Implementación de Políticas de Restricción de Dispositivo USB

Realizado por: Arturo Martín-Vegue González

Para: 4Geeks Academy

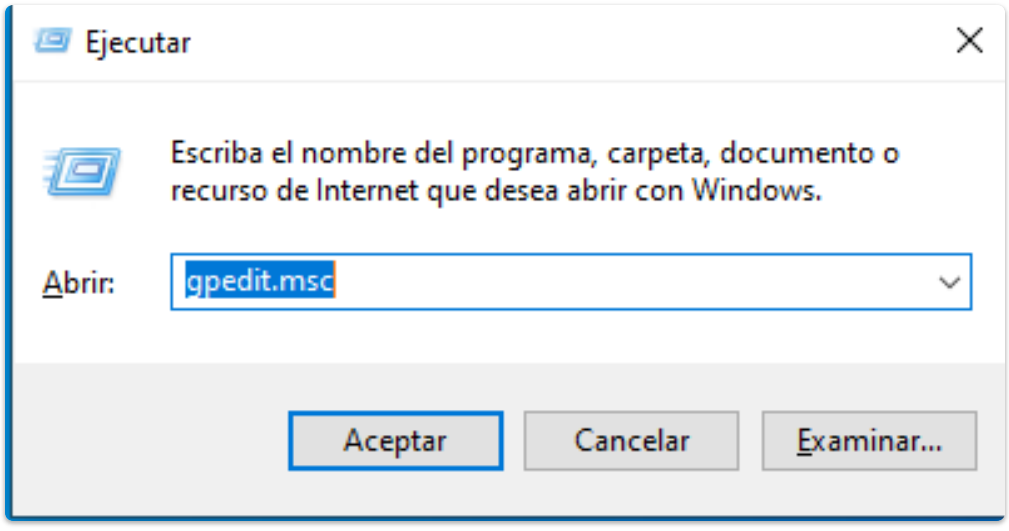
En este documento se detallará el proceso para restringir el acceso en un sistema Windows 10 (virtualizado en *VirtualBox*) a usuarios no privilegiados y aplicar filtros para que otros, dependiendo de su rol, sí puedan.

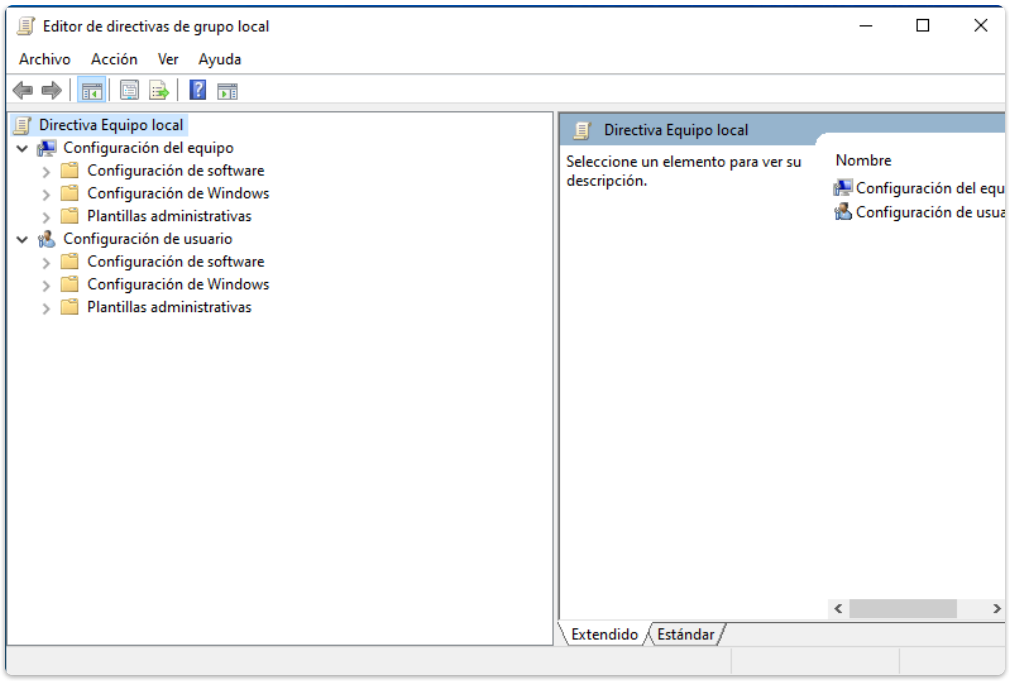
Se adjuntarán capturas y una breve descripción del proceso.

a. Restringir el Acceso a Dispositivo Extraíble

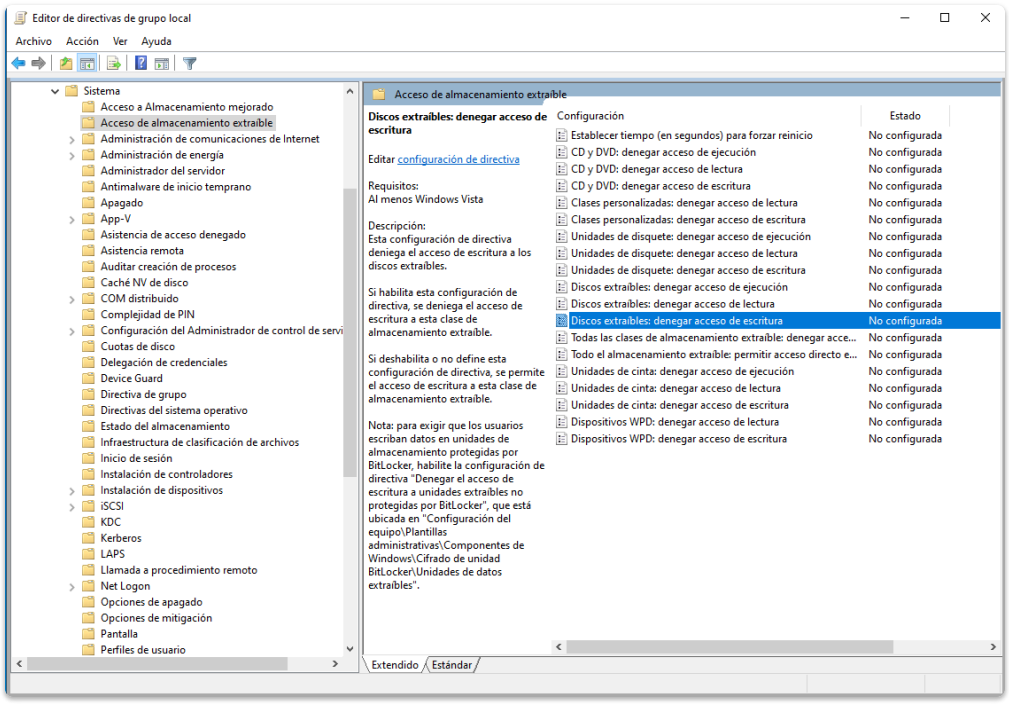
Se comienza restringiendo el acceso a todos los usuarios aplicando el principio de menor privilegio.

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

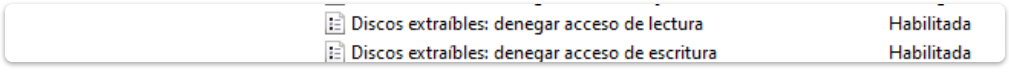




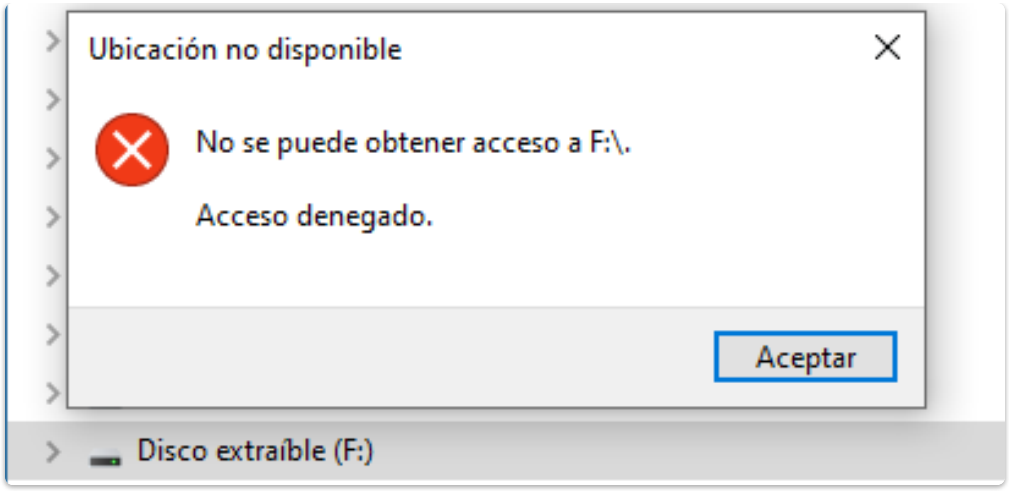
- A continuación se navega hacia las Políticas de Dispositivos Extraíbles en: `Configuración del equipo > Plantillas administrativas > Sistema > Acceso de almacenamiento extraíble` y se aplican las Políticas de Prohibición de Acceso a Dispositivos USB.



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



- 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.

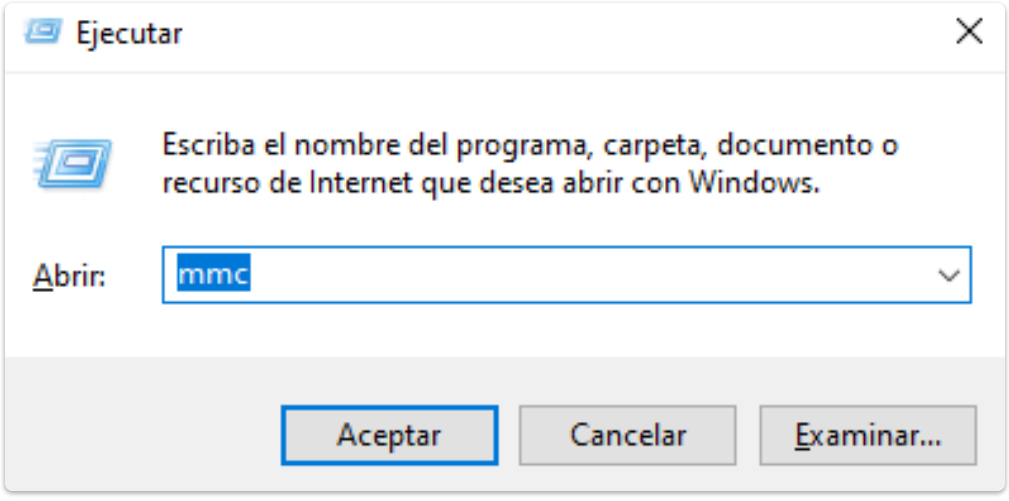
¿Por qué se utiliza en este caso? Aunque la herramienta estándar `gpedit.msc` permite editar las Políticas de Grupo Locales, tiene una limitación crítica: aplica la configuración de usuario a todas las cuentas del equipo (incluido administradores).

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".

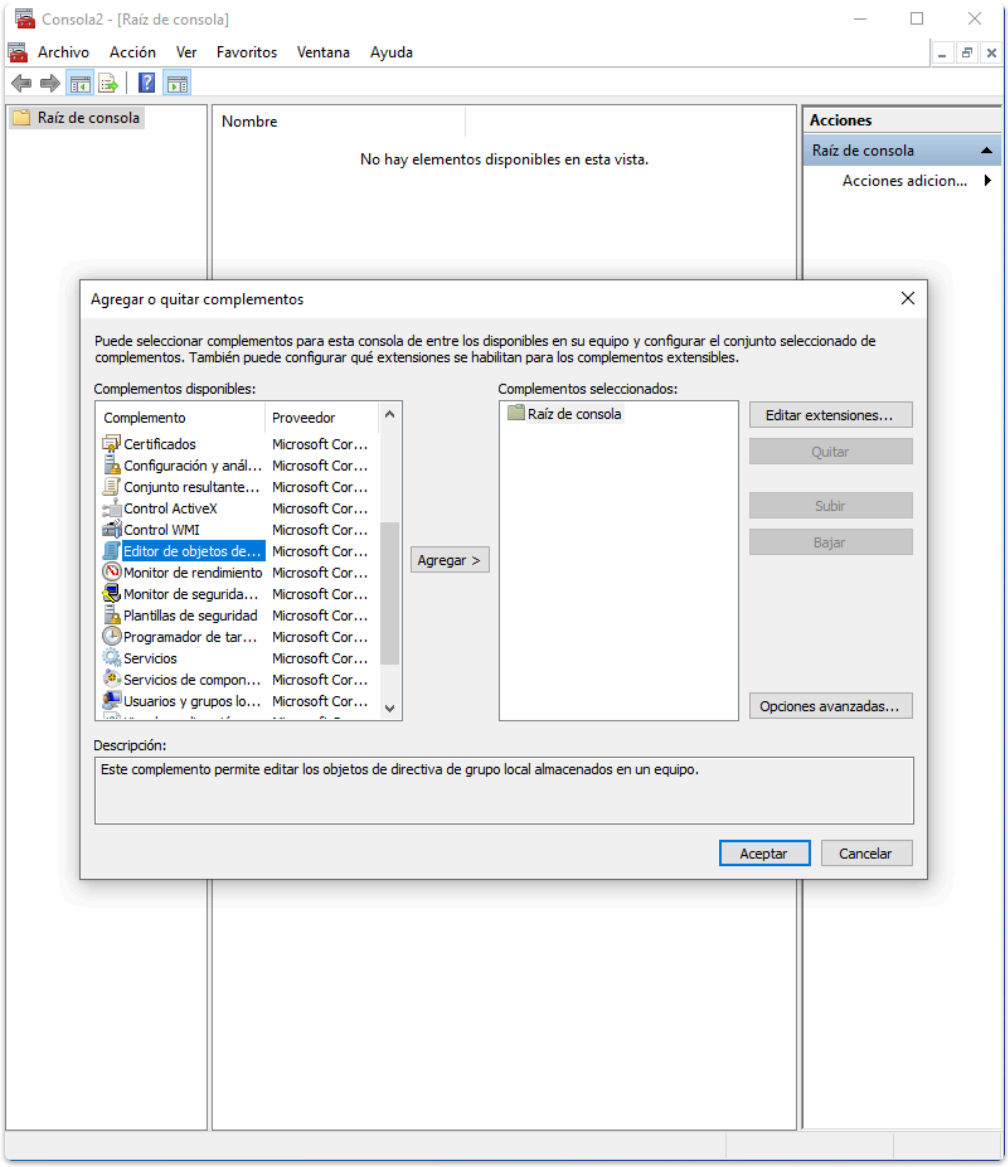
Procedimiento

1. Añadir Directiva de Grupo en MMC

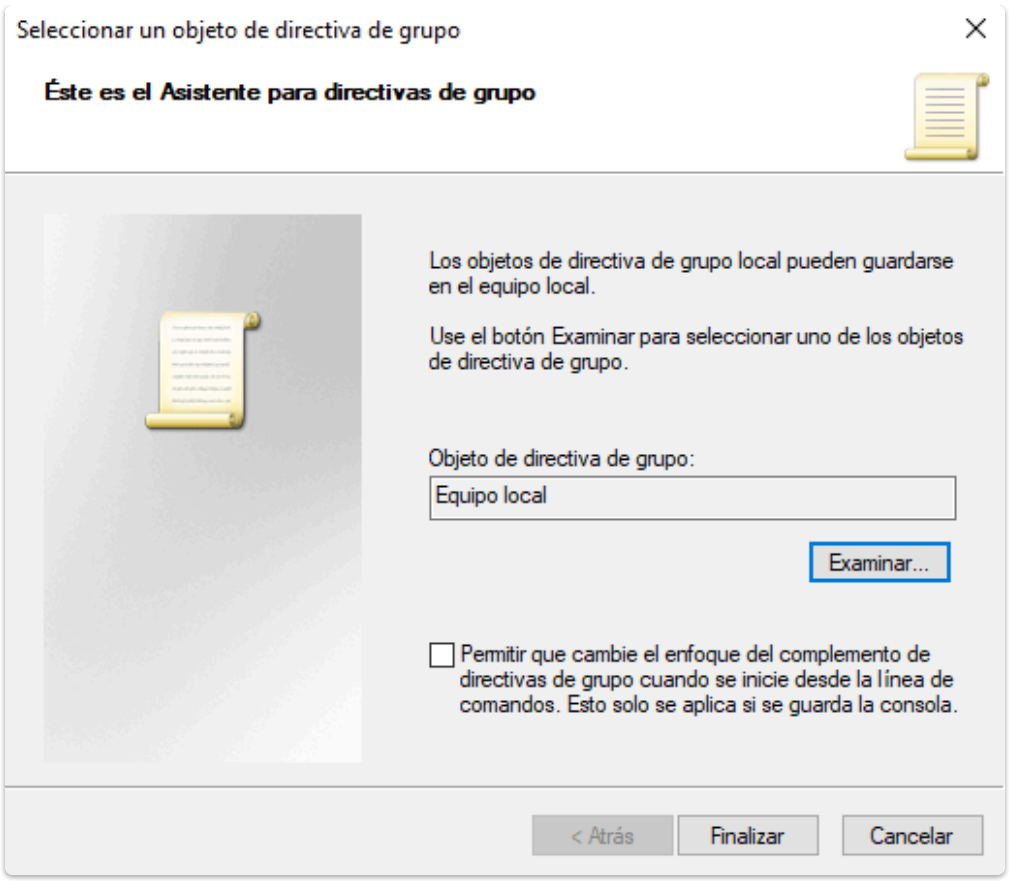
- Entramos en MMC a través de `Win + R`



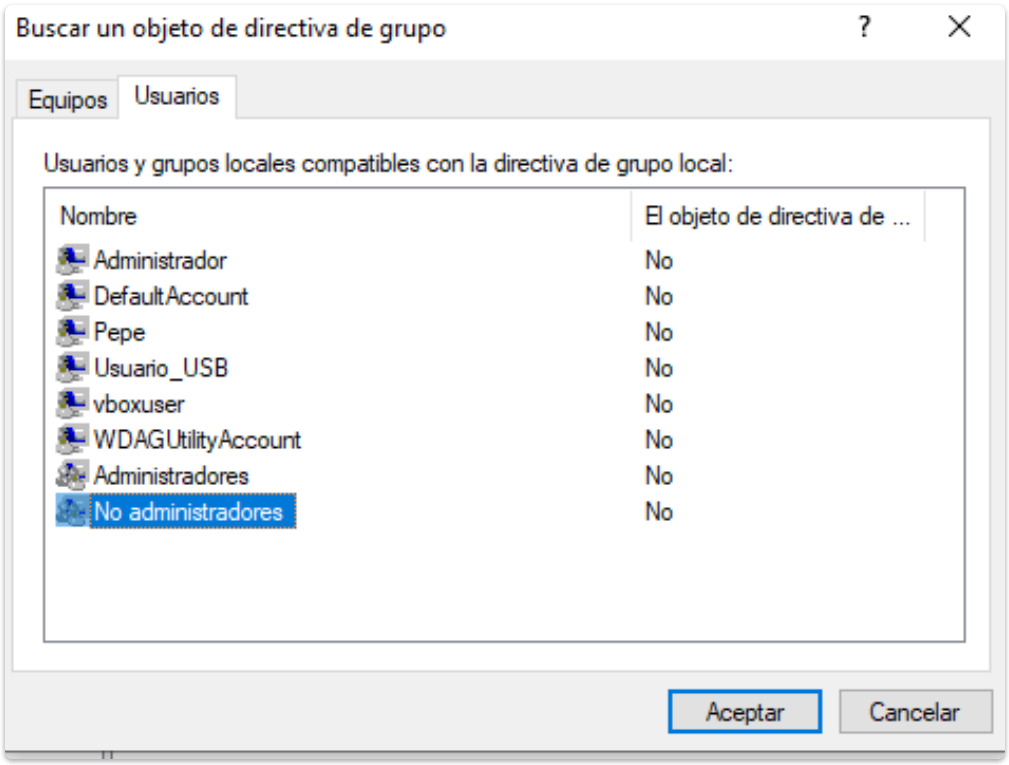
- Cargamos la herramienta en archivo y pinchando en `Agregar o quitar complemento` buscando la opción `Editor de objetos de directiva de grupo` y pinchando en agregar.



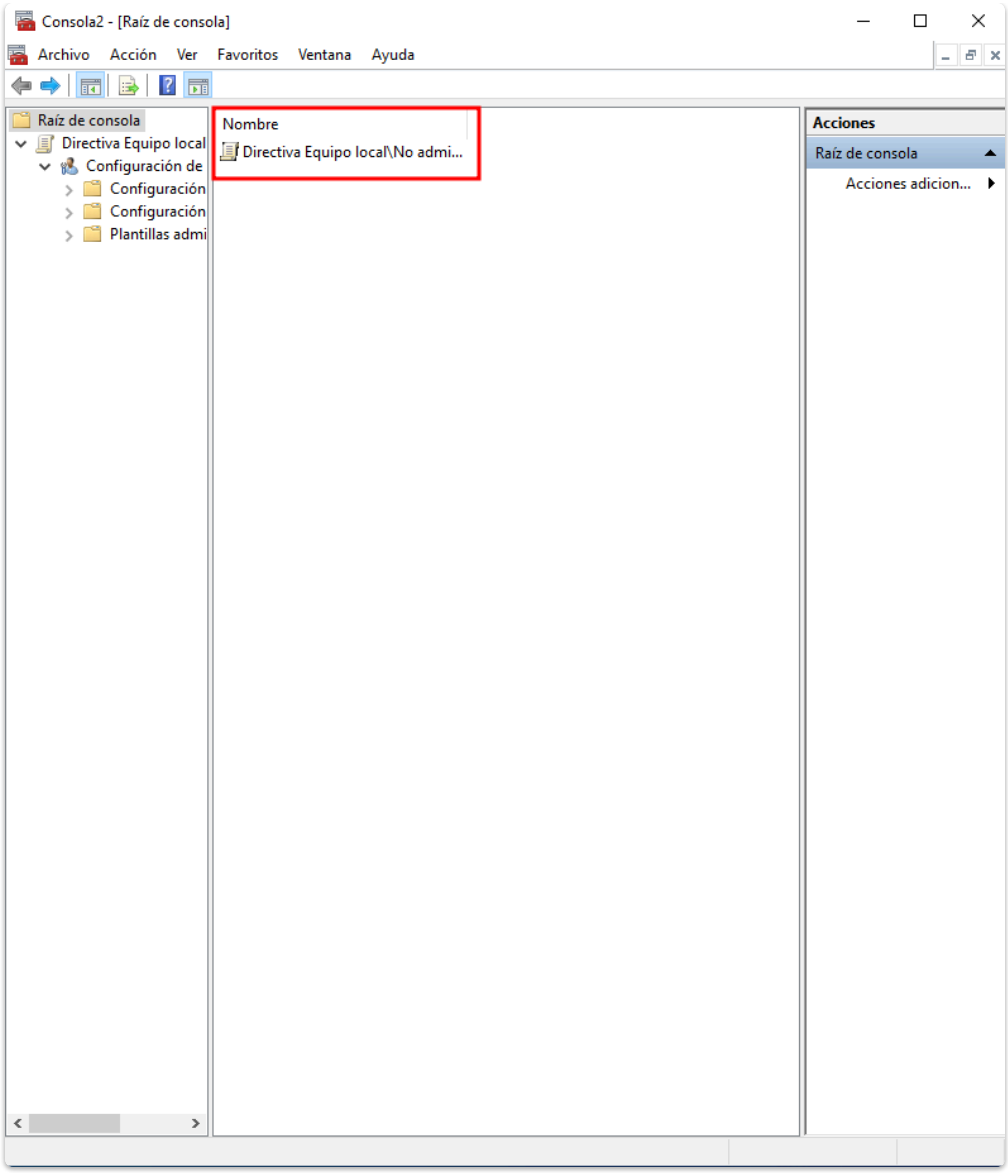
- En el menú que se abre, pinchamos en `Examinar`.



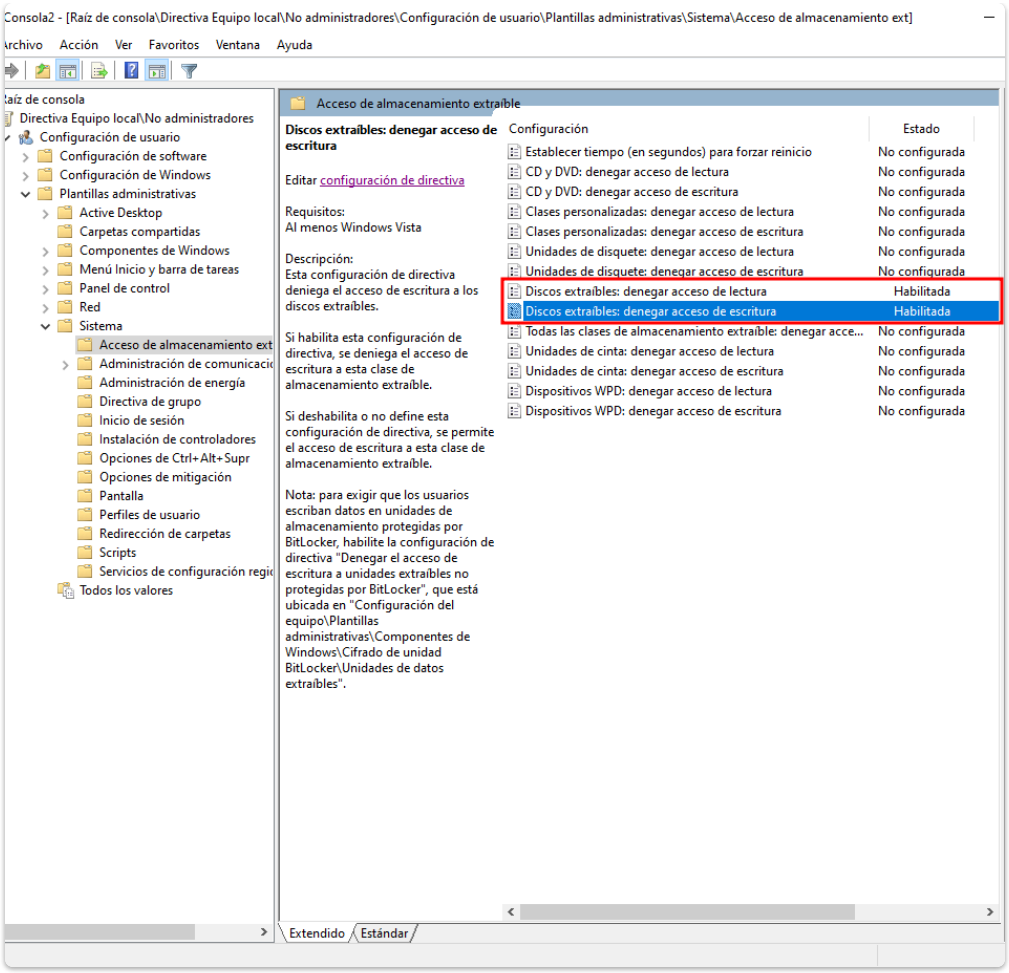
- Y una vez ahí, pinchamos en la pestaña `Usuarios` y seleccionamos "No administradores"



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

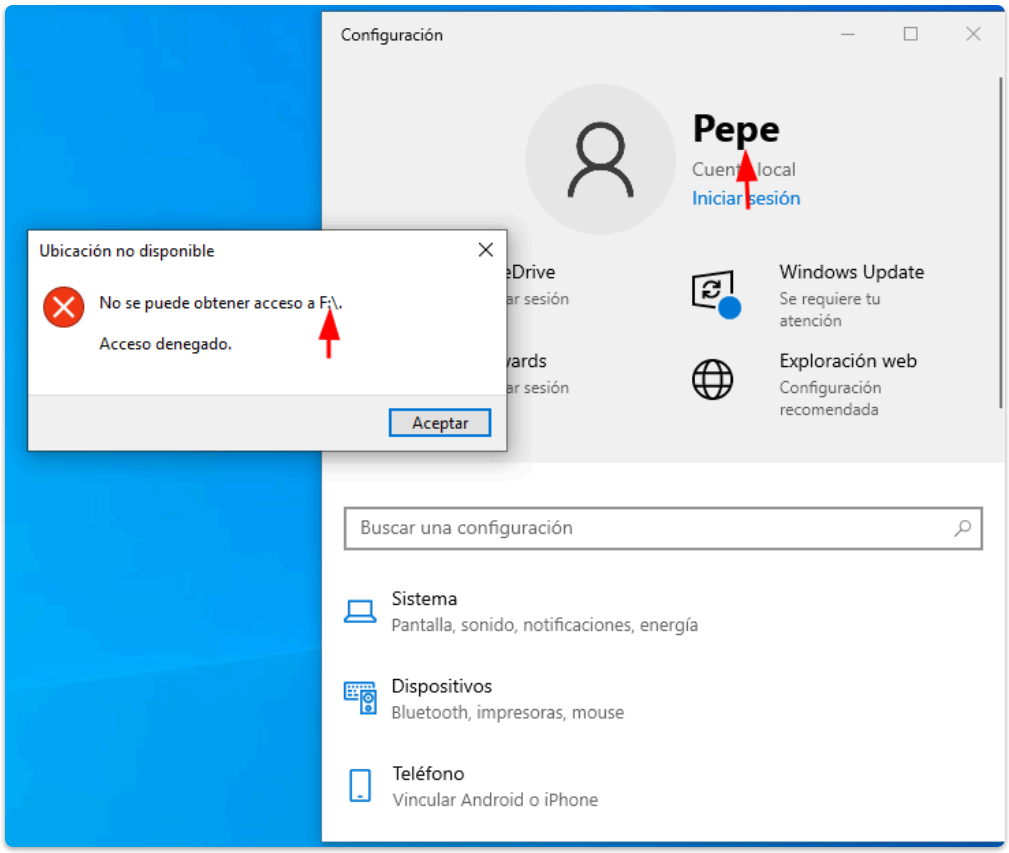


- Y como en `gpedit` buscamos en `Configuración del equipo > Plantillas administrativas > Sistema > Acceso de almacenamiento extraíble` y denegamos el permiso de *lectura* y *escritura*.



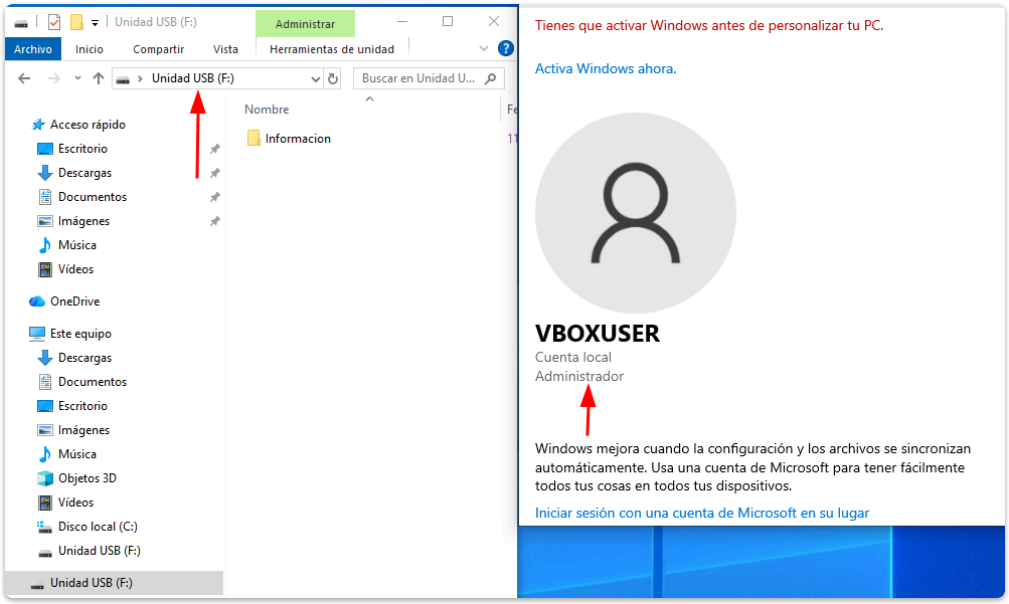
2. Comprobación

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.