Proyecto DLP

4Geeks Academy

FELIPE ALONSO GOMEZ HENRY
ESTUDIANTE BOOTCAMP CIBERSEGURIDAD

4Geeks

Contenido

4Geeks

Propuesta DLP

Analista: Felipe Gómez Henry

Fecha: 11-05-2025

Introducción

La prevención de Pérdida de Datos (DLP) es un conjunto de estrategias y herramientas diseñadas para detectar, monitorear y prevenir la exfiltración accidental o intencional de información confidencial y/o sensible de la organización. Tiene como objetivo principal proteger los activos digitales, como propiedad intelectual, información personal identificable (PII), secretos comerciales o datos financieros.

Clasificación de datos

Clasificación	Descripción
Datos Públicos	Información disponible sin restricciones (paginas web, comunicados, redes sociales).
Datos Internos	Información accesible solo por personal autorizado (manuales, protocolos, operaciones del sistema).
Datos Sensible	Información crítica cuya divulgación causaría daños (base de datos de usuarios, credenciales, planes estratégicos, propiedad intelectual).

Acceso y control – Principio de menor privilegio

Para garantizar el acceso restringido a datos sensibles:

- Principio: Cada usuario solo accede a lo estrictamente necesario para cumplir su función.
- Política:
  - Uso de grupos de seguridad por función.
  - Revisión de permisos cada 3 meses.
- Flujo de revisión:
  - Solicitud > Aprobación por Líder de Área > Validación por Seguridad TI > Registro en sistema (SIEM).
  - Roles responsables:
    - Líder del área (verificación de necesidad).
    - Oficial de Seguridad TI (auditoría y documentación).
    - Administrador de Sistemas (asignación técnica).

Monitoreo y Auditoría

- Logs almacenados por al menos 90 días.
- Reportes mensuales para análisis de comportamiento.

Prevención de Filtraciones

Estrategias de protección de datos en la red:

- Cifrado:
  - En tránsito: TLS 1.2/1.3.
  - En reposo: BitLocker, EFS o cifrado en bases de datos (TDE).
- Herramientas DLP:
  - Inspección de contenido por patrones (ej: números de tarjetas, RUTs, emails corporativos).
  - Políticas de bloqueo/alerta según contexto.
- Restricciones técnicas:
  - Bloqueo de puertos USB y servicios de nube no autorizados.
  - Prevención de impresiones de documentos clasificados.

Estrategias de educación y concientización

Se tiene como objetivo crear o modificar la cultura de seguridad de una empresa.

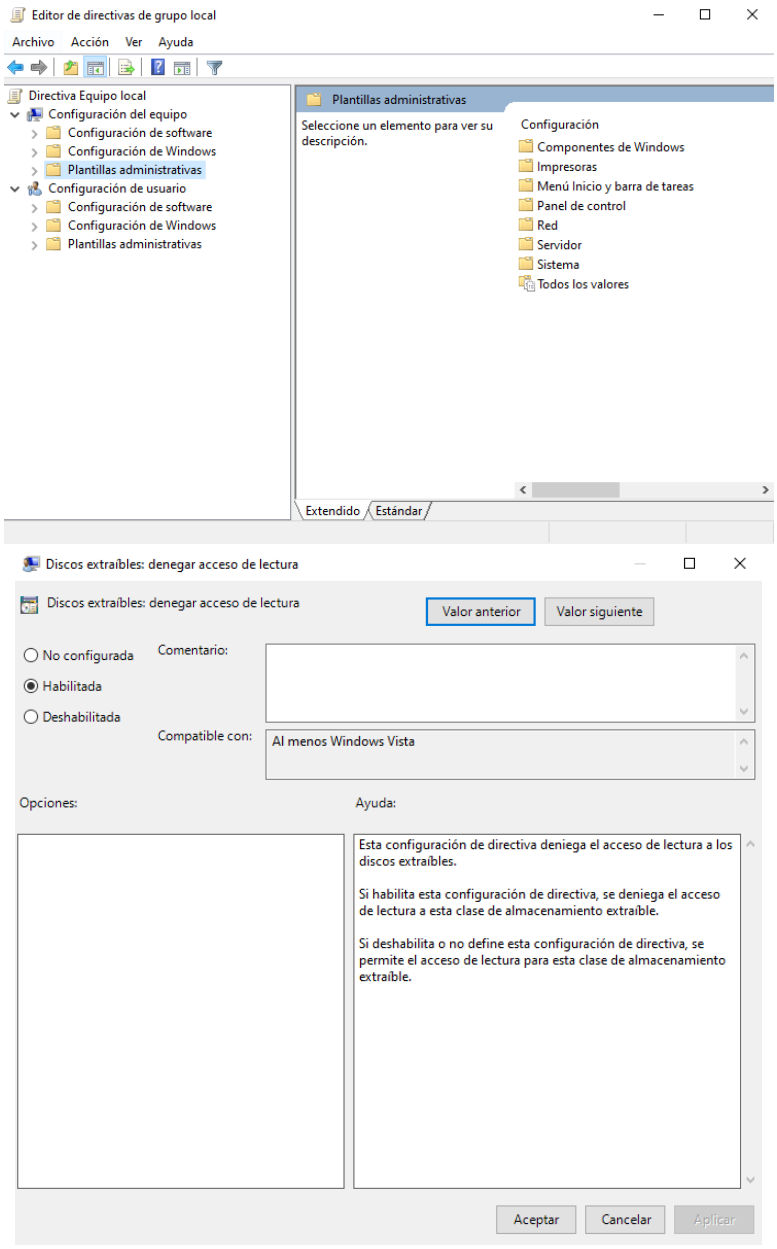
- Capacitación obligatoria semestral:
  - Simulacros de phishing.
  - Buenas prácticas con dispositivos móviles y USB.
  - Reconocimiento de información confidencial.
- Campañas mensuales de seguridad.
- Política de sanción escalonada en caso de incumplimiento.

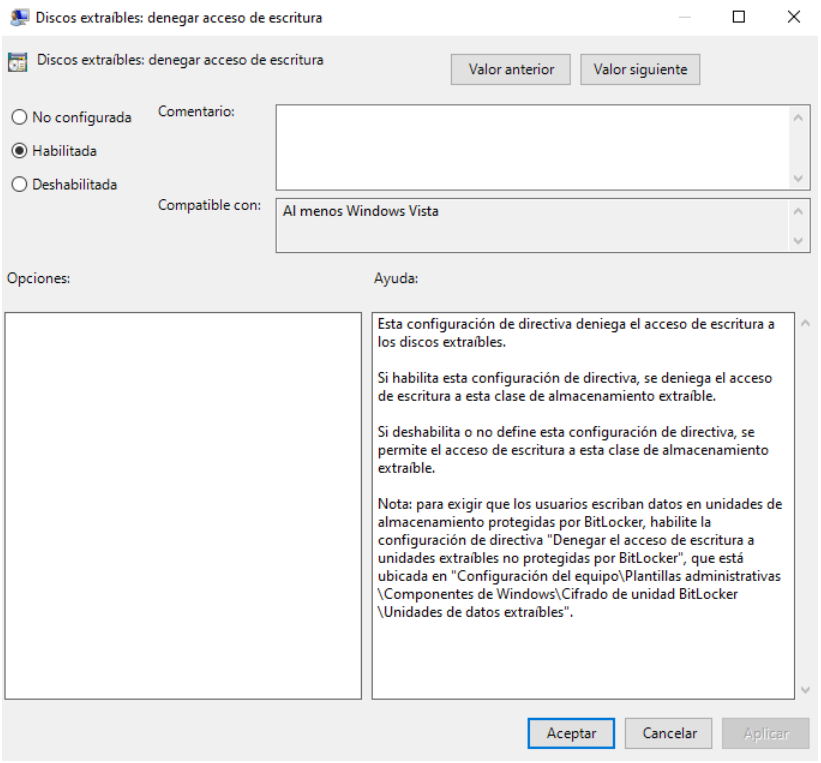
Implementación de políticas de restricción de dispositivos USB: Máquina Virtual Windows

Abrir el Editor de Políticas de Grupo (GPO):

- Presiona Win + R
- Escribe: gpedit.msc → Enter

4Geeks


Editor de directivas de grupo local
Archivo Acción Ver Ayuda
Directiva Equipo local
Configuración del equipo
Configuración de software
Configuración de Windows
Plantillas administrativas
Configuración de usuario
Configuración de software
Configuración de Windows
Plantillas administrativas
Plantillas administrativas
Seleccione un elemento para ver su descripción.
Configuración
Componentes de Windows
Impresoras
Menú Inicio y barra de tareas
Panel de control
Red
Servidor
Sistema
Todos los valores
Extendido
Estándar
Discos extraíbles: denegar acceso de lectura
Discos extraíbles: denegar acceso de lectura
Valor anterior
Valor siguiente
No configurada
Habilitada
Deshabilitada
Comentario:
Compatible con:
Al menos Windows Vista
Opciones:
Ayuda:
Esta configuración de directiva deniega el acceso de lectura a los discos extraíbles.
Si habilita esta configuración de directiva, se deniega el acceso de lectura a esta clase de almacenamiento extraíble.
Si deshabilita o no define esta configuración de directiva, se permite el acceso de lectura para esta clase de almacenamiento extraíble.
Aceptar
Cancelar
Aplicar



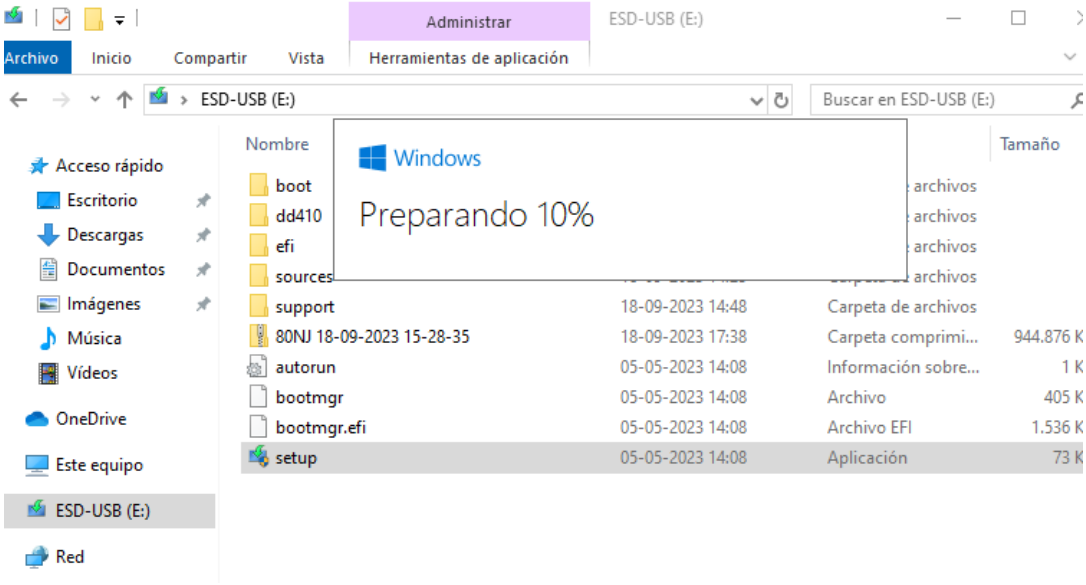
- Configurar las políticas, realizando doble clic en cada una y luego seleccionar “Habilitada”:
    - Discos extraíbles: Denegar acceso de lectura
    - Discos extraíbles: Denegar acceso de escritura
- Ejecutar en una terminal (cmd) el comando gpupdate /force
- Reiniciar Sistema
- Luego de crear un usuario normal ingresamos con las credenciales de dicho usuario.
- Luego se intenta acceder a pendrive conectado a puerto usb, lo cual no se logra debido a que pide permiso y credenciales del admin del equipo.
- Para especificar si un usuario puede acceder o no libremente a los dispositivos se debe crear un grupo local de trabajo ejecutando el siguiente comando en un cmd con permisos de admin

```
C:\Windows\system32>net localgroup USBPermitidos /add
```

- Para especificar que usuario podr[a acceder al usb se ejecuta el siguiente comando en la misma terminal:

```
C:\Windows\system32>net localgroup USBPermitidos usuario_test2 /add
Se ha completado el comando correctamente.
```

- Ahora el usuario puede acceder sin problemas al dispositivo usb>



Conclusion

La implementación de políticas de seguridad para el control de dispositivos USB es una medida fundamental dentro de una estrategia de Prevención de Pérdida de Datos (DLP). Este proyecto ha demostrado cómo configurar una máquina virtual para restringir el uso de almacenamiento removible mediante directivas de grupo, asegurando que solo los usuarios autorizados puedan acceder a estos dispositivos. Además, se abordó una solución práctica para habilitar excepciones mediante la creación de grupos locales y tareas programadas, adaptándose a entornos sin Active Directory. Esta separación de privilegios permite aplicar el principio del menor privilegio de forma efectiva, reduciendo el riesgo de fuga de datos por vía física. Al combinar políticas técnicas con monitoreo continuo y concientización del personal, las organizaciones pueden fortalecer significativamente su postura de seguridad. Este enfoque integral ayuda a proteger activos críticos y asegura el cumplimiento de normativas, minimizando los vectores de exfiltración tanto internos como externos.