen. El usuario que realiza la operación se convierte en el propietario de la carpeta o del archivo.

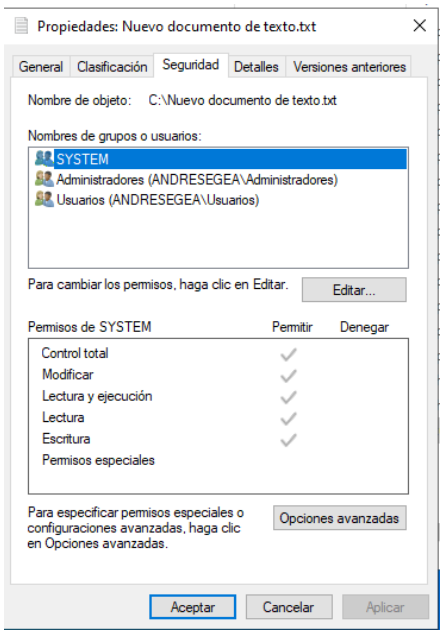
Si el formato del volumen de destino es FAT, los permisos no se pueden transferir a la carpeta o al archivo de destino debido a la imposibilidad de FAT para gestionar la seguridad de la manera en que lo hace NTFS.

4.5. Asignación de permisos

Cuando se crea un volumen NTFS se asigna de manera predeterminada Control Total a todos.

Éste es el punto de partida, pero obviamente hay que implementar un esquema de seguridad antes de introducir información en el volumen NTFS.

El mecanismo básico para asignar o modificar permisos es la ficha Seguridad del cuadro de diálogo Propiedades del objeto.



En la ficha Seguridad aparecen estos campos:

- ✓ Nombre: es el nombre del grupo o del usuario. La lista se puede modificar pulsando el botón Agregar, que hace aparecer un cuadro de diálogo con todos los usuarios, grupos y equipos disponibles. También es posible quitar equipos, grupos o usuarios por medio del botón Quitar.
- ✓ Permisos: cada tipo de permiso se puede asignar o denegar explícitamente. Para eso, cada tipo de permiso tiene una casilla de verificación. Los tipos de permisos que aparecen dependen del tipo de objeto.

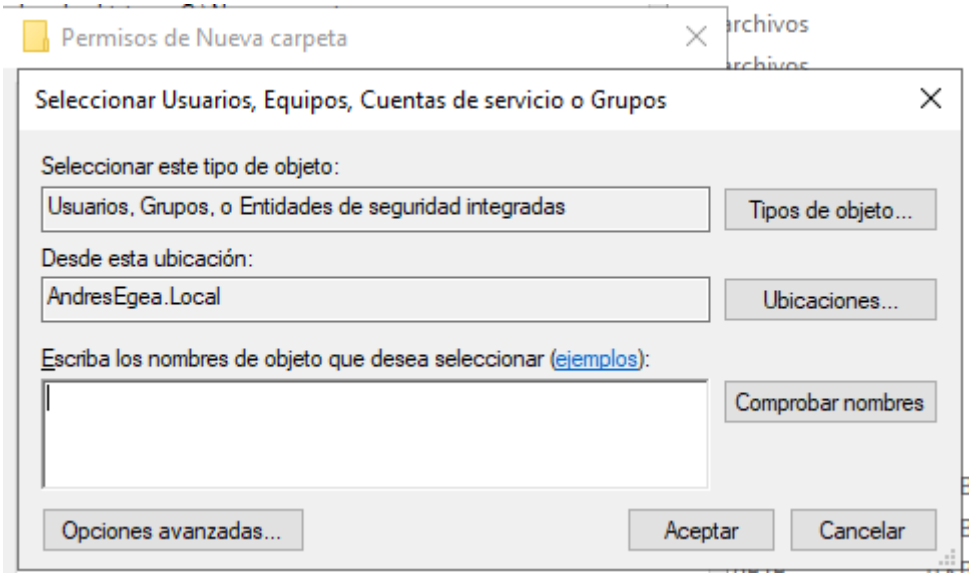
4.5.1. Asignar permisos

Para asignar permisos sobre una carpeta, siga los siguientes pasos:

1. En el explorador haga clic con el botón secundario del ratón sobre la carpeta a la que se quiere asignar permisos. Del menú emergente se elige la entrada Propiedades.

2. Aparece el cuadro de dialogo Propiedades de la carpeta o archivo. Haga clic en la ficha de Seguridad.

3. Pulse el botón Editar y luego Agregar y aparecerá el cuadro de diálogo Seleccionar Usuarios, o Grupos.



4. En el apartado Ubicaciones, en la parte superior del cuadro de diálogo, seleccione el dominio o el equipo desde el que se quiere elegir la cuenta de grupo o de usuario. Una vez seleccionado, pulse Buscar ahora.

5. Seleccione un grupo de la lista de nombres de grupos y usuarios. Haga clic en Aceptar.

6. En la ficha Seguridad se ha agregado el grupo seleccionado. Ahora debe asignarle (o denegar) los permisos correspondientes usando las casillas de verificación Permitir o Denegar.

7. Al finalizar, haga clic en Aplicar para hacer que los cambios entren en vigencia.

4.5.2. Asignación de permisos especiales

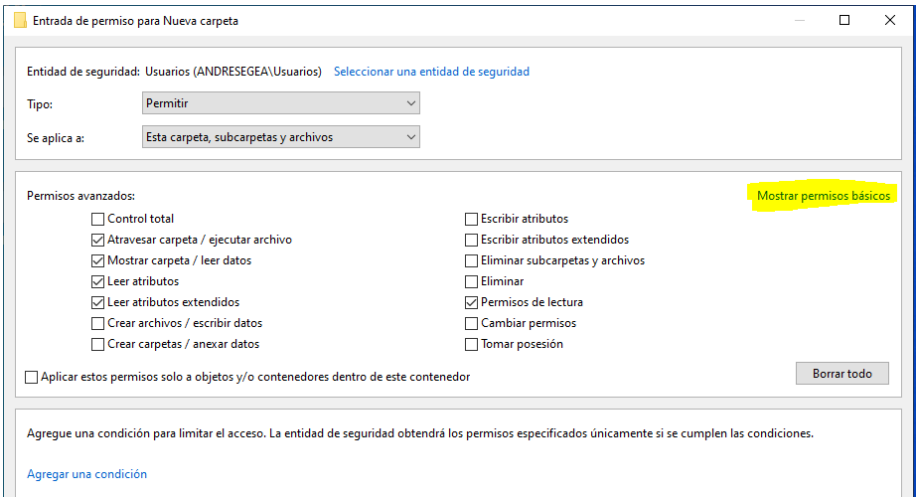
Los permisos especiales NTFS se pueden dar tanto a usuarios como a grupos de usuarios.

Para ello debe seguir los siguientes pasos:

1. En el cuadro de dialogo de Propiedades de una carpeta o de un archivo, sobre la pestaña de seguridad , haga clic en Opciones Avanzadas.

2. En Configurar de seguridad avanzada, en Entradas de Permisos seleccione la cuenta de usuario o grupo para el que se quiere aplicar estos permisos especiales y después haga clic en Ver.

3. En el cuadro de dialogo de Entrada de Permisos , pulse en Mostrar permisos avanzados configure las opciones que se describen.



Opción	Descripción
Nombre	El nombre de la cuenta de usuario o grupo.
Aplicar a	Especifica el nivel de jerarquía de la carpeta en la que se heredarán los permisos. Por defecto son Esta carpeta, subcarpetas y archivos.
Permisos	Permiten los permisos de acceso especial
Aplicar estos permisos a objetos y/o contenedores sólo dentro de este contenedor	Especifica los archivos y subcarpetas que heredarán los permisos. Seleccionar este check box para propagar estos permisos a los ficheros y subcarpetas. Dejarlo en blanco para que no se produzca la herencia
Borrar todo	Limpia todos los permisos seleccionados

Tabla 7.5: Características de la entrada de permisos de un objeto

4.5.3. Cambiar permisos

El procedimiento para cambiar los permisos sobre un archivo o una carpeta a un usuario o grupo que ya tiene permisos sobre dicho archivo o carpeta es el siguiente:

1. Abra el cuadro de diálogo de Propiedades de la carpeta o el archivo.
2. Seleccione la ficha Seguridad y haga clic en el botón Opciones Avanzadas.
3. En el cuadro de diálogo Configuración de seguridad avanzada del objeto haga clic en el botón VER de la ficha Permisos . Se visualiza el cuadro de diálogo

Las distintas opciones de permisos del cuadro de diálogo se han detallado en la sección anterior, se elige la combinación adecuada para el usuario o grupo seleccionado.

4. Al terminar, pulse Aceptar.

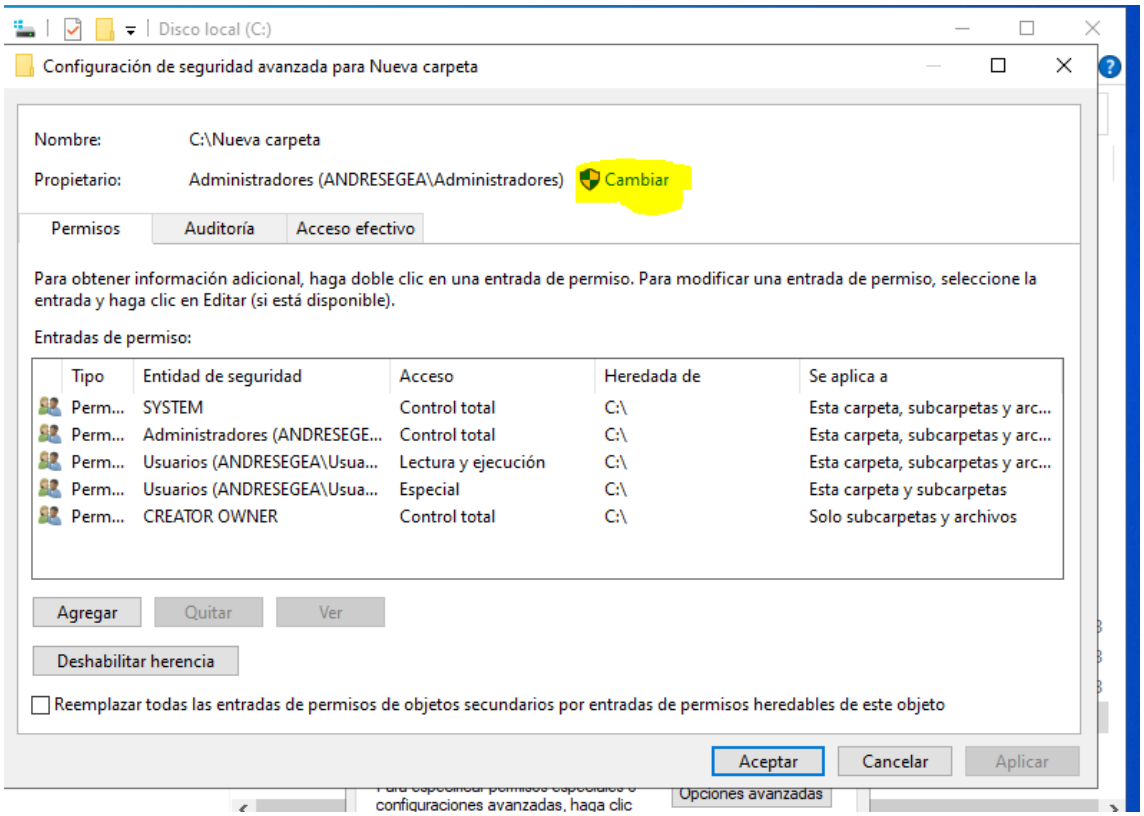
4.5.4. Tomar posesión de un archivo o de una carpeta

Tal como se ha visto anteriormente, esta acción la debe realizar el actual propietario del objeto, el administrador o un usuario que tenga control total sobre el objeto. Se deben seguir los siguientes pasos:

1. Abra el cuadro de diálogo de Propiedades desde la carpeta o el archivo.

2. Seleccione la ficha Seguridad y haga clic en el botón Opciones Avanzadas.

3. En el cuadro de diálogo Configuración de seguridad avanzada



4. En **propietario** pulse sobre Cambiar, elige el nombre del nuevo propietario o se puede elegir entre otros usuarios o grupos.

5. Para tomar posesión de todas las subcarpetas y archivos que están contenidas en la carpeta, marque la casilla de verificación Reemplazar **propietario en su contenedores y objetos.**

6. Haga clic en Aceptar.