

[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:

| Directiva | Configuración de seguridad |
|---|---|
| Acceso a redes: canalizaciones con nombre accesibles anónimamente | Clásico: usuarios locales se autentican (Deshabilitada) |
| Acceso a redes: modelo de seguridad y uso compartido para cuentas locales | Habilitada |
| Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación... | Deshabilitada |
| Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM | Habilitada |
| Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM | Deshabilitada |
| Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos | Deshabilitada |
| Acceso a redes: recursos compartidos accesibles anónimamente | No está definido |
| Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos | Habilitada |
| Acceso a redes: rutas del Registro accesibles remotamente | System\CurrentControlSet\Control\Pro |
| Acceso a redes: rutas y subrutas del Registro accesibles remotamente | System\CurrentControlSet\Control\Pri |
| Acceso de red: evitar que clientes con permiso realicen llamadas remotas a SAM | No está definido |
| Acceso de red: permitir traducción SID/nombre anónima | Deshabilitada |
| Apagado: borrar el archivo de paginación de la memoria virtual | Deshabilitada |
| Apagado: permitir apagar el sistema sin tener que iniciar sesión | Habilitada |
| Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad | Deshabilitada |
| Auditoría: auditar el acceso de objetos globales del sistema | Deshabilitada |
| Auditoría: auditar el uso del privilegio de copias de seguridad y restauración | Deshabilitada |
| Auditoría: forzar la configuración de subcategorías de la directiva de auditoría (Windows Vista o p...) | No está definido |
| Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros | Deshabilitada |
| Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite) | Habilitada |
| Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre) | Deshabilitada |
| Configuración del sistema: subsistemas opcionales | |

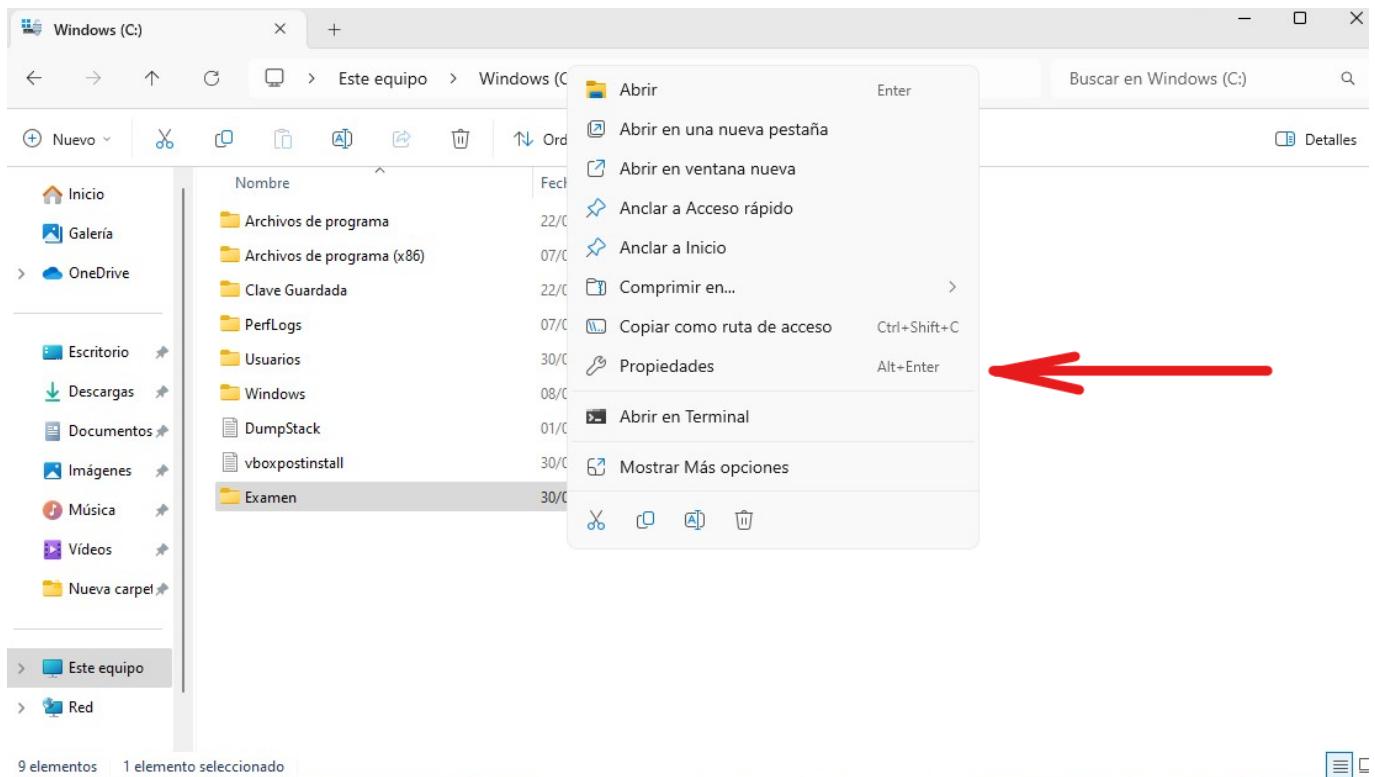
También se puede utilizar el registro (regedit) en "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" para customizar algunos parámetros de UAC:

| Nombre | Tipo | Datos |
|------------------------------|-----------|------------------------|
| ab([predeterminado]) | REG_SZ | (valor no establecido) |
| ConsentPromptBehaviorAdmin | REG_DWORD | 0x00000005 (5) |
| ConsentPromptBehaviorUser | REG_DWORD | 0x00000003 (3) |
| dontdisplaylastusername | REG_DWORD | 0x00000000 (0) |
| DSCAutomationHostEnabled | REG_DWORD | 0x00000002 (2) |
| EnableCursorSuppression | REG_DWORD | 0x00000001 (1) |
| EnableFullTrustStartupTasks | REG_DWORD | 0x00000002 (2) |
| EnableInstallerDetection | REG_DWORD | 0x00000001 (1) |
| EnableLUA | REG_DWORD | 0x00000001 (1) |
| EnableSecureUIAPaths | REG_DWORD | 0x00000001 (1) |
| EnableUIADesktopToggle | REG_DWORD | 0x00000000 (0) |
| EnableUwpStartupTasks | REG_DWORD | 0x00000002 (2) |
| EnableVirtualization | REG_DWORD | 0x00000001 (1) |
| legalnoticecaption | REG_SZ | |
| legalnoticetext | REG_SZ | |
| PromptOnSecureDesktop | REG_DWORD | 0x00000001 (1) |
| scforceoption | REG_DWORD | 0x00000000 (0) |
| shutdownwithoutlogon | REG_DWORD | 0x00000001 (1) |
| SupportFullTrustStartupTasks | REG_DWORD | 0x00000001 (1) |
| SupportUwpStartupTasks | REG_DWORD | 0x00000001 (1) |
| undockwithoutlogon | REG_DWORD | 0x00000001 (1) |
| ValidateAdminCodeSignatures | REG_DWORD | 0x00000000 (0) |

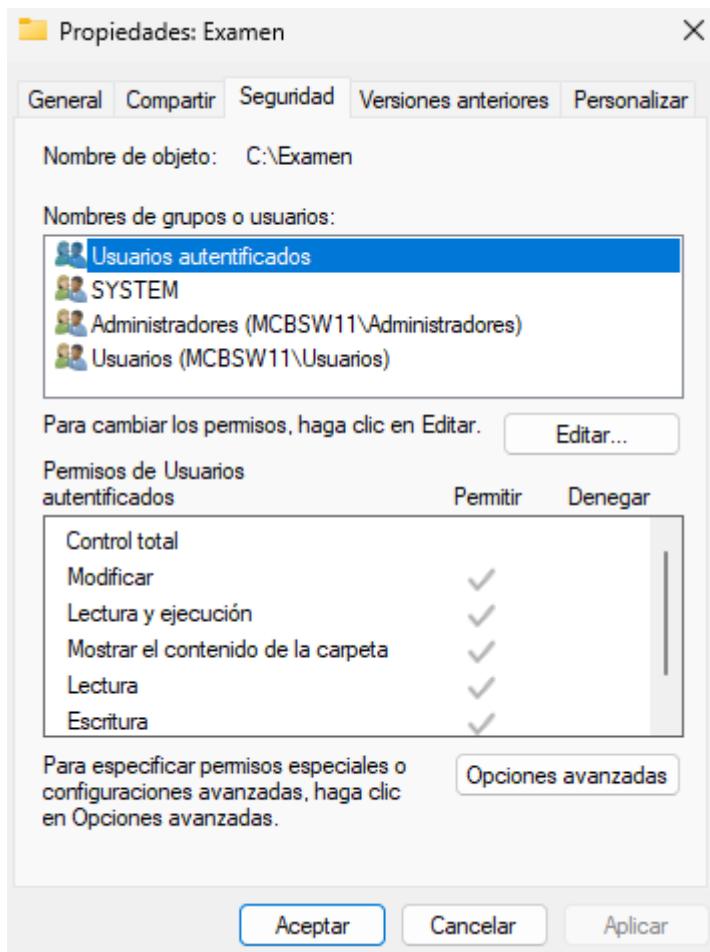
Sobre una carpeta “Examen” creada en “C:\” se van a realizar las siguientes configuraciones de UAC:

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:

Configuración de seguridad avanzada para Examen

Nombre: C:\Examen
Propietario: MCBS (MCBSW11\MCBS) Cambiar

Permisos Auditoría Acceso efectivo

Para obtener información adicional, haga doble clic en una entrada de permiso. Para modificar una entrada de permiso, seleccione la entrada y haga clic en Editar (si está disponible).

Entradas de permiso:

| Entidad de seguridad | Tipo | Acceso | Heredada de | Se aplica a |
|---|---------|---------------------|-------------|------------------------------------|
| Administradores (MCBSW11\Administradores) | Perm... | Control total | C:\ | Esta carpeta, subcarpetas y arc... |
| SYSTEM | Perm... | Control total | C:\ | Esta carpeta, subcarpetas y arc... |
| Usuarios (MCBSW11\Usuarios) | Perm... | Lectura y ejecución | C:\ | Esta carpeta, subcarpetas y arc... |
| Usuarios autenticados | Perm... | Modificar | C:\ | Esta carpeta, subcarpetas y arc... |

Reemplazar todas las entradas de permisos de objetos secundarios por entradas de permisos heredables de este objeto

Tras eso se presiona en el botón de agregar:

Entrada de permiso para Examen

Entidad de seguridad: Seleccionar una entidad de seguridad

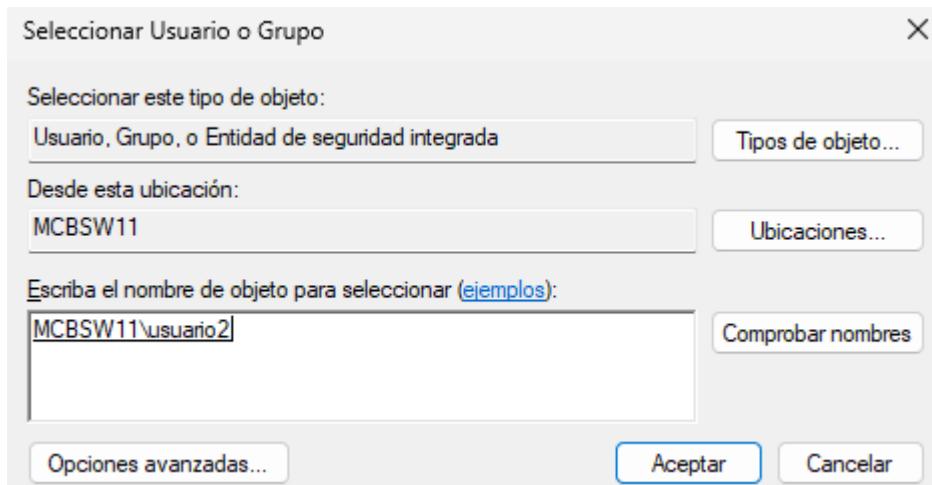
Tipo: Permitir
Se aplica a: Esta carpeta, subcarpetas y archivos

Permisos básicos:

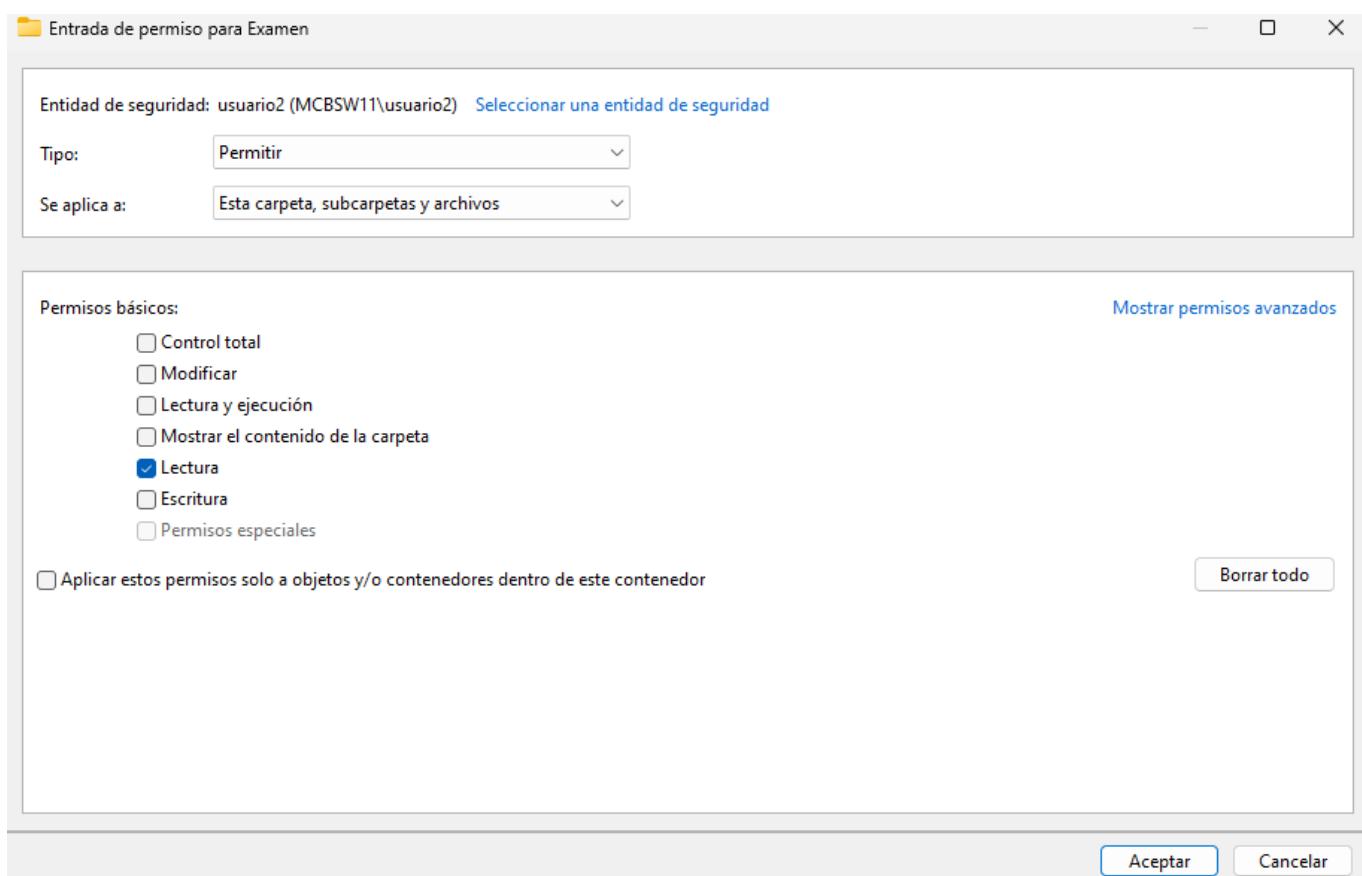
- Control total
- Modificar
- Lectura y ejecución
- Mostrar el contenido de la carpeta
- Lectura
- Escritura
- Permisos especiales

Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor

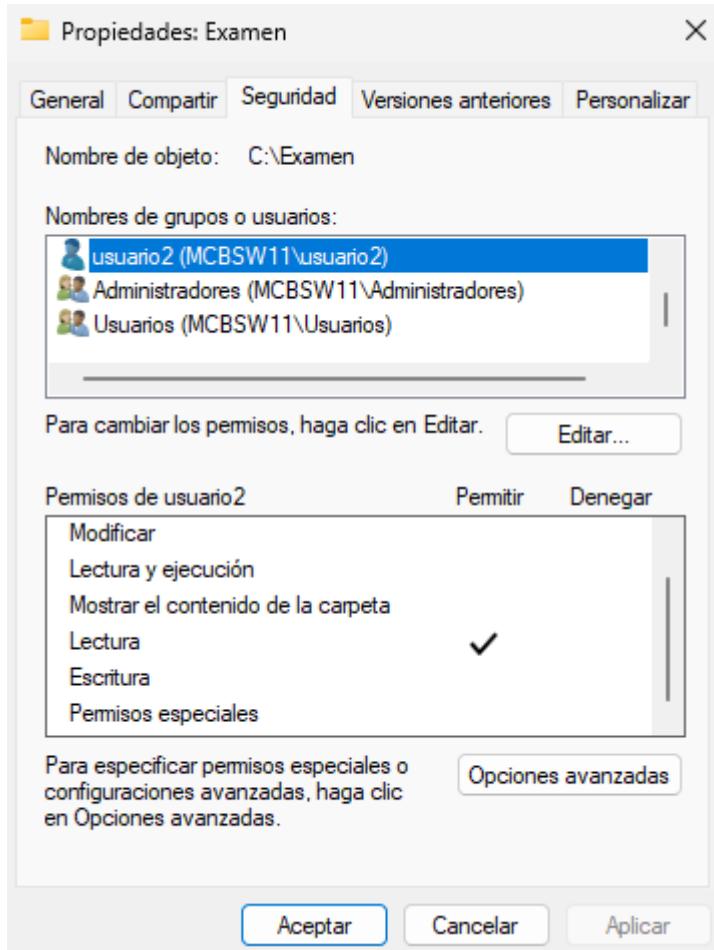
A continuación se presiona en el texto donde pone “Seleccionar una Entidad de Seguridad”, en la ventana que se abre se introduce el nombre de usuario2, y se presiona en comprobar nombres, tras eso debería de aparecer el nombre del equipo seguido del de Usuario2 separados por una barra:



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 de lectura:

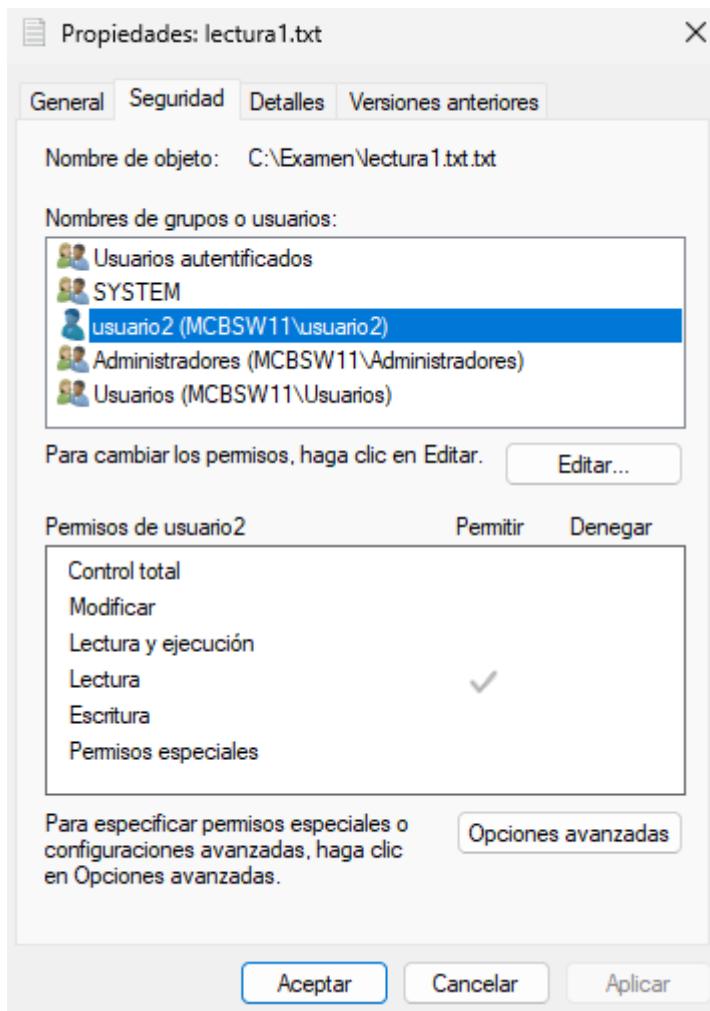


Finalmente se aplican los cambios y usuario2 quedará con los permisos establecidos:



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.

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

From:
<https://knoppia.net/> - Knoppia

Permanent link:
https://knoppia.net/doku.php?id=master_cs:fortificacion:p10&rev=1746028775

Last update: 2025/04/30 15:59

