

# Windows 10

## Permisos locales NTFS

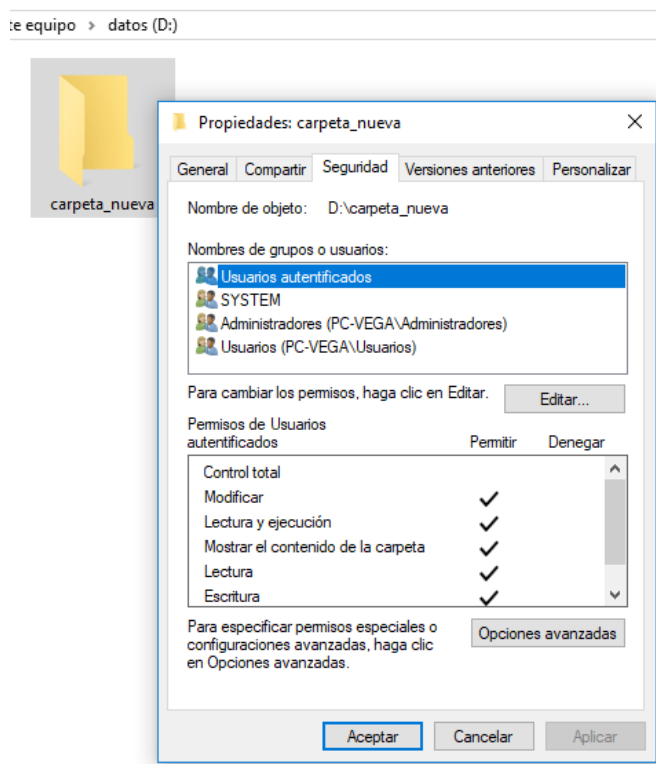
### 1. Los permisos NTFS de archivos y carpetas

Todo administrador debe saber definir permisos NTFS para carpetas o archivos y controlar su acceso en la mayor medida posible empleando los recursos compartidos. Un permiso define el derecho de realizar una operación sobre un recurso.

La definición precisa de los permisos permite evitar la fuga de datos y los problemas de seguridad. Por defecto, el propietario de un recurso es el único habilitado para definir sus permisos, pudiendo cederlos a un usuario o a un grupo. Un administrador puede tomar posesión de un archivo empleando el comando **takeown**.

Los permisos NTFS protegen los datos contra accesos no autorizados efectuados localmente o desde la red, junto a los del recurso compartido. El administrador puede definir **permisos básicos** (lectura, modificación, etc.) o **permisos especiales** (tomar posesión, leer atributos, etc.), más precisos.

Estos permisos pueden definirse haciendo clic con el botón derecho en una carpeta o archivo y, a continuación, seleccionando **Propiedades**. Seguidamente, haga clic en la pestaña **Seguridad** y, a continuación, en el botón **Editar** para atribuir los permisos adecuados.

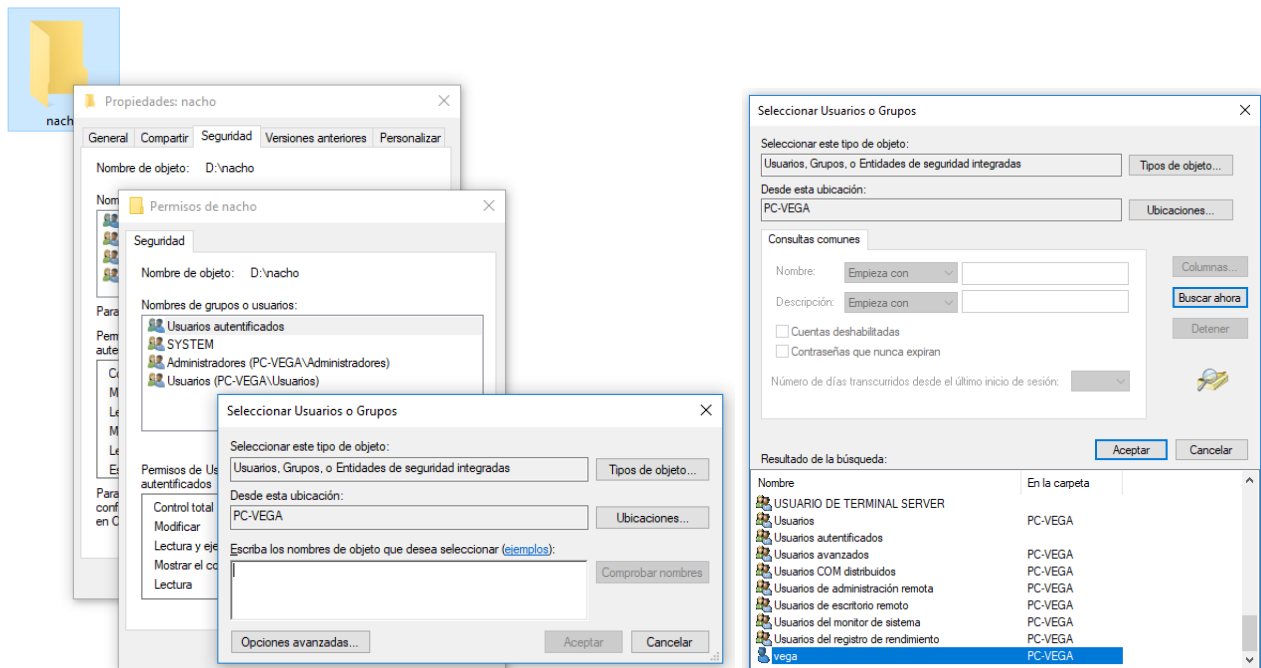


Entre los permisos básicos de archivos y carpetas se incluyen **Control total, Modificar, Leer y ejecutar, Mostrar el contenido de la carpeta, Leer y Escribir**.

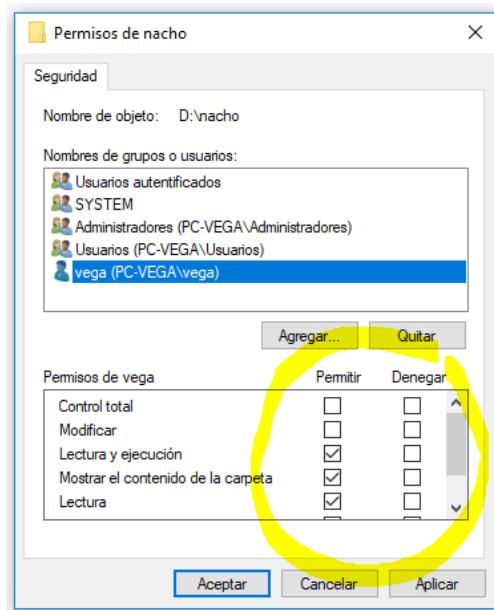
#### 1.1. Configurar los permisos NTFS explícitamente para un grupo o usuario que no aparece por defecto.

Para configurar, ver, cambiar o quitar permisos básicos de archivos y carpetas:

- Haga clic en *Inicio, Equipo* y busque el archivo o la carpeta para el que desea configurar permisos.
- Haga clic con el botón secundario del ratón en el archivo o en la carpeta, haga clic en **Propiedades** y, después, haga clic en la **ficha Seguridad**.
- Para configurar los permisos de un grupo o de un usuario que no aparece en el cuadro **Nombres de grupos o usuarios**, haga clic en **Editar** y luego **Agregar**, escriba el nombre del grupo o del usuario para el que desea configurar los permisos y, después, haga clic en **Aceptar**.
- Si no sabe el nombre del grupo o usuario, puede hacer clic en **Opciones avanzadas** y luego **Buscar ahora**, le aparecerán así un listado con todos los grupos y usuarios del sistema.



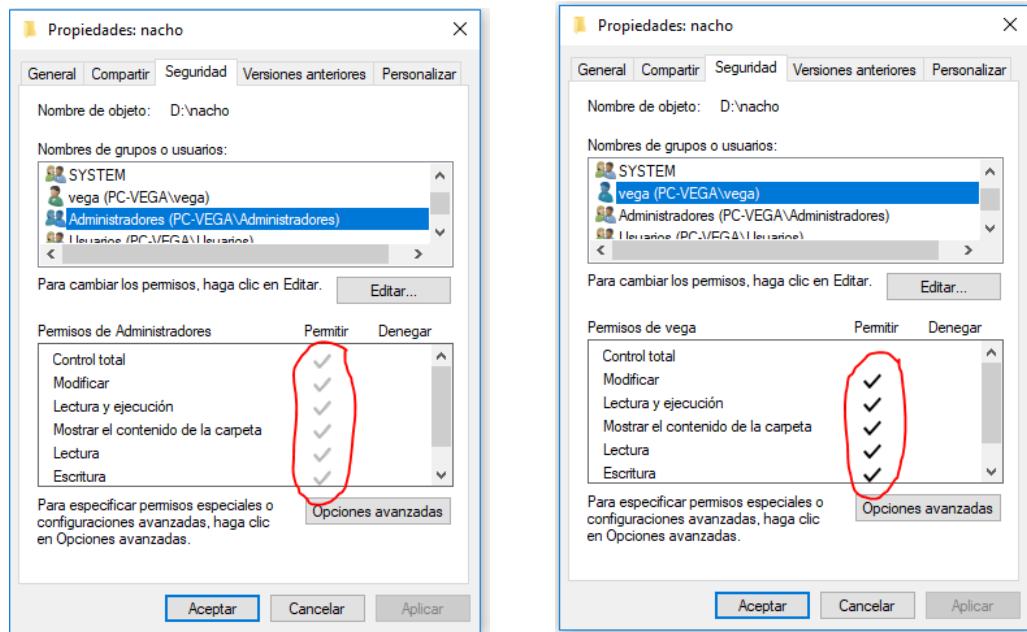
- Para cambiar o quitar permisos de un grupo o un usuario existente, desde la **ficha Seguridad → Editar** → seleccione un grupo o usuario en el cuadro **Nombres de grupos o usuarios**.
- Para permitir o denegar un permiso, haga clic para activar la casilla de verificación **Permitir** o **Denegar** en el cuadro **Permisos para usuario o grupo**, donde usuario o grupo es el nombre del usuario o el grupo.
- Para quitar un grupo o usuario del cuadro **Nombres de grupos o usuarios**, haga clic en **Quitar**.



## 2. Herencia de permisos

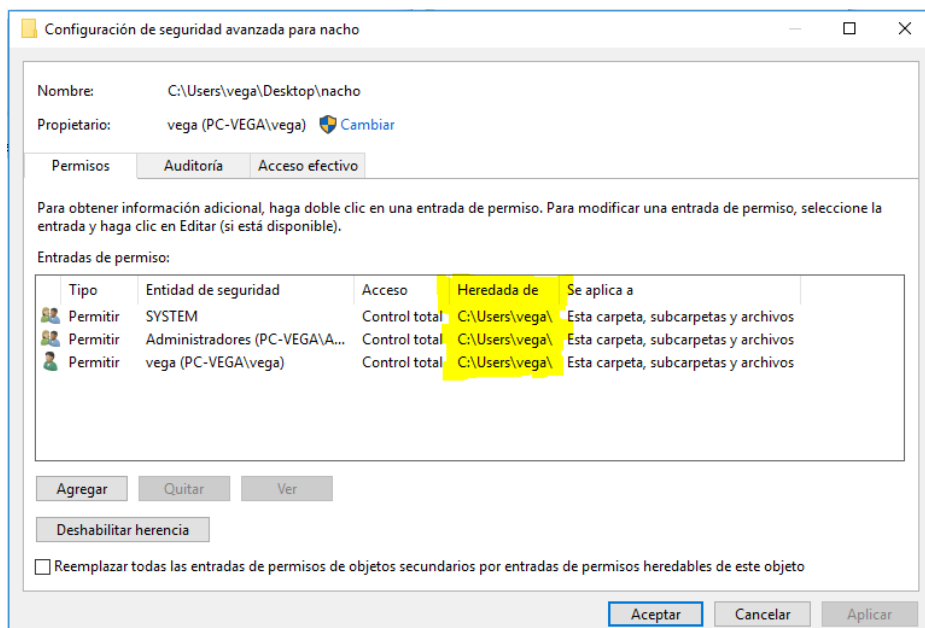
### 2.1. Permisos explícitos y heredados

Los permisos asignados como se ha visto en el punto anterior se denominan **permisos explícitos** al ser asignados de manera explícita para esa carpeta o archivo. Pero también pueden heredarse permisos desde la carpeta principal que contiene nuestra carpeta o archivo, en ese caso los **permisos heredados** aparecen **sombreados** en la pestaña *Seguridad* del objeto (imagen inferior izquierda)., en cambio los permisos explícitos definidos expresamente para dicho objeto aparecen **en negro** (imagen inferior derecha).



Un permiso definido explícitamente es siempre prioritario a un permiso heredado. Sin embargo, si el acceso a un objeto se le aplica *Denegar* por herencia y se define explícitamente el permiso *Permitir*, se mantendrá este último.

Podemos ver desde qué carpeta se están heredando los permisos para un objeto (subcarpeta o archivo). Para ello debes ir a las **Opciones avanzadas** del cuadro de **Propiedades** del objeto:

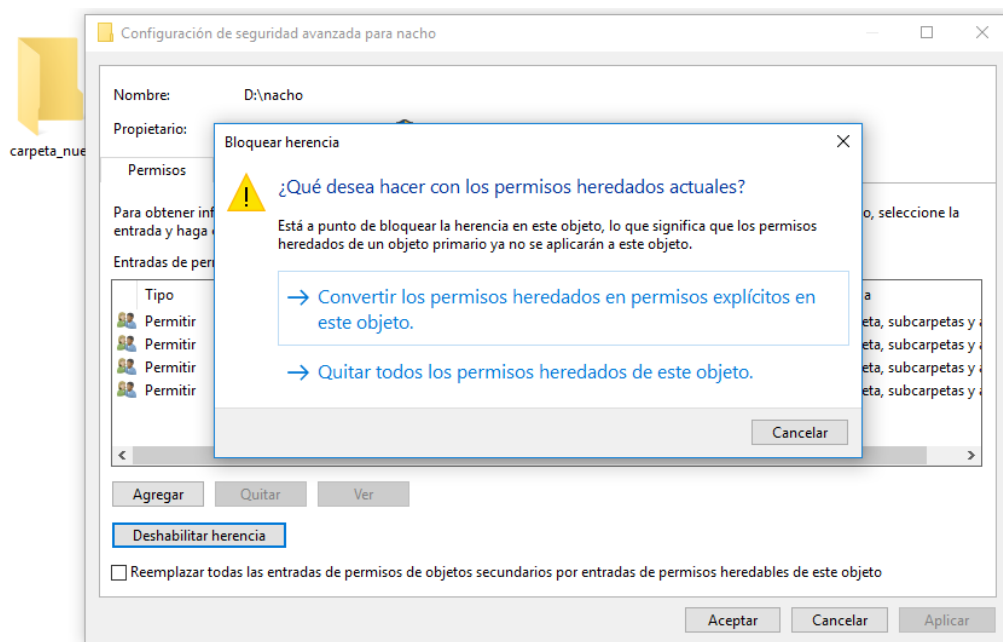


## 2.2. Bloquear la herencia de permisos en una carpeta desde niveles superiores

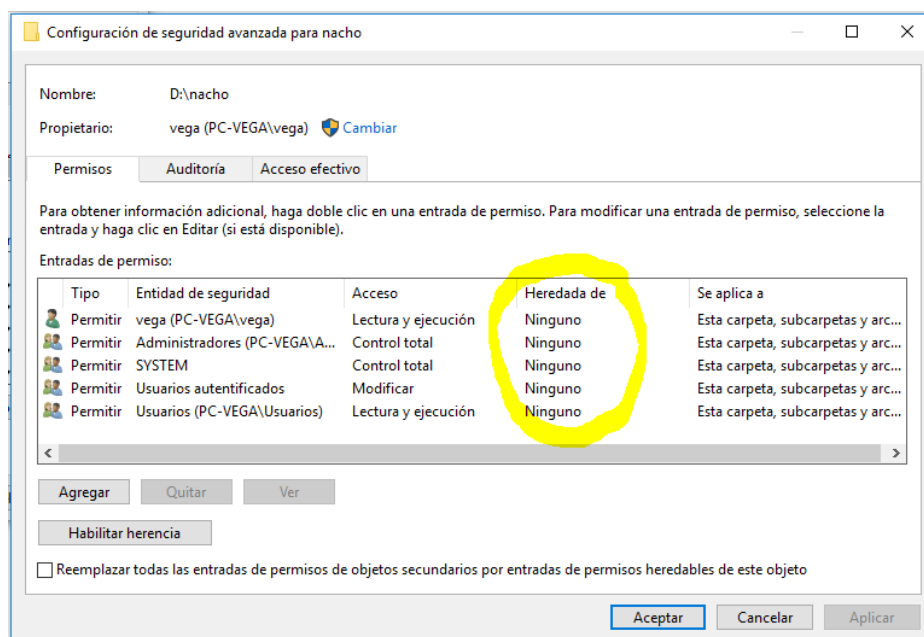
La herencia de permisos NTFS en una carpeta secundaria puede estar bloqueada, elevando así carpeta al rango de primaria. Durante ese proceso, el usuario deberá decidir entre copiar los permisos existentes o comenzar con una base virgen.

Para **bloquear o romper la herencia** en una carpeta almacenada en una partición NTFS:

- ➔ Desde el *Explorador de Windows* y como administrador, haga clic con el botón derecho en una carpeta y, a continuación, seleccione **Propiedades**. Haga clic en la pestaña **Seguridad** y, a continuación, en el botón **Opciones avanzadas**.
- ➔ Haga clic en el botón **Deshabilitar herencia**. Escoja **Convertir los permisos heredados en permisos explícitos en este objeto** o bien opte por **Quitar todos los permisos heredados de este objeto**.



Ahora en la configuración de seguridad avanzada de la carpeta en cuestión aparecerán todos los permisos como **no heredados** desde ninguna carpeta principal (ver imagen)



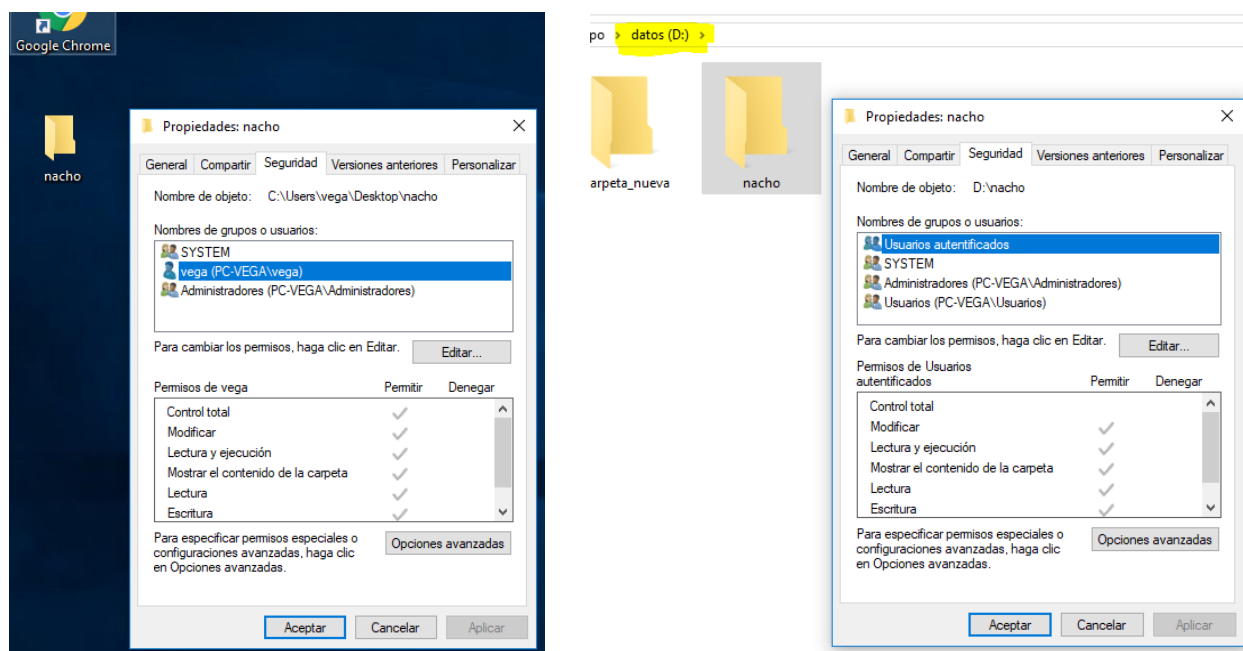
### ▪ Copiar/Mover objetos entre particiones NTFS:

Cuando se **copia** una carpeta/archivo en otra partición o en la misma partición NTFS, su copia hereda los permisos definidos en la partición de destino, eliminando los permisos explícitos y/o heredados que pudieran tener el objeto en su ubicación original.

Si se **mueve** una carpeta/archivo en la misma partición NTFS, sucede lo mismo, pero esta vez se mantienen en el objeto aquellos permisos que le hayan sido asignados explícitamente. En cambio, si se mueve entre particiones NTFS diferentes, la carpeta/archivo heredará siempre los permisos de la carpeta de destino (eliminando los permisos explícitos que pudiese tener en su ubicación original); esto es, mover y copiar entre particiones diferentes tiene el mismo resultado respecto a los permisos.

Por ejemplo, en la imagen inferior a la derecha se ven los permisos por defecto en una carpeta creada dentro del *Escritorio*, en el *perfil del usuario* (C:\Users\vega donde sólo él y el grupo *Administradores* tienen permisos). Y a la derecha, la misma carpeta una vez copiada a *Datos* (Distinta partición NTFS, D:\) pudiendo apreciarse cómo se han heredado los permisos establecidos en esta última partición para todos los usuarios (si hubiese tenido algún permiso explícito desaparecerá en la copia). Pasar de este modo una carpeta o archivo a una partición diferente de C:\ puede ser una manera de hacer accesible dichos objetos a todos los usuarios del sistema.

Si en lugar de copiar se mueve la carpeta, los permisos aparecen como explícitos en lugar de heredados.



Una carpeta (principal) puede contener una o más subcarpetas (secundarias). Un **permiso definido explícitamente** para la carpeta principal se propagará a sus subcarpetas (si no está rota la herencia en las secundarias). De esta forma, cualquier modificación en el nivel más alto de la jerarquía se transferirá a los niveles inferiores.

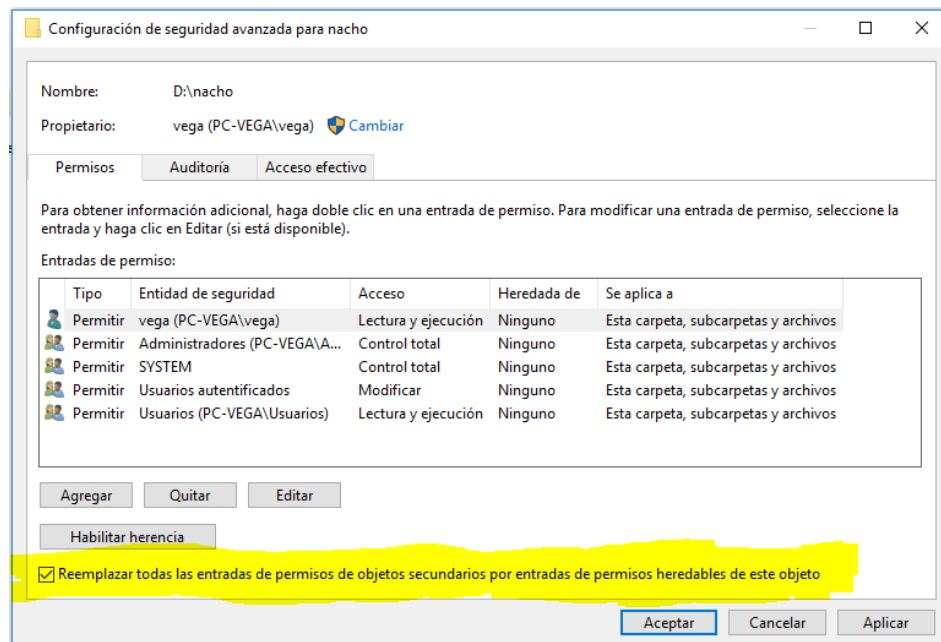
En caso de copiar o mover a una **partición diferente de NTFS** como, por ejemplo, **FAT**, la carpeta perderá todos sus permisos.

El comando **robocopy** permite mantener los permisos en las carpetas o archivos durante las acciones copiar o mover.

### 2.3. Propagar la herencia de permisos a los archivos y carpetas secundarias

Después de configurar los permisos en una carpeta principal, los nuevos archivos y subcarpetas que se crean en la carpeta heredan por defecto estos permisos. Si desea que los archivos y las carpetas secundarios hereden obligatoriamente los permisos de la carpeta principal:

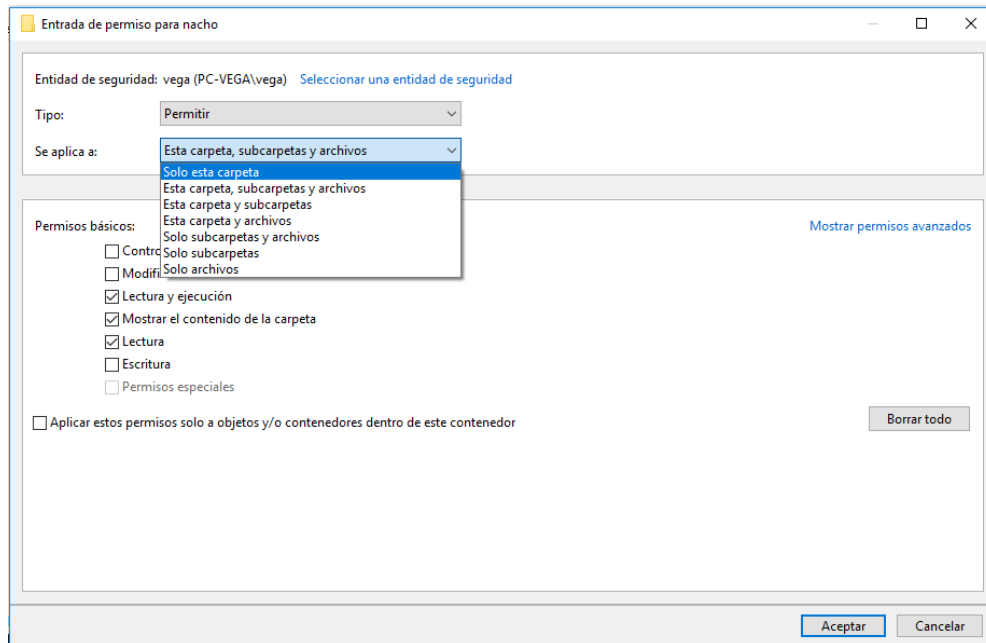
- Vaya a la pestaña **Seguridad** de la carpeta.
- Haga clic en **Opciones avanzadas**.
- Active la casilla de verificación **Reemplazar todas las entradas de permisos de objetos secundarios por entradas de permisos heredables de este objeto**.



Esta es la manera de **forzar a que los objetos secundarios hereden todos los permisos de una carpeta principal**. De esta manera se sustituyen todas las entradas de permisos que puedan tener los objetos secundarios por entradas de permisos heredadas desde la carpeta principal en la que se fuerza la herencia.

Sin embargo, puede no querer forzar a heredar todos los permisos de la carpeta principal, y sí **impedir que sólo determinados archivos o subcarpetas hereden los permisos de la carpeta principal**, en este caso:

- Desde el *Explorador de Windows* y como administrador, haga clic con el botón derecho en una carpeta y, a continuación, seleccione **Propiedades**. Haga clic en la pestaña **Seguridad** y, a continuación, en el botón **Opciones avanzadas**.
- Clic en **Agregar** para asignar permisos a un usuario o grupo sobre esta carpeta.
- Seleccionar una entidad de seguridad para elegir qué usuario o grupo.
- Elegir en **Se aplica a**: si queremos que los permisos sean válidos **Sólo en esta carpeta**, o bien queremos que sean heredados por objetos secundarios hasta el nivel o tipo que queramos. Podemos elegir entre subcarpetas o archivos, entre la carpeta primaria y las siguientes subcarpetas que pudieran crearse o existan, así como todas las posibles combinaciones entre esas opciones (ver imagen).



Podemos encontrarnos que las casillas de verificación para asignar permisos no están disponibles en la anterior ventana. En este caso el archivo o la carpeta tiene permisos heredados de la carpeta principal. Entonces, hay tres formas de hacer cambios en los permisos heredados:

- Haga los cambios en la carpeta principal, de forma que el archivo o la carpeta herede los permisos.
- Haga clic para seleccionar el permiso opuesto (*Permitir* o *Denegar*) para omitir el permiso heredado.
- Desactive la herencia como ya se ha visto anteriormente, incluyendo las entradas de permisos indicadas aquí de forma explícita. Cuando lo haga, puede hacer cambios en los permisos, o quitar el usuario o el grupo de la lista de permisos. Sin embargo, el archivo o la carpeta no hereda permisos de la carpeta principal.

## 2.4. Prioridad entre Permitir y Denegar

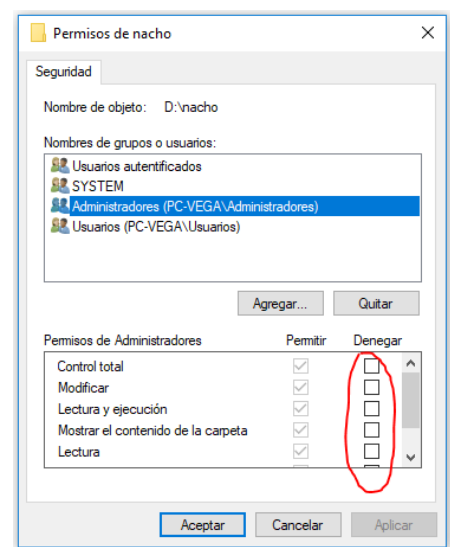
Cuando utilice la configuración **Denegar y Permitir**, tenga en cuenta lo siguiente:

- **Permitir:** estos permisos son acumulativos, por lo que los permisos de un usuario están determinados por el efecto acumulativo de todos los grupos a los que pertenece el usuario.
- **Denegar:** estos permisos reemplazan a los de Permitir. Tenga cuidado cuando aplique los permisos Denegar.

En la mayoría de los casos, Denegar reemplaza a Permitir a menos que una carpeta herede una configuración conflictiva de distintas carpetas principales. Cuando esto ocurre, la configuración heredada de la carpeta principal más cercana al objeto en el subárbol tiene prioridad.

Hay que recordar, como se comentó antes, que, si el acceso a un objeto se le aplica Denegar por herencia y se define explícitamente el permiso Permitir, se mantendrá este último.

Los permisos heredables sólo los heredan los objetos secundarios. Cuando configure permisos para el objeto principal, puede decidir si los archivos o las subcarpetas pueden heredarlos con la configuración “Se



***aplica en***", que vimos anteriormente; pudiendo determinar de manera precisa qué permisos tiene un usuario o un grupo sobre un objeto revisando sus **permisos efectivos**.



### 3. Tipos de permisos NTFS

Entre los permisos de carpetas se incluyen **Control total**, **Modificar**, **Leer y ejecutar**, **Mostrar el contenido de la carpeta**, **Leer y Escribir**. Cada uno de estos permisos consta de un grupo lógico de permisos especiales que se enumeran y definen en las próximas secciones.

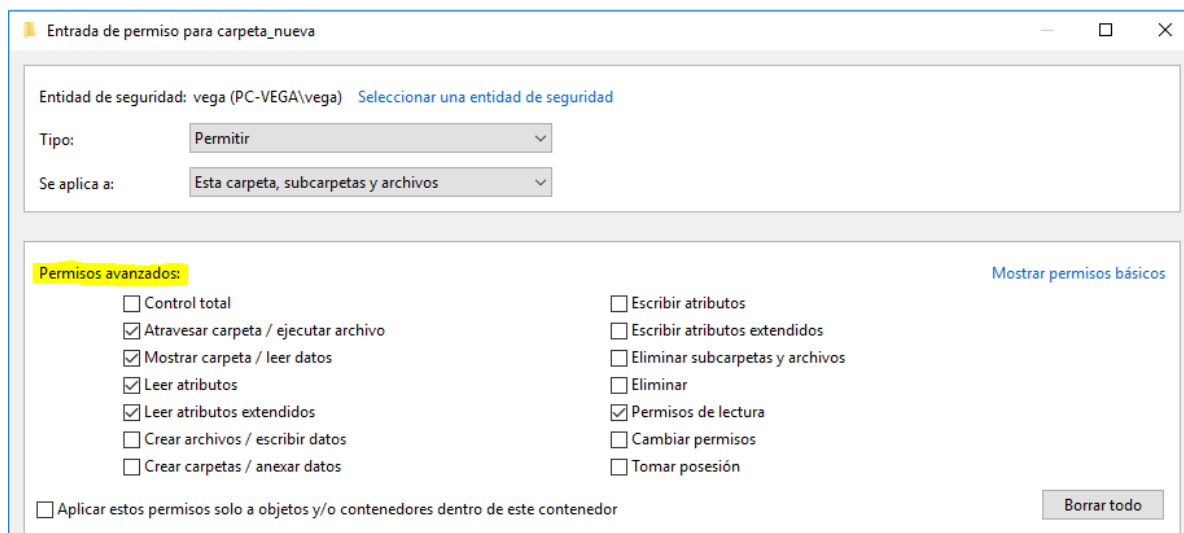
#### 3.1. Permisos básicos

- **Control total** → Permite a un usuario cambiar los permisos, tomar posesión, eliminar subcarpetas y archivos y realizar las acciones permitidas por todos los demás permisos
- **Modificar** → Permite modificar y eliminar un archivo y realizar las acciones permitidas por los permisos de Escribir y Lectura y Ejecución.
- **Lectura y Ejecución** → Concede a un usuario los derechos necesarios para ejecutar aplicaciones y realizar las acciones permitidas por el permiso Leer.
- **Leer** → Permite a un usuario leer un archivo y ver atributos de archivo, propiedades y permisos.
- **Escribir** → Permite a un usuario sobrescribir un archivo, cambiar los atributos de archivos y ver los permisos y propiedad del archivo.

#### 3.2. Permisos avanzados de archivos y carpetas.

**[NO ENTRAN EN EXAMEN  
excepto permiso especial Tomar Posesión ver 3.3]**

**Nota:** aunque parece que **Mostrar el contenido de la carpeta** y **Leer y ejecutar** tienen los mismos permisos especiales, estos permisos se heredan de manera diferente. **Mostrar el contenido de la carpeta** lo heredan las carpetas, pero no los archivos, y sólo aparece al ver los permisos de carpetas. **Leer y ejecutar** lo heredan tanto los archivos como las carpetas y siempre está presente cuando ve los permisos de archivos o de carpetas.



#### ▪ **Control total**

Los grupos o los usuarios a los que se concede **Control total** para una carpeta pueden eliminar cualquier archivo de dicha carpeta, cualesquiera que sean los permisos que protegen al archivo.

#### ▪ **Recorrer carpeta o ejecutar archivo**

**Para carpetas:** el permiso **Recorrer carpeta** permite o impide que el usuario pase de una carpeta a otra para llegar a otros archivos o carpetas, incluso aunque el usuario no tenga permisos para las carpetas recorridas (sólo se aplica a carpetas). **Recorrer carpeta** sólo surte efecto cuando al grupo o al usuario no se le ha concedido el permiso **Omitir comprobación de recorrido**, que comprueba los derechos de usuario en

el complemento Directiva de grupo. De manera predeterminada se concede al grupo **Todos** el derecho de usuario **Omitir comprobación de recorrido**.

**Para archivos:** el permiso **Ejecutar archivos** permite o deniega la ejecución de los archivos de programa (sólo se aplica a archivos).

Al configurar el permiso **Recorrer carpeta** en una carpeta no se configura automáticamente el permiso **Ejecutar archivo** en todos los archivos de dicha carpeta.

- **Listar carpeta / Leer datos**

El permiso **Listar carpeta** permite o impide que el usuario vea los nombres de archivo y de subcarpeta en la carpeta. El permiso **Listar carpeta** sólo afecta al contenido de dicha carpeta, no a si se muestra o no el contenido de la carpeta para la que está configurando el permiso. Esto se aplica sólo a carpetas.

El permiso **Leer datos** permite o impide ver datos de archivos (sólo se aplica a archivos).

- **Atributos de lectura**

El permiso **Atributos de lectura** permite o impide que el usuario vea los atributos de un archivo o de una carpeta, como sólo lectura y oculto. Los atributos están definidos por el sistema de archivos NTFS.

- **Atributos extendidos de lectura**

El permiso **Atributos extendidos de lectura** permite o impide que el usuario vea los atributos extendidos de un archivo o de una carpeta. Los atributos extendidos están definidos por los programas y pueden variar de uno a otro.

- **Crear archivos / Escribir datos**

El permiso **Crear archivos** permite o impide al usuario crear archivos en la carpeta (se aplica sólo a carpetas).

El permiso **Escribir datos** permite o impide que el usuario haga cambios en el archivo y sobrescriba contenido existente (se aplica sólo a archivos).

- **Crear carpetas / Anexar datos**

El permiso **Crear carpetas** permite o impide al usuario crear carpetas en la carpeta (se aplica sólo a carpetas).

El permiso **Anexar datos** permite o impide que el usuario haga cambios en el final del archivo pero que no cambie, elimine ni sobrescriba datos existentes (se aplica sólo a archivos).

- **Atributos de escritura**

El permiso **Atributos de escritura** permite o impide que el usuario cambie los atributos de un archivo o de una carpeta, como sólo lectura y oculto. Los atributos están definidos por el sistema de archivos NTFS.

El permiso **Atributos de escritura** no implica la creación o eliminación de archivos o carpetas; sólo incluye el permiso para hacer cambios en los atributos de un archivo o de una carpeta.

- **Atributos extendidos de escritura**

El permiso **Atributos extendidos de escritura** permite o impide que el usuario cambie los atributos extendidos de un archivo o de una carpeta. Los atributos extendidos están definidos por los programas y pueden variar de uno a otro.

El permiso **Atributos extendidos de escritura** no implica que el usuario pueda crear o eliminar archivos o carpetas; sólo incluye el permiso para hacer cambios en los atributos de un archivo o de una carpeta.

- **Eliminar**

El permiso **Eliminar** permite o impide que el usuario elimine el archivo o la carpeta. Si no tiene el permiso **Eliminar** para un archivo o una carpeta, puede eliminarlo si se le han concedido los permisos Eliminar subcarpetas y archivos en la carpeta principal.

### ▪ **Eliminar subcarpetas y archivos**

El permiso **Eliminar subcarpetas y archivos** permite o impide que el usuario elimine subcarpetas y archivos, incluso aunque no se haya concedido el permiso **Eliminar** para la subcarpeta o el archivo. Este permiso se aplica sólo a las carpetas.

### ▪ **Permisos de Lectura**

El permiso **Leer permisos** permite o impide que el usuario lea permisos del archivo o de la carpeta, como **Control total**, **Leer y Escribir**.

### ▪ **Cambiar permisos**

El permiso **Cambiar permisos** permite o impide que el usuario cambie permisos del archivo o de la carpeta, como **Control total**, **Leer y Escribir**.

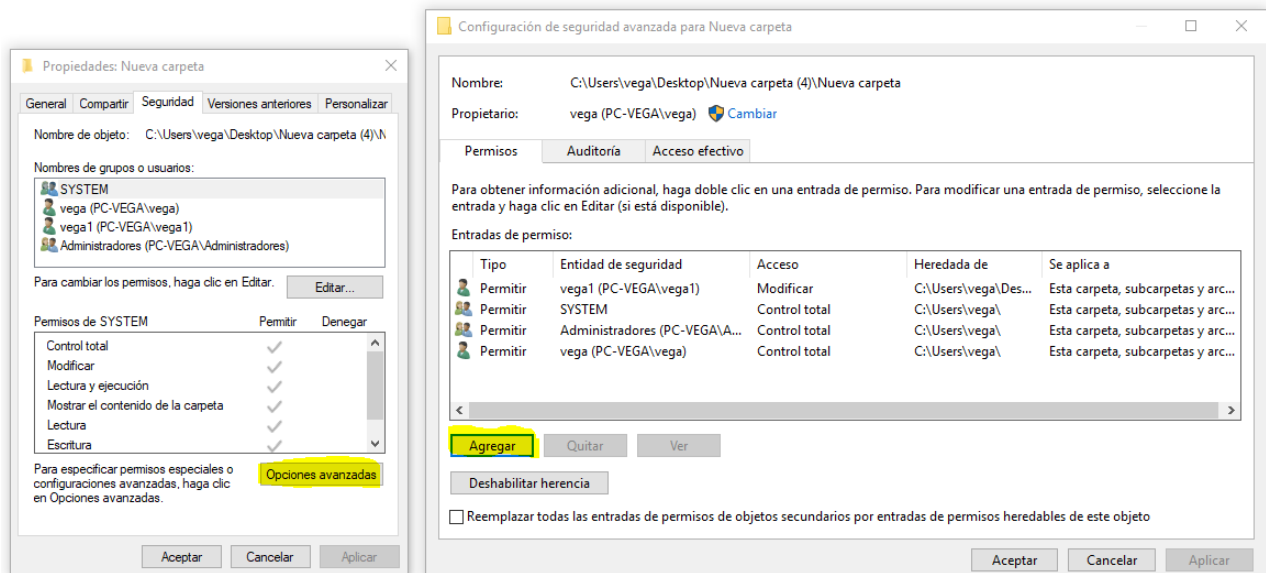
### ▪ **Tomar posesión**

El permiso **Tomar posesión** permite o impide que el usuario tome posesión del archivo o carpeta. El propietario de un archivo o carpeta puede cambiar los permisos correspondientes, cualesquiera que sean los permisos existentes que protegen el archivo o la carpeta.

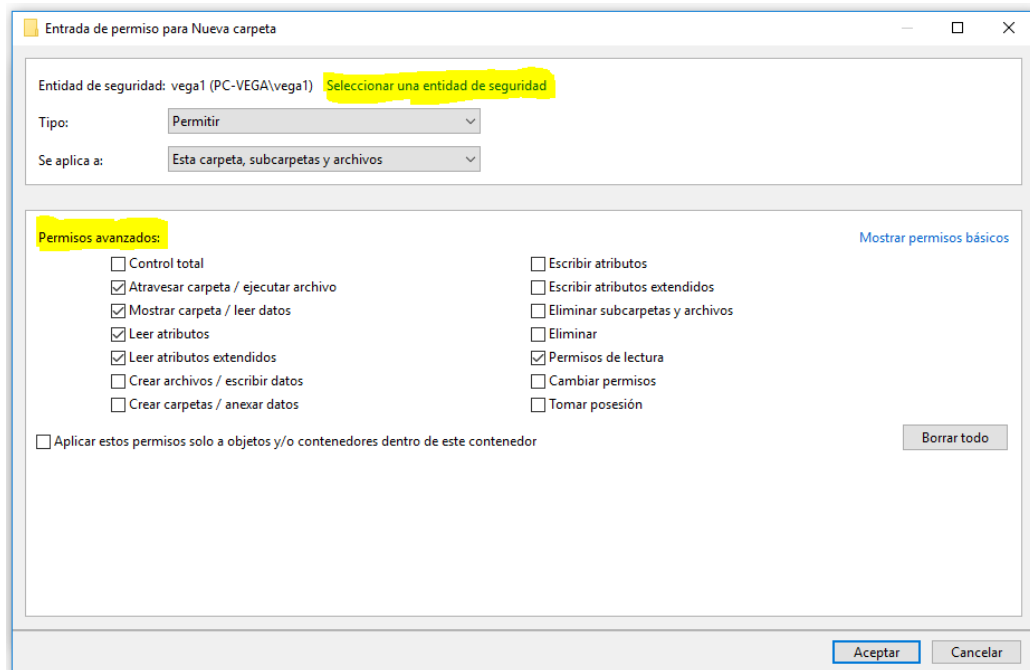
## 3.3. Configurar, ver, cambiar o quitar permisos avanzados de archivos y carpetas

Para configurar, ver, cambiar o quitar permisos especiales para archivos y carpetas:

1. Haga clic en **Inicio**, **Equipo** y busque el archivo o la carpeta para el que desea configurar permisos especiales.
2. Haga clic con el botón secundario del ratón en el archivo o carpeta, haga clic en **Propiedades** y, después, haga clic en la ficha **Seguridad**.
3. Haga clic en **Opciones avanzadas** y siga estos pasos:
  - **Seleccionar una entidad de seguridad:** usuario o grupo sobre el que se aplicarán los permisos.



- En el cuadro **Entrada de permiso**, seleccione **Permitir** o **Denegar**.
- En el cuadro **Se aplica en**, haga clic en las opciones donde quiere que se propaguen los permisos heredables.
- Para configurar la seguridad de manera que las subcarpetas y los archivos no hereden estos permisos, haga clic para desactivar la casilla de verificación **Aplicar estos permisos a objetos y/o contenedores sólo dentro de este contenedor**.



En el cuadro **Configuración de seguridad avanzada del objeto** aparecerá la entrada de permisos especiales como **Acceso “especial”**.

Entradas de permiso:

Tipo	Entidad de seguridad	Acceso	Heredada de	Se aplica a
Denegar	vega (PC-VEGA\vega)	<b>Especial</b>	Ninguno	Esta carpeta, subcarpetas y ar...
Permitir	Administradores (PC-VEGA\...	Control total	Ninguno	Esta carpeta, subcarpetas y ar...
Permitir	SYSTEM	Control total	Ninguno	Esta carpeta, subcarpetas y ar...
Permitir	Usuarios autenticados	Modificar	Ninguno	Esta carpeta, subcarpetas y ar...
Permitir	Usuarios (PC-VEGA\Usuarios)	Lectura y ejecución	Ninguno	Esta carpeta, subcarpetas y ar...

**PRECAUCIÓN:** si hace clic para activar la casilla de verificación **Reemplazar las entradas de permisos de objetos secundarios por entradas de permisos heredables de este objeto**; Incluyéndolas con las entradas indicadas aquí de forma explícita, de forma que todas las subcarpetas y los archivos tengan sus entradas de permisos, restablezca los mismos permisos que el objeto principal. Después de hacer clic en **Aplicar** o en **Aceptar** no puede deshacer esta operación si hace clic para desactivar las casillas de verificación.

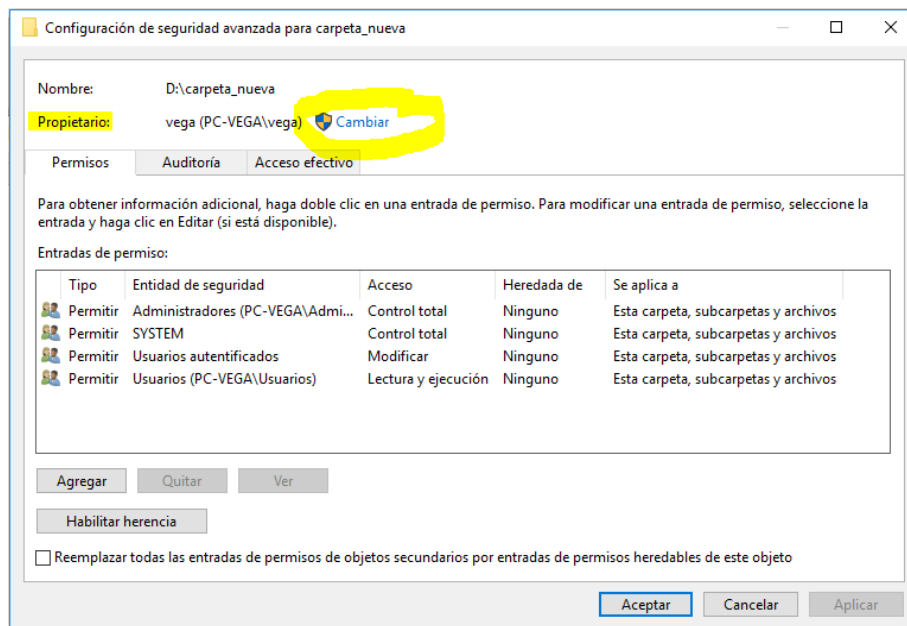
### 3.4. Tomar posesión del archivo o carpeta.

Cada archivo o carpeta situada en un volumen NTFS posee un propietario. El propietario de un recurso es, de modo predeterminado, el que ha creado ese recurso y forma parte automáticamente del grupo creador propietario.

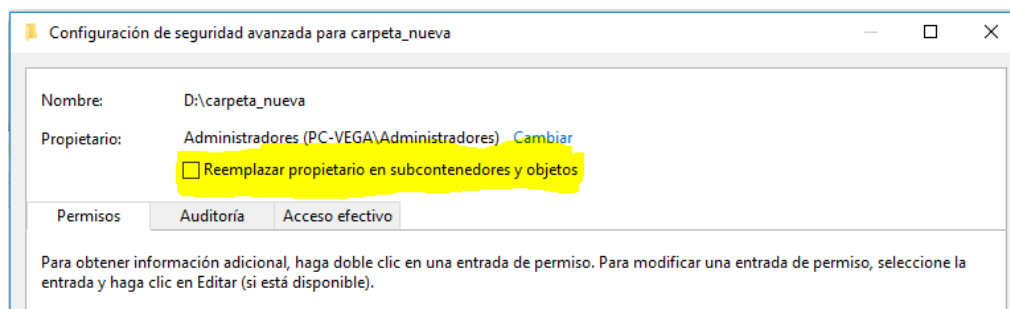
Un usuario no puede tomar posesión de un recurso si no posee el permiso especial **Tomar Posesión**. Además, sólo puede tomar posesión de un recurso y, en ningún caso hacer a otro usuario propietario de éste.

Para **tomar posesión** (una vez otorgado el permiso **TOMAR POSESIÓN** por parte del propietario a dicho usuario) debe seguir las instrucciones siguientes:

- Entrar en sesión el usuario que va a coger la propiedad.
- En la pestaña **Seguridad** del archivo o carpeta, clic en el botón **Opciones Avanzadas**.
- Pestaña **Propietario**.



Vemos quien es el propietario de la carpeta y podemos cambiarlo. Observamos que el grupo *administradores* siempre puede tomar posesión. Y que podemos forzar a cambiar el propietario a su vez en todos los objetos secundarios a partir de este, activando la siguiente casilla de verificación:



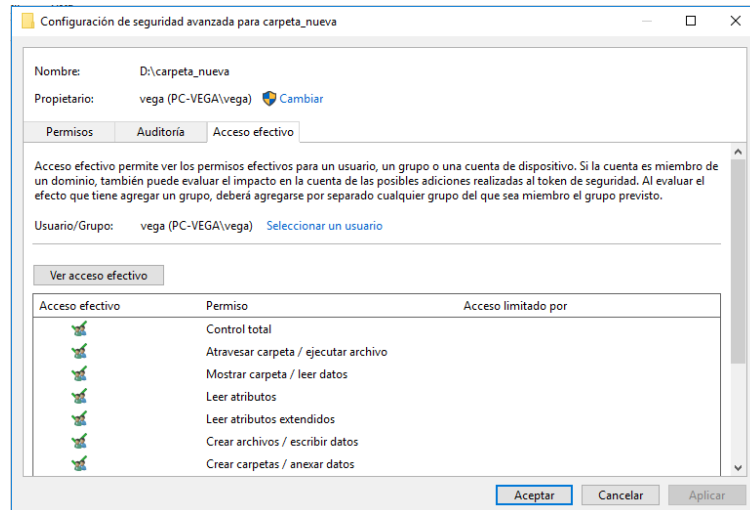
**RECUERDA:** Al usuario previamente se la ha asignado el permiso avanzado “*Tomar posesión*”

### 3.5. Ver los permisos efectivos de archivos y carpetas

Los permisos efectivos son la combinación de los permisos de los que dispone el usuario y los de todos los grupos a los que pertenece.

Para ver los permisos efectivos de archivos y carpetas:

- Busque el archivo o la carpeta para el que desee ver los permisos efectivos.
- Haga clic con el botón secundario del ratón en el archivo o en la carpeta, haga clic en **Propiedades** y, después, haga clic en la ficha **Seguridad**.
- Haga clic en **Opciones avanzadas** y, después, haga clic en la ficha **Acceso efectivo**.
- Haga clic en Seleccionar un usuario.
- Escriba el nombre del usuario o grupo sobre el que quiere revisara sus permisos efectivos y haga clic en **Aceptar**. Las casillas de verificación activadas indican los permisos efectivos del usuario o el grupo para dicho archivo o carpeta.



La ficha **Acceso efectivo** muestra información que se calcula a partir de las entradas de permisos existentes. Por tanto, la información que aparece en esa página es de sólo lectura y no permite cambiar los permisos de un usuario si activa o desactiva casillas de verificación de permisos.



## NOTAS A TENER EN CUENTA CON LOS PERMISOS

- Sólo puede configurar permisos en las unidades formateadas para utilizar el sistema de archivos NTFS.
- Para cambiar los permisos debe ser el propietario o que el propietario le permita cambiar los permisos.
- Los grupos o los usuarios a los que se concede *Control total* para una carpeta pueden eliminar archivos y subcarpetas de dicha carpeta, cualesquiera que sean los permisos que protegen a los archivos y las subcarpetas.
- Si las casillas de verificación del cuadro *Permisos para usuario grupo* están sombreadas, o si el botón *Quitar* no está disponible, el archivo o la carpeta tiene permisos heredados de la carpeta principal.
- Si hace clic para desactivar la casilla de verificación "Heredar del objeto principal las entradas de permisos relativas a los objetos secundarios. Incluirlas junto con las entradas indicadas aquí de forma explícita, el archivo o la carpeta heredará los permisos del objeto principal". Quita la herencia.
- Cuando agrega un nuevo usuario o grupo, de manera predeterminada el usuario o el grupo tiene permisos *Leer y ejecutar*, *Mostrar el contenido de la carpeta* y *Leer*.
- El grupo *Todos* recibe permisos de cada unidad NTFS Permitir *Control total* a la raíz.
- Denegar los permisos siempre tienen prioridad sobre Permitir.
- Los permisos explícitos tienen prioridad sobre permisos heredados.
- Tienen prioridad los permisos de los archivos sobre las carpetas. (Escribir la ruta).
- Los permisos son acumulativos.
- El grupo *Todos* no incluye el permiso *Inicio de sesión anónimo*.