
IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DLP
Restricción de dispositivos de almacenamiento externo (USB)

Indice

1. Introducción

Este informe documenta la implementación de políticas de seguridad orientadas a la **Prevención de Pérdida de Datos (DLP)** dentro de un entorno corporativo. Se ha seguido el principio de **menor privilegio**, controlando el acceso a información sensible y reforzando la seguridad mediante la restricción de dispositivos de almacenamiento externos, como memorias USB.

1.1 Objetivo General

- **Fase 1:** Definir e implementar políticas DLP eficaces.
- **Fase 2:** Aplicar medidas técnicas como la restricción de dispositivos USB, validando su funcionalidad en un entorno de pruebas.

---

2. Política de Seguridad DLP

2.1 Introducción al DLP

La Prevención de Pérdida de Datos (DLP) consiste en estrategias y herramientas diseñadas para evitar accesos o filtraciones no autorizadas de datos sensibles. Entre sus objetivos destacan:

- Protección de datos confidenciales.
- Cumplimiento normativo (RGPD, ISO 27001…).
- Disuasión de fugas maliciosas o accidentales.
- Reducción del impacto reputacional y económico ante incidentes de seguridad.

2.2 Clasificación de Datos

Categoría	Descripción	Ejemplos
Datos Públicos	Información sin restricciones.	Publicaciones, contenido web, promociones.
Datos Internos	Uso interno, no confidencial.	Políticas, procedimientos internos.
Datos Sensibles	Requiere control estricto y cifrado.	Datos de clientes, informes financieros.

Todos los documentos deben clasificarse con etiquetas visibles.

2.3 Acceso y Control

- Accesos definidos por roles y departamentos.
- Revisión periódica de permisos.
- Accesos temporales con expiración automática.
- Restricciones de edición según tipo de dato y responsabilidad.

2.4 Monitoreo y Auditoría

- Software DLP y SIEM (p. ej., Wazuh, Elastic SIEM).
- Logs de acceso y modificaciones.
- Auditorías automáticas mensuales.
- Alertas por comportamiento anómalo.

2.5 Medidas de Prevención

- Cifrado AES-256 en reposo y tránsito.
- Bloqueo de USB sin autorización.
- VPN obligatoria para acceso remoto.
- Firewall con DPI y watermarking digital.

2.6 Formación y Cultura de Seguridad

- Curso de formación obligatorio.
- Simulacros de phishing y concienciación periódica.
- Guías y vídeos de buenas prácticas.
- Incentivos por reporte de vulnerabilidades.

---

3. Implementación Técnica: Restricción de Dispositivos USB

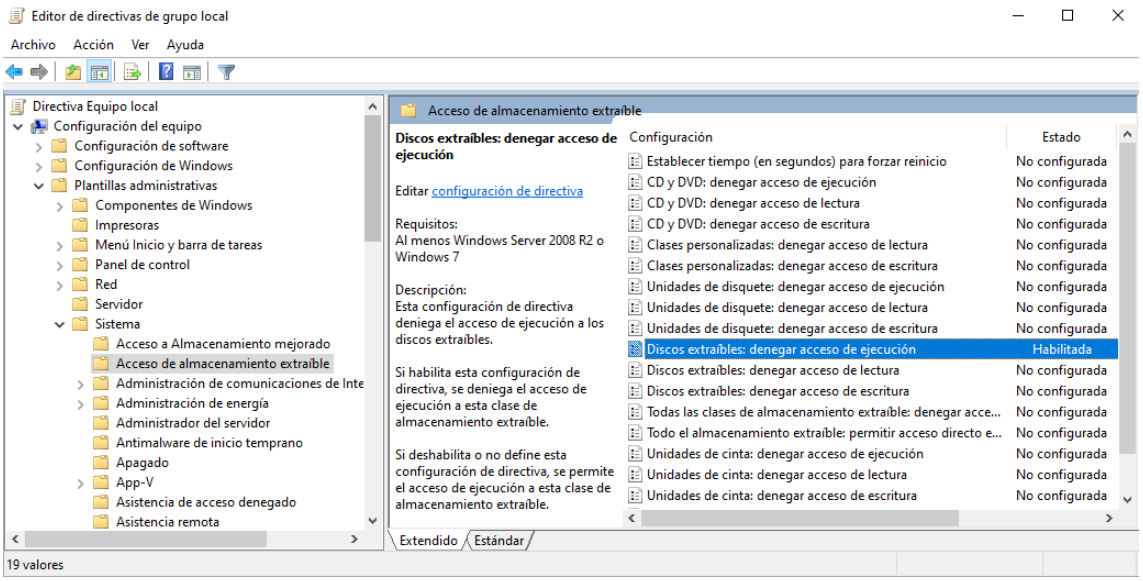
3.1 Preparación del Entorno

- **VirtualBox Extension Pack** instalado para soporte USB.
- Activado soporte USB 2.0 o 3.0 en la VM.

- Dispositivo USB conectado a la VM desde el menú > Dispositivos > USB.

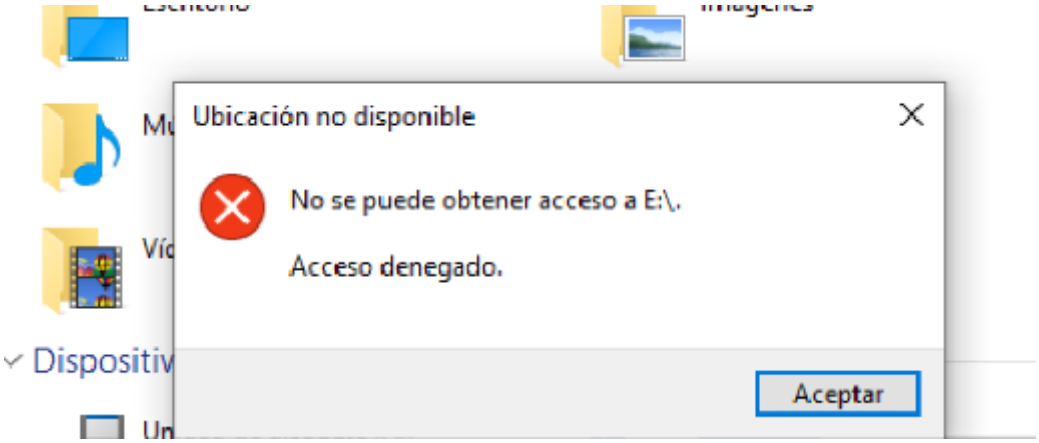
3.2 Aplicación de Políticas en Windows

- Acceso al gpedit.msc.
- Navegación: Configuración del equipo > Plantillas administrativas > Sistema > Acceso de almacenamiento extraíble.
- Activadas las políticas:
    - **Denegar acceso de lectura a discos extraíbles.**
    - **Denegar acceso de escritura a discos extraíbles.**



3.3 Validación

- Prueba de acceso a USB desde cuenta estándar.
- Confirmación del mensaje de denegación.



3.4 Usuario Regular

- Usuario estándar creado sin privilegios.
- Prueba de acceso a USB con dicho usuario.

---

4. Conclusión

La implementación de políticas de Prevención de Pérdida de Datos (DLP) es un pilar fundamental en la protección de la información sensible dentro de cualquier organización moderna. A lo largo de este proyecto se ha demostrado que, con una correcta clasificación de la información, una adecuada segmentación de accesos y la aplicación de medidas técnicas efectivas, se pueden reducir significativamente los riesgos de fuga de datos, tanto intencionadas como accidentales.

Uno de los principales logros de esta práctica ha sido la configuración de restricciones de dispositivos USB, una de las vías más comunes para la exfiltración de información confidencial. A través del uso de políticas de grupo en entornos Windows, se ha validado con éxito que es posible bloquear tanto la lectura como la escritura en medios extraíbles, impidiendo que usuarios no autorizados puedan copiar datos sensibles o introducir archivos potencialmente maliciosos en la infraestructura interna.

Este control, aunque aparentemente simple, representa una barrera sólida frente a múltiples vectores de ataque. La facilidad con la que un dispositivo USB puede introducir software malicioso o extraer información crítica hace imprescindible su regulación. La creación de usuarios sin privilegios y la validación de las políticas aplicadas refuerzan aún más el enfoque de seguridad basado en el principio de menor privilegio, asegurando que cada persona acceda únicamente a los recursos que necesita para desempeñar sus funciones.

Además, se ha subrayado la importancia de fomentar una cultura de ciberseguridad en la organización, donde la formación continua y la concienciación sean partes inseparables de las políticas técnicas. La tecnología, por sí sola, no es suficiente: el factor humano sigue siendo el eslabón más débil si no se acompaña de educación, simulacros y una comunicación fluida sobre riesgos y responsabilidades.

En conjunto, esta práctica no solo ha servido para aplicar una política específica, sino que ha sentado las bases para un modelo integral de gestión de la seguridad de la información, combinando herramientas técnicas, buenas prácticas y criterios de gobernanza. Se trata de una iniciativa replicable, escalable y adaptable a distintos entornos y necesidades empresariales.

A medida que las amenazas evolucionan, también deben hacerlo nuestras políticas y herramientas. Por ello, este trabajo es solo el primer paso de un proceso continuo de mejora, revisión y adaptación de las estrategias DLP. El camino hacia una organización verdaderamente segura requiere compromiso constante, análisis riguroso y una visión proactiva de la seguridad como valor estratégico.