Los permisos NTFS

Cada vez que abre sesión, la información de identificación utilizada por el usuario (nombre de usuario y contraseña) se transfiere a un monitor de seguridad local que accede al Administrador de seguridad (SAM de *Security Account Manager*). Este último, asignará un token de acceso que determinará los derechos de acceso que posee ese usuario para todos los objetos "asegurables" (claves del Registro, archivos, carpetas, servicios, procesos, etc.) Este descriptor de seguridad revisa dos informaciones:

- El SID del usuario.
- La lista DACL del objeto al que intenta acceder el usuario.

A continuación, explicaremos estas dos nociones.

1. Los SID de usuarios

Un SID (*Security IDentifier*) es una manera única de identificar a un usuario o grupo de usuarios. Podemos encontrar estos identificadores en los token de acceso, en las ACL (*Access Control List*) y en las bases de seguridad de cuentas.

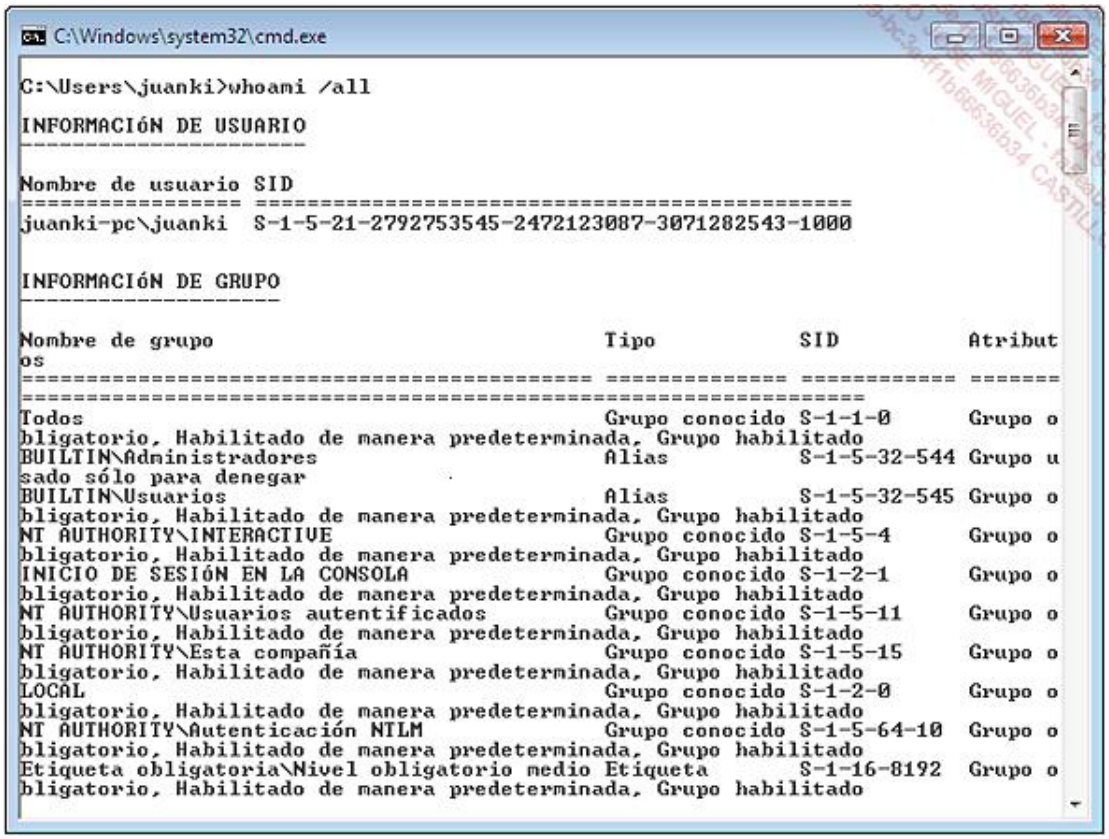
Diríjase al apartado siguiente para ver una descripción completa sobre el mecanismo de las ACL.

Los SID son datos de longitud variable que forman una representación jerárquica del actor designado: S-R-I-XXX-XXX-XXX.

- S: la letra S (para recordar que se trata de un SID).
- R: el número del formato binario de SID.
- I: número entero que identifica la autoridad que ha emitido el SID.
- XXX-XXX-XXX: serie de longitud variable, formada de identificadores de subautoridad o identificadores relativos (*Relative IDentifier* o RID).

Puede visualizar los SID de esta manera:

En la línea de comandos, teclee: **`whoami /all`**.



Se muestra la información siguiente:

- El SID correspondiente al grupo Administradores es S-1-5-32-544.
- La autoridad que ha emitido este SID tiene como identificador el número 5.
- La subautoridad tiene como identificador el número 32.
- 544 es el RID del grupo Administradores.

Puede comprobar los resultados mostrados con los siguientes comandos:

- **`whoami`**
- **`whoami /user /priv`**
- **`whoami /groups`**

Se mostrarán los privilegios del usuario que está conectado en ese momento. Puede obtener algunos SID de usuarios o entidades de seguridad abriendo este árbol de Registro: *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList*. Finalmente, los SID de algunas entidades se muestran en este otro árbol: HKEY_USERS.

2. Las listas de control de acceso

Una lista de control de acceso discrecional (DACL o *Discretionary Access Control Lists* o también ACL) es un mecanismo que permite proteger recursos como los archivos y las claves del Registro. Las DACL contienen las entradas de control de acceso (ACE o *Access Control Entry*) que funcionan como registros para cada usuario o grupo de usuarios que su SID señala. Estas entradas asocian una entidad de seguridad (una cuenta de usuario, un grupo de cuentas, una entidad de sistema) con una regla que define el uso del recurso. Las DACL y las ACE permiten

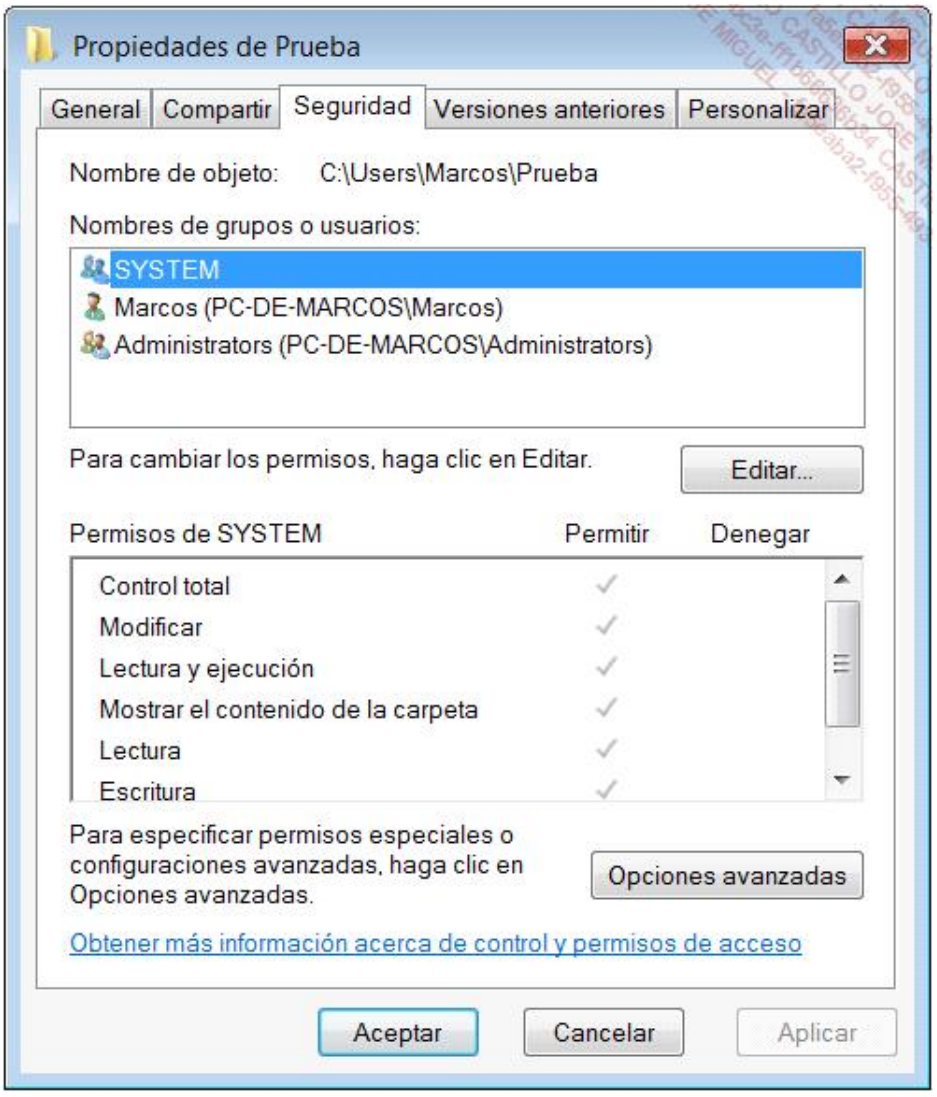
aceptar o rechazar los privilegios de acceso a los recursos según los permisos que usted quiera darle a las cuentas de usuario. También puede crear una ACE y aplicarla a la DACL de un archivo para impedir que nadie, salvo un administrador, pueda modificar el archivo.

Una lista de control de acceso de sistema (SACL o "ACE de auditoría") es un mecanismo que controla los mensajes de auditoría asociados a un recurso. Las SACL contienen ACE que definen las reglas de auditoría para un recurso determinado.

Así pues, podrá utilizar las DACL para asegurarse de que sólo un administrador puede modificar un archivo y las SACL para asegurarse de que se guarden todos los intentos conseguidos de apertura del archivo. Es posible distinguir las ACE positivas y ACE negativas:

- En el Explorador de Windows, abra su directorio de usuario.
- Cree una nueva carpeta llamada *Prueba*.
- Haga clic con el botón secundario del ratón en el submenú **Propiedades**.
- Haga clic en la pestaña **Seguridad**.

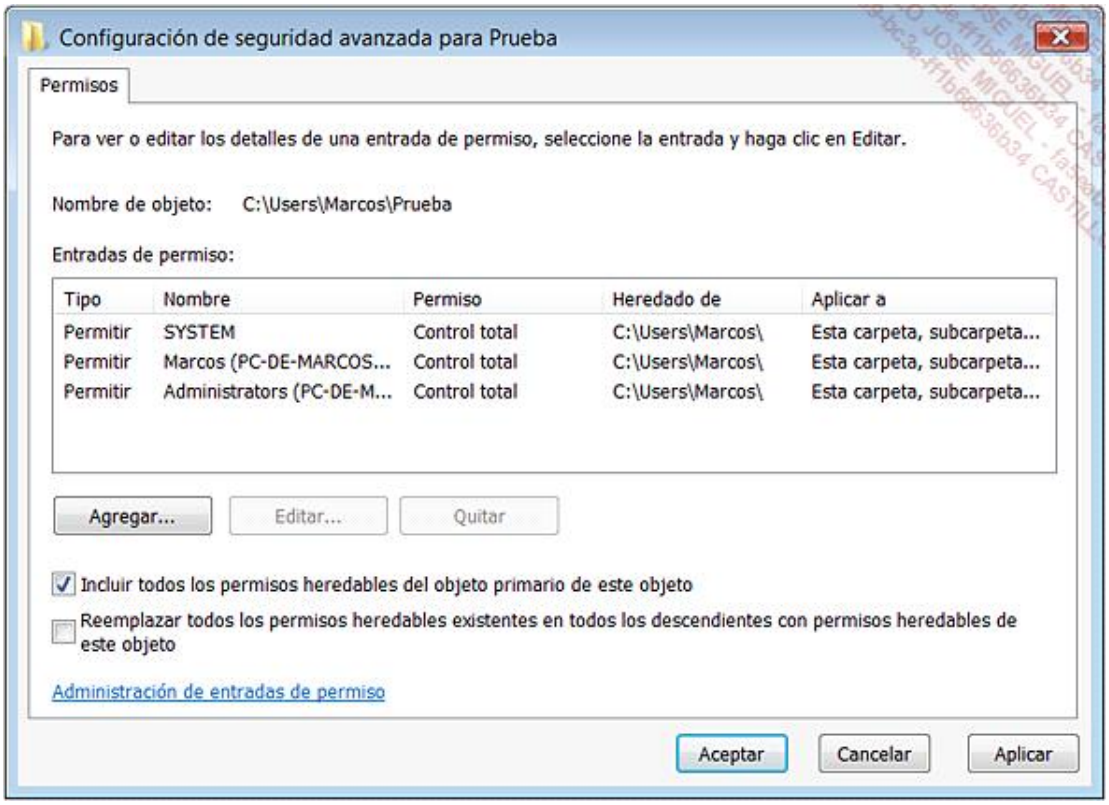
Tenga en cuenta que las ACE o autorizaciones visibles aparecen en gris.



De hecho, la carpeta que acaba de crear ha heredado los permisos en vigor de la carpeta principal. Este mecanismo

de encadenamiento se conoce como "herencia" y lo primero que haremos será desactivarlo.

- Haga clic en los botones **Opciones avanzadas** y **Editar**.
- Desactive la casilla **Incluir todos los permisos heredables del objeto primario de este objeto** y haga clic en **Copiar**.
- Haga clic en el botón **Desactivar la herencia** y a continuación en el vínculo **Convertir autorizaciones heredadas en autorizaciones explícitas de este objeto**.
- Haga clic en **Aceptar**.
- En Windows 8, para desactivar la herencia desde las propiedades de la carpeta, en la pestaña **Seguridad**, haga clic en el botón **Avanzado**. El resto del procedimiento es idéntico al de Windows 7.



- A continuación, haga clic dos veces en **Aceptar**.
- Haga clic en el botón **Editar**.
- Seleccione su nombre de usuario.

Ahora puede seleccionar las casillas **Denegar** para configurar una ACE negativa.

Cuando el sistema inicia una comprobación de acceso, empezará de manera sistemática, por las ACE negativas. Así pues, los permisos "Denegar" siempre tienen prioridad sobre los permisos "Permitir".

Último elemento, hemos visto que el principio más importante se basa en un problema de "no divulgación de la información". Existe una particularidad en los sistemas operativos NT: cuando un usuario crea un archivo, él es el propietario (Owner). El SID del propietario se coloca en el descriptor de seguridad que el sistema de archivos NTFS tiene para el objeto correspondiente. El propietario tiene permisos para leer el descriptor de seguridad y así, por ejemplo, modificar la ACL de un archivo. Para conocer el propietario de la carpeta que acaba de crear, haga clic en la pestaña **Seguridad**, después en el botón **Opciones avanzadas** y en la pestaña **Propietario**.

En Windows 8, se visualiza directamente el propietario de la carpeta. Puede hacer clic en el botón **Modificar** para

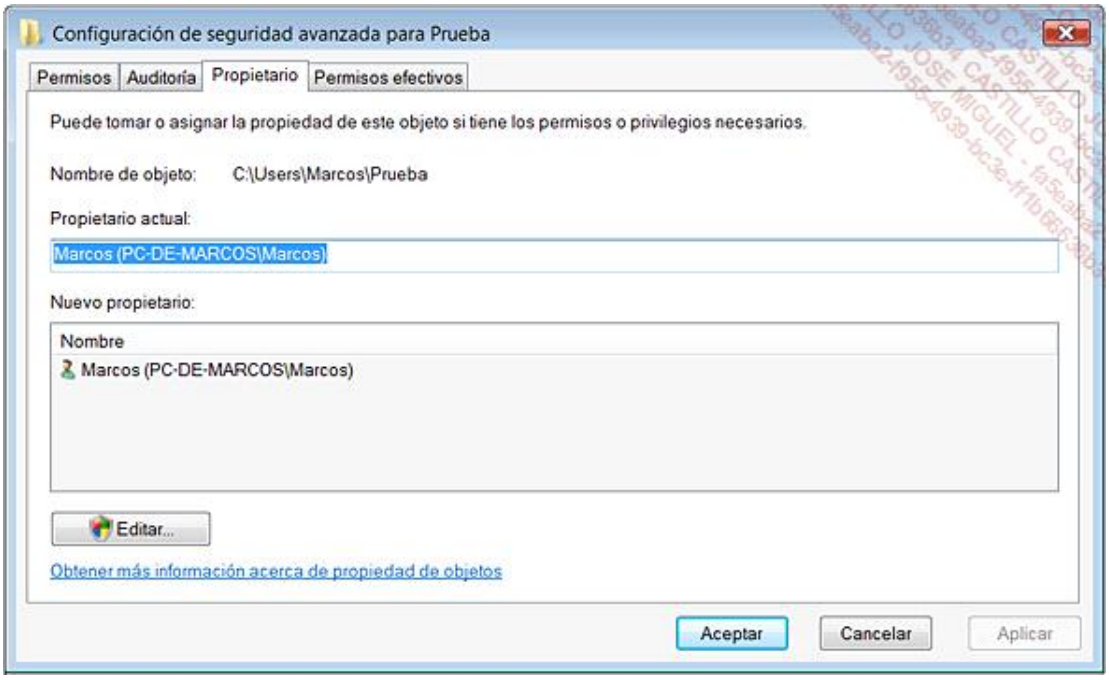
cambiar de propietario.

El propietario de un objeto siempre tiene permisos para leer y modificar la DACL de los objetos que él ha creado, motivo por el que el control de acceso se califica de discrecional (está a discreción del propietario).

3. Tomar posesión de un objeto

- Haga clic en el botón **Opciones avanzadas** y, a continuación, en la pestaña **Propietario**.

En Windows 8, se visualiza directamente el propietario de la carpeta en los parámetros de seguridad avanzados de la propia carpeta.



Por defecto, será su cuenta de usuario la que aparezca como el propietario del recurso. Esto se puede cambiar rápidamente de la siguiente manera:

- Haga clic en **Editar**.

Aparecerá automáticamente una lista con el grupo de administradores. En Windows 8, debe buscar o directamente introducir la cuenta o grupo de usuarios que desea definir como propietarios. Puede añadir otros grupos de usuarios haciendo clic en el botón correspondiente.

- Seleccione el grupo de administradores y haga clic en **Aplicar**.
- Si desea que esta operación se aplique a todos los objetos secundarios, seleccione la casilla **Remplazar el propietario en subcontenedores y objetos**.

Un cuadro de diálogo le avisará de que tendrá que cerrar las propiedades del objeto para que el cambio de propietario sea efectivo.

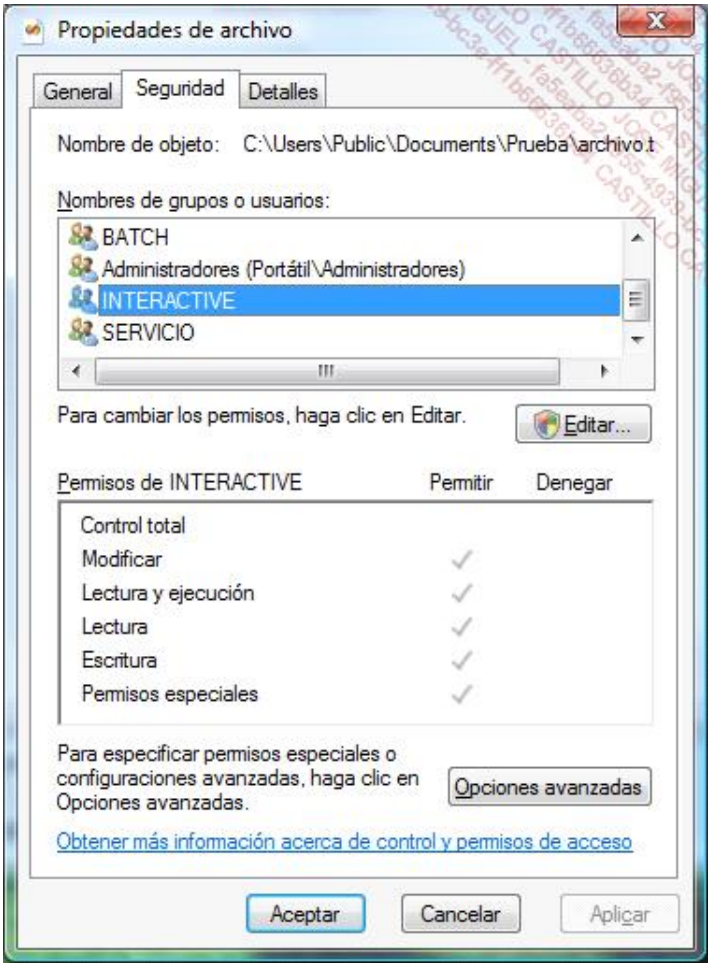
4. Utilizar los permisos NTFS

Pongamos ahora el ejemplo de un administrador llamado Juan que desea compartir una carpeta con permiso de

escritura con un usuario llamado Marcos y con permiso de sólo lectura con otra usuaria llamada Ana.

- Primero cree una carpeta llamada *Prueba*, dentro de la carpeta *Usuario/Acceso público/Documentos públicos*.
- Dentro de ésta, cree el archivo que deberá ser visible, lo puede llamar *Archivo.txt*.

Cualquier usuario tendrá acceso a la carpeta y podrá modificar el documento, ya que la entidad de sistema INTERACTIVE posee las autorizaciones especiales para el contenido de esta carpeta. La entidad reúne a todos los usuarios que han abierto una sesión interactiva en Windows.



- Empiece por desactivar el mecanismo de herencia, copiar los permisos y eliminar el grupo INTERACTIVE.

La carpeta ya no será accesible para los usuarios Marcos y Ana.

Hay que señalar que debido a que usted forma parte del grupo de administradores, no tendrá ningún problema de acceso a la carpeta.

- Una vez que ha realizado este primer paso, añada el usuario llamado Ana.

Ana podrá visualizar el contenido del archivo, pero no podrá eliminarlo, modificarlo ni crear otros documentos.

Por defecto, las tres autorizaciones genéricas que se han añadido son las siguientes: **Lectura y ejecución - Mostrar el contenido de la carpeta - Lectura**.

- Ahora añada el usuario llamado Marcos.

Acceda a los permisos efectivos haciendo clic en el botón **Opciones avanzadas** y seleccione estas cuatro casillas:

- **Crear archivos/escribir datos**
- **Crear carpetas/anexar datos**
- **Escribir atributos**
- **Escribir atributos extendidos**

Por lo que respecta al usuario, éste puede editar el contenido del archivo y añadir otros documentos, pero en ningún caso podrá:

- Cambiar el conjunto de permisos NTFS.
- Tomar posesión de la carpeta.
- Eliminar la carpeta o el archivo.

5. Tomar posesión de un directorio

El comando TakeOwn permite a un administrador (en Windows) recuperar el acceso que se le ha denegado a un archivo al haberse cambiado el propietario del archivo.

La sintaxis es la siguiente:

```
TAKEOWN [/S sistema] [/U usuario [/P contraseña]]] /F nombre_de_archivo
[/A] [/R [/D linea_de_comandos]]
```

Los modificadores son:

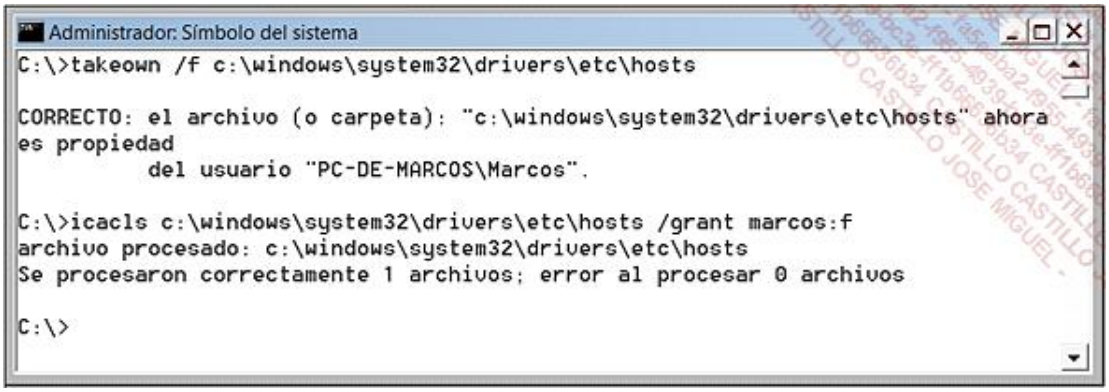
- **/s**: indica el sistema remoto al que conectarse.
- **/u: [dominio\]usuario**: especifica el contexto de usuario en el que el comando debe ejecutarse. Este modificador no puede utilizarse sin /s.
- **/p: [contraseña]**: define la contraseña del contexto de un usuario determinado.
- **/f : nombre_de_archivo**: indica el nombre del archivo o directorio. Puede utilizar el carácter genérico * para englobar varios archivos.
- **/a**: asigna la posesión al grupo de administradores y no al usuario actual. Este modificador no es específico, la posesión del archivo se asignará al usuario conectado en ese momento.
- **/r**: trata el comando en modo recursivo. La operación se realizará en un conjunto de directorios y subdirectorios.
- **/d: línea_de_comandos**: permite definir una respuesta predeterminada que se utilizará aunque el usuario actual no posea el permiso "mostrar lista de carpetas" en un directorio. Esto se produce durante el proceso recursivo (/R) de subdirectorios. Utilice los valores "O" para tomar posesión o "N" para ignorar.

Aquí le mostramos un ejemplo de uso. Después de una instalación de Windows, algunos directorios situados en otra partición ya no son accesibles, ni siquiera desde una cuenta de usuario con privilegios de administrador. La explicación es sencilla: las ACL se configuran en función del SID que ya no existe en el sistema. En este caso, puede utilizar estos dos comandos:

- **takeown /f Nombre_del_directorio /r /d o**. Un mensaje le avisará: "CORRECTO: el archivo (o carpeta): ubicación y Nombre_de_archivo" es propiedad del usuario "PC\Nombre_de_usuario".
- **icacls Nombre_del_directorio /grant administradores:f /t**

¡El acceso al directorio será entonces posible! Tenga en cuenta que deberá ejecutar el Símbolo del sistema como administrador, de lo contrario aparecerá un mensaje que indica que el acceso ha sido denegado. Vea otro ejemplo de comandos que le permitirán tomar posesión del archivo Hosts:

- **takeown /f c:\windows\system32\drivers\etc\hosts**
- **icacls c:\windows\system32\drivers\etc\hosts /grant marc:f**



Más adelante explicaremos la sintaxis de icacls.

6. Modificar las listas de control de acceso

Mediante el Símbolo del sistema, puede modificar las ACL de los archivos utilizando una herramienta llamada icacls. Aquí le mostramos las diferentes sintaxis posibles:

```
Icacls Nombre /save Nombre_de_archivo [/T] [/C] [/L]
```

Almacena las listas de control de acceso para todos los archivos coincidentes en Nombre_de_archivo. Este comando le permitirá utilizar luego el parámetro /restore.

```
icacls Nombre_de_directorio [/substitute Antiguo_SID Nuevo_SID [...]]
/restore Nombre_de_archivo [/C] [/L]
```

Aplica las listas de control de acceso guardadas en los archivos actuales del directorio.

```
icacls Nombre /setowner usuario [/T] [/C] [/L]
```

Cambia el propietario de todos los archivos coincidentes.

```
icacls Nombre /findsid SID [/T] [/C] [/L]
```

Busca todos los archivos correspondientes que contienen una lista de control de acceso donde se menciona el SID de manera explícita.

```
icacls Nombre /verify [/T] [/C] [/L]
```

Busca todos los archivos cuya lista de control de acceso no esté en formato canónico o cuya longitud no sea coherente con el número de entradas de control de acceso.

```
icacls Nombre /reset [/T] [/C] [/L]
```

Reemplaza las listas de control de acceso por las listas heredadas de manera predeterminada por todos los archivos correspondientes.

```
icacls Nombre [/grant[:r] SID:autorización[...]]
```

Concede los derechos de acceso al usuario especificado.

- Con el modificador :r, los permisos reemplazan cualquier permiso explícito concedido previamente.
- Sin el modificador :r, los permisos se agregan a cualquier permiso explícito concedido anteriormente.

```
icacls Nombre /deny ISD:autorización
```

Deniega de manera explícita los derechos de acceso al usuario especificado. Se agrega a los permisos indicados una entrada de control de acceso de denegación explícita y se eliminan los mismos permisos de cualquier concesión explícita.

```
icacls Nombre /remove[:[g|d]] SID
```

Suprime todas las repeticiones de SID en la lista de control de acceso.

- Con el modificador :g, se eliminan todas las repeticiones de derechos concedidos a este SID.
- Con el modificador :d, se eliminan todas las repeticiones de derechos denegados a este SID.

```
icacls Nombre /setintegritylevel [(CI)(OI)]
```

Este nivel añade de forma explícita una ACE de integridad (un nivel de integridad) a la carpeta correspondiente. El nivel puede ser:

- **L[ow] - Bajo**
- **M[edium] - Medio**
- **H[igh] - Alto**

Las opciones de herencia para la ACE de integridad pueden preceder al nivel y se aplican sólo a los directorios.

Los SID pueden especificarse con un formato numérico o un nombre descriptivo. Si utiliza un formato numérico, agregue un asterisco al principio del SID.

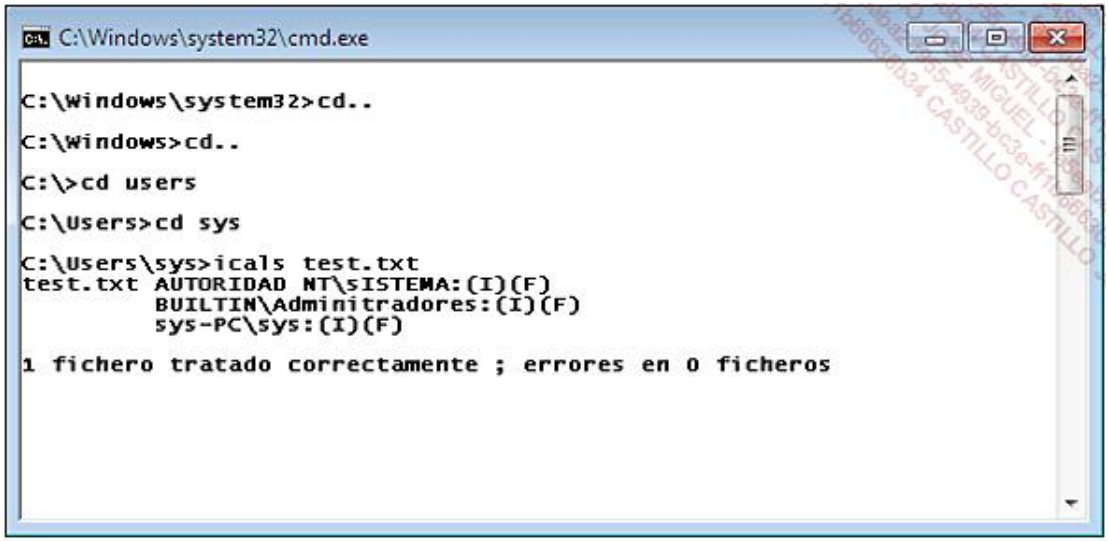
- **/T** indica que esta operación se realiza en todos los archivos o directorios coincidentes que se encuentran en los directorios especificados en el nombre.
- **/C** indica que esta operación continuará en todos los errores de archivo. Se seguirán mostrando los mensajes de error.
- **/L** indica que esta operación se realiza directamente en el vínculo simbólico en lugar de en su destino.

No dude en consultar el archivo de ayuda de este comando para obtener más información.

7. Utilizar icacls

- De la misma manera que antes, cree un directorio llamado *Prueba* en el directorio del usuario.
- Visualice la lista de las ACL utilizando el siguiente comando: **icacls test.txt**.

Tres usuarios o grupos de usuarios aparecerán en una lista: usted, el grupo SISTEMA y el grupo Administradores.



- Todos poseen control total sobre el directorio: (F).
- La ACL es heredada: (IO).
- La herencia se aplica al contenedor (la carpeta): (CI).
- También se aplica a los objetos (subcarpetas y archivos): (OI).

Para salvar la máscara de permisos, teclee: **icacls test.txt /save "Permisos de la carpeta Prueba"**

El archivo se puede abrir con el Bloc de notas de Windows y enumera los SID de usuario y la lista de permisos mediante la sintaxis SDDL.

Para eliminar los grupos de administradores, utilice el siguiente comando: **icacls test.txt /remove:g administradores**

Para activar el mecanismo de herencia, teclee: **icacls test.txt /reset**

Para permitir un acceso de escritura en la lista de control de acceso de la carpeta *Prueba*, introduzca: **icacls archivo /grant juan:(WDAC)**.

Este permiso aparecerá en: "Permisos especiales".