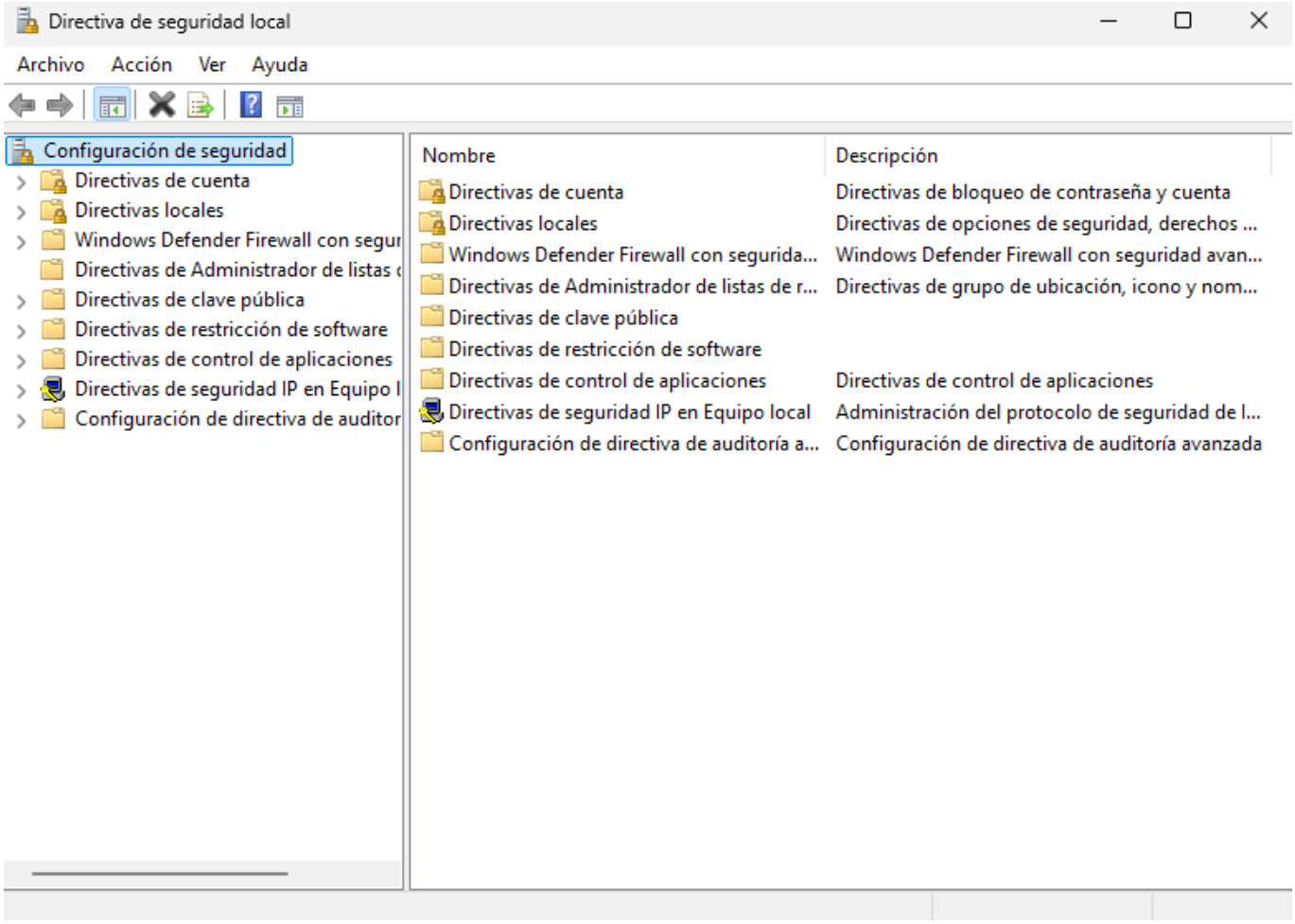
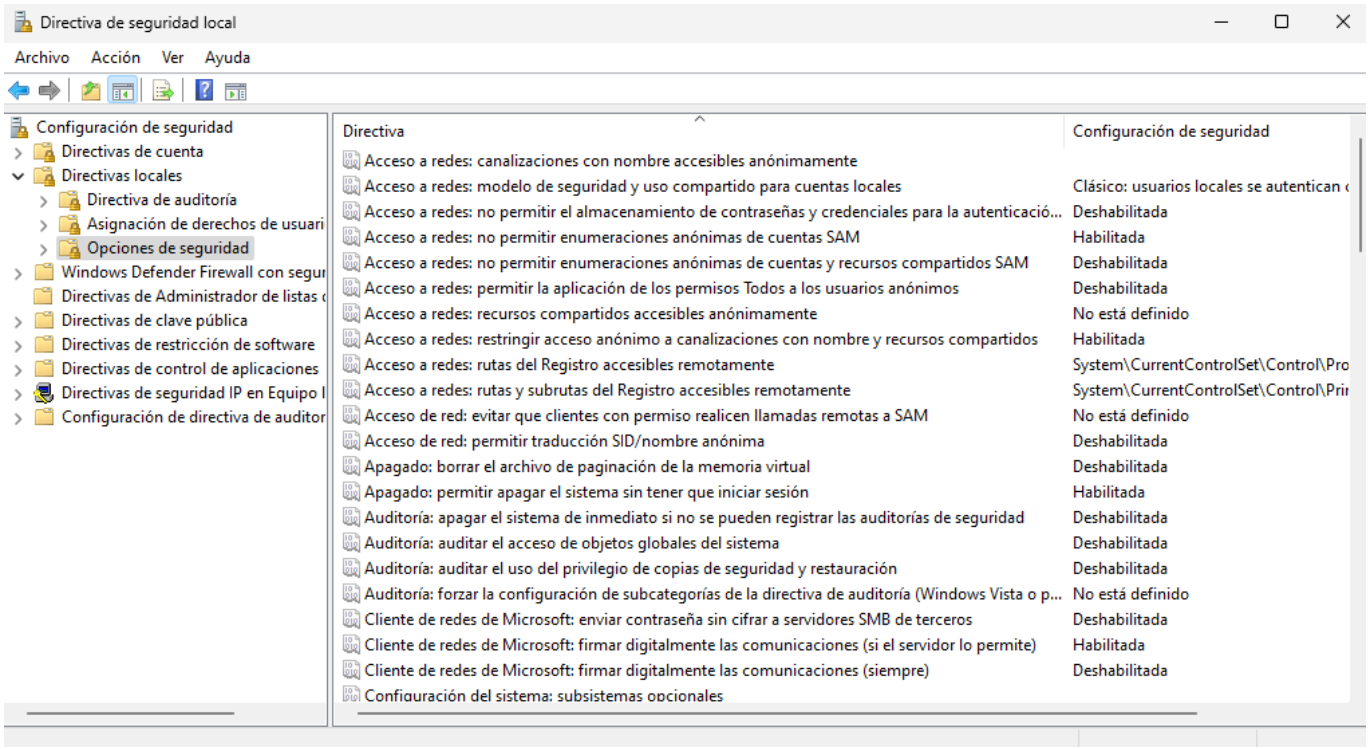
[FORT] Práctica 10: NTFS y APPLOCKER

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

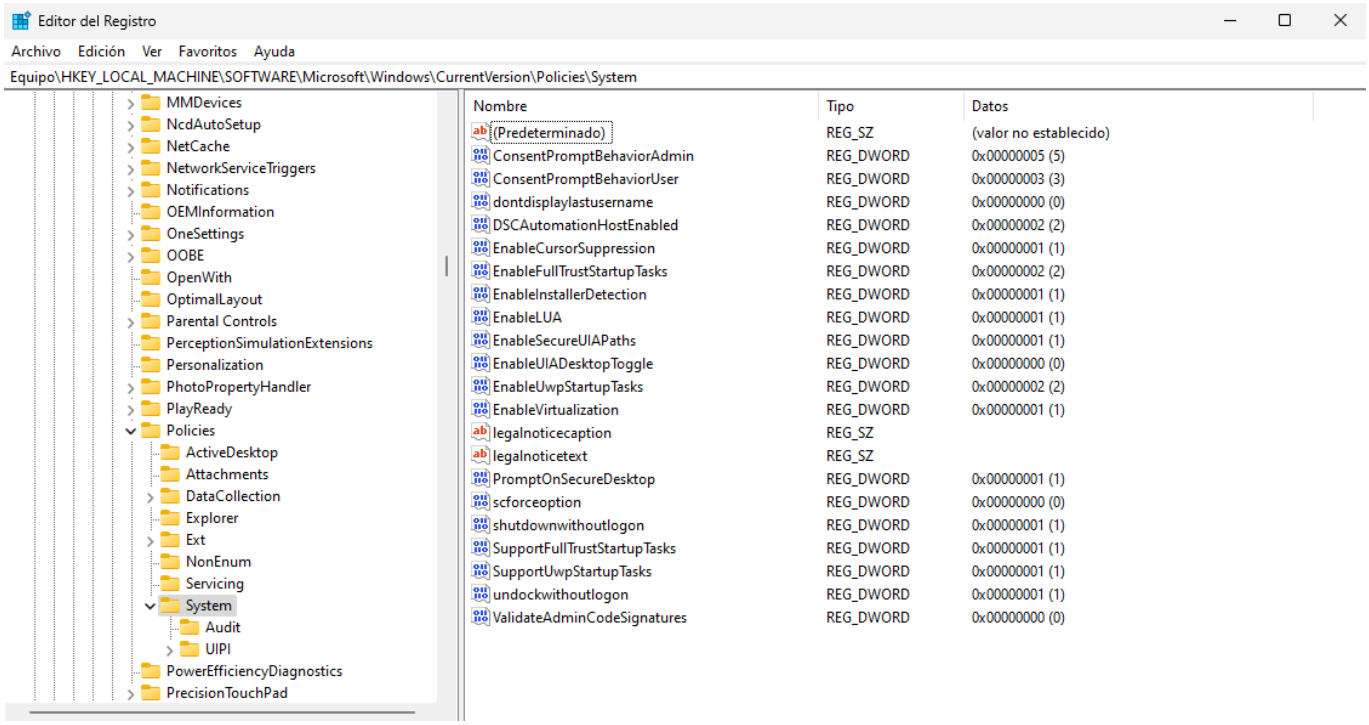
Si, se puede customizar con mayor precisión mediante el uso de Directivas de Seguridad Local (secpol.msc):



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



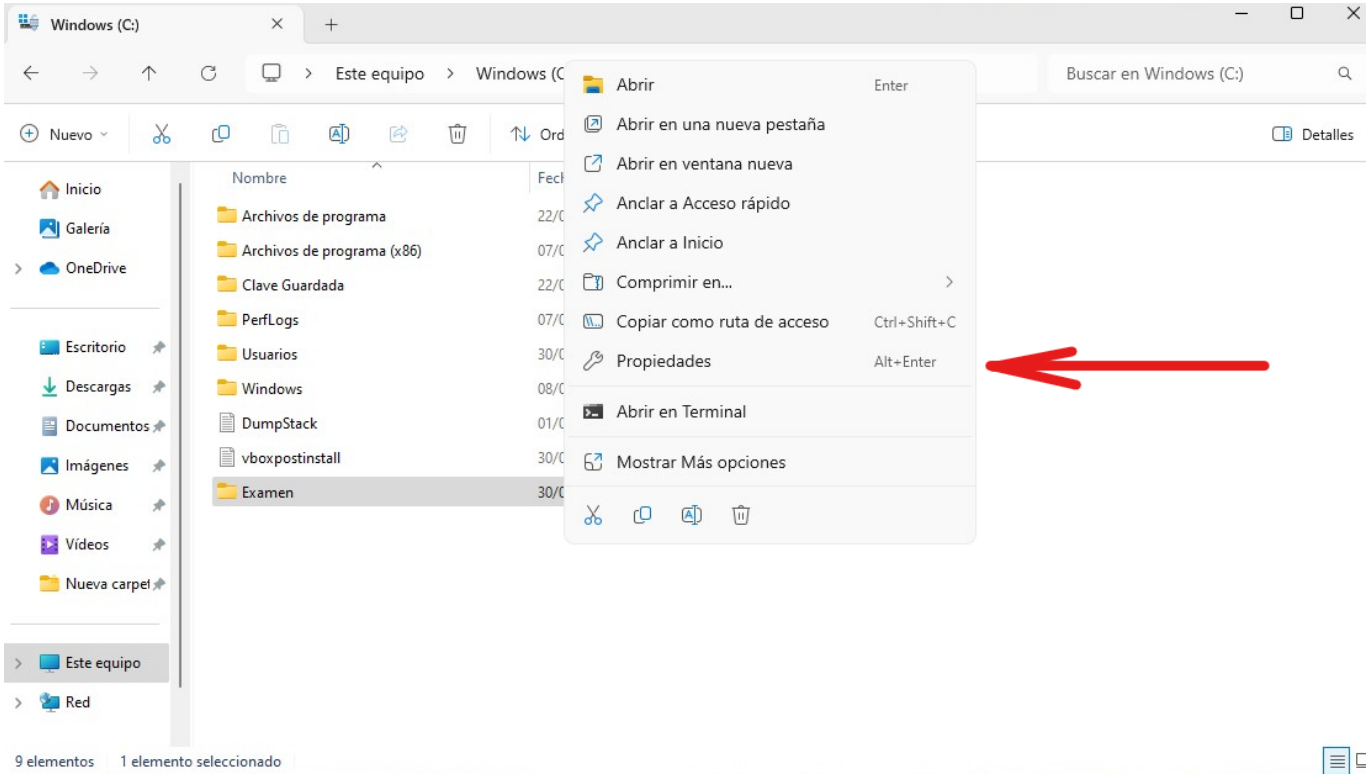
También se puede utilizar el registro (regedit) en “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System” para customizar algunos parámetros de UAC:



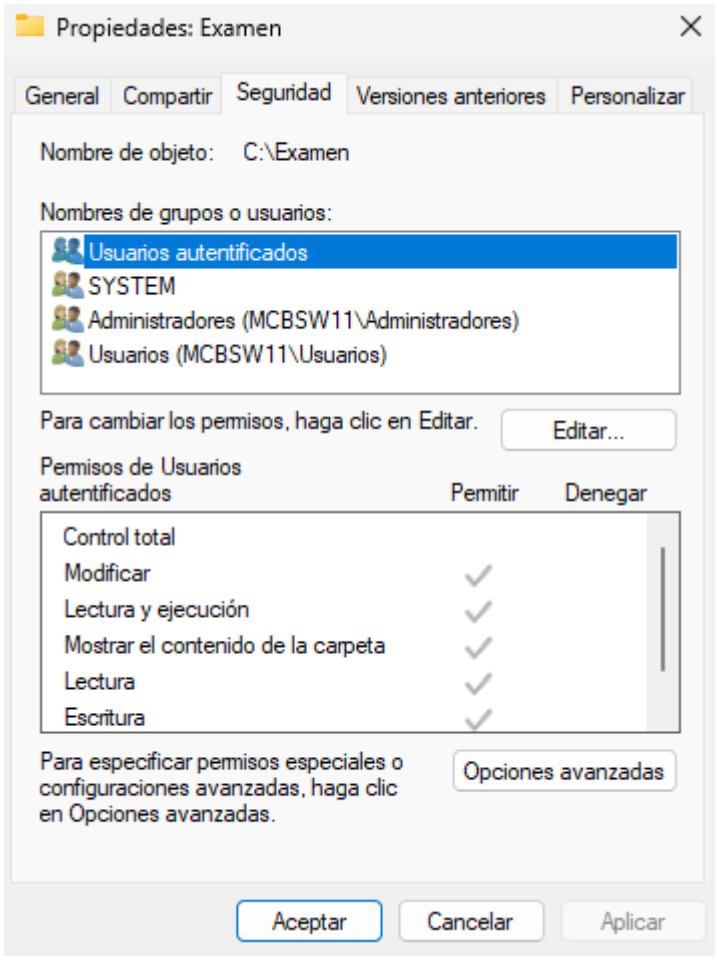
Sobre una carpeta “Examen” creada en “C:\” se van a realizar las siguientes configuraciones de UAC:

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

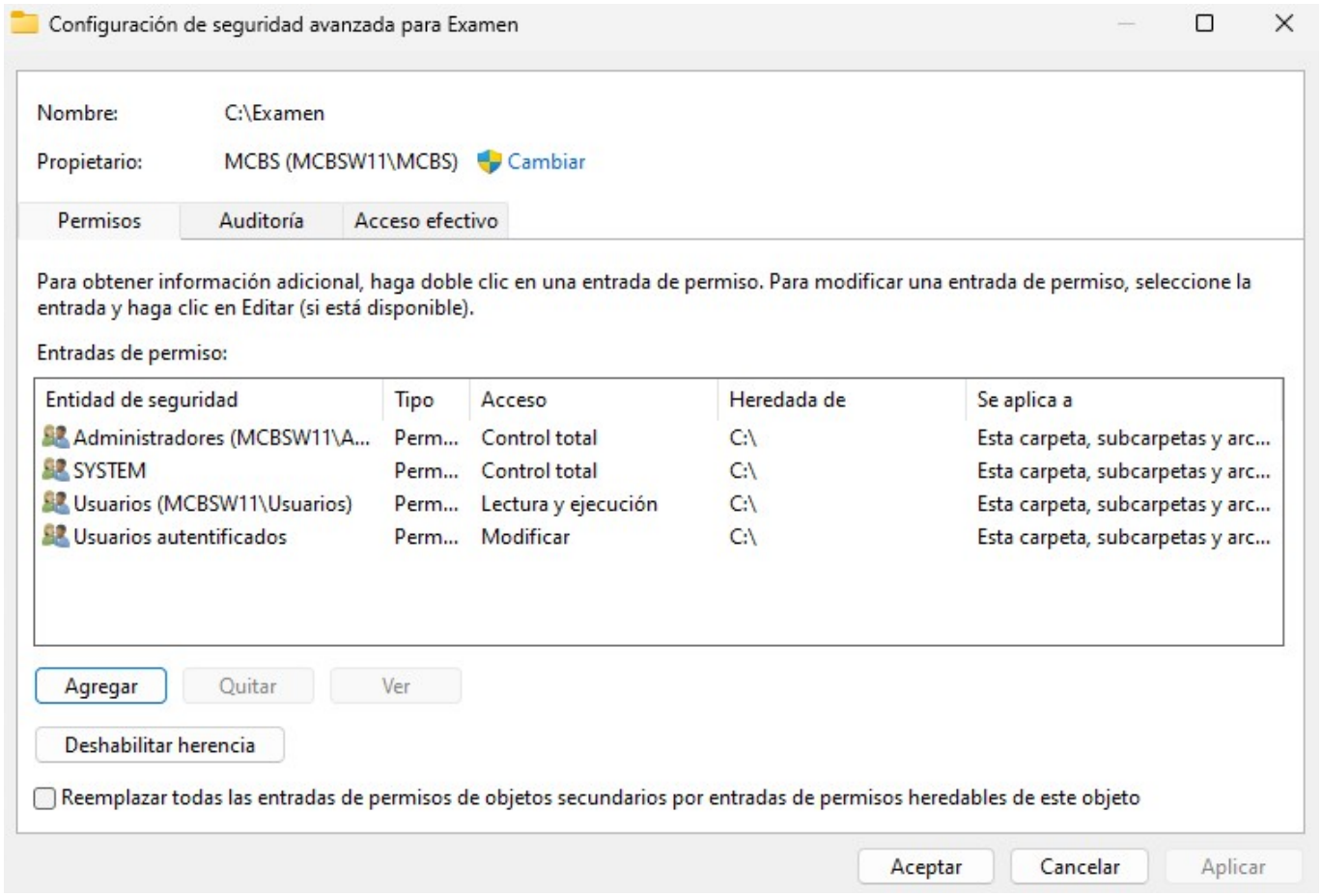
Para realizar esta configuración primero hay que dirigirse a las propiedades de la carpeta Examen:



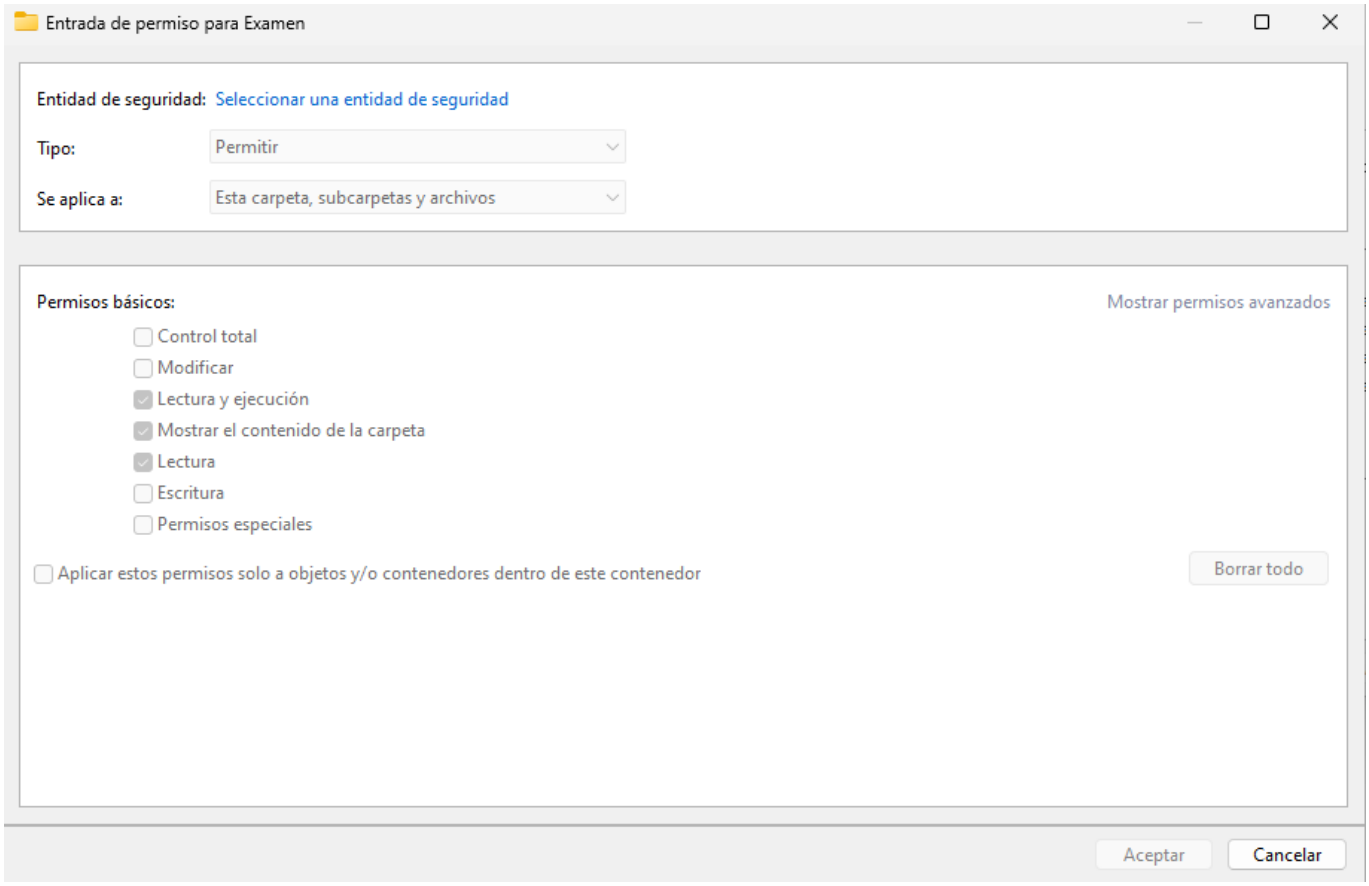
En la ventana que saldrá hay que dirigirse a la pestaña de seguridad:



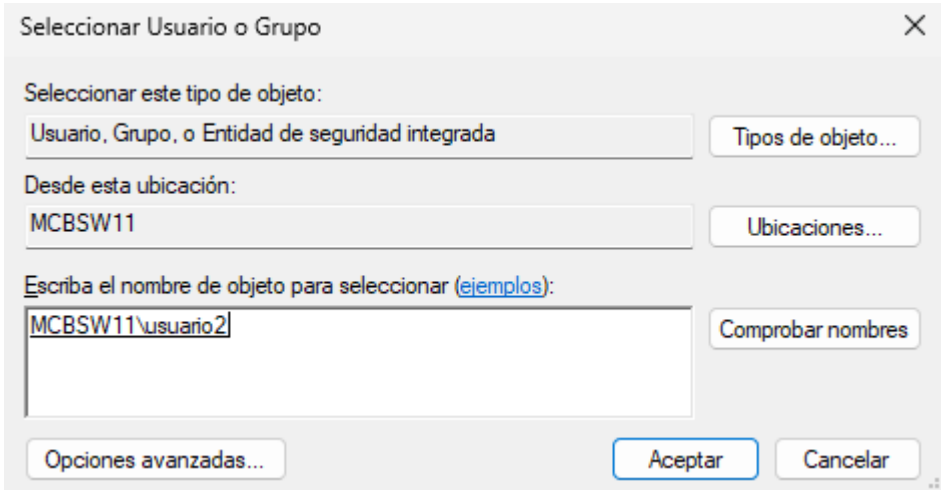
En dicha pestaña se presiona sobre el botón “Opciones Avanzadas” para que se muestre la siguiente ventana:



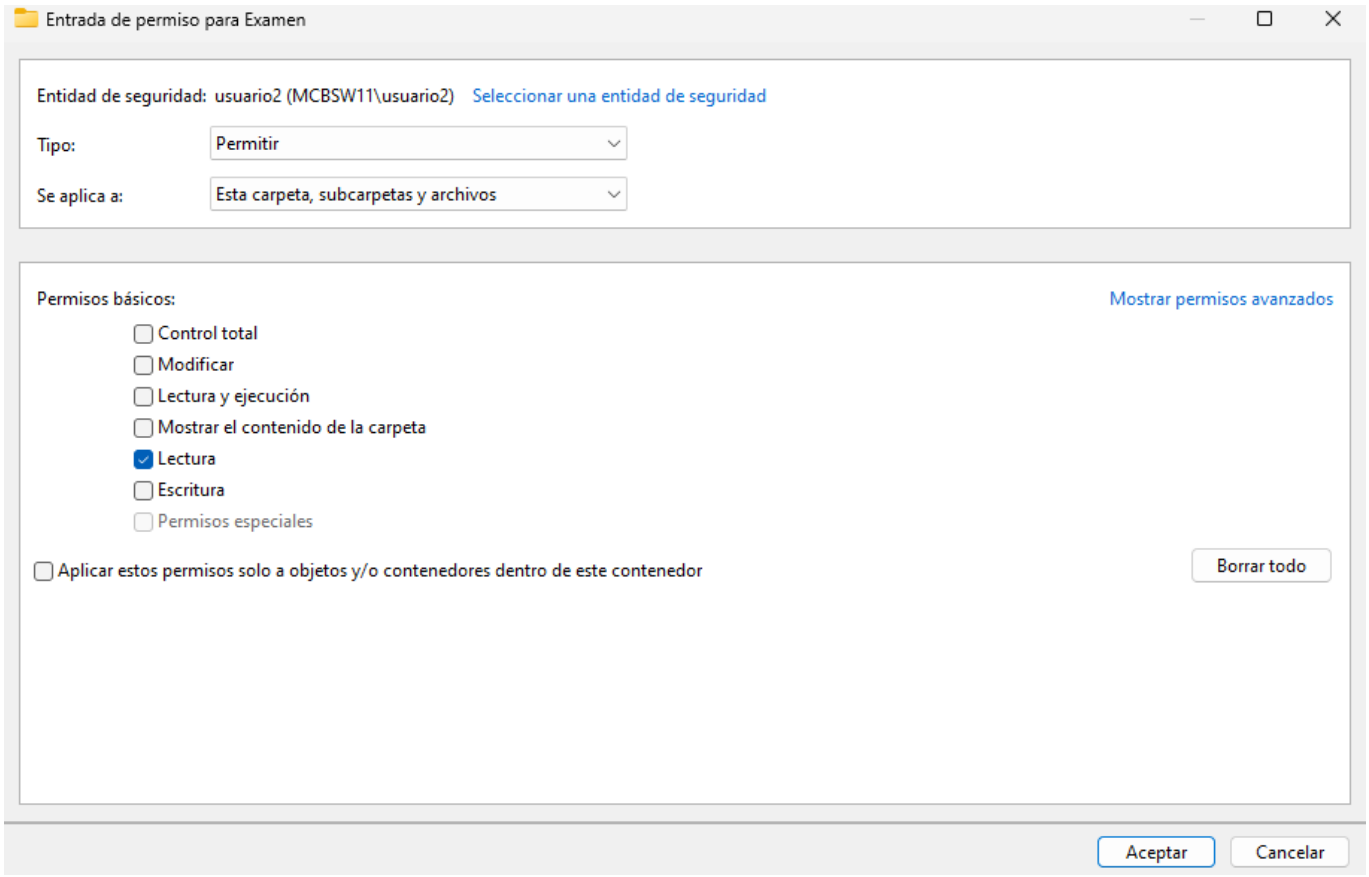
Tras eso se presiona en el botón de agregar:



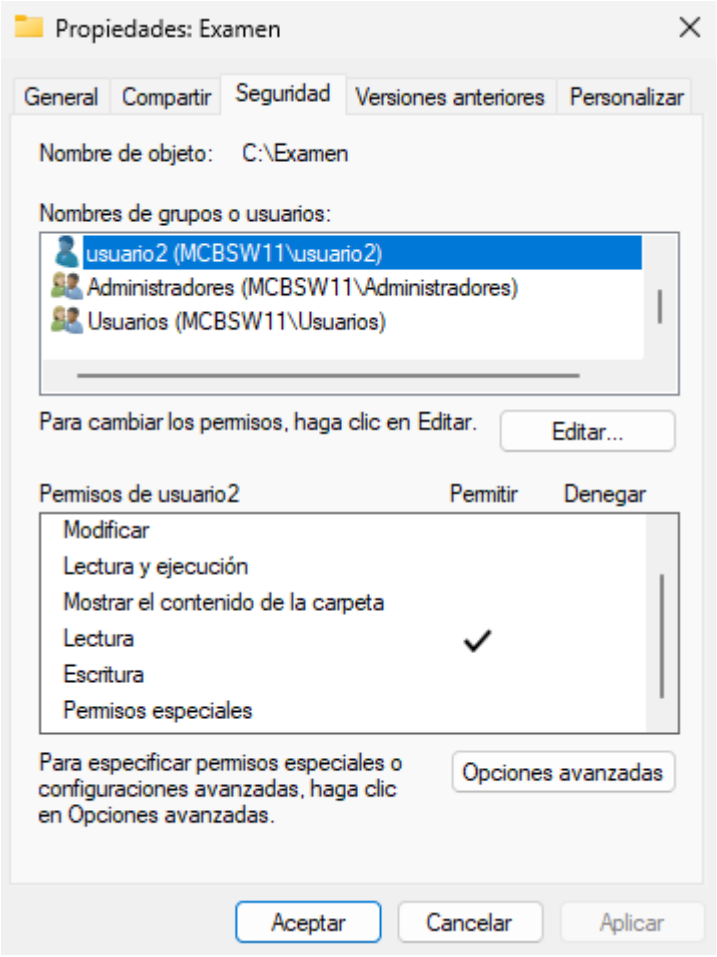
A continuación se presiona en el texto donde pone “Seleccionar una Entidad de Seguridad”, en la ventana que se abre se introduce el nombre de usuario2, y se presiona en comprobar nombres, tras eso debería de aparecer el nombre del equipo seguido del de Usuario2 separados por una barra:



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:

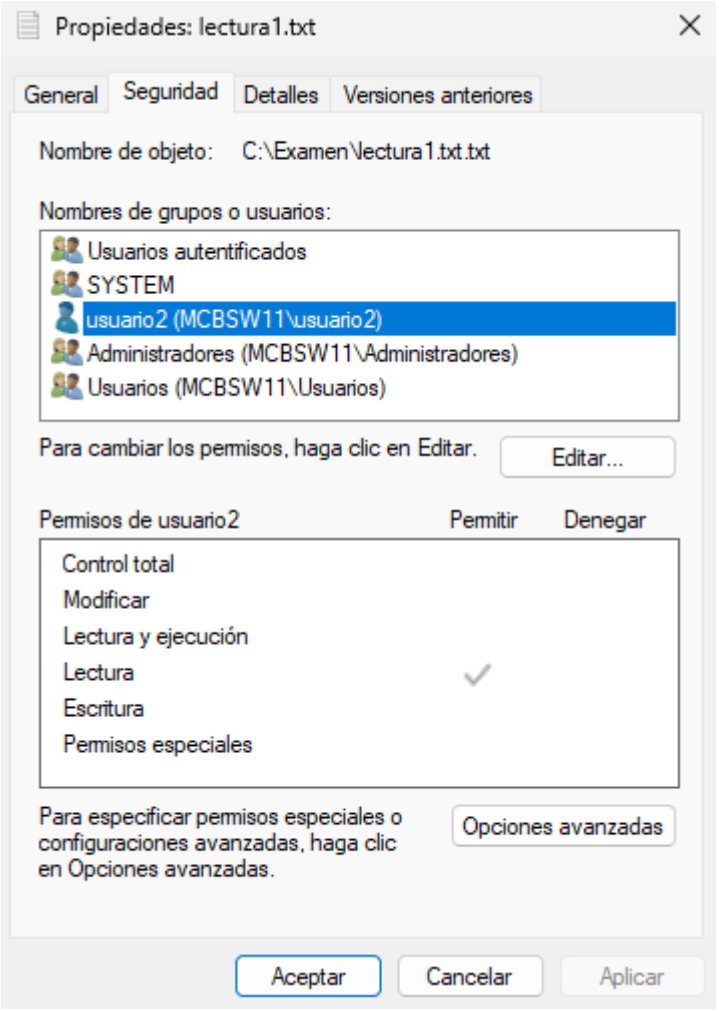


Finalmente se aplican los cambios y usuario2 quedará con los permisos establecidos:



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

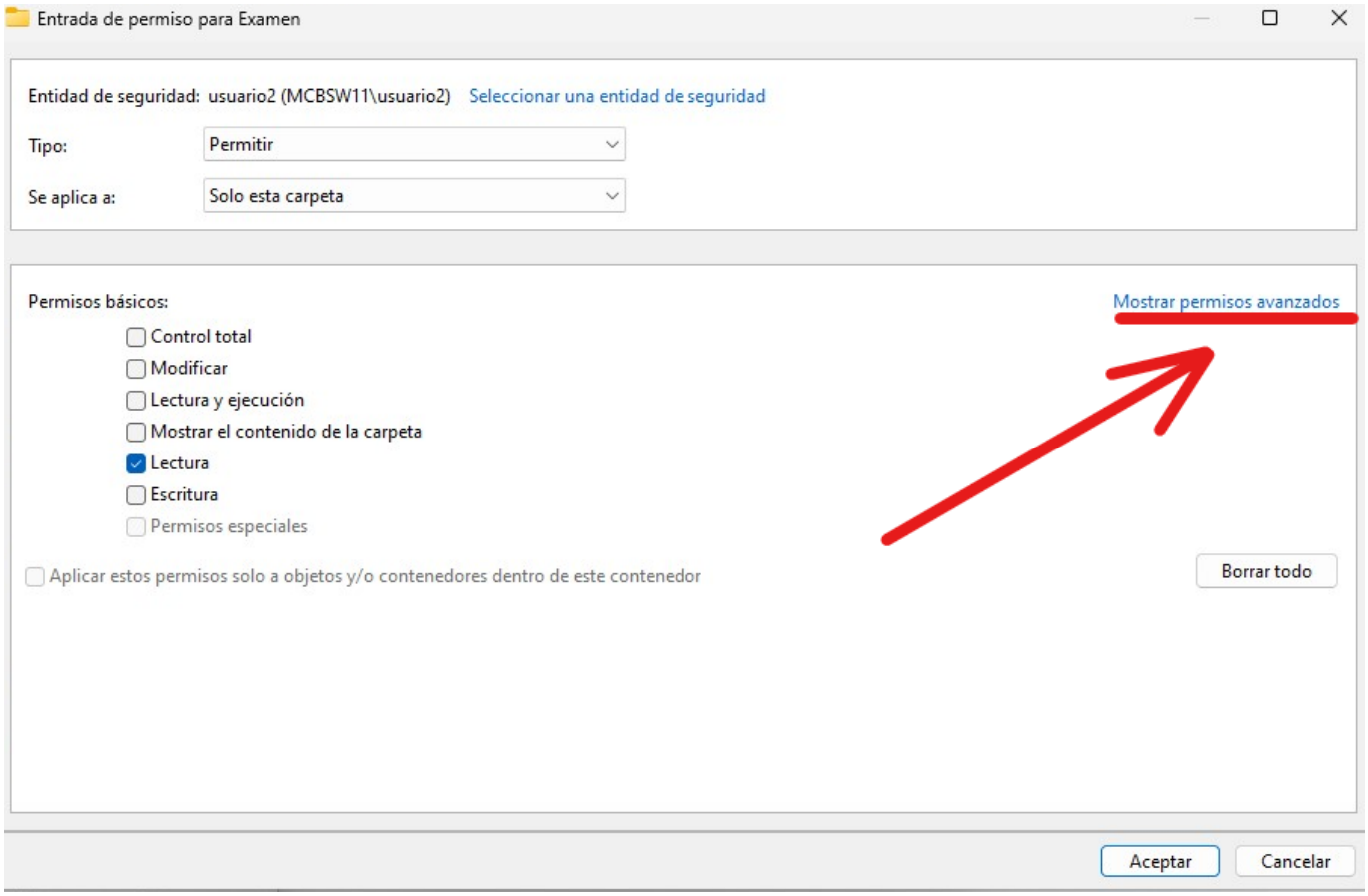
Para aplicar esta configuración se siguen los pasos del anterior apartado y tras eso se procede a ir a las propiedades del archivo lectura1.txt, a la pestaña de seguridad:



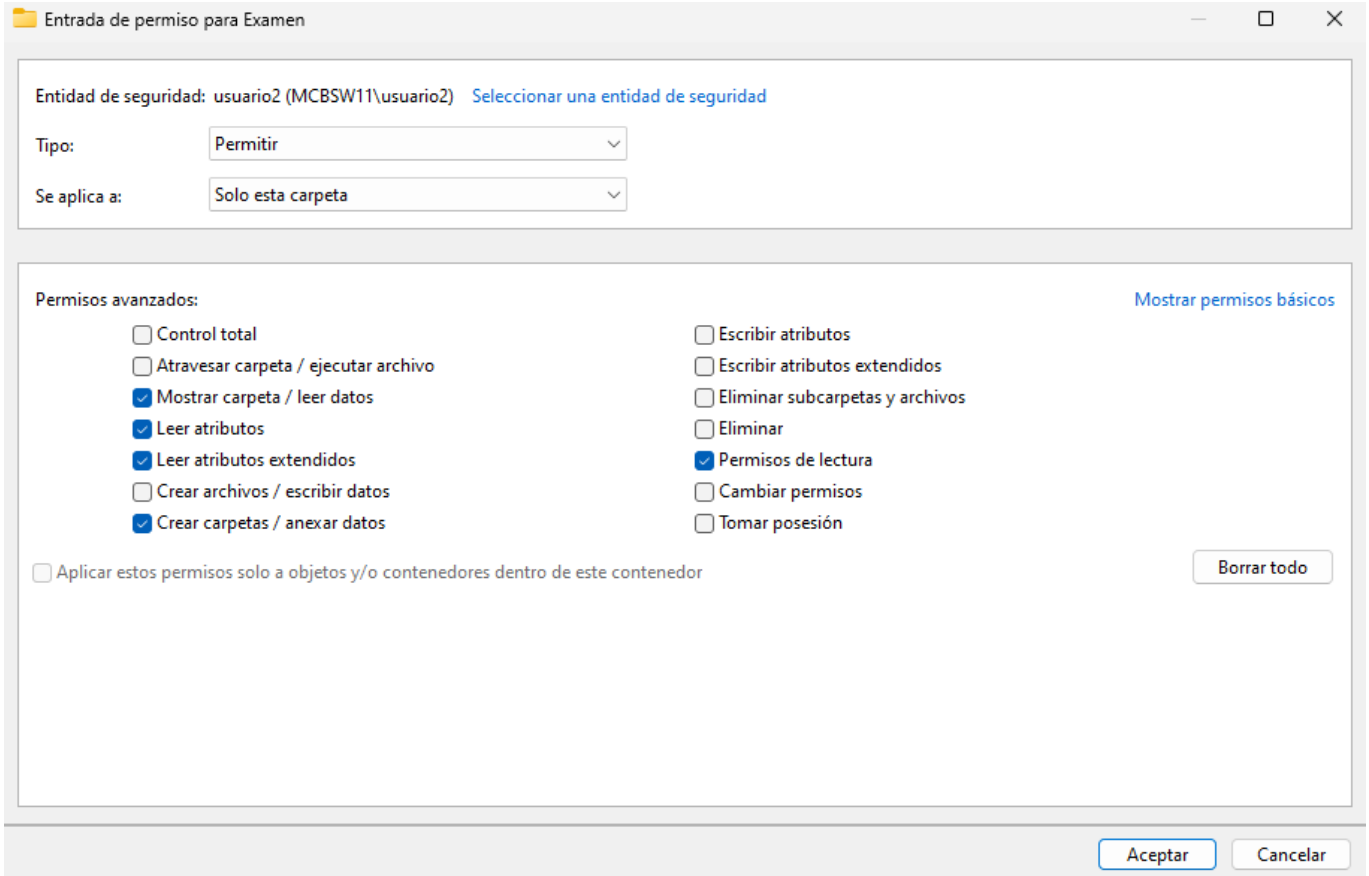
Se selecciona el usuario2 y se establece el permiso de lectura desmarcando los demás.

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:

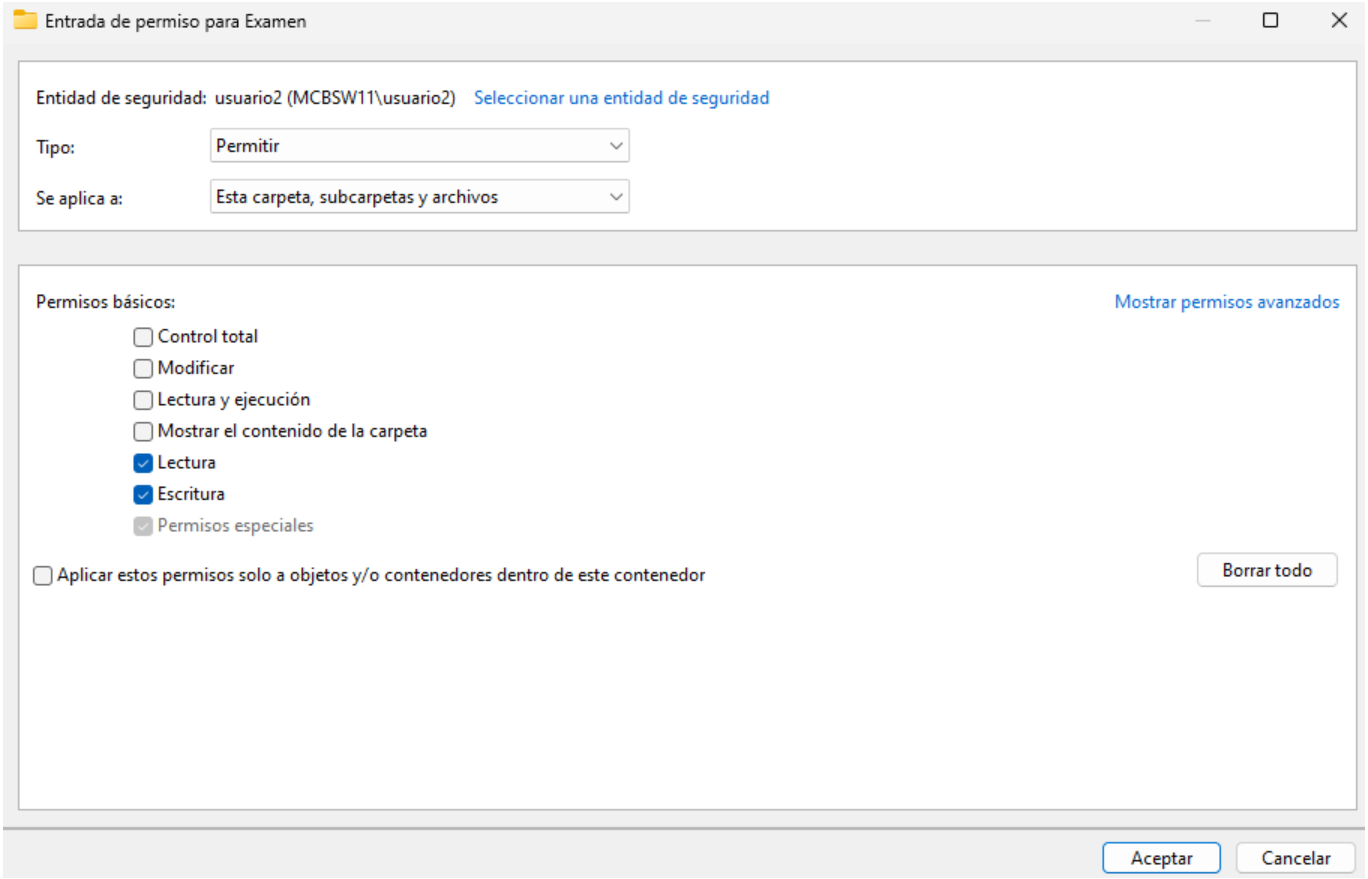


En “Se Aplica A” seleccionamos “Esta carpeta” y se procede a habilitar el permiso “Crear Carpetas / Anexar Datos”:



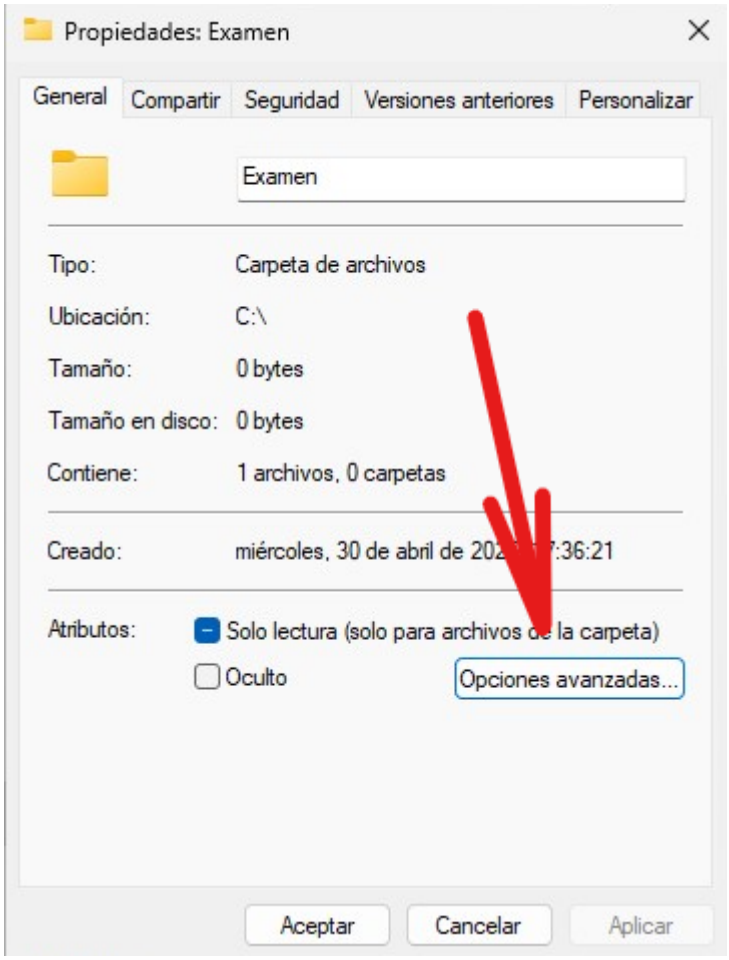
d) ACCESO TOTAl: El usuario 2 tiene el control total sobre la carpeta y componentes

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

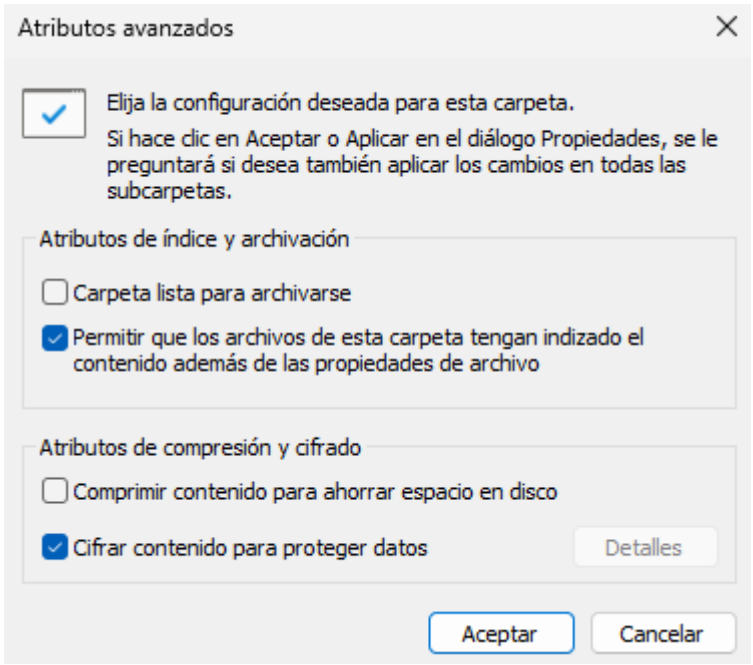


e) CIFRADO: Solo pueden acceder al contenido de un archivo cifrado los propietarios y los agentes de recuperación por defecto

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



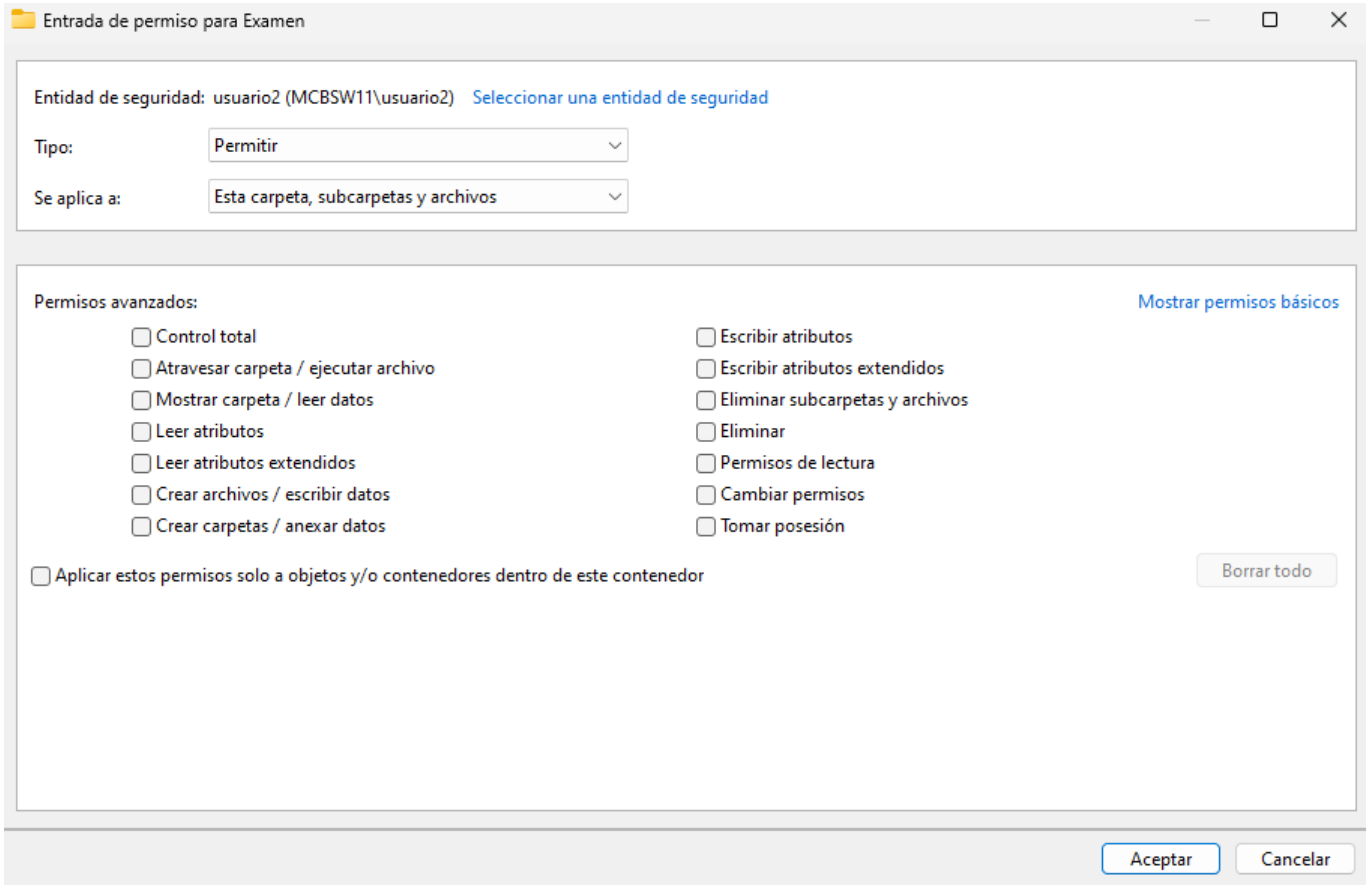
Aparecerá una ventana en la que se debe marca la casilla de “Cifrar contenido para proteger datos”:



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?

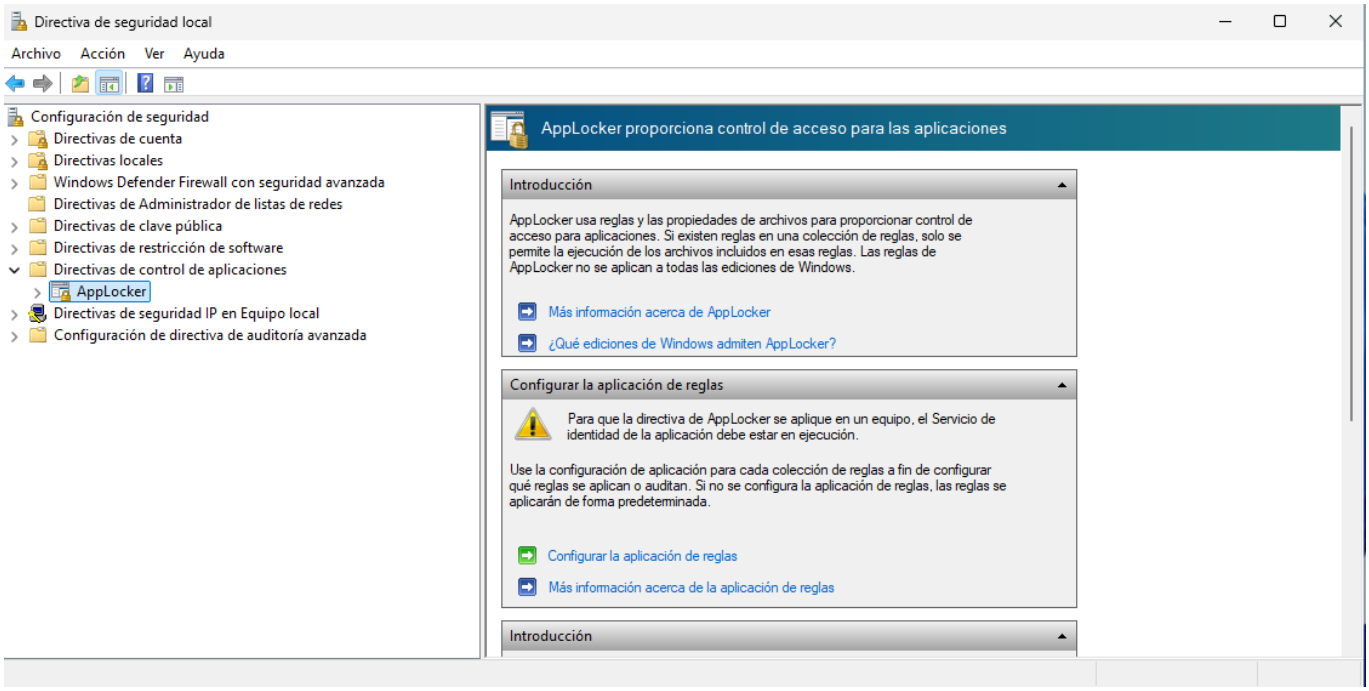
Se puede configurar con políticas de grupo (gpedit) o políticas de active directory (gpo). Generalmente, desde un punto de vista organizacional lo mejor sería realizar la configuración con políticas de active directory para los equipos de una empresa. En este caso, como no tenemos un servidor AD la mejor opción sería mediante políticas de grupo.

b) ¿Por qué es necesario crear las reglas automáticamente para que funcione AppLocker?

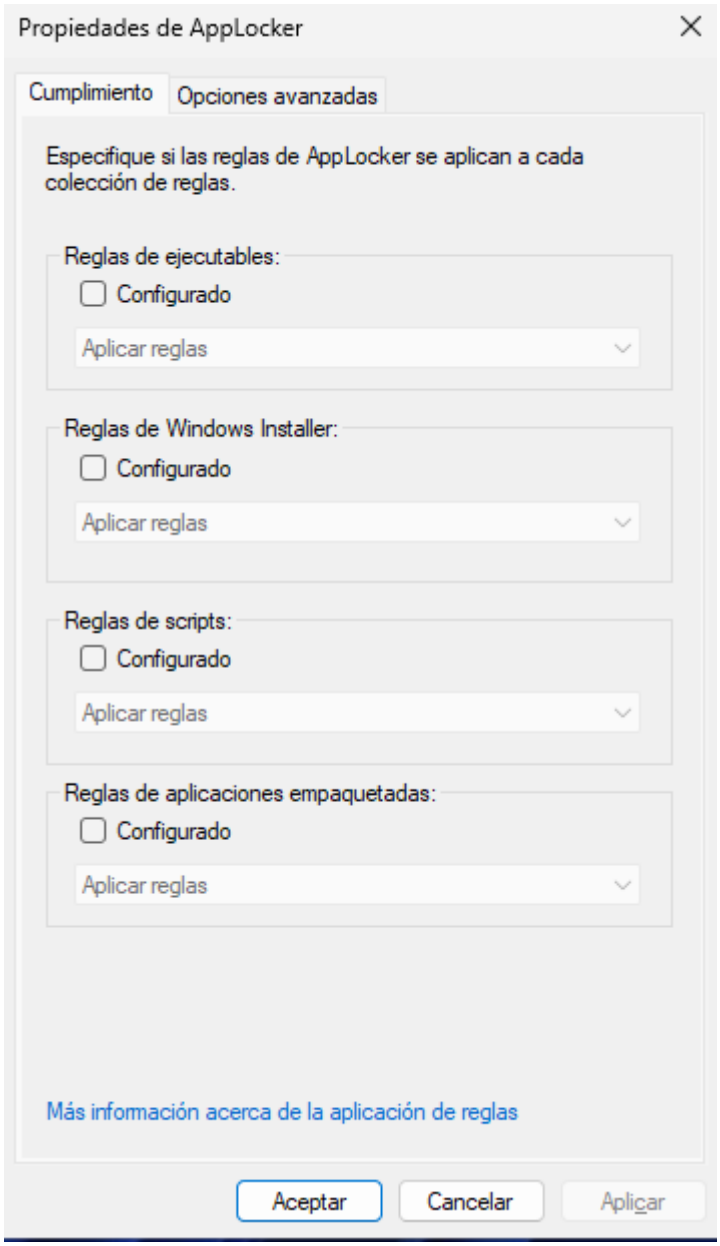
Por un lado el beneficio de crear las reglas automáticamente es una mayor velocidad en el proceso, ahorrando así tiempo de configuración, por otro lado también puede prevenir problemas que se puedan generar creando las reglas manualmente.

c) Instala Notepad++ y bloquea la aplicación ¿Que opciones te muestra AppLocker para identificar la aplicación? ¿Cual sería la mejor opción?

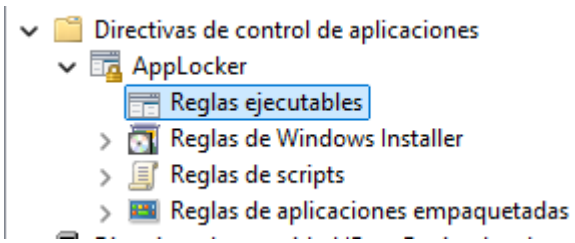
Para bloquear Notepad++ lo primero que debemos hacer es ir a “Directivas de seguridad Local”, donde podemos localizar Applocker dentro de la sección de directivas de control de aplicaciones:



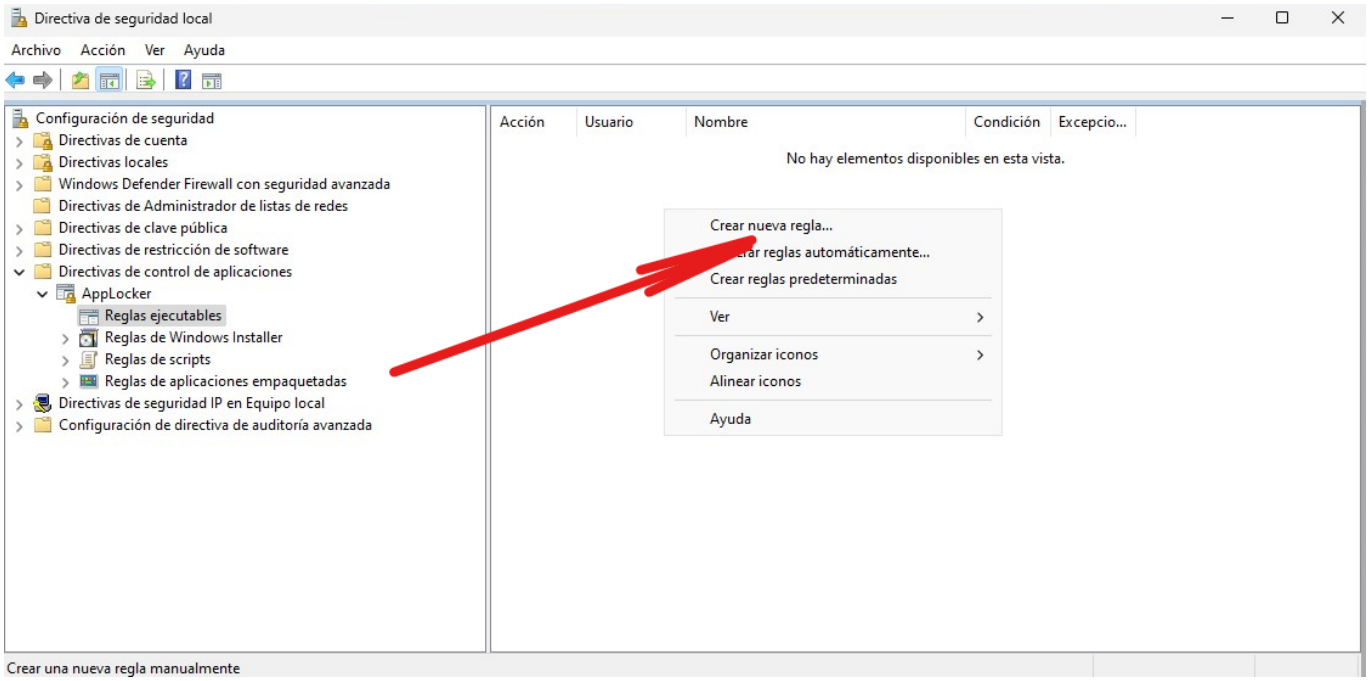
A continuación presionamos sobre “Configurar la aplicación de reglas” y aparecerá la siguiente ventana:



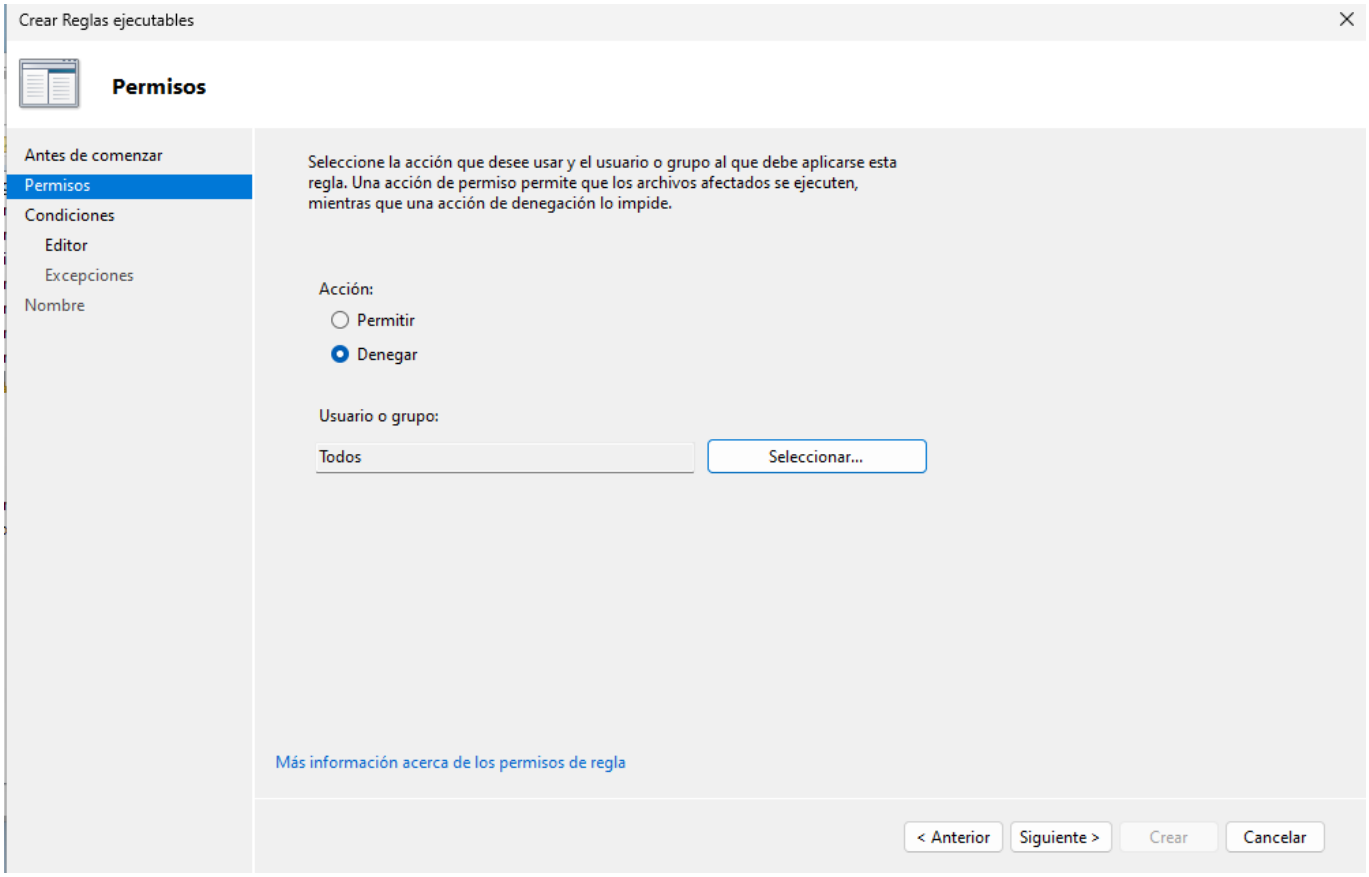
Aquí se habilitan las reglas de ejecutables. Tras eso debería de aparecer una sección de reglas de ejecutables:



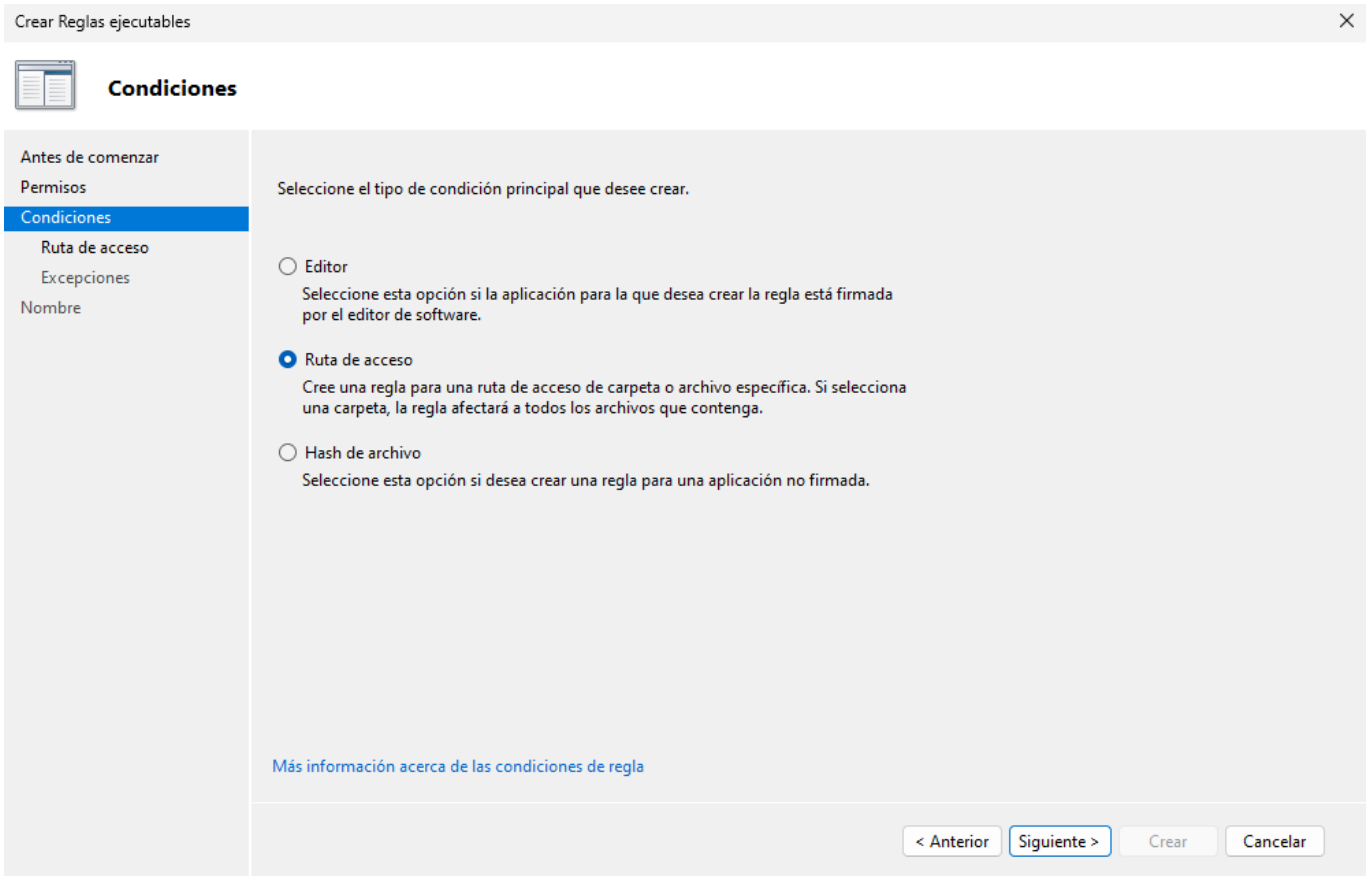
Tras eso hacemos click derecho un presionamos en “Crear una nueva Regla”:



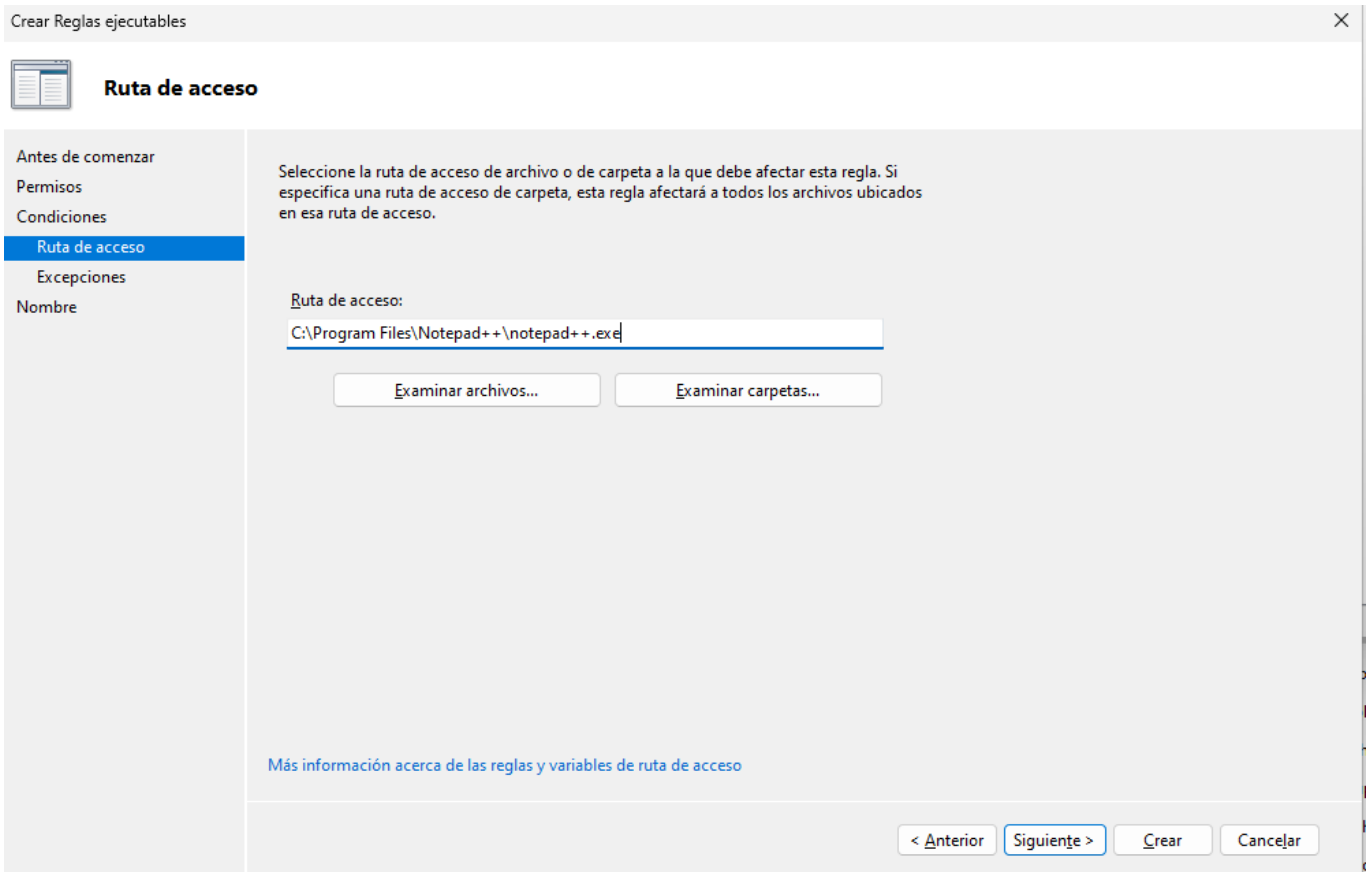
Le damos a siguiente y en la sección de permisos seleccionamos denegar:



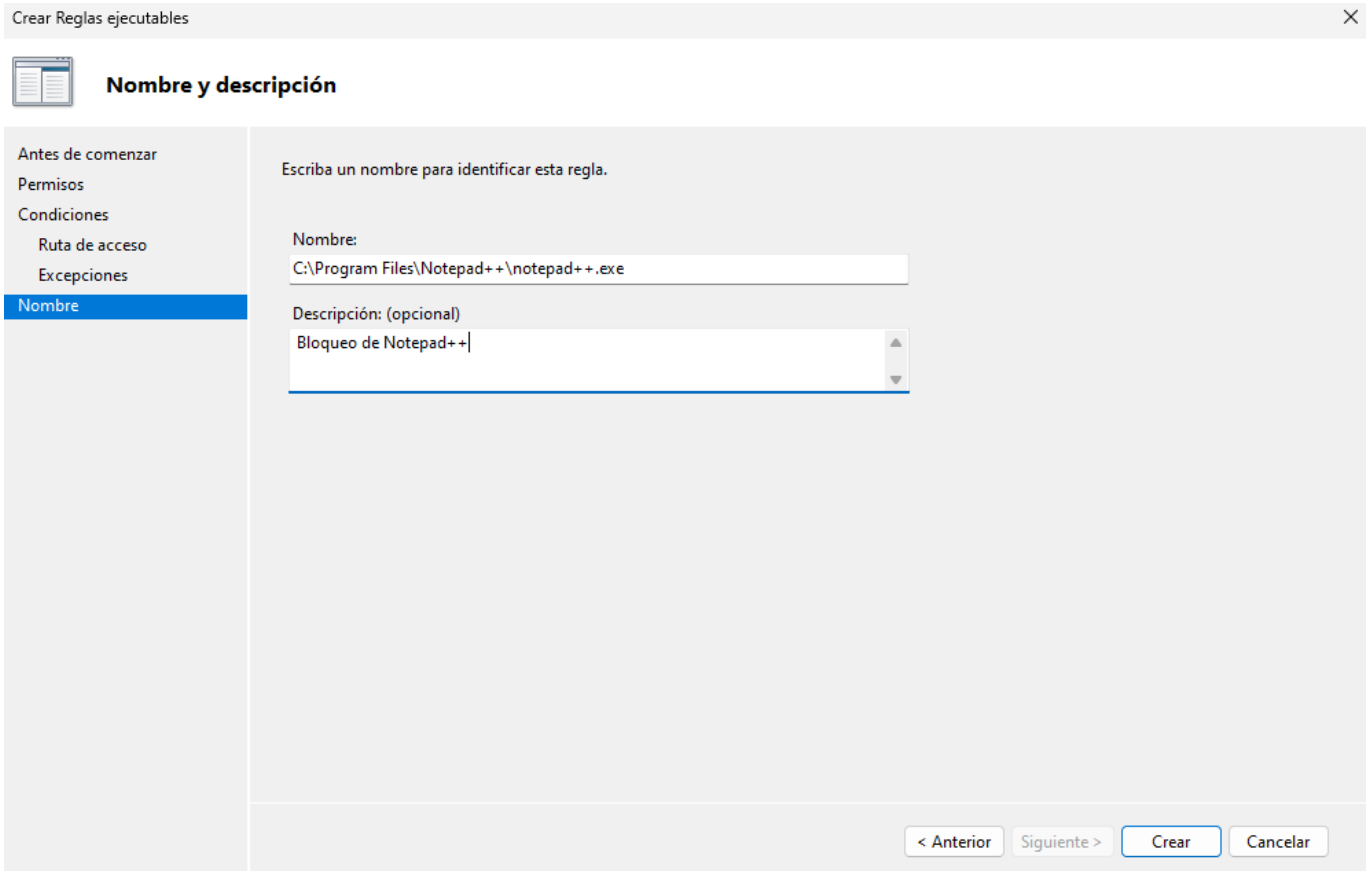
AppLocker nos permite identificar el programa de las 3 maneras que se pueden observar en la siguiente captura:



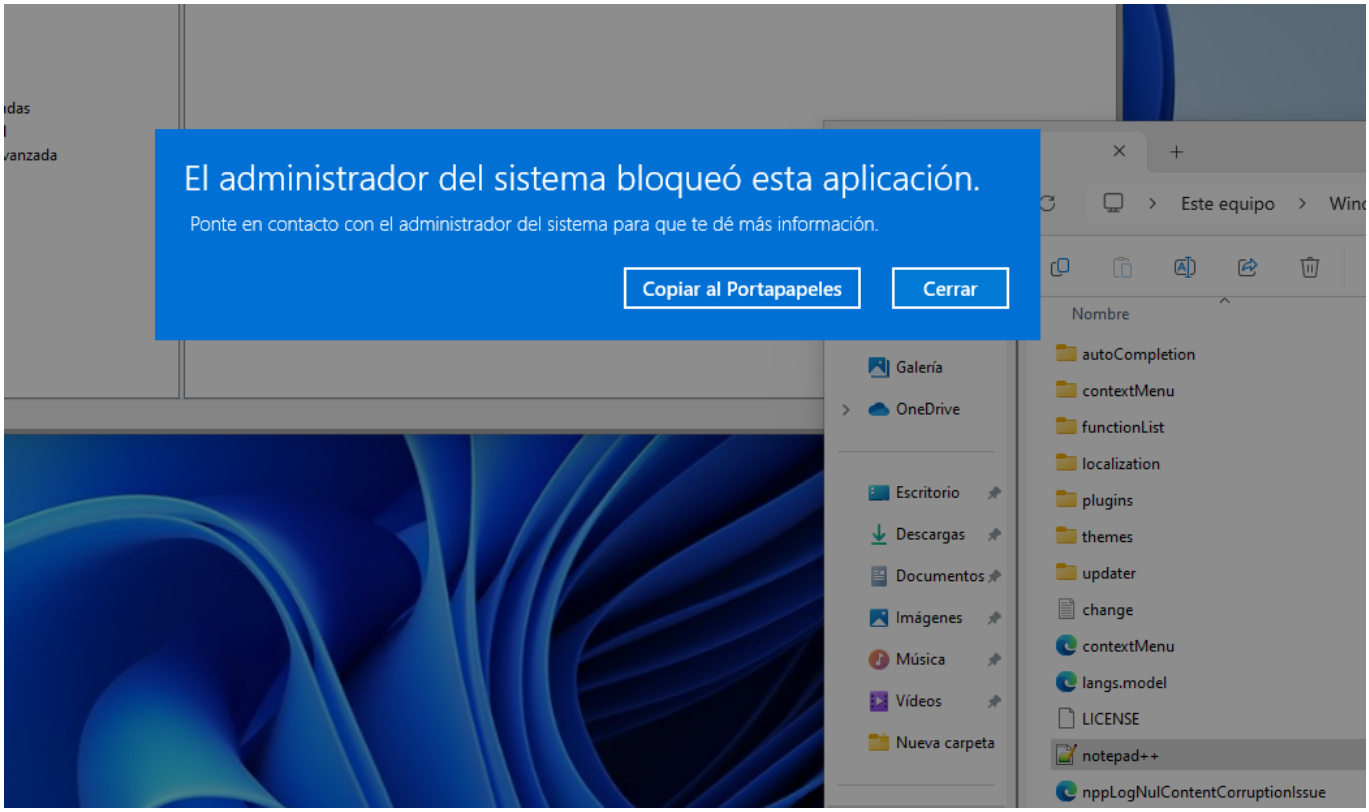
En este caso se selecciona la ruta de archivo:



Finalmente se le da a siguiente hasta llegar a la última sesión y se crea la nueva regla:



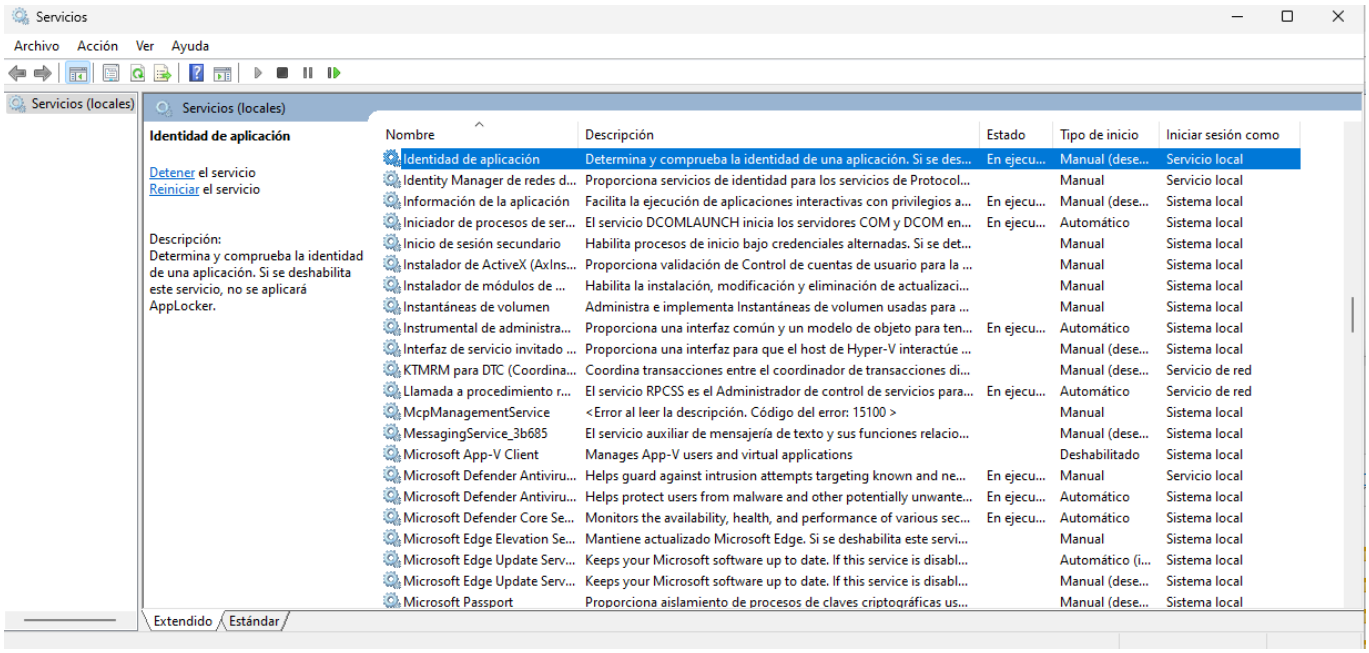
Si ahora se intenta ejecutar notepad++ aparece un mensaje diciendo que la aplicación está bloqueada:



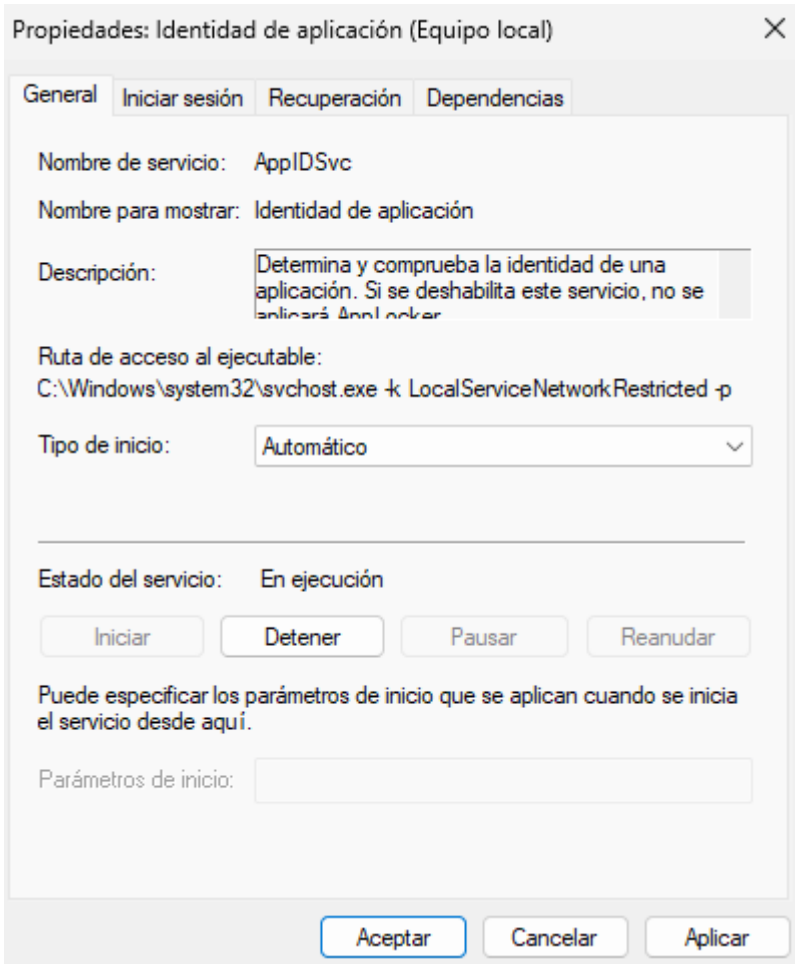
En este caso se ha identificado la aplicación por ruta por su simpleza, pero lo mejor sería identificarla mediante hash para dificultad la evasión del bloqueo moviendo el ejecutable de sitio, de todas formas esto también puede tener sus desventajas ya que si la aplicación se actualiza el hash puede cambiar y el bloqueo dejaría de ser efectivo.

d) ¿Que servicios es necesario modificar para que funcione AppLocker?¿Que cambios tenemos que realizar?

Sería necesario habilitar el servicio de Application identity:



En este caso también se configura para que se inicie automáticamente en el arranque:



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?

En este caso AppLocker ha funcionado sin necesidad de reiniciar el equipo, pero en caso de que no comenzara a funcionar sin un reinicio se puede usar el siguiente comando para forzar la aplicación de la directiva:

```
gpupdate /force
```