

Implementación de Políticas de Restricción de Dispositivo USB

Realizado por: Arturo Martín-Vegue González

Para: 4Geeks Academy

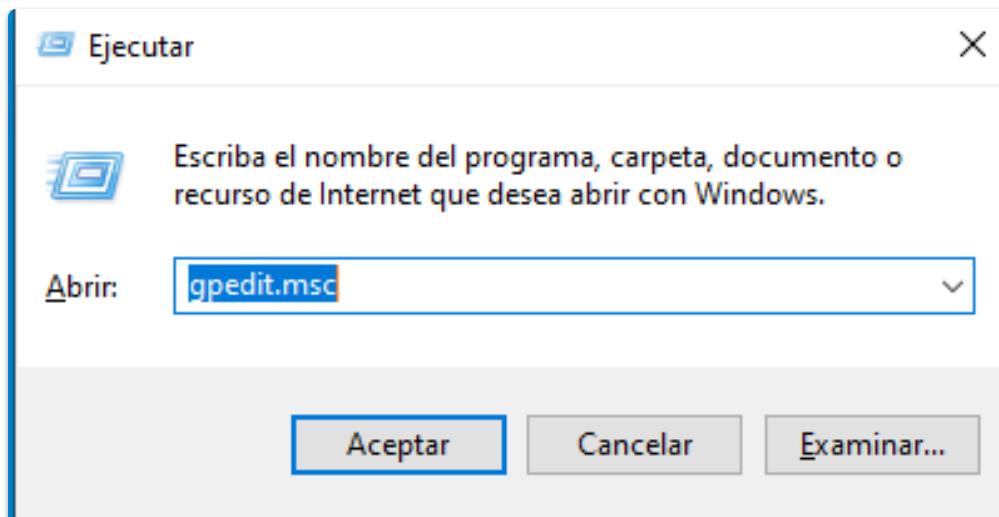
En este documento se detallará el proceso para restringir el acceso en un sistema Windows 10 (virtualizado en [VirtualBox](#)) a usuarios no privilegiados y aplicar filtros para que otros, dependiendo de su rol, sí puedan.

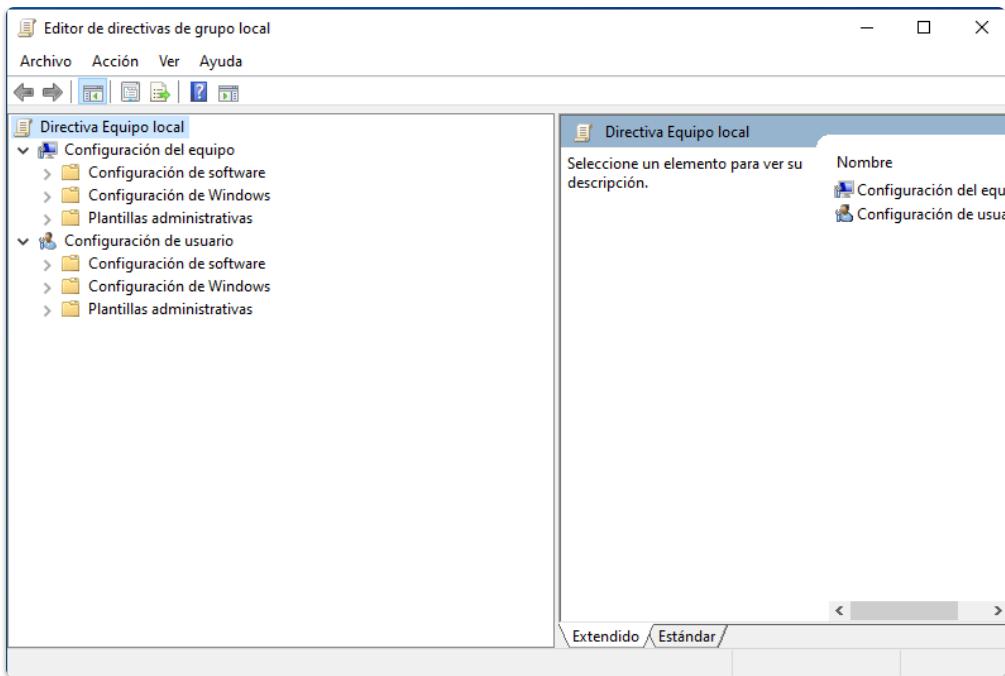
Se adjuntarán capturas y una breve descripción del proceso.

a. Restringir el Acceso a Dispositivo Extraíble

Se comienza restringiendo el acceso a todos los usuarios aplicando el principio de [menor privilegio](#).

- Se entra en el [Editor de Políticas de Grupo \(Group Policy Editor\)](#) con el comando `gpedit.msc`.





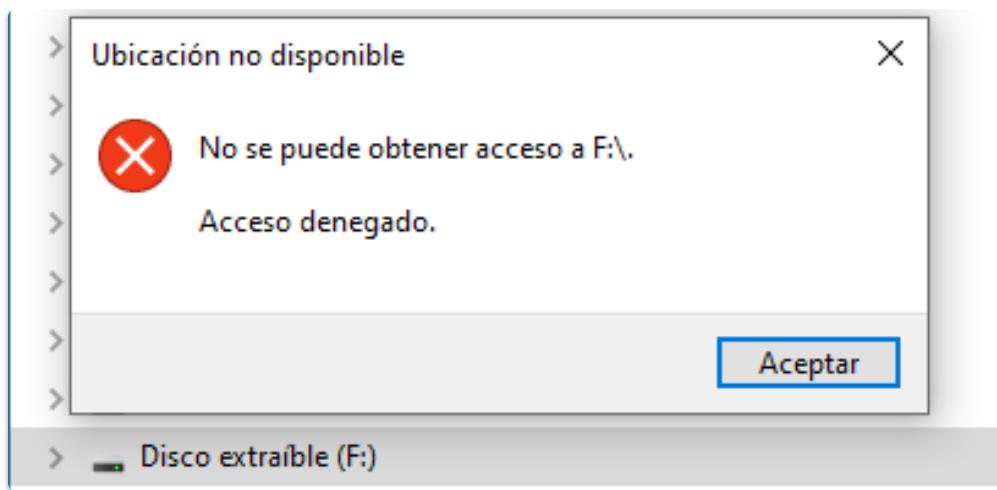
- A continuación se navega hacia las **Políticas de Dispositivos Extraíbles** en: **Configuración del equipo > Plantillas administrativas > Sistema > Acceso de almacenamiento extraíble** y se aplican las **Políticas de Prohibición de Acceso a Dispositivos USB**.

| Configuración | Estado |
|---|-----------------------|
| Establecer tiempo (en segundos) para forzar reinicio | No configurada |
| CD y DVD: denegar acceso de ejecución | No configurada |
| CD y DVD: denegar acceso de lectura | No configurada |
| CD y DVD: denegar acceso de escritura | No configurada |
| Clases personalizadas: denegar acceso de escritura | No configurada |
| Unidades de disco: denegar acceso de ejecución | No configurada |
| Unidades de disco: denegar acceso de lectura | No configurada |
| Unidades de disco: denegar acceso de escritura | No configurada |
| Discos extraíbles: denegar acceso de ejecución | No configurada |
| Discos extraíbles: denegar acceso de lectura | No configurada |
| Discos extraíbles: denegar acceso de escritura | No configurada |
| Todas las clases de almacenamiento extraíble: denegar acceso de ejecución | No configurada |
| Todo el almacenamiento extraíble: permitir acceso directo e... | No configurada |
| Unidades de cinta: denegar acceso de ejecución | No configurada |
| Unidades de cinta: denegar acceso de lectura | No configurada |
| Unidades de cinta: denegar acceso de escritura | No configurada |
| Dispositivos WPD: denegar acceso de lectura | No configurada |
| Dispositivos WPD: denegar acceso de escritura | No configurada |

- Aplicando las políticas de denegación de **lectura** y **escritura** y reiniciando el equipo para que se apliquen.

| | |
|--|------------|
| Discos extraíbles: denegar acceso de lectura | Habilitada |
| Discos extraíbles: denegar acceso de escritura | Habilitada |

- Se verifica que funcionen.



b. Configuración de Permisos a Usuarios Específicos

Para aplicar la asignación de permisos por grupo o usuarios se utilizará la **Microsoft Management Console (MMC)**. Es un marco de trabajo de Windows que proporciona una interfaz para la administración del sistema.

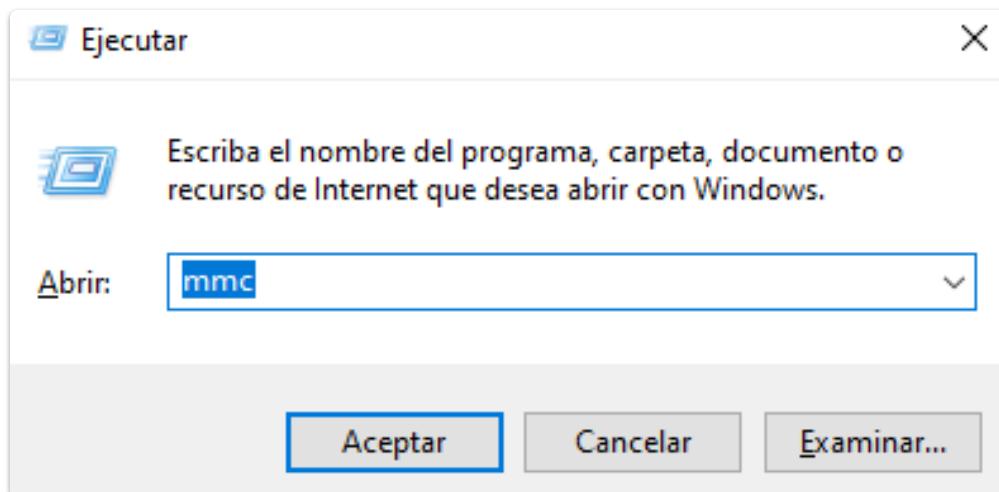
¿Por qué se utiliza en este caso? Aunque la herramienta estándar `gpedit.msc` permite editar las Políticas de Grupo Locales, tiene una limitación crítica: aplica la configuración de usuario a **todas** las cuentas del equipo (incluido administradores).

Para implementar una política de DLP discriminatoria basada en "**menor privilegio**", utilizamos la MMC para cargar el complemento "**Editor de objetos de directiva de grupo**" apuntando específicamente al conjunto de usuarios "**No administradores**".

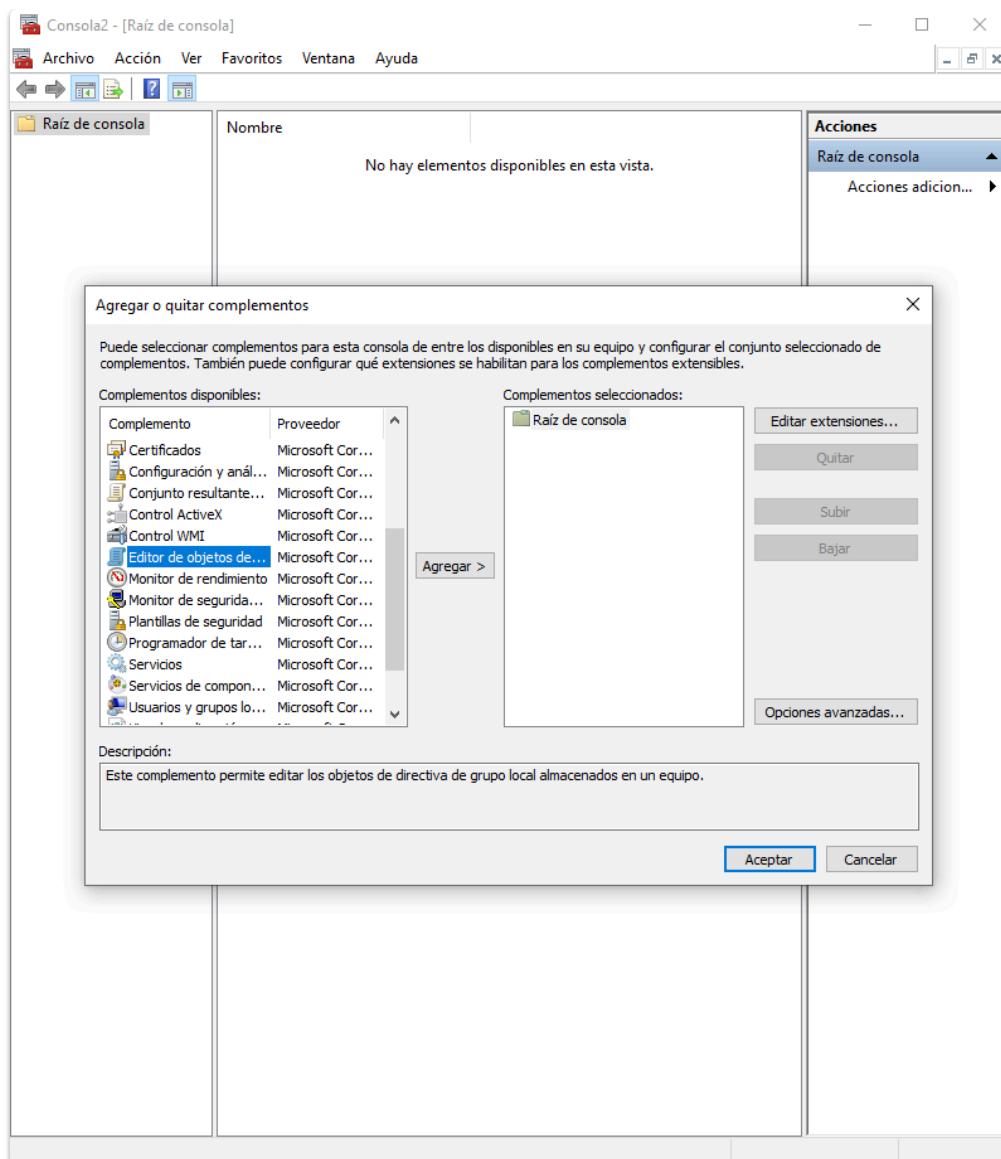
Procedimiento

1. Añadir Directiva de Grupo en MMC

- Entramos en MMC a través de `Win + R`



- Cargamos la herramienta en archivo y pinchando en Agregar o quitar complemento buscando la opción **Editor de objetos de directiva de grupo** y pinchando en agregar.



- En el menú que se abre, pinchamos en **Examinar**.

Seleccionar un objeto de directiva de grupo

X

Éste es el Asistente para directivas de grupo



Los objetos de directiva de grupo local pueden guardarse en el equipo local.

Use el botón Examinar para seleccionar uno de los objetos de directiva de grupo.

Objeto de directiva de grupo:

Equipo local

Examinar...

Permitir que cambie el enfoque del complemento de directivas de grupo cuando se inicie desde la línea de comandos. Esto solo se aplica si se guarda la consola.

< Atrás

Finalizar

Cancelar

- Y una vez ahí, pinchamos en la pestaña **Usuarios** y seleccionamos "No administradores"

Buscar un objeto de directiva de grupo

?

X

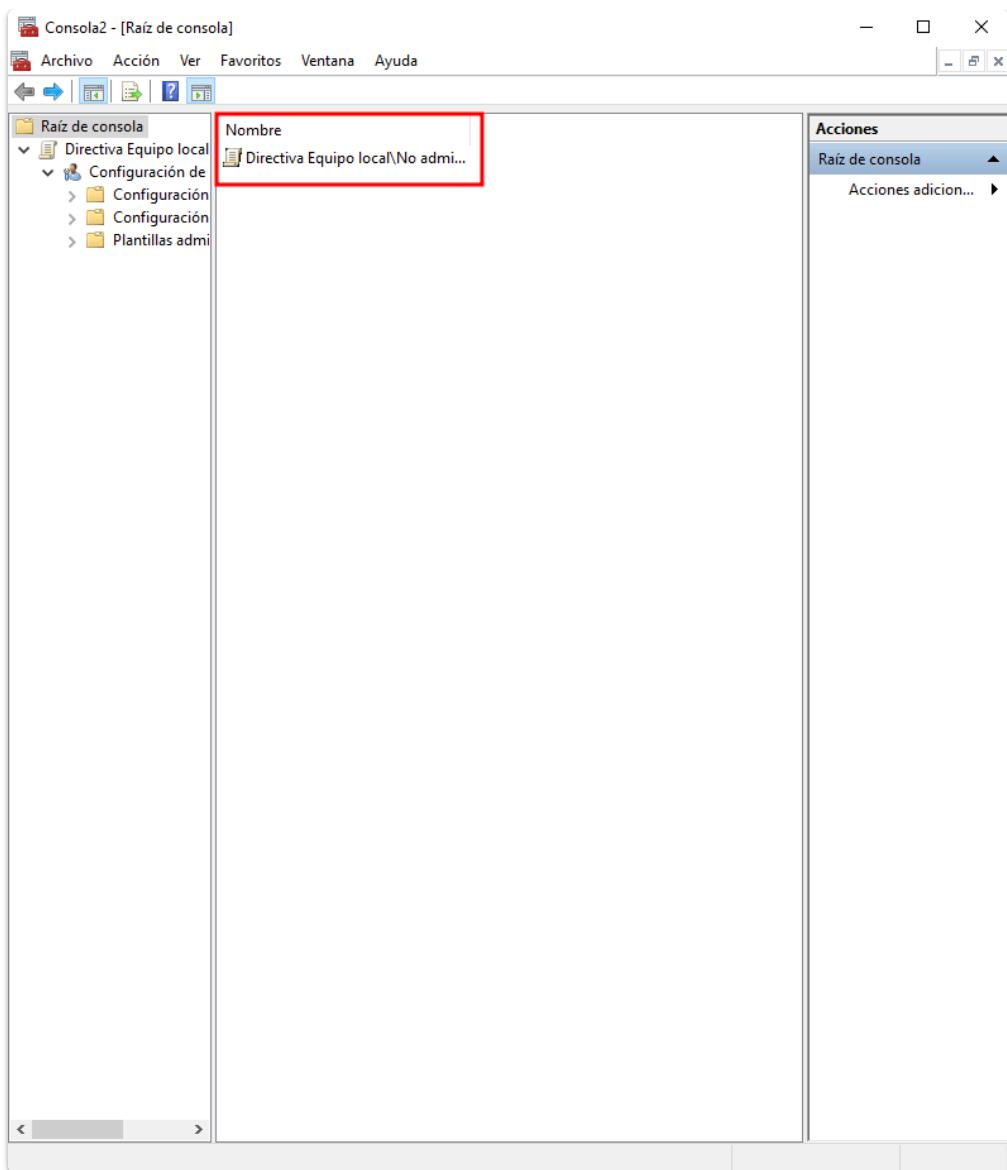
Equipos Usuarios

Usuarios y grupos locales compatibles con la directiva de grupo local:

| Nombre | El objeto de directiva de ... |
|---------------------------|-------------------------------|
| Administrador | No |
| DefaultAccount | No |
| Pepe | No |
| Usuario_USB | No |
| vboxuser | No |
| WDAGUtilityAccount | No |
| Administradores | No |
| No administradores | No |

Aceptar Cancelar

- Una vez hecho, pinchamos dos veces en la nueva opción que aparece en la derecha.



- Y como en `gpedit` buscamos en `Configuración del equipo > Plantillas administrativas > Sistema > Acceso de almacenamiento extraíble` y denegamos el permiso de *lectura* y *escritura*.

Consola2 - [Raíz de consola\Directiva Equipo local\No administradores\Configuración de usuario\Plantillas administrativas\Sistema\Acceso de almacenamiento ext]

Archivo Acción Ver Favoritos Ventana Ayuda

Raíz de consola

Directiva Equipo local\No administradores

Configuración de usuario

Configuración de software

Configuración de Windows

Plantillas administrativas

- Active Desktop
- Carpetas compartidas
- Componentes de Windows
- Menú inicio y barra de tareas
- Panel de control
- Red

Sistema

- Acceso de almacenamiento extraible
- Administración de comunicación
- Administración de energía
- Directiva de grupo
- Inicio de sesión
- Instalación de controladores
- Opciones de Ctrl+Alt+Supr
- Opciones de mitigación
- Pantalla
- Perfiles de usuario
- Redirección de carpetas
- Scripts
- Servicios de configuración regional

Todos los valores

Acceso de almacenamiento extraible

Discos extraíbles: denegar acceso de escritura

Configuración

| Estado |
|-------------------|
| No configurada |
| Habilitada |
| Habilitada |
| No configurada |

Requisitos:

Al menos Windows Vista

Descripción:

Esta configuración de directiva deniega el acceso de escritura a los discos extraíbles.

Si habilita esta configuración de directiva, se deniega el acceso de escritura a esta clase de almacenamiento extraíble.

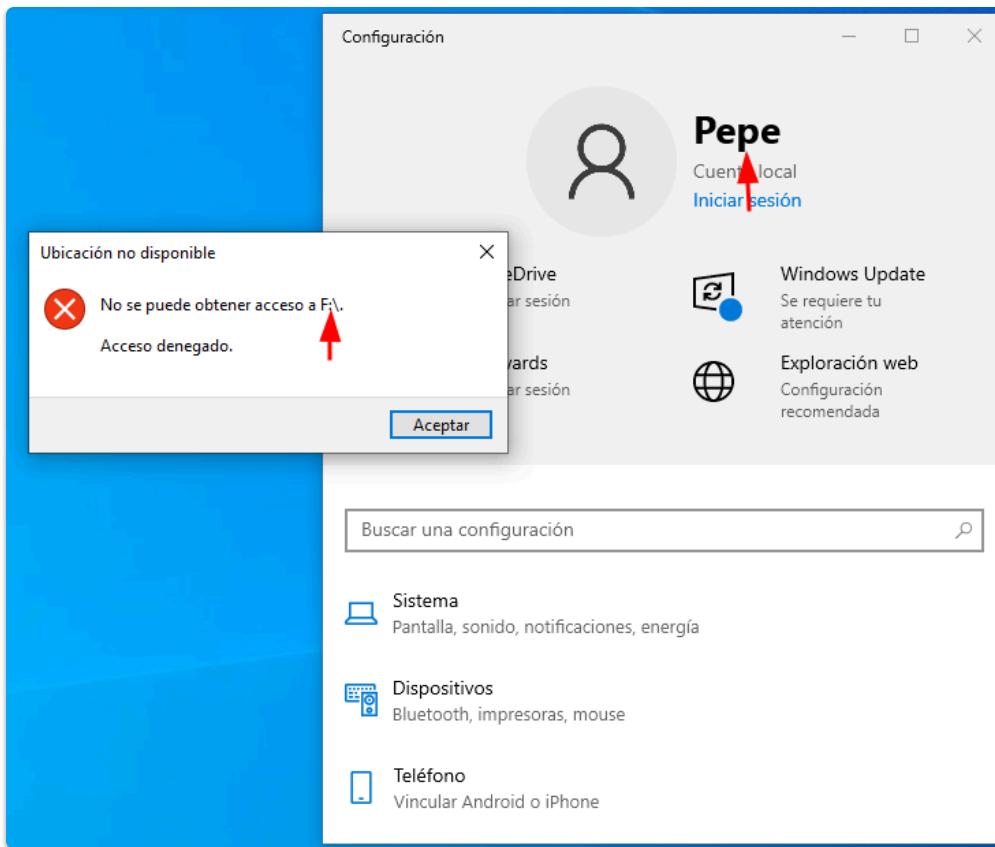
Si deshabilita o no define esta configuración de directiva, se permite el acceso de escritura a esta clase de almacenamiento extraíble.

Nota: para exigir que los usuarios escriban datos en unidades de almacenamiento protegidas por BitLocker, habilite la configuración de directiva "Denegar el acceso de escritura a unidades extraíbles no protegidas por BitLocker", que está ubicada en "Configuración del equipo\Plantillas administrativas\Componentes de Windows\Cifrado de unidad BitLocker\Unidades de datos extraíbles".

Extendido / Estándar

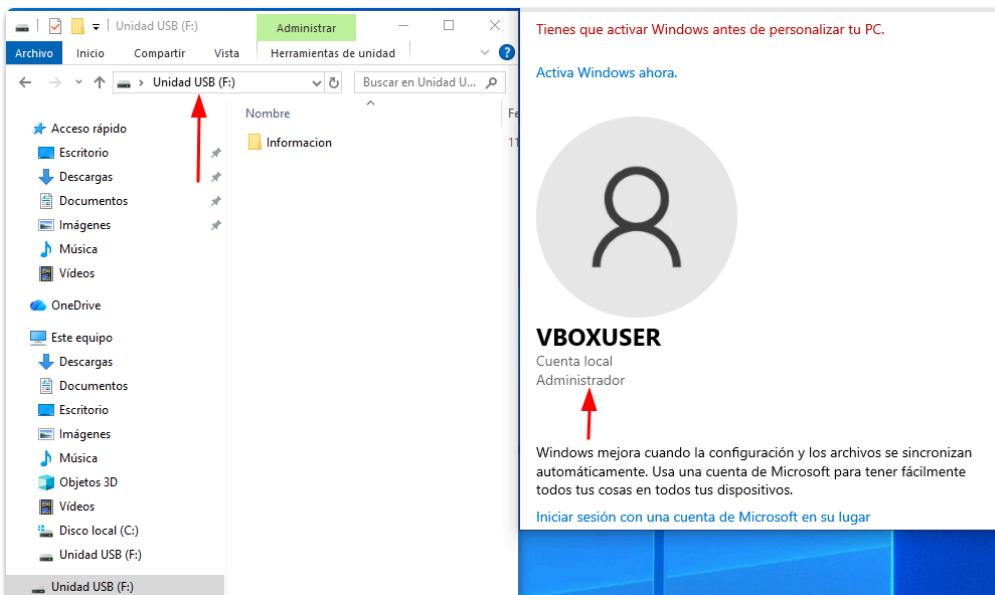
2. Comprobación

Con un usuario previamente creado, en este caso **Pepe**, probamos a entrar en el medio extraíble USB.



- Como se puede observar, no puede acceder a "F:" que es el USB introducido.

Una vez hecho esto, probamos ahora con el usuario administrador, `vboxuser`.



Nota: En un entorno empresarial real con Active Directory, esta restricción no se aplicaría usuario a usuario. Se utilizaría el **Filtrado de Seguridad** de las GPO (Group Policy Objects) vinculadas a Unidades Organizativas o Grupos de Seguridad, permitiendo una gestión centralizada y escalable.