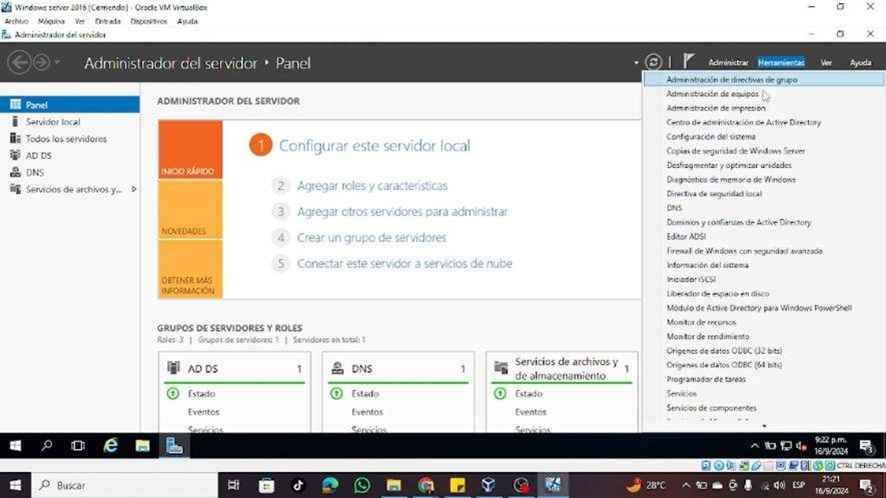
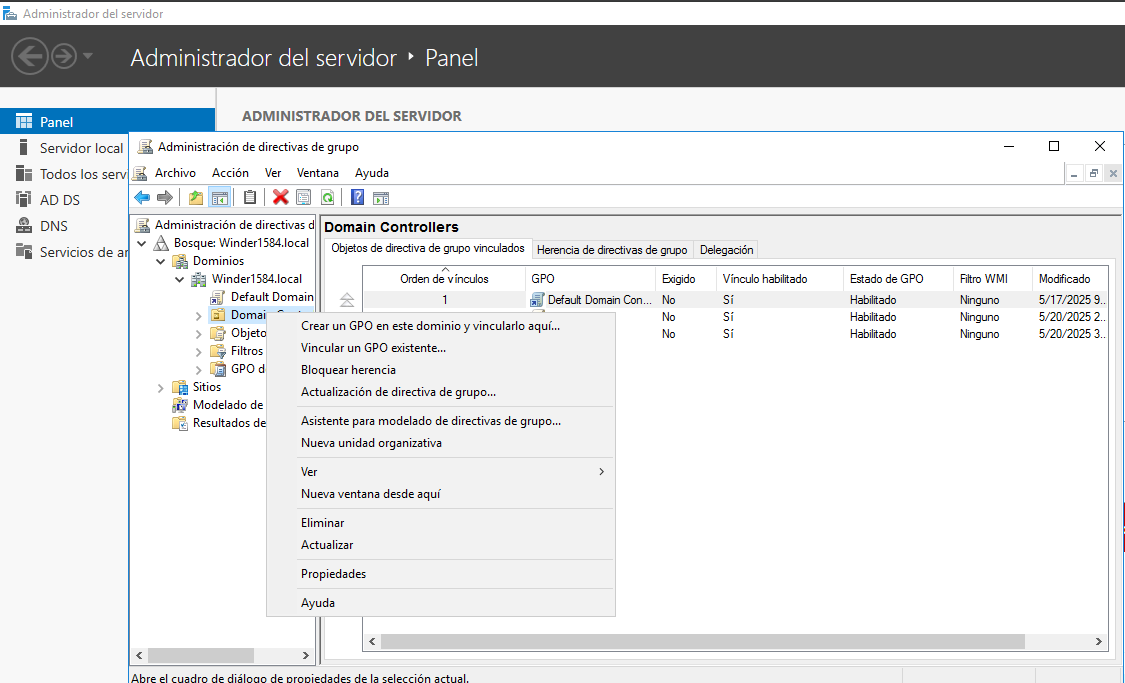
**Crear una GPO habilitando Credential Guard y desplegarla a los equipos del dominio.**

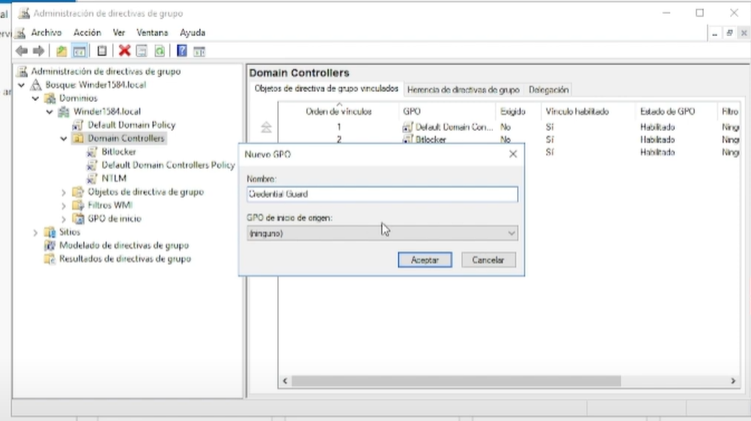
En el administrador del servidor los siguientes pasos > Herramientas Administrativas y luego Administración de Directivas de Grupo.



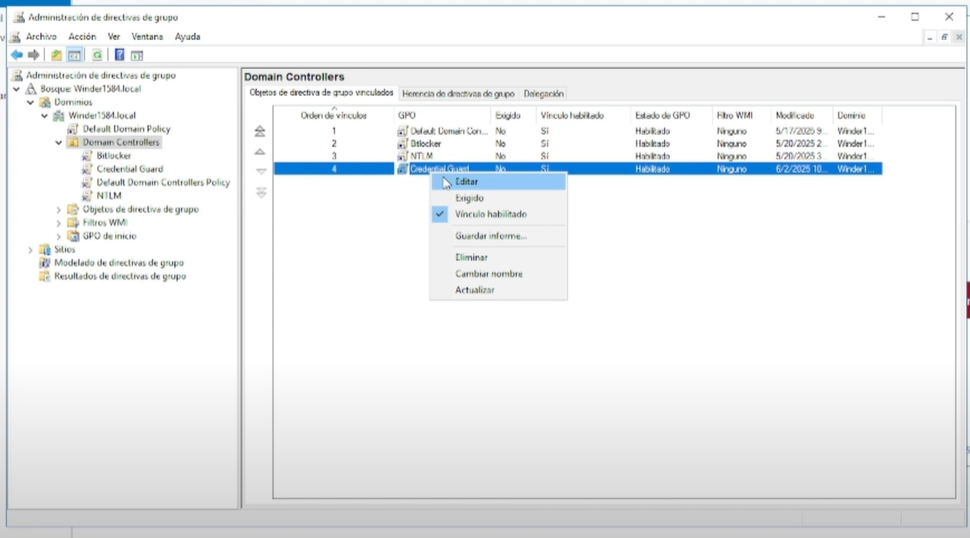
Dentro del Administración de Directivas de Grupo desplazamos el bosque y nos dirigimos hasta el dominio y damos clic derecho sobre el dominio para aplicar la política y selecciona Crear un GPO en este dominio.



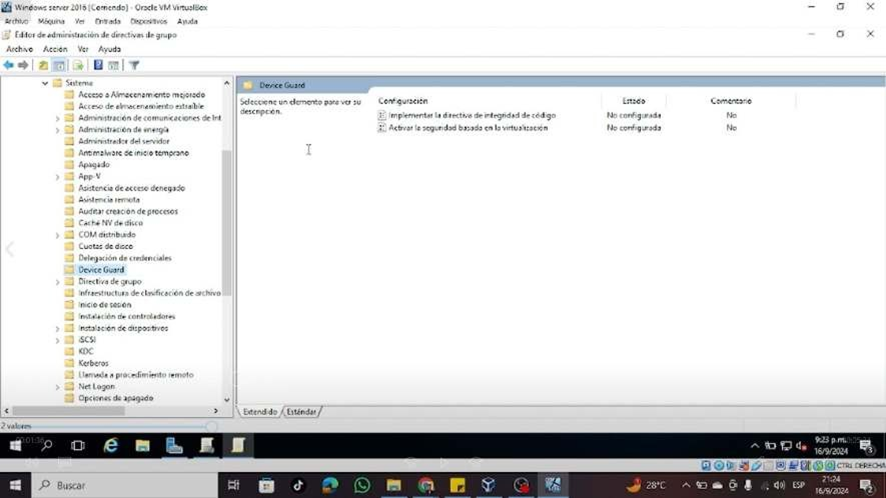
Se le asignará un nombre para poder distinguirla de las demás, por ejemplo, " Credential Guard".



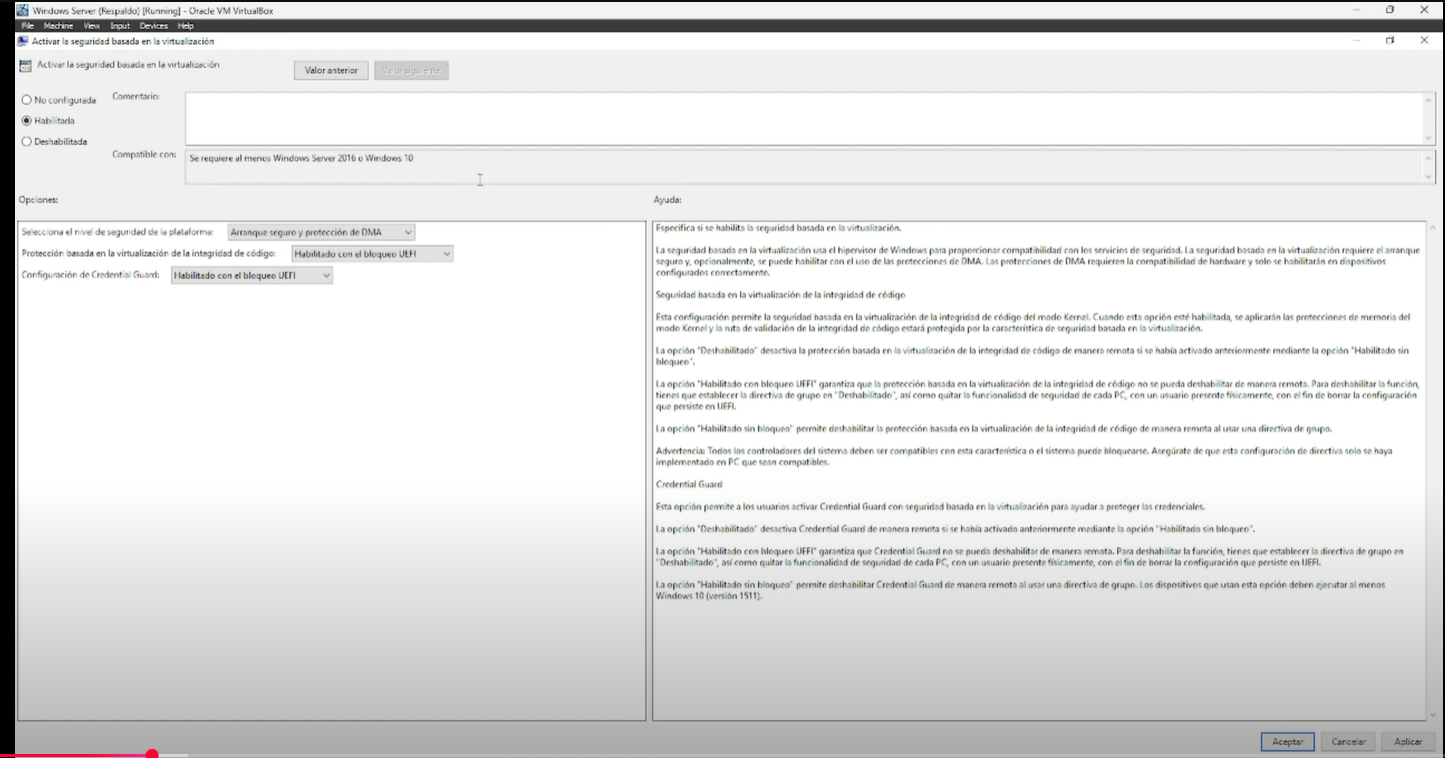
Haz clic derecho en la GPO creada y das clic en Editar.



Dentro de la GPO se realizan los siguientes pasos Directiva > Plantillas administrativas > Sistema > Device Guard.

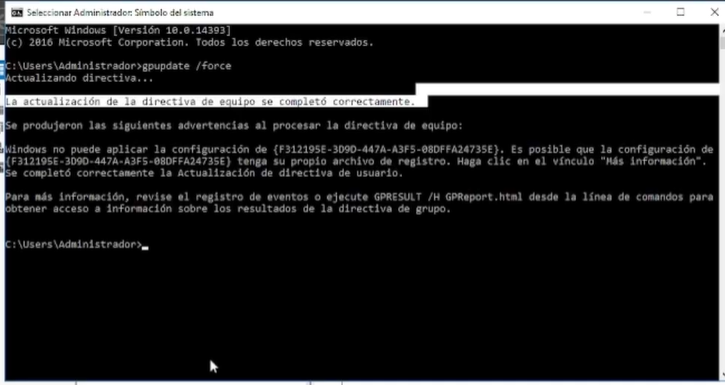


Selecciona la política de activar la seguridad basada en la virtualización y das clic en habilitar, luego habilitamos con el bloque UEFI en ambas casillas damos aplicar y aceptar



Ya con estos pasos está activado y configurado el credential guard para todos los equipos que estén dentro del dominio.

Actualizamos lo que son las directivas



**Añadir ejemplos de uso y abundar sobre los ataques “pass the hash”**

## **¿Qué es un ataque *Pass the Hash*?**

Un ataque **Pass the Hash (PtH)** es una técnica utilizada por atacantes para autenticarse en sistemas remotos utilizando el **hash de una contraseña** en lugar de la contraseña en texto claro. No necesitan descifrar la contraseña; simplemente aprovechan el hecho de que los sistemas aceptan el hash como una forma válida de autenticación.

### **¿Cómo funciona?**

1. **Obtención del hash**: El atacante compromete un sistema (por ejemplo, con malware o vulnerabilidades locales) y extraer los hashes de contraseñas almacenados, por ejemplo, desde el archivo SAM en Windows o de la memoria del sistema.
2. **Uso del hash**: Utilizando herramientas especializadas, el atacante se autentica en otros sistemas de la red (por ejemplo, a través de SMB o RDP), usando el hash como si fuera la contraseña.
3. **Movimiento lateral**: Una vez dentro, el atacante puede repetir el proceso para escalar privilegios o propagarse por la red.

**Ejemplos de Uso de *Pass the Hash***

**Mimikatz** es una herramienta común para extraer hashes en sistemas Windows.

privilege::debug

sekurlsa::logonpasswords

Este comando puede mostrar los hashes de sesión activos, incluyendo NTLM hashes.

Luego, con herramientas como **PsExec** modificadas o **Impacket**, se puede usar el hash directamente:

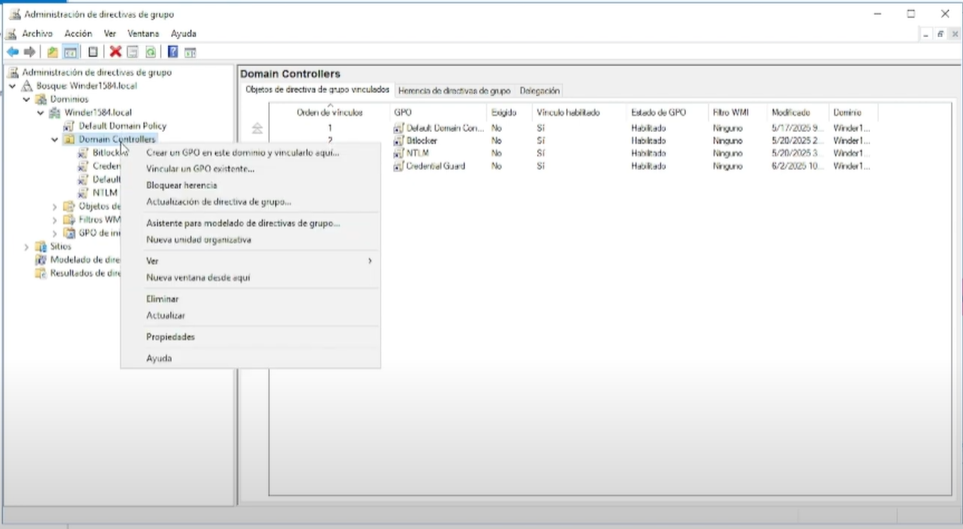
psexec.py -hashes :aad3b435b51404eeaad3b435b51404ee:25d55ad283aa400af464c76d713c07ad Administrator@victima.local

## **Prevención y Mitigación**

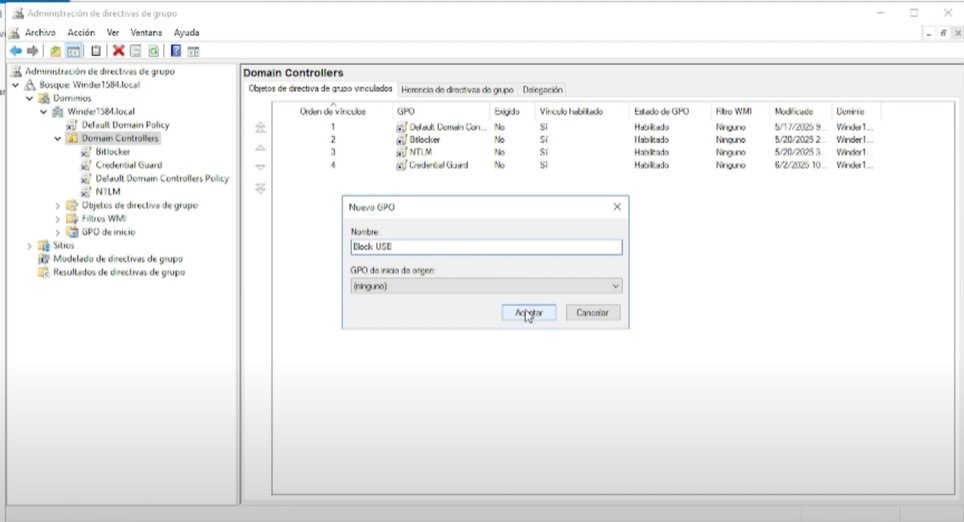
1. **Usar autenticación moderna**: Implementar **Kerberos** y deshabilitar NTLM si es posible.
2. **Habilitar LSA Protection**: Protege procesos críticos del sistema como lsass.exe.
3. **Evitar sesiones de administrador innecesarias**: Menos privilegios significa menor riesgo de extracción de hashes útiles.

**Crear una GPO que bloquee el acceso de los dispositivos de almacenamiento USB.**

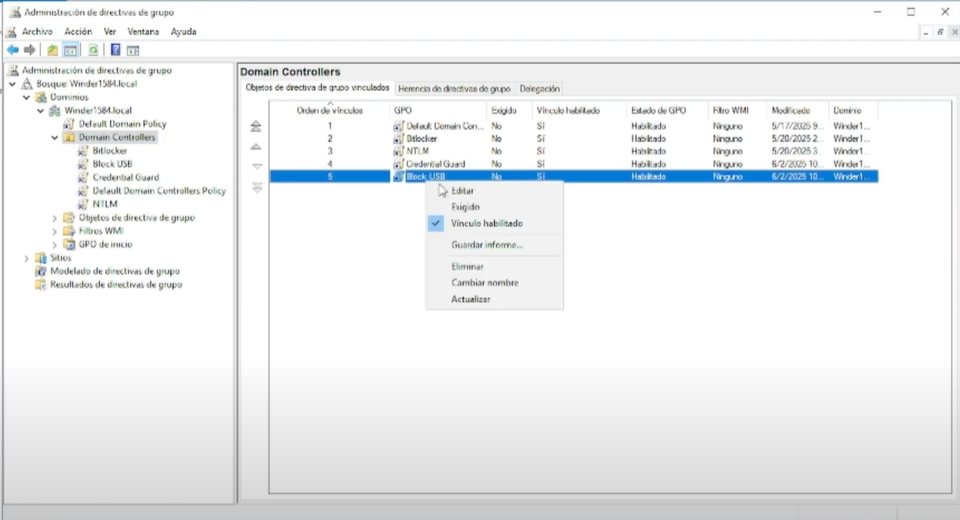
En el mismo Administrador de Directivas de Grupo donde se creó la anterior GPO, haz clic en el dominio y selecciona Crear un GPO en este dominio y enlazarlo aquí.



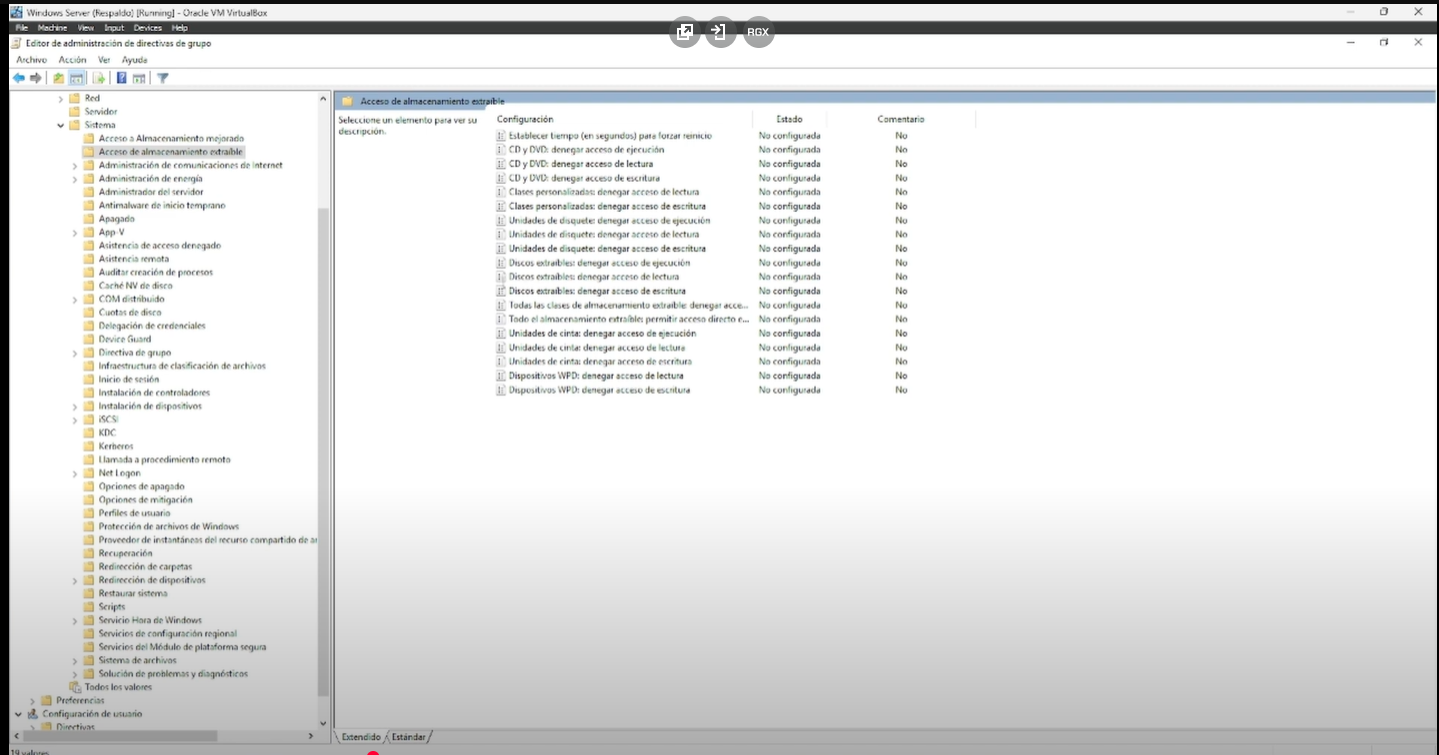
Se le asignará un nombre descriptivo para poder distinguirla de las demás, por ejemplo, "BlockUSB".



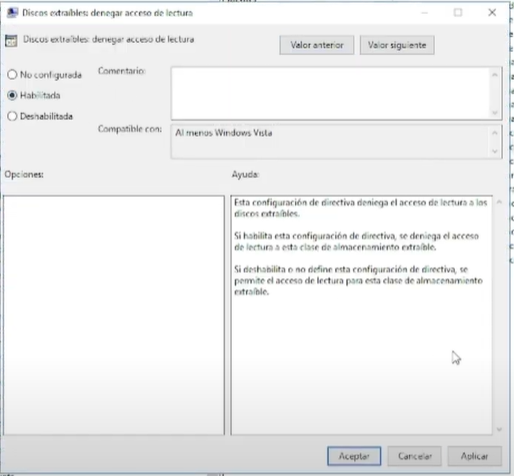
Clic derecho en la GPO creada y damos clic en Editar.



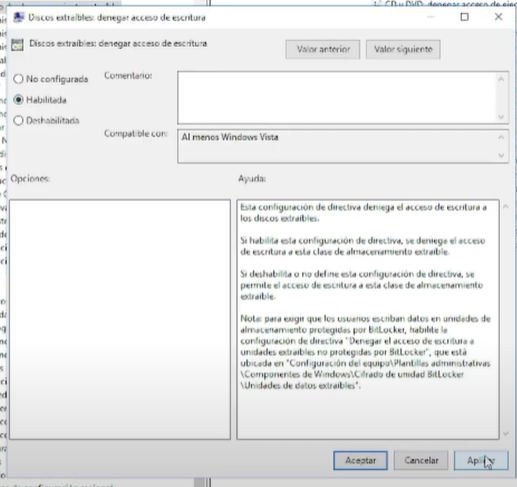
Dentro de la GPO se realizan los siguientes pasos Directiva > Plantillas administrativas > Sistema > Acceso de almacenamiento extraíble.



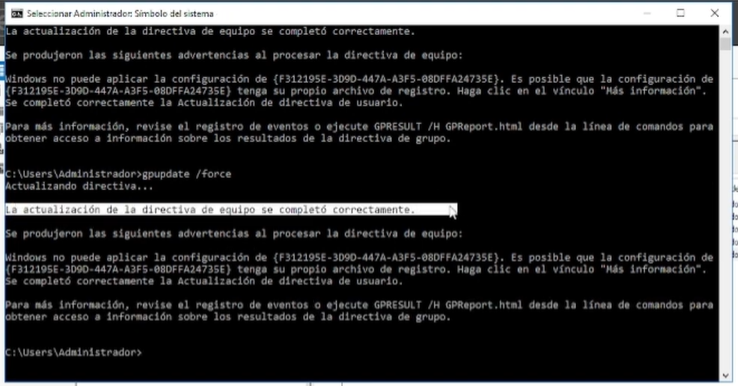
Buscamos la opción "Discos extraíbles: Denegar el acceso lectura" y damos clic en habilitar, luego aplicar y por último aceptar



Buscamos la opción "Discos extraíbles: Denegar el acceso escritura" y damos clic en habilitar, luego aplicar y por último aceptar



Actualizamos lo que son las directivas nuevamente



Ya con esto pasos está activado y configurado el bloqueo a los dispositivos extraíble USB para todos los equipos que estén dentro del dominio