

Políticas de Seguridad DLP.

INDICE

1.	Objetivo General:	2
2.	Parte 1: Creación de Políticas de Seguridad DLP:	2
I.	Introducción al DLP	2
II.	Clasificación de Datos	2
i)	Datos Públicos	2
ii)	Datos Internos.....	2
iii)	Datos Sensibles o Confidenciales	3
III.	Acceso y Control	3
i)	Políticas de acceso	3
ii)	Flujo de revisión de permisos	3
IV	Monitoreo y Auditoría	4
i)	Reglas de Monitoreo	4
ii)	Reglas de Auditoría.....	4
iii)	Herramientas de Monitoreo y Auditoría	4
V	Prevención de Filtraciones	5
i)	Cifrado de la información	5
ii)	Herramientas de DLP (Data Loss Prevention)	5
VI	Educación y Concientización	5
3.	Parte 2: Implementación de Políticas de Restricción de Dispositivos USB	6
I.	Configuración de la máquina virtual Windows 10 para acceso a dispositivo USB	6
II.	Restricción de Dispositivos USB en Windows 10 (máquina virtual)	7
III.	Validación y prueba de la restricción de USB	8
IV.	Creación y prueba de un usuario regular	8
V.	Habilitación de excepciones para usuarios específicos	10

Políticas de Seguridad DLP

1. Objetivo General:

Parte 1: Definir y establecer políticas de DLP que ayuden a proteger la información confidencial.

Parte 2: Implementar medidas específicas, como la **restricción del uso de dispositivos USB**, para asegurar que las políticas de DLP se apliquen en la práctica.

2. Parte 1: Creación de Políticas de Seguridad DLP:

I. Introducción al DLP

Hoy en día la protección de los datos se ha convertido en una prioridad estratégica para las organizaciones. La Prevención de Pérdida de Datos (DLP), es un conjunto de tecnologías, políticas y procesos que se diseñan para detectar, monitorear y proteger la información sensible contra accesos no autorizados, fugas accidentales o exfiltraciones maliciosas, asegurando que solo circulen por canales seguros y autorizados.

La importancia del DLP dentro de una organización radica en su capacidad de reducir riesgos operativos, legales y reputacionales asociados a incidentes de fuga de información.

En definitiva, el DLP se posiciona como un componente esencial dentro de una estrategia integral de ciberseguridad, ya que protege los datos confidenciales que son uno de los activos más valiosos de cualquier organización.

II. Clasificación de Datos

La organización clasifica los datos en función de su sensibilidad, de acuerdo a lo siguiente:

i) Datos Públicos

En este caso la organización define que estos datos los puede divulgar libremente sin que esto le genere riesgos operativos, financieros o reputacionales. Esta información puede estar destinada a ser compartida con clientes, proveedores y con la comunidad en general.

Esta información podría ser comunicados de prensa, material de marketing o la información contenida en su sitio web corporativo.

De acuerdo a lo anterior los datos públicos requieren un nivel mínimo de protección, aunque deben mantenerse actualizados y verificados para garantizar la imagen de la organización.

ii) Datos Internos

En este caso la organización define este tipo de información como uso exclusivo dentro de la organización, limitándose a empleados o colaboradores autorizados.

Si bien su filtración no tendría un impacto catastrófico, si podría ocasionar algunos inconvenientes como afectar la eficiencia operativa o exponer procesos internos.

Esta información podría estar constituida por manuales de procedimientos, políticas internas, reportes de desempeño, organigramas y documentación administrativa en general.

Por lo anterior estos datos deben gestionarse con medidas de control de acceso y no deben compartirse fuera de la organización.

iii) Datos Sensibles o Confidenciales

En este caso la información es la más crítica para la organización, cuya divulgación no autorizada podría causar, graves daños en términos legales, financieros o reputacionales.

Este grupo de información contendría datos personales de clientes y empleados, información financiera, propiedad intelectual, proyectos estratégicos, credenciales de acceso y contratos confidenciales.

Por lo anterior, dado su alto nivel de riesgo, requieren un manejo estricto mediante cifrado, políticas de acceso con privilegios mínimos, monitoreo constante (podría ser con DLP) y medidas adicionales como acuerdos de confidencialidad.

III. Acceso y Control

En el acceso y control la organización aplicará el Principio del Mínimo Privilegio, estableciendo políticas de acceso y definiendo el flujo de revisión de permisos, indicando qué roles dentro de la organización serán responsables de estas revisiones y cómo se llevarán a cabo. De esta manera se garantizará que cada usuario, sistema o proceso tenga únicamente los permisos estrictamente necesarios para desempeñar sus funciones, sin acceso adicional a información que no sean indispensables, de esta manera, se minimiza el riesgo de fugas de datos, uso indebido o acceso no autorizados.

i) Políticas de acceso

- **Asignación mínima necesaria:** El acceso se otorga solo a los recursos que un usuario requiere para cumplir su rol.
- **Segregación de funciones:** Evitar que un mismo usuario concentre permisos que podrían generar conflictos de interés.
- **Control periódico de permisos:** Los accesos deben revisarse de forma regular para verificar que sigan siendo adecuados al rol y funciones del usuario.
- **Revocación inmediata:** Cuando un empleado cambia de puesto o deja la organización, sus permisos se eliminan o ajustan de forma inmediata.

ii) Flujo de revisión de permisos

- **Solicitud de acceso:** El usuario solicita el acceso a través de un sistema formal.
- **Aprobación inicial:** El jefe directo valida la necesidad del acceso y aprueba la solicitud.
- **Asignación técnica:** El área de TI o Seguridad asigna los permisos conforme a la política de menor privilegio.
- **Revisión periódica:**
 - **Responsables:**
 - **Jefes de área:** Son los que validan que los permisos de sus equipos sean acordes a las funciones actuales.
 - **Área de Seguridad de la Información:** Es la responsable de supervisar que los accesos cumplan con políticas y normativas internas/externas.

- **Área de TI:** Es la responsable de ejecutar los ajustes técnicos necesarios.
- **Periodicidad:** Las revisiones se realizarán al menos cada 6 meses o ante cambios de rol.
- **Auditoría:** Los resultados de las revisiones se documentan y se mantienen disponibles para auditorías internas y externas.

IV Monitoreo y Auditoría

La organización establecerá reglas claras para el monitoreo continuo de los datos sensibles y la auditoría sistemática de todas las actividades relacionadas con su uso, con el fin de prevenir accesos indebidos, detectar anomalías y garantizar el cumplimiento de normativas de seguridad y privacidad.

i) Reglas de Monitoreo

- **Supervisión de accesos:** Todos los intentos de acceso a datos sensibles deben ser registrados, indicando usuarios, fecha, hora y recurso accedido.
- **Detección de anomalías:** Se generarán alertas ante comportamientos inusuales, como accesos fuera de horario laboral, múltiples intentos fallidos o descargas masivas de información.
- **Control de canales de salida:** El monitoreo abarcará el uso de correos electrónicos, dispositivos extraíbles, servicios en la nube y colas de impresión para detectar movimientos de datos sensibles no autorizados.
- **Conservación de registros:** Los logs se almacenarán de manera centralizada y protegida durante un período definido para permitir análisis forense en caso de incidentes.

ii) Reglas de Auditoría

- **Auditorías periódicas:** Se realizarán revisiones trimestrales para evaluar la efectividad de los controles, la pertinencia de los accesos y la integridad de los registros.
- **Trazabilidad completa:** Cada evento relacionado con datos sensibles debe ser trazable desde el usuario que lo originó hasta la acción ejecutada.
- **Separación de funciones:** El área de Seguridad de la Información revisará los registros, mientras que TI se encargará de la administración técnica de las herramientas.
- **Cumplimiento normativo:** Las auditorías estarán alineadas con marcos como ISO/IEC27001, GDPR o normativas locales de protección de datos.

iii) Herramientas de Monitoreo y Auditoría

- **DLP (Data Loss Prevention):** Controlará el movimiento de información sensible dentro y fuera de la organización, generando alertas en caso de intentos de fuga por correo electrónico, USB, servicios en la nube o impresoras.
- **SIEM (Security Information and Event Management):** Herramientas como Splunk, QRadar o ELK Stack centralizarán los registros de sistemas, redes y aplicaciones, permitiendo correlacionar eventos y detectar incidentes de seguridad en tiempo real.
- **EDR (Endpoint Detection and Response):** Complementará la visibilidad al monitorear las actividades en estaciones de trabajo y servidores, detectando accesos indebidos o procesos maliciosos.

- **Sistemas de auditoría interna:** Herramientas de gestión de identidades (Identity and Access Management, IAM) se usarán para revisar asignaciones de permisos y cambios de roles.

V Prevención de Filtraciones

La organización evitará la filtración de datos sensibles, utilizando tecnologías como el cifrado y herramientas de DLP.

i) Cifrado de la información

- Todos los datos sensibles almacenados en servidores, base de datos y dispositivos portátiles estarán protegidos mediante cifrado fuerte.
- La transmisión de información a través de redes internas y externas se realizará mediante protocolos seguros como TLS o VPN, garantizando la confidencialidad en tránsito.
- El uso de cifrado en dispositivos móviles y portátiles será obligatorio, de modo que la pérdida o robo de equipos no exponga información crítica.

ii) Herramientas de DLP (Data Loss Prevention)

- Se aplicarán soluciones DLP para monitorear, clasificar y controlar el movimiento de información sensible dentro y fuera de la organización.
- El sistema generará alertas o bloqueará automáticamente intentos de compartir datos confidenciales a través de correo electrónico, almacenamiento en la nube, dispositivos extraíbles o impresiones no autorizadas.
- Las reglas de DLP estarán alineadas a las categorías de clasificación de datos previamente definidos (públicos, internos, sensibles o confidenciales).

VI Educación y Concientización

La seguridad de la información también depende del comportamiento del personal, por ello la organización implementará un programa continuo de educación y concientización que asegure que todos los empleados comprendan las políticas de seguridad y los riesgos asociados al manejo de datos sensibles.

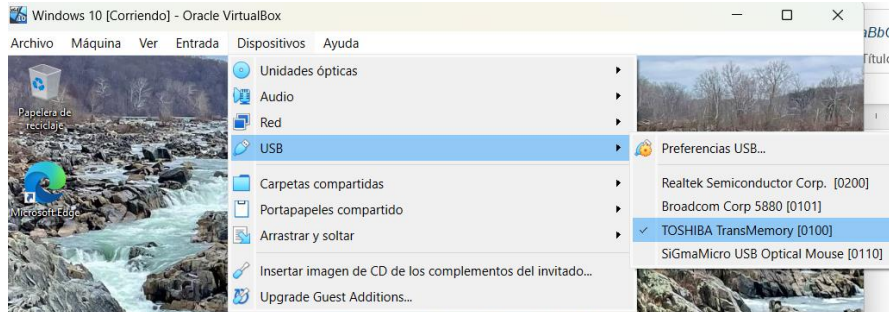
- Inducción Inicial: Todo nuevo colaborador recibirá una capacitación obligatoria sobre políticas de seguridad.
 - Capacitación Periódica: Se impartirán cursos y talleres semestralmente para actualizar al personal sobre nuevas amenazas y cuando corresponda en el caso de nuevas políticas.
 - Comunicación interna: Se distribuirán boletines electrónicos y carteles informativos en áreas comunes para reforzar los mensajes claves de seguridad.
- iv) Evaluación y Mejora continua:** Se aplicarán evaluaciones cortas después de cada sesión de capacitación para medir la comprensión, revisando los resultados y ajustando los contenidos en función de las necesidades detectadas.

3. Parte 2: Implementación de Políticas de Restricción de Dispositivos USB

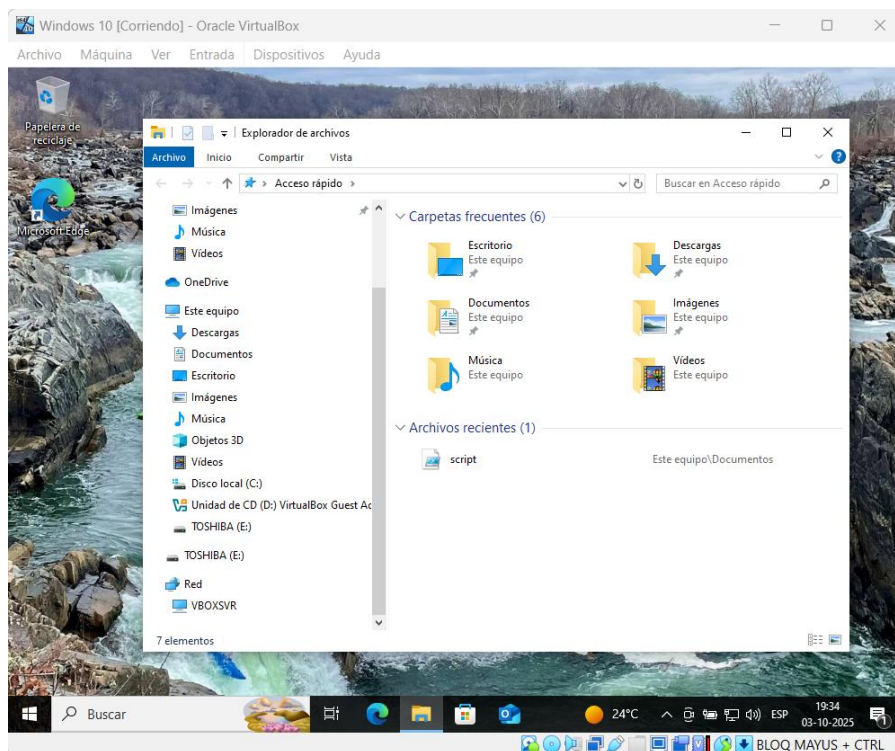
Esta parte consiste en la implementación de políticas de restricción del uso de **dispositivos USB**. Estas restricciones son esenciales para evitar la filtración de datos confidenciales por medio de dispositivos de almacenamiento removibles. Esta política está directamente vinculada a las políticas de DLP creadas en la primera parte del ejercicio.

Esta práctica estará enfocada en la máquina virtual Windows 10.

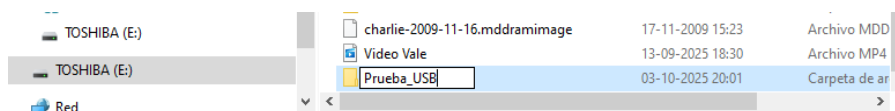
I. Configuración de la máquina virtual Windows 10 para acceso a dispositivo USB



El USB conectado es la unidad E:, como se muestra a continuación:



Se crea una nueva carpeta en el USB:

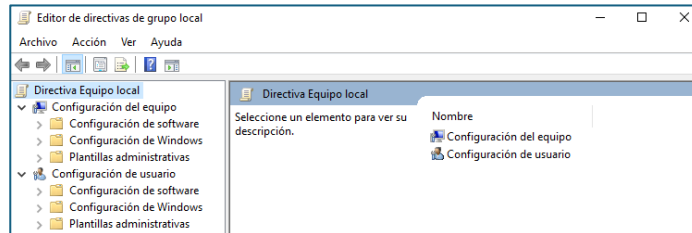


> Unidad de CD (D:) VirtualBox Guest Ac	Protocolo de Transferencia	09-09-2016 10:11	Carpeta de a
> TOSHIBA (E:)	Planos 14004	11-12-2023 16:12	Carpeta de a
> TOSHIBA (E:)	Programas	13-10-2015 15:42	Carpeta de a
	Prueba_USB	03-10-2025 20:01	Carpeta de a
	Python para Procesamiento de Datos	28-06-2021 19:54	Carpeta de a

II. Restricción de Dispositivos USB en Windows 10 (máquina virtual)

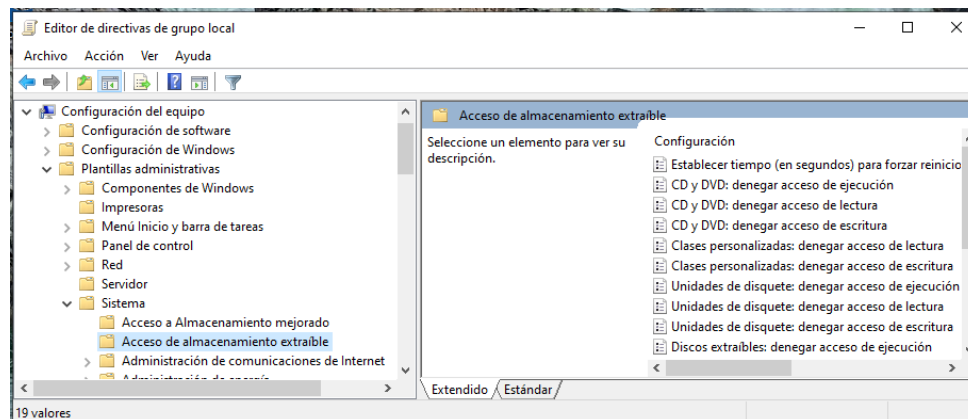
- Abrir el Editor de Políticas de Grupo (Group Policy Editor) → win +R

Escribir: *gpedit.msc* Enter



- Navegar a las Políticas de Dispositivos Removibles

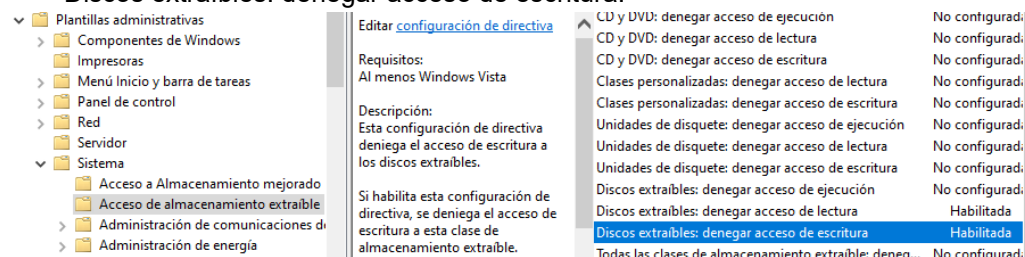
Configuración del equipo > Plantillas administrativas > Sistema > Acceso de almacenamiento removable



- Configurando la Política de Prohibición de Acceso a Dispositivos USB.

Para evitar que los usuarios puedan leer o escribir en dispositivos USB conectados se activarán las siguientes políticas:

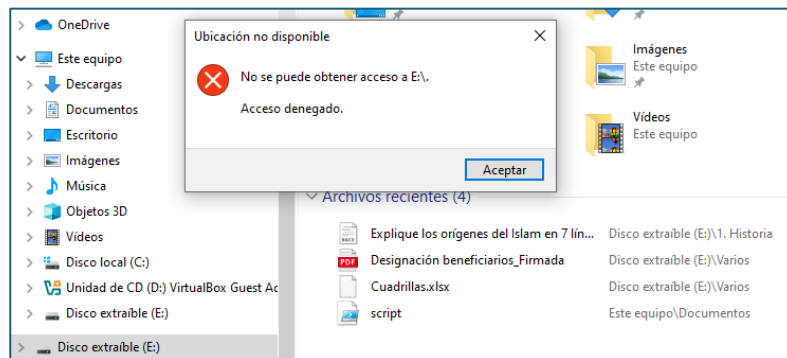
- Discos extraíbles: denegar acceso de lectura.
- Discos extraíbles: denegar acceso de escritura.



- Se reiniciará la máquina virtual Windows10 para que se apliquen los cambios.

III. Validación y prueba de la restricción de USB

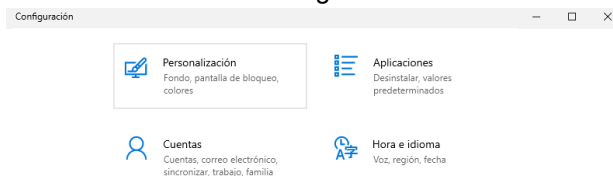
- i) **Prueba de Restricción de USB.** Ahora se verá si se puede acceder a un dispositivo USB, para lo cual se conectará un dispositivo USB a la máquina virtual Windows10 y se intentará acceder al dispositivo desde una cuenta de usuario estándar (sin privilegios administrativos).
- ii) **Verificando la Restricción de Acceso.** Si las políticas están correctamente configuradas, los usuarios estándar no podrán acceder al dispositivo USB.



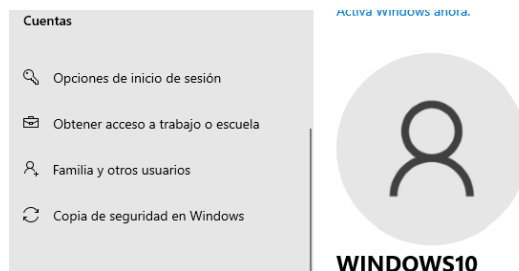
Como se puede ver las políticas las políticas de denegación están correctamente configuradas. Aparece el mensaje de “Acceso denegado”.

IV. Creación y prueba de un usuario regular

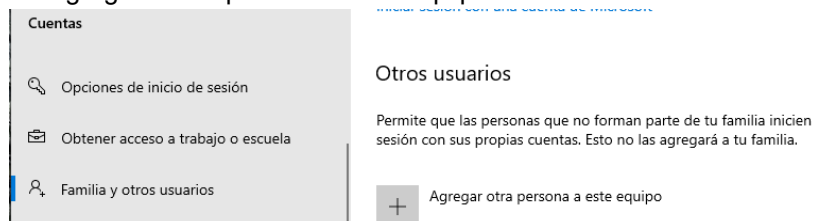
- i) Crear un nuevo usuario regular en Windows.



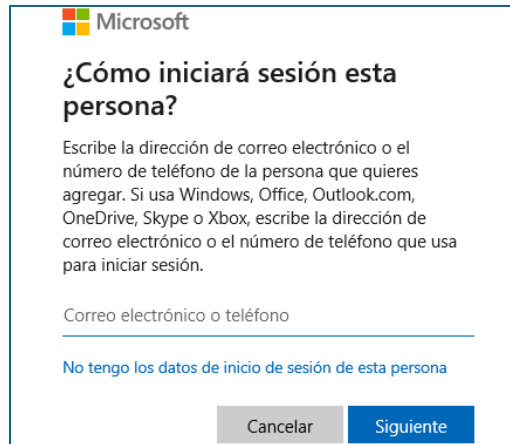
Cuentas > Familia y otros usuarios



- ii) **Agregar a otra persona a este equipo**



Seleccionar “No tengo los datos de inicio de sesión de esta persona”



Microsoft

¿Cómo iniciará sesión esta persona?

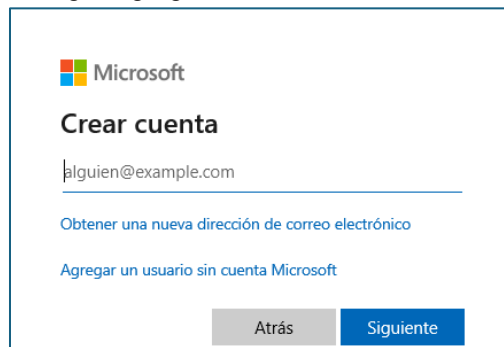
Escribe la dirección de correo electrónico o el número de teléfono de la persona que quieres agregar. Si usa Windows, Office, Outlook.com, OneDrive, Skype o Xbox, escribe la dirección de correo electrónico o el número de teléfono que usa para iniciar sesión.

Correo electrónico o teléfono

[No tengo los datos de inicio de sesión de esta persona](#)

Cancelar **Siguiente**

Y luego “Agregar un usuario sin cuenta de Microsoft”



Microsoft

Crear cuenta

alguien@example.com

[Obtener una nueva dirección de correo electrónico](#)

[Agregar un usuario sin cuenta Microsoft](#)

Atrás **Siguiente**

iii) Creando un usuario estándar (sin privilegios) y contraseña.

Crear un usuario para este equipo

Si quieres usar una contraseña, elige algo que te resulte fácil de recordar, pero que sea difícil de adivinar para los demás.

¿Quién va a usar este PC?

usuario1

Dale seguridad.

••••••••

••••••••

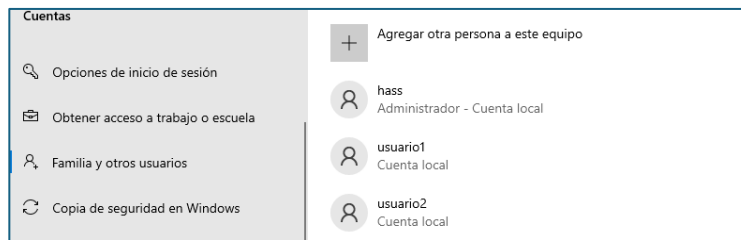
En caso de que olvides la contraseña

Primera pregunta de seguridad

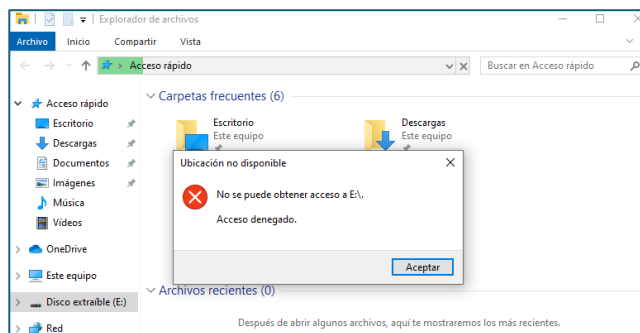
Respuesta

Siguiente

Atrás



- iv) Probando la restricción con el usuario regular.
Se iniciará sesión con el usuario regular usuario1 y se conectará un dispositivo USB para verificar que no tenga acceso debido a las restricciones aplicadas.



Como se puede ver no tiene acceso producto a las restricciones aplicadas.

V. Habilitación de excepciones para usuarios específicos

De acuerdo a lo investigado para restringir el acceso a dispositivos removibles a algunos usuarios, no a todos, como lo realizado anteriormente, se debe realizar en “Configuración de usuario” para ir restringiendo de acuerdo a necesidad y no a todos los usuarios como se hizo anteriormente al utilizar “Configuración del equipo”.

