Fuente: Bing Chat AI

Introducción a los permisos de Windows

DEPARTAMENTO DE INFORMÁTICA. UNIVERSIDAD DE OVIEDO

Seguridad de Sistemas Informáticos | 2023 – 2024 (V4.0 *"S-81 Isaac Peral"*)

Contenido

Introducción

En este documento trataremos de explicar cómo proteger los ficheros (nuestras máquinas virtuales) que, tal vez, debamos almacenar en el disco de uno de los ordenadores del laboratorio, que son compartidos por muchos estudiantes.

La mejor forma de trabajar es que cada alumno tenga su propio disco SSD USB 3.0. Es la mejor opción porque puedes crear ahí las máquinas virtuales, trabajar directamente con ellas, tanto en clase como en casa. Si este es tu caso, puedes obviar esta guía.

Pero si no puedes permitirte (o no quieres) comprar uno de estos discos, siempre puedes usar el disco D: (o el mayor que tu máquina tenga) del ordenador del laboratorio para almacenar tus máquinas virtuales. En este caso, sólo podrás trabajar en las prácticas en esa máquina concreta, y debes asegurarte de que los ficheros que dejas en esa máquina permanecerán inalterados hasta la próxima vez que vayas al laboratorio a trabajar.

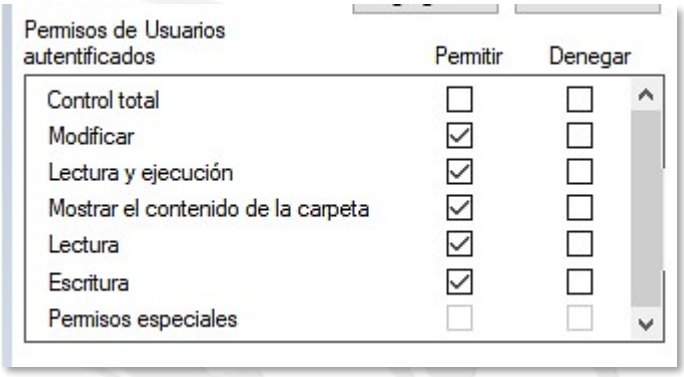
Tras una breve introducción sobre cómo funciona el sistema NTFS se incluye una guía paso a paso para hacerlo. Hay que comentar finalmente que esta guía es básicamente **para la gente que trabaje en máquinas de laboratorio** o bien en casa pero tenga dudas acerca de los permisos de su *Windows*. Si ya estás familiarizado con ellos o trabajas en casa, seguramente no te aporte gran cosa.

Visión general del Sistema NTFS

El sistema de ficheros por defecto que utiliza *Windows* se denomina NTFS. Este sistema de ficheros utiliza Listas de Control de Acceso para gestionar los permisos que un usuario (o grupo) tiene para cada fichero del disco.

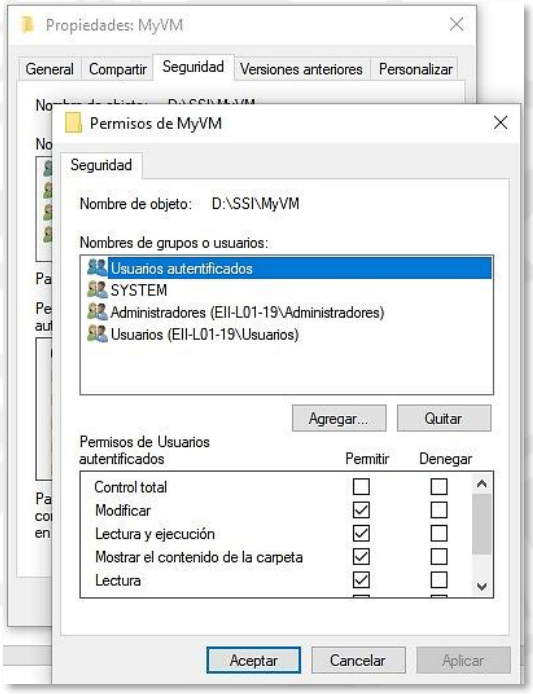
NTFS se basa en la utilización de 13 tipos diferentes de acceso, pero normalmente están agrupados en 7 tipos de acceso básicos:

- Control total.
- Modificar.
- Lectura y ejecución.
- Mostrar el contenido de la carpeta.
- Leer.
- Escribir.
- Permisos especiales.



El significado de cada permiso está bastante claro por su nombre.

Para cada usuario/grupo los permisos pueden darse (*Allow* – Permitir) o no (*Deny* – Denegar):



En este ejemplo podemos ver que los usuarios que pertenezcan a "Usuarios autentificados" pueden modificar, leer y ejecutar, Mostrar el contenido de la carpeta y leer el fichero en cuestión. Para ver los permisos de otro usuario o grupo de la lista basta con seleccionarlo en dicha lista.

Hay varias reglas que aplica el sistema operativo cuando un proceso quiere acceder a un fichero para verificar si el acceso es factible o no. Podemos simplificarlas como sigue:

- Cualquier usuario/grupo que no esté en la lista no puede acceder al fichero.

- Si se puede aplicar más de una regla (por ejemplo, un usuario que sea a la vez del grupo “administrador” y “usuario”) las reglas de Denegar tienen más prioridad que las de permitir.
- Prevalecen los permisos de ficheros sobre los de directorios.
- Prevalecen los permisos asignados sobre los no asignados.
- Prevalecen los permisos explícitos (los indicados al propio objeto) sobre los heredados.

Herencia de permisos

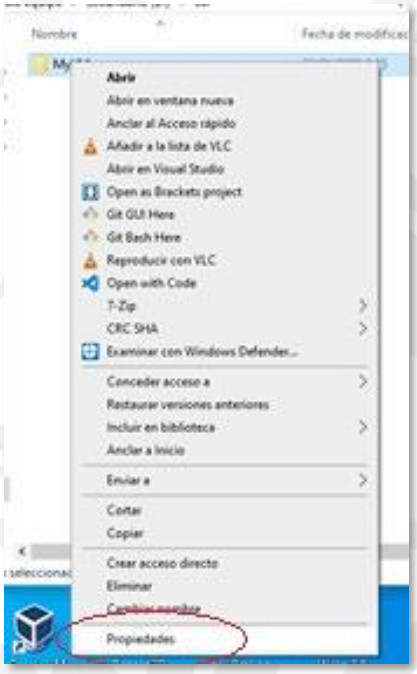
Para simplificar la asignación de permisos a ficheros y directorios, *Windows* incluye un mecanismo de herencia de permisos. Así, los permisos de un fichero o directorio están, por defecto, heredados de los de la carpeta a la que pertenece. Y no sólo están heredados, sino que están ligados a ellos, de manera que si se cambian los permisos de una carpeta también se cambian los de los objetos que contiene. No se pueden cambiar los permisos de un objeto si la herencia está habilitada para él.

Por lo tanto, si queremos cambiar los permisos de un fichero o carpeta, lo primero que debemos hacer es deshabilitar la herencia para él.

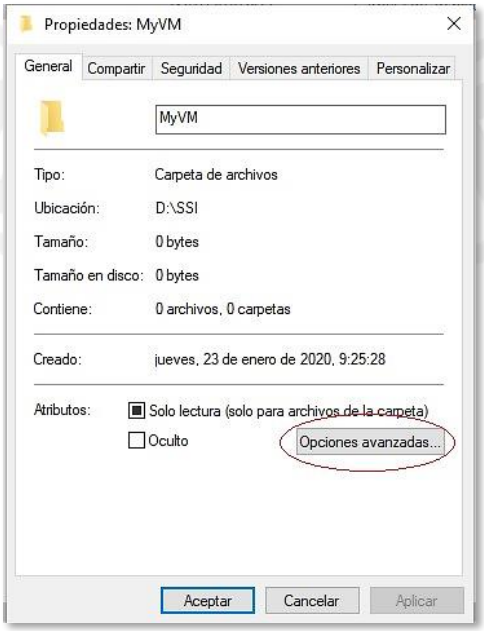
Protección de nuestras máquinas virtuales

La estructura de directorios que vamos a utilizar para almacenar nuestras máquinas virtuales en el disco local será la siguiente:

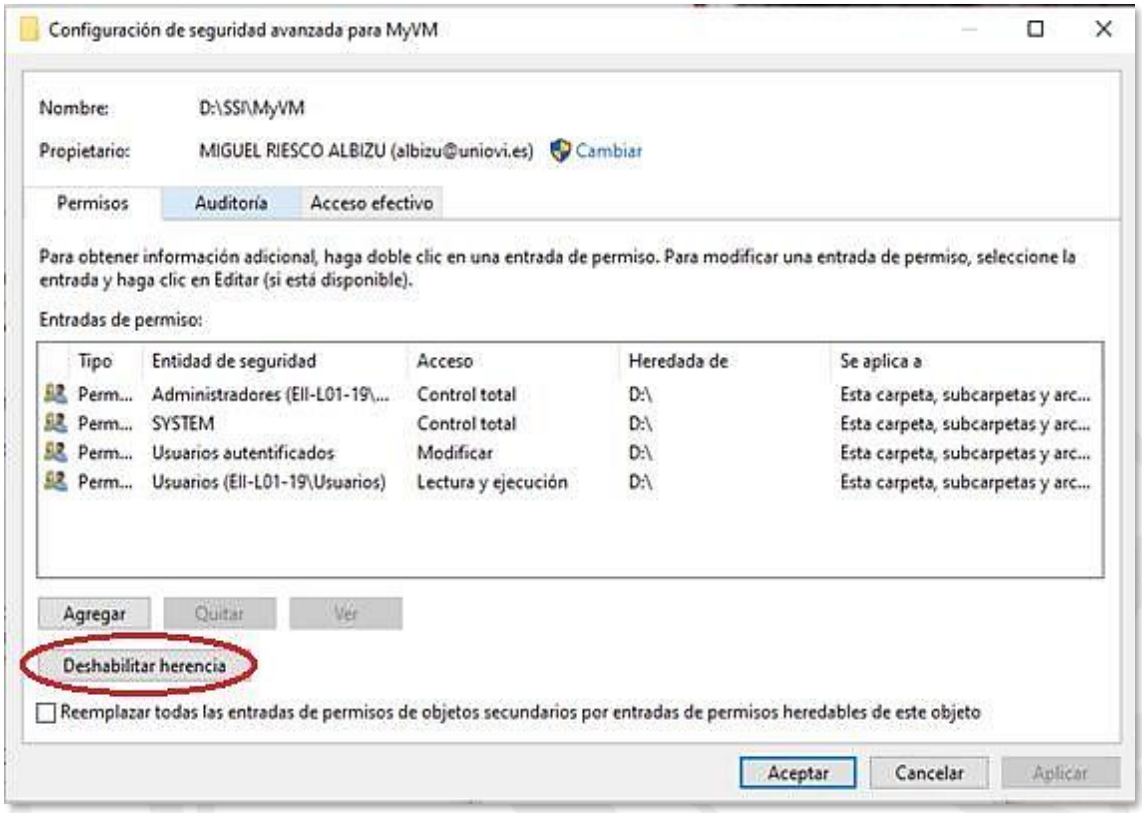
- En el disco D: tiene que haber un directorio denominado SSI. Si no está, créalo.
- Crea un directorio dentro de SSI con tu UO como nombre. Este será el lugar donde almacenarás tus máquinas virtuales, por lo que es el directorio que vamos a proteger.
- Para proteger este directorio (el directorio **UOxxxx**) vamos a cambiar sus propiedades. Tras pulsar el botón derecho sobre el directorio, elegimos "Propiedades" en el desplegable:



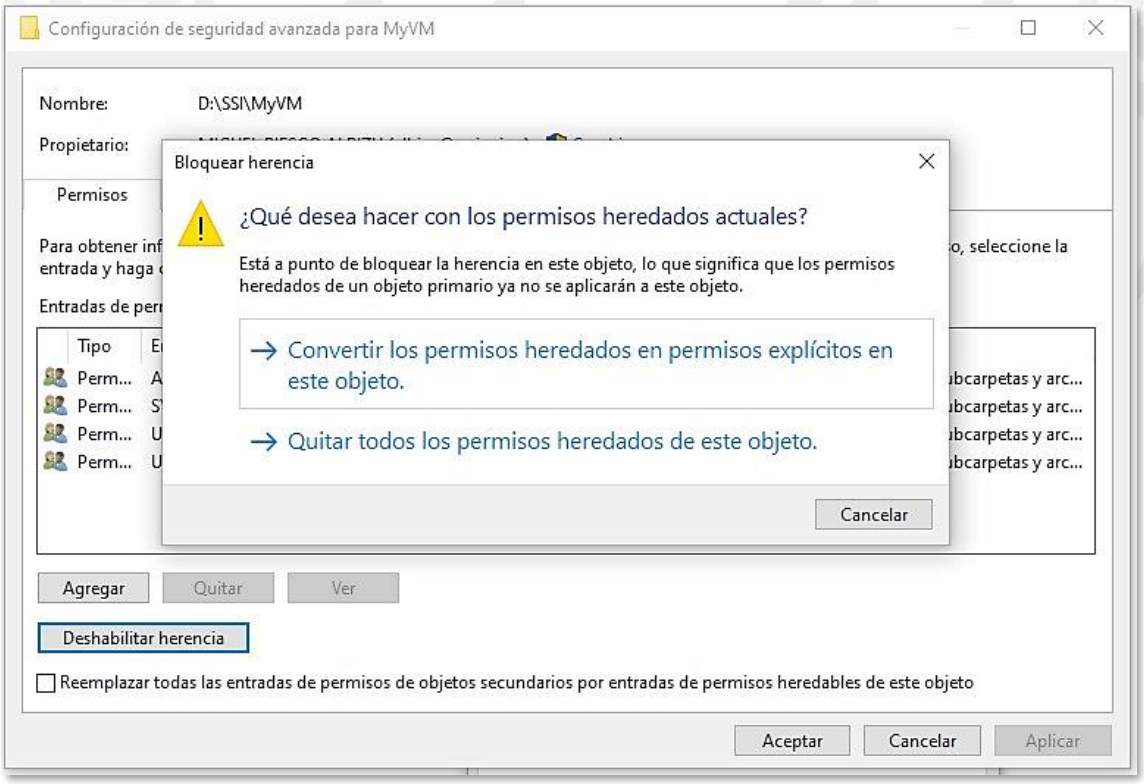
- El cuadro de propiedades aparecerá. Como lo que necesitamos hacer antes de nada es deshabilitar la herencia, debemos acceder a "Opciones avanzadas":



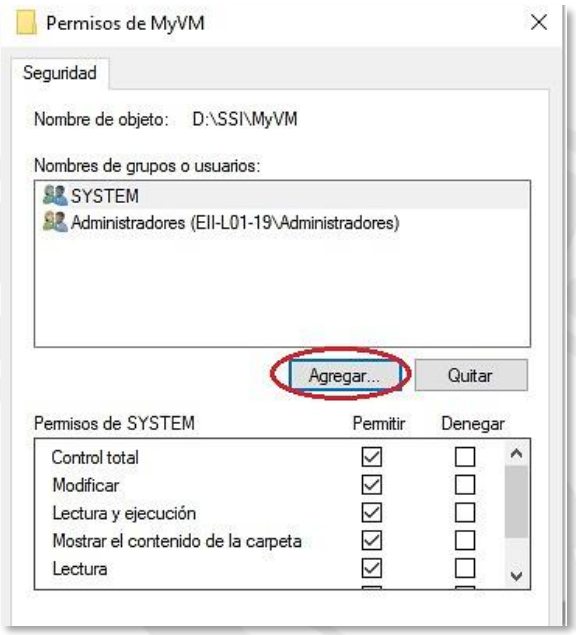
- En esta ventana hay varias opciones. Nos interesa "***Deshabilitar herencia***":



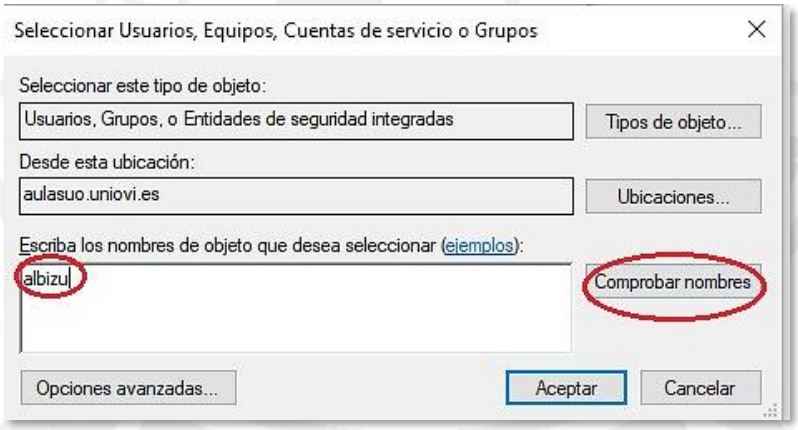
- Ahora aparecen dos opciones: "***Convertir los permisos heredados en permisos explícitos en este objeto***", que dejará los mismos permisos que tiene pero haciéndolos explícitos, o "***Quitar todos los permisos heredados***". Los dos son posibles, pero casi mejor elegimos la primera opción.



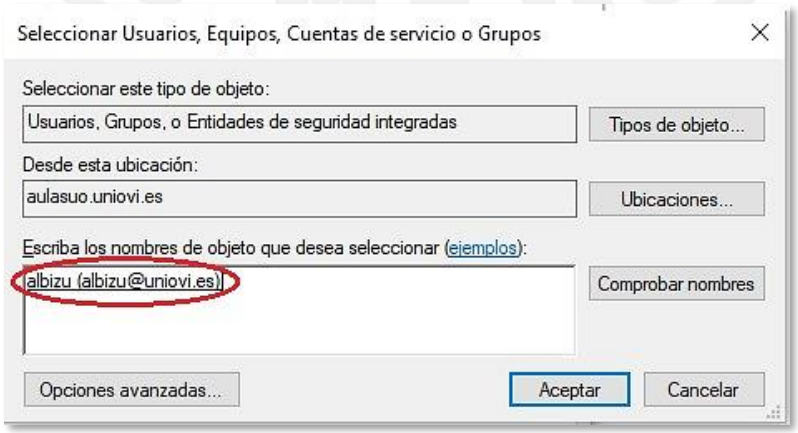
- Tras aceptar en la ventana anterior, ya podemos evitar que otros usuarios accedan a nuestro directorio. Para hacerlo, eliminaremos los grupos "***Usuarios autenticados***" y "*Usuarios*" de la lista de usuarios y grupos que tienen algún permiso sobre el fichero. Para ello, sólo tenemos que seleccionar uno de esos grupos y pulsar "*Quitar*"
- El paso final será garantizar que nuestro propio usuario tenga acceso a la carpeta. Para ello, pulsando Agregar, añadiremos un nuevo elemento a la ACL. Primero agregamos el usuario:



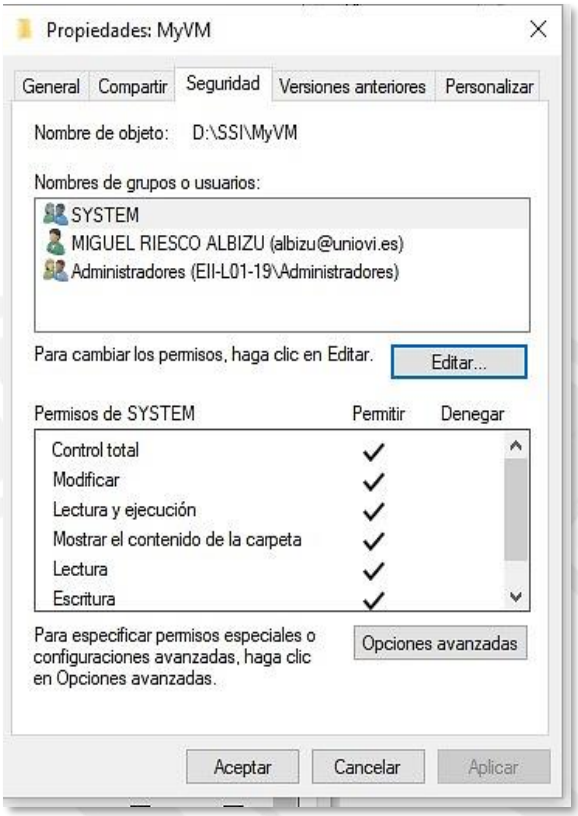
- Esto nos llevará a la siguiente ventana, donde introduciremos nuestro identificador de usuario (UO):



- Tras presionar "Comprobar nombres", si el usuario existe el sistema completará el nombre:



- Tras presionar "*Aceptar*", asignaremos el permiso de "***Acceso Total***" tras presionar "*Editar*" en la ventana siguiente. El resultado final debe ser similar al siguiente:



Y ya está. Esto debería ser suficiente para permitirnos a nosotros (y sólo a nosotros) trabajar con esa carpeta. Los usuarios *System* y *Administrators* también pueden acceder, pero estos pueden hacerlo en cualquier caso.