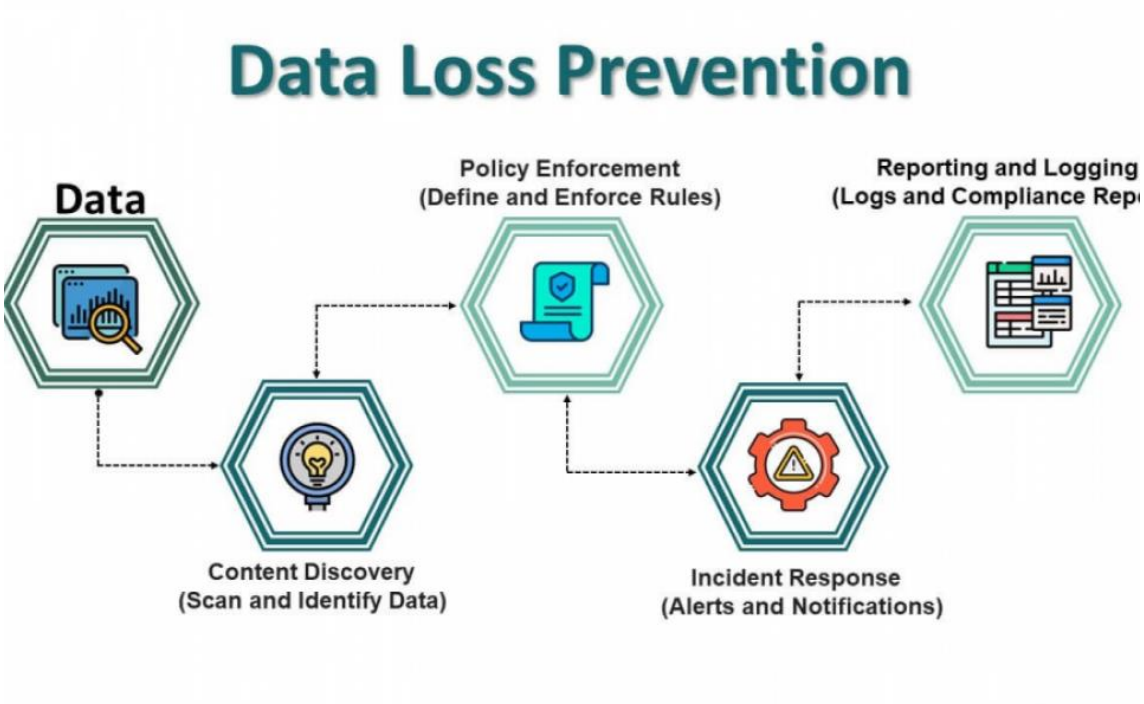
Data Loss Prevention

(DLP)



Joel González.

Introducción al Data Loss Prevention (DLP)

El Data Loss Prevention (DLP) es un conjunto de estrategias, políticas y herramientas diseñadas para prevenir la pérdida, fuga o uso indebido de información confidencial dentro de una organización.
Su objetivo principal es proteger datos críticos, como información personal, financiera, propiedad intelectual o datos comerciales, asegurando que solo el personal autorizado pueda acceder a ellos.
Implementar políticas de DLP permite mitigar riesgos como filtraciones accidentales, ataques internos (insider threats) y exfiltración de datos mediante dispositivos removibles o canales no autorizados.

Clasificación de datos

Para proteger de forma correcta la información, las organizaciones deben clasificar los datos dependiendo su nivel de sensibilidad.

Las categorías que podemos establecer son:

1- Datos públicos.

- Información destinada a ser compartida externamente.
- Ejemplos: Comunicados de prensa, publicidad, contenido

2- Datos internos.

- Información de uso exclusivo dentro de la organización que no debe divulgarse públicamente.
- Ejemplos: Procedimientos internos, manuales operativos, reportes de desempeño.

3- Datos sensibles.

- Información confidencial que, de ser divulgada, podría causar daños financieros, legales o de reputación de la empresa.
- Ejemplos: Datos personales de empleados o clientes. Estados financieros, secretos comerciales.

Acceso y control.

Bajo el principio del menor privilegio, se establece que cada empleado solo tendrá acceso a la información estrictamente necesaria para realizar sus funciones.

Políticas de acceso:

- Los permisos de acceso serán revisados y aprobados por el área de TI y el responsable de seguridad de la información.
- Los supervisores directos verificaran periódicamente la necesidad de acceso de cada usuario.
- Se llevará un registro de cambios de permisos.

Flujo de revisión de permisos:

- El Administrador de Sistemas configura y aplica los controles de acceso.
- El responsable de Seguridad de la Información (CISO) supervisa la correcta aplicación de la política.
- Auditorías trimestrales validaran la coherencia entre los permisos asignados y los roles funcionales.

Monitoreo y Auditoría

Para garantizar el cumplimiento de las políticas DLP, se implementarán medidas de monitoreo continuo:

Herramientas:

- Soluciones SIEM para recolectar, relacionar y analizar eventos de seguridad.
- Software DLP específico, capaz de detectar transferencias inusuales de datos, envío de información confidencial por correo y uso de dispositivos externos.

Reglas de auditoría:

- Registrar todas las actividades relacionadas con datos clasificados como sensibles.
- Alertar sobre accesos no autorizados o inusuales.
- Mantener registros de logs por un periodo de al menos 1 año.

Prevención de Filtraciones

Se aplicarán controles técnicos y administrativos para prevenir la filtración de datos:

- Uso de cifrado en reposo y en tránsito para todos los datos sensibles.
- Restricción del uso de dispositivos USB y medios removibles mediante políticas de grupo o software de endpoint protection.
- Configuración de firewalls y filtros de contenido para bloquear transferencias no autorizadas hacia usuarios externos.

Educación y Concientización del personal.

Para garantizar el éxito de las políticas DLP, se establecerá un programa de capacitación:

- Capacitaciones periódicas sobre la importancia de la protección de datos.
- Talleres de buenas prácticas de seguridad: manejo seguro de dispositivos USB, gestión de contraseñas, detección de correos sospechosos.
- Firmas de acuerdos de confidencialidad y recordatorios de las consecuencias legales de incumplir las políticas.

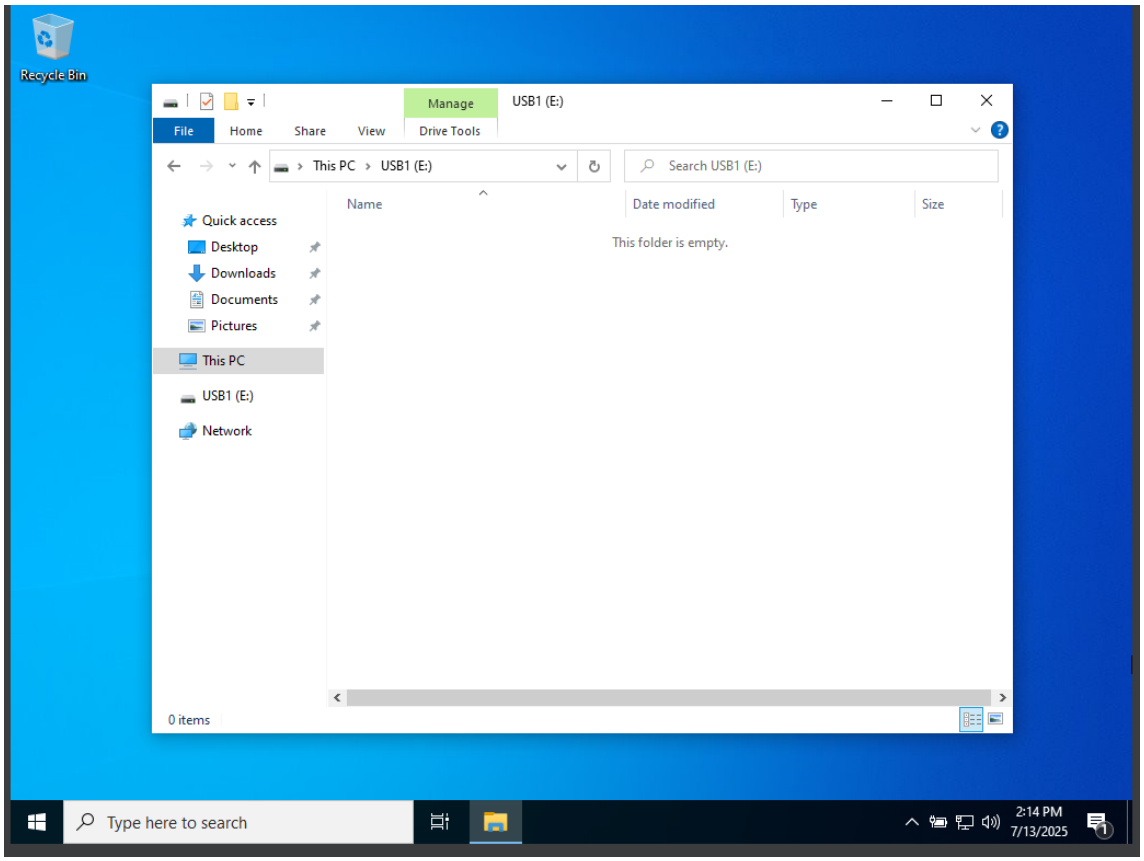
Conclusiones.

- La correcta implementación de políticas y herramientas DLP nos ayudara a reforzar datos confidenciales.
- La correcta clasificación de datos nos permitirá aplicar medias de seguridad mas eficaces y nos ayudará a optimizar recursos.
- Restringir el acceso a la información solo a quienes realmente la necesitan, minimizan los riesgos de ataque.
- El monitoreo continuo y las auditorias periódicas nos ayudan a mantener un buen funcionamiento y a estar al tanto de la seguridad de nuestro entorno.

Practica 2

Implementación de Políticas de Restricción de Dispositivos USB

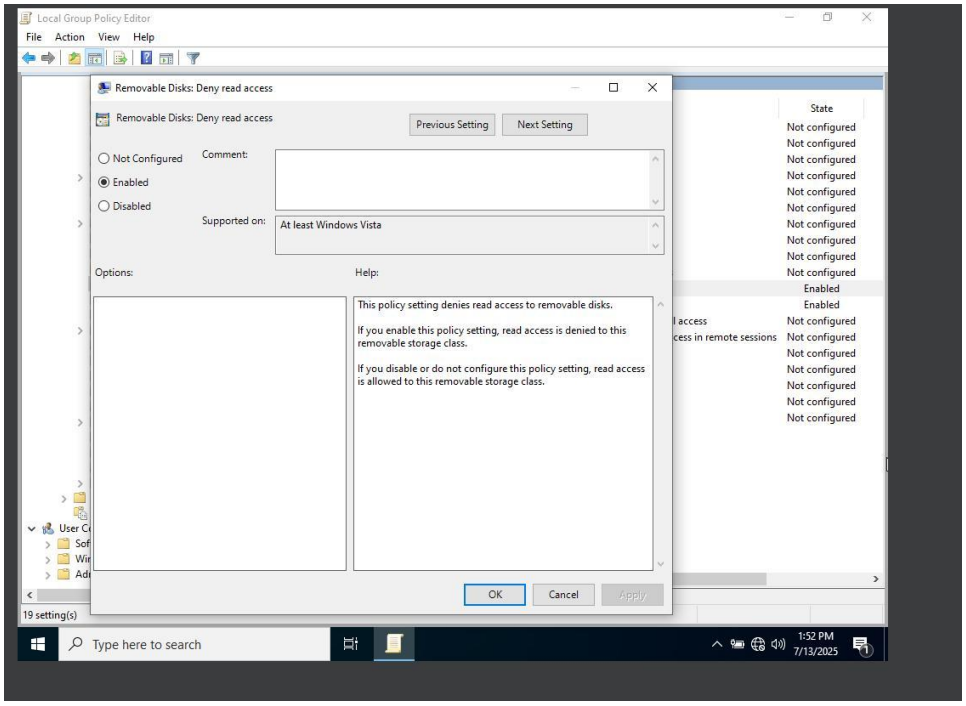
En el primer paso accedemos de forma normal al pc para asegurarnos de que accedemos a la memoria USB, al introducir la memoria al equipo la detecta enseguida, a continuación, vamos a PC y abrimos la USB que acabamos de introducir en el equipo y verificamos que accedemos sin ningún problema.



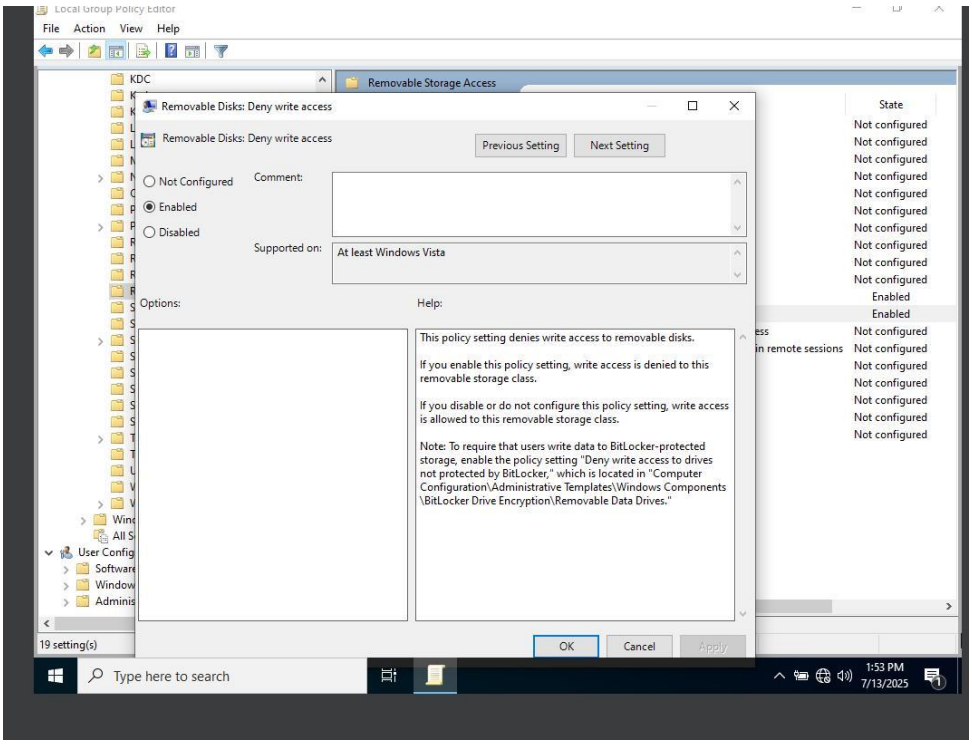
Restricción de Dispositivos USB en Windows.

Accedemos al Editor de políticas de grupo para desactivar la lectura de memorias USB o cualquier otro medio extraíble, denegamos tanto la lectura como la escritura.

Denegamos acceso de lectura.

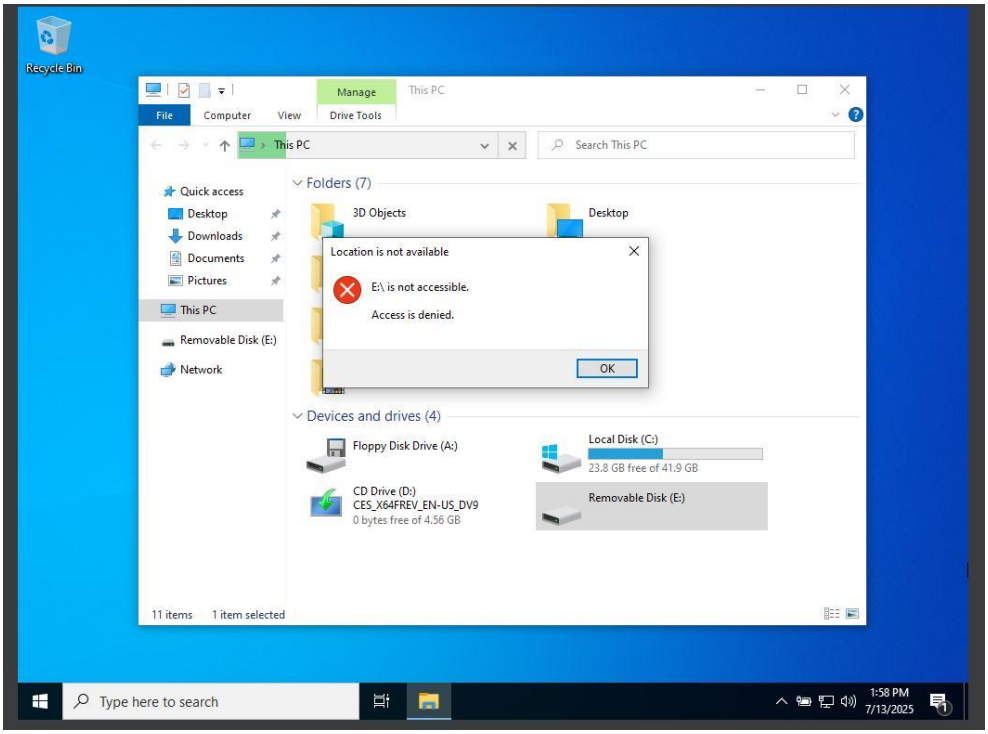


Denegamos acceso de escritura.

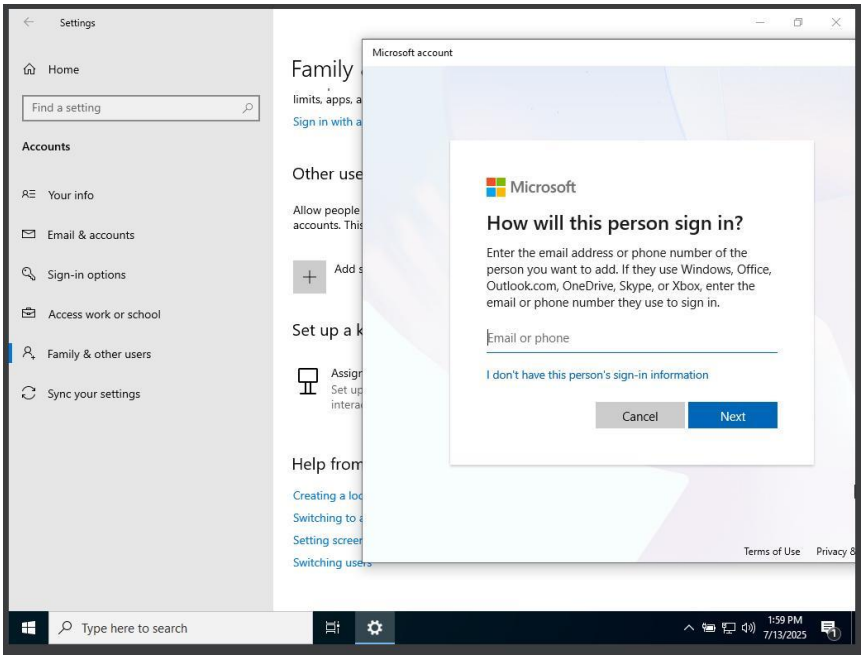


Después de este paso reiniciamos el equipo para que surjan efecto los cambios.

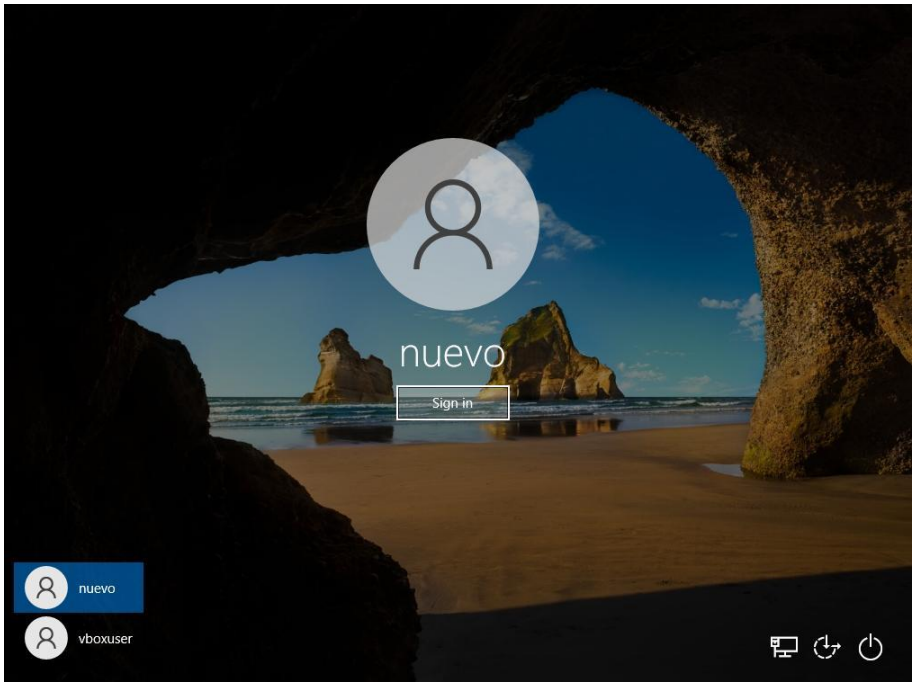
Una vez reiniciado el equipo probamos acceder al USB que, aunque lo reconoce al introducirlo al momento de querer acceder a el nos indica error y nos dice que el dispositivo no esta disponible.



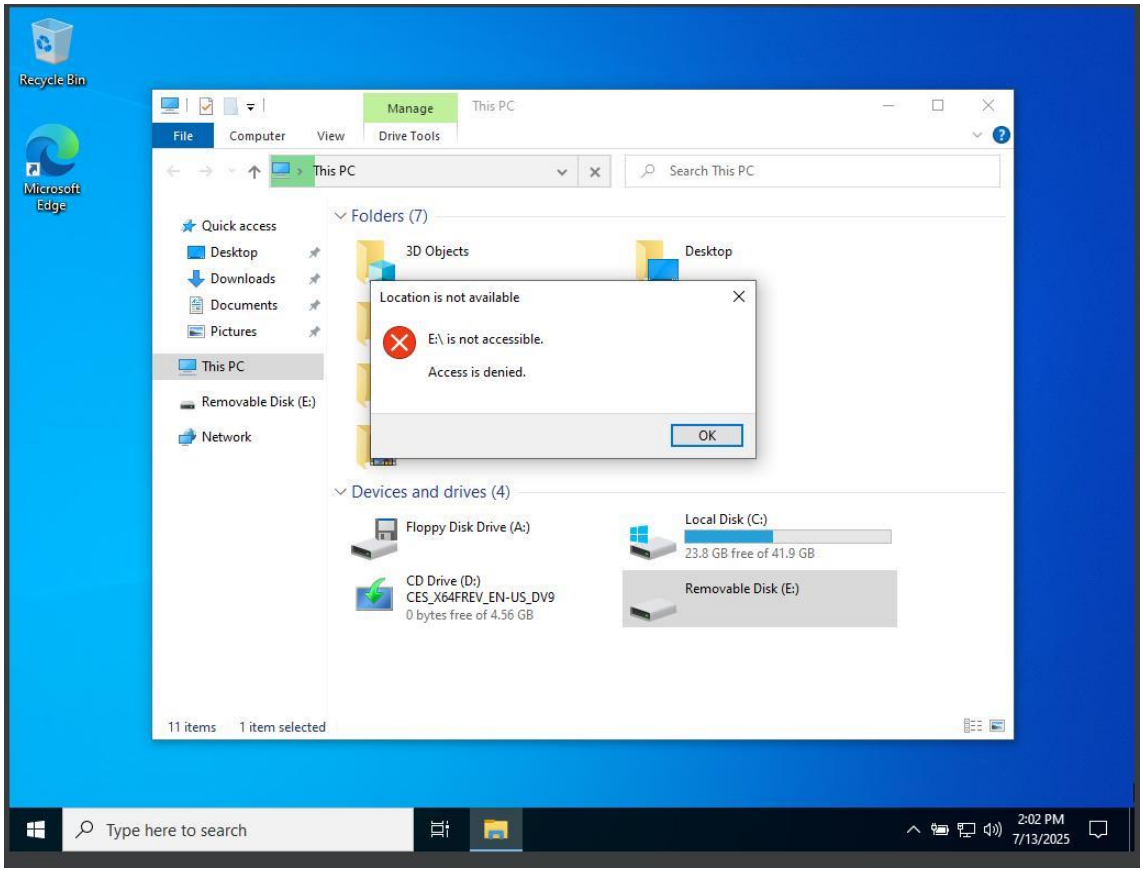
Para realizar una prueba más, generamos otro **usuario** estándar para asegurarnos que el tampoco pueda tener acceso a los dispositivos externos.



Iniciamos sesión con el nuevo usuario



Intentamos acceder al USB desde esta cuenta y vemos que tampoco es posible acceder a los dispositivos externos.



Opciones para habilitar excepciones con usuarios específicos

1- Desde el registro del sistema.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices

Ajustamos permisos con regedit para ciertos grupos de usuarios que tengan permisos de lectura/ejecución o puedan sobrescribir sobre ellos.

2-Software de endpoint DLP.

Cuando las políticas de Windows se quedan cortas algunas empresas usan software DLP, ya que se pueden crear reglas dinámicas, para permitir o bloquear dispositivos extraíbles por usuario o por grupos, horarios o ubicación.

Algunos ejemplos de este software son:

- Symantec DLP.
- Forcepoint.
- McAfee.
- Endpoint protector.