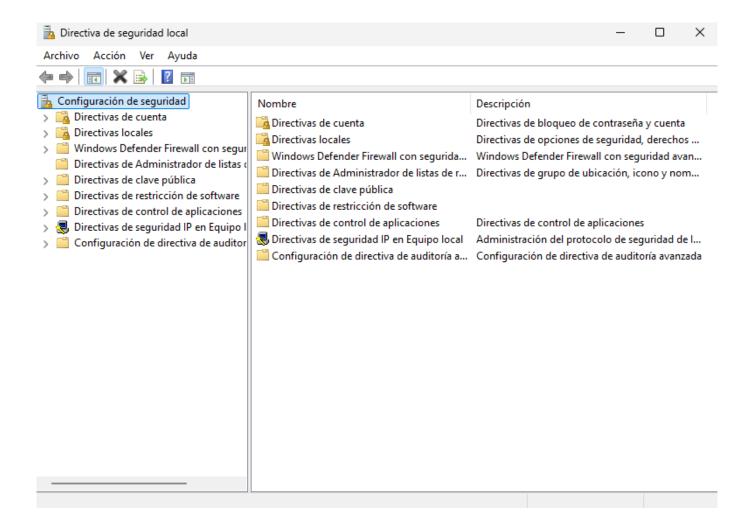
[FORT] Práctica 10: NTFS y APPLOCKER

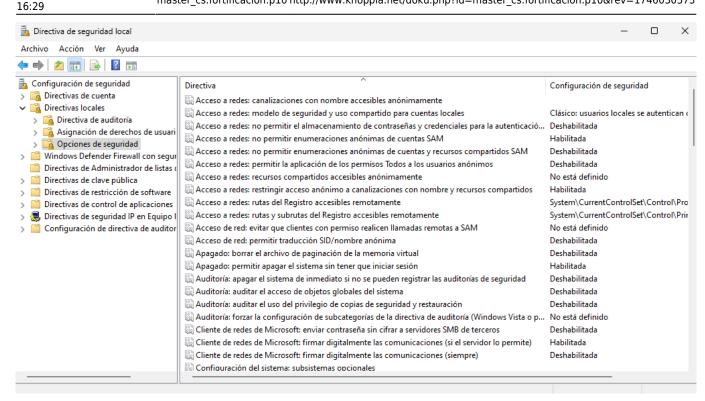
1. ¿Es posible customizar la seguridad de UAC de una manera más precisa?

Si, se puede customizar con mayor precisión mediante el uso de Directivas de Seguridad Local (secpol.msc):

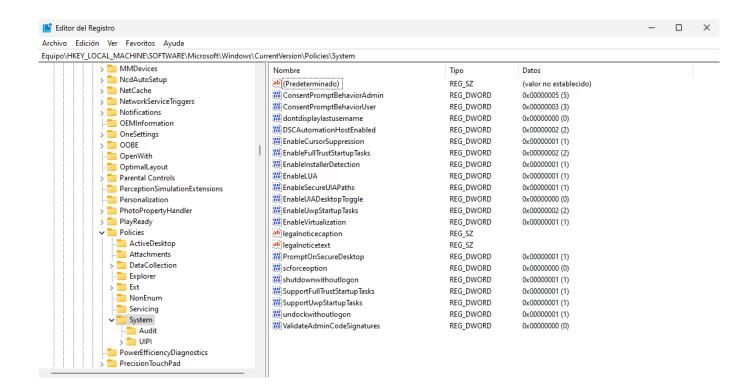


Con estas directivas se pueden realizar ajustes en las políticas como las de opciones de seguridad:

Last update: 2025/04/30



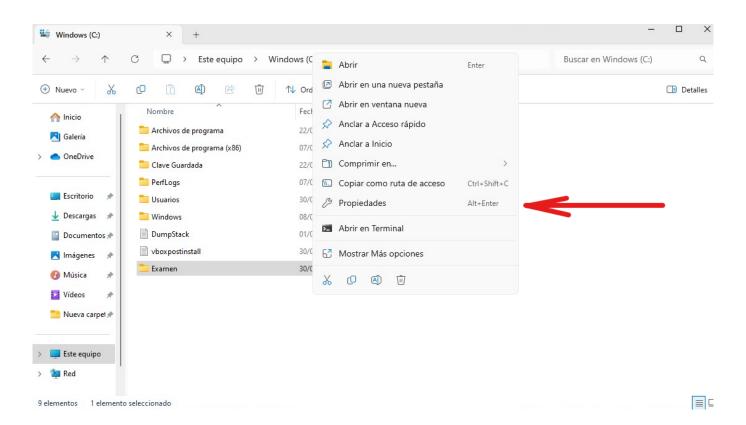
También se puede utilizar el registro (regedit) en "HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" para customizar algunos parámetros de UAC:



Sobre una carpeta "Examen" creada en "C:\" se van a realizar las siguientes configuraciones de UAC:

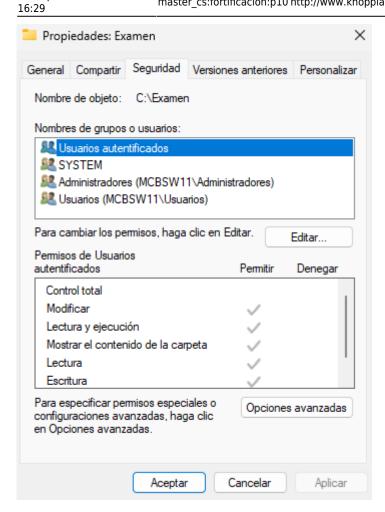
a) LECTURA: El usuario2 puede leer contenido pero no eliminar o crear carpetas/archivos

Para realizar esta configuración primero hay que dirigirse a las propiedades de la carpeta Examen:

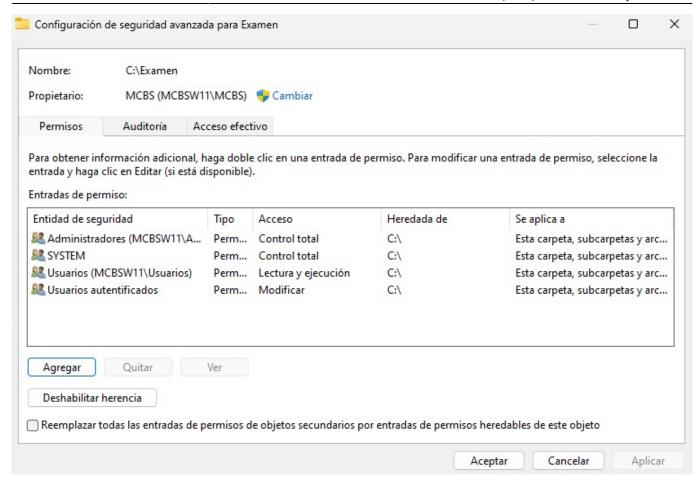


En la ventana que saldrá hay que dirigirse a la pestaña de seguridad:

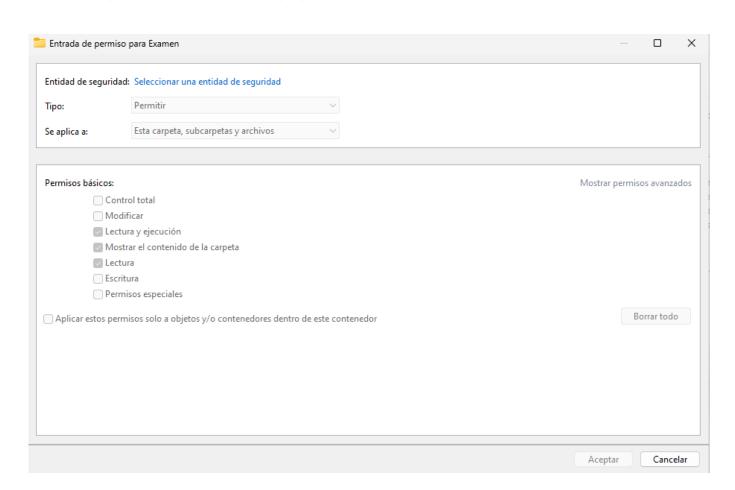
Last update: 2025/04/30



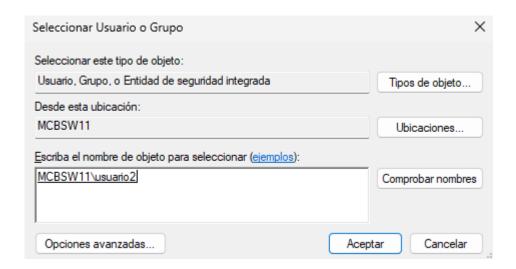
En dicha pestaña se presiona sobre el botón "Opciones Avanzadas" para que se muestre la siguiente ventana:



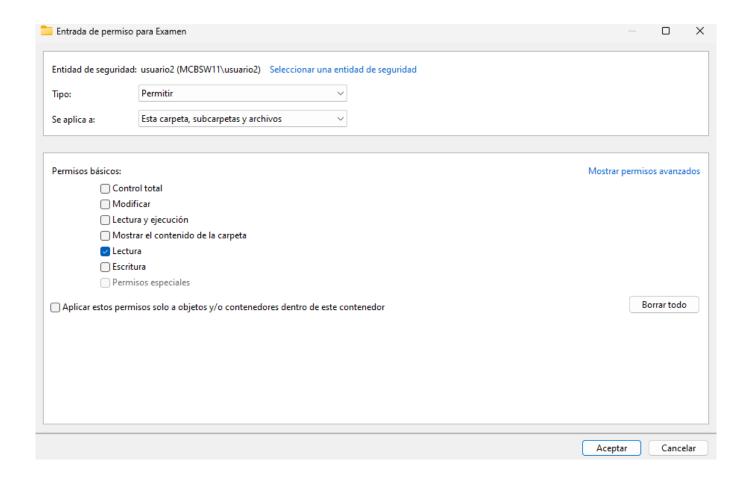
Tras eso se presiona en el botón de agregar:



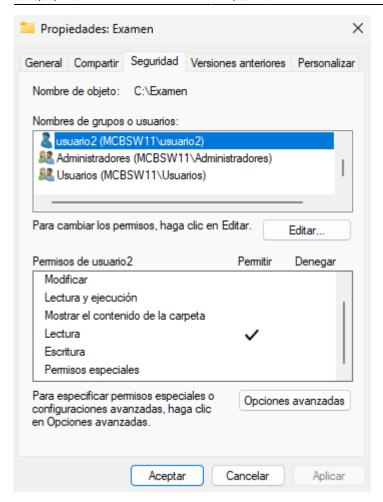
A continuación se presiona en el texto donde pone "Seleccionar una Entidad de Seguridad", en la ventana que se abre se introduce el nombre de usuario2, y se presiona en comprobar nombres, tras eso debería de aparecer el nombre del equipo seguido del de Usuario2 separados por una barra:



Tras eso se vuelve a la ventana anterior, donde ahora se pueden seleccionar los permisos, en este caso como el usuario solo puede realizar lectura, se retiran todos los permisos salvo el delectura:



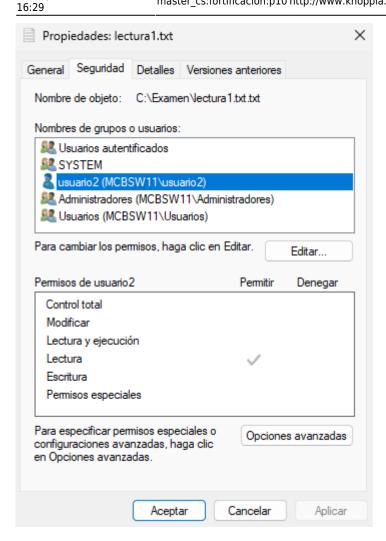
Finalmente se aplican los cambios y usuario2 quedará con los permisos establecidos:



b) SOLO LECTURA: El usuario 2 Solo puede leer el contenido de la carpeta y del archivo lectura1.txt

Para aplicar esta configuración se siguen los pasos del anterior apartado y tras eso se procede a ir a las propiedades del archivo lectura1.txt, a la pestaña de seguridad:

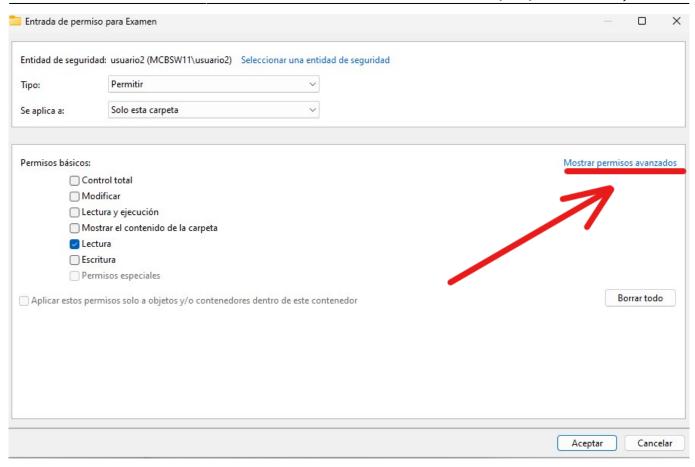
Last update: 2025/04/30



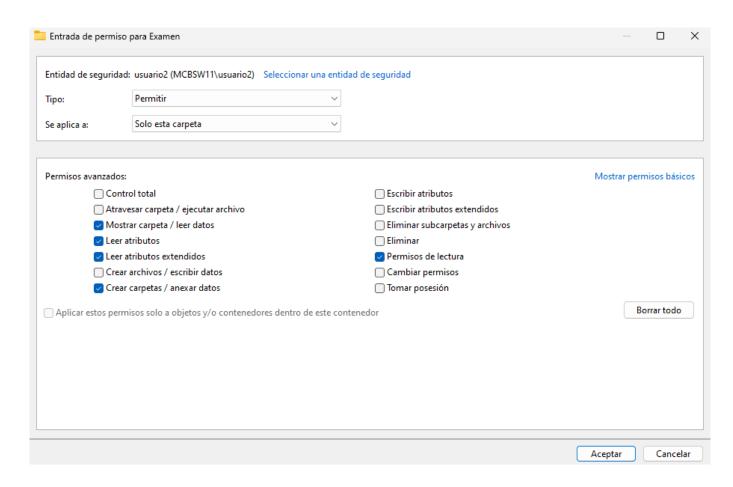
Se selecciona el usuario2 y se establece el permiso de lectura desmarcando los demás.

c) LECTURA + AÑADIR: El usuario2 solo puede leer el contenido de la carpeta y del archivo añadir.txt. Puede crear carpetas y dentro de estas puede crear archivos.

Se siguen los pasos de los anteriores apartados y tras eso se procede a modificar los permisos de la carpeta Examenes comenzando por cambiar los permisos de usuario2 presionando en mostrar permisos avanzados:

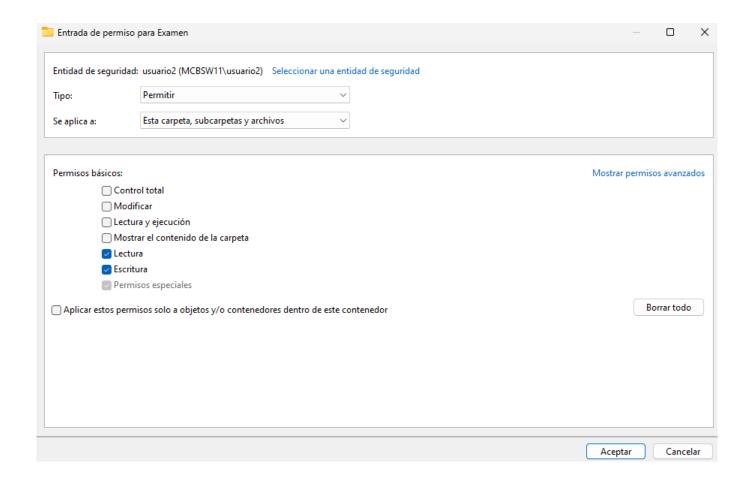


En "Se Aplica A" seleccionamos "Esta carpeta" y se procede a habilitar el permiso "Crear Carpetas / Anexar Datos":



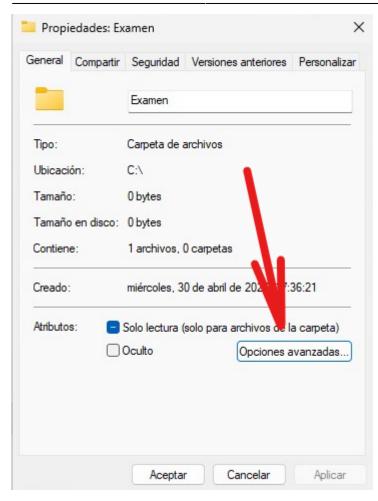
d) ACCESO TOTAl: El usuario 2 tiene el control total sobre la carpeta y componentes

Para dar control total sobre la carpeta y sus componentes a Usuario 2 se selecciona el permiso control total:

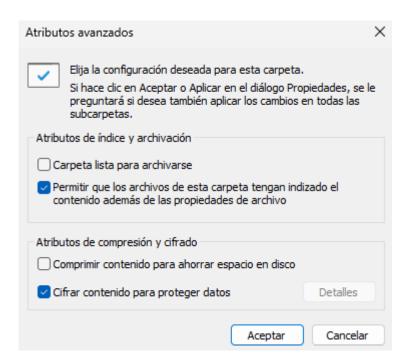


e) CIFRADO: Solo pueden acceder al contenido de un archivo cifrado los propietarios y los agentes de recuperación por defecto

Para cifrar la carpeta, en propiedades, se presiona en "Opciones Avanzadas":



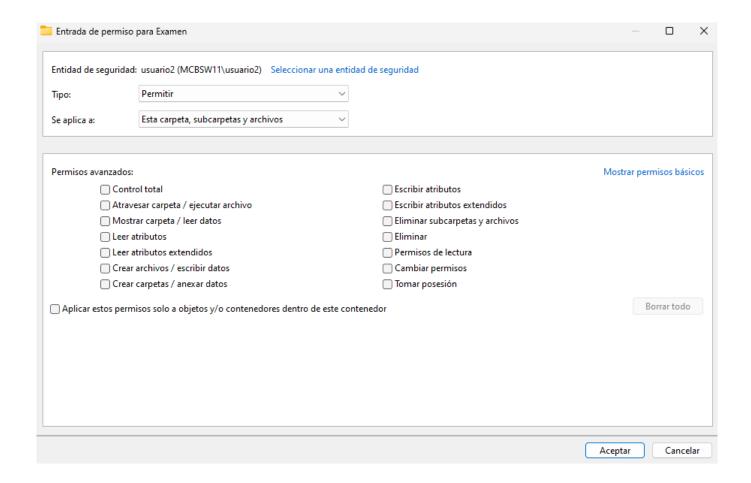
Aparecerá una ventana en la que se debe marca la casilla de "Cifrar contenido para proteger datos":



Tras eso se presiona en aceptar y aplicar para realizar el cifrado, en este caso se va a cifrar tanto la carpeta como archivos y subcarpetas.

f) PROHIBIDO: El usuario2 no tiene acceso a esta carpeta, tampoco de lectura

Para bloquear completamente el acceso y lectura de una carpeta a usuario2 se le retiran todos los permisos:



2. AppLocker

- a) ¿Que dos métodos tenemos de configuración de AppLocker? ¿Cual consideras que es la mejor opción?
- b) ¿Por qué es necesario crear las reglas automáticamente para que funcione AppLocker?
- c) Instala Notepad++ y bloquea la aplicación ¿Que opciones te muestra AppLocker para identificar la aplicación? ¿Cual sería la mejor opción?
- d) ¿Que servicios es necesario modificar para que funcione AppLocker?¿Que cambios tenemos que realizar?

e) AppLocker se configura a través de directivas de grupo ¿Que comando se debe usar para aplicar los cambios realizados y que el sistema AppLocker funcione sin reiniciar el equipo?

From:

http://www.knoppia.net/ - Knoppia

Permanent link:

http://www.knoppia.net/doku.php?id=master_cs:fortificacion:p10&rev=1746030573

