4Geeks Academy
Bootcamp de Ciberseguridad

Informe de Prevención de Pérdida de Datos (DLP)

Estudiante: Jorge Teran
Cohorte: Ciberseguridad 2025

Data Loss Prevention (DLP)

un conjunto de prácticas, normas y tecnologías orientadas a evitar la pérdida, filtración o mal uso de la información sensible de una organización. Su relevancia se debe a que garantiza la **confidencialidad, integridad y disponibilidad** de los datos, reduciendo el riesgo de incidentes que puedan ocasionar consecuencias económicas, legales o dañar la reputación de la empresa.

En la actualidad, donde los ciberataques y las filtraciones de información son cada vez más comunes, contar con políticas de DLP resulta esencial para asegurar la **continuidad operativa**, cumplir con los marcos regulatorios y preservar la confianza de clientes y aliados comerciales.

Clasificación de Datos

La organización clasificará los datos en tres categorías principales, en función de su nivel de sensibilidad y el impacto que tendría su divulgación:

1. **Datos Públicos**
    - Información que puede ser divulgada sin restricciones.
    - Ejemplo: material de marketing, información publicada en la web corporativa.
2. **Datos Internos**
    - Información de uso exclusivo dentro de la organización.
    - Ejemplo: reportes internos, procedimientos operativos, datos de empleados.
3. **Datos Sensibles**
    - Información crítica cuya exposición puede causar un impacto severo en la empresa o en terceros.
    - Ejemplo: datos financieros, credenciales de acceso, información de clientes, propiedad intelectual.

Acceso y Control

- Se aplicará el **principio del menor privilegio**, donde cada empleado tendrá acceso únicamente a la información necesaria para desempeñar sus funciones.
- La gestión de permisos se realizará de la siguiente forma:
    - **Responsables de revisión de permisos:** Equipo de Seguridad Informática y Recursos Humanos.

- **Periodicidad:** Revisión trimestral de accesos y privilegios.
- **Flujo de revisión:**
    1. Solicitud de acceso → Responsable de área.
    2. Validación de necesidad → Departamento de Seguridad.
    3. Aprobación/Rechazo → Dirección de TI.

Monitoreo y Auditoría

Para garantizar la seguridad de los datos sensibles, se implementarán procesos de monitoreo y auditoría:

- **Herramientas de monitoreo:**
    - Soluciones **SIEM** (Security Information and Event Management) para detectar actividades sospechosas en tiempo real.
    - Herramientas **DLP** específicas para monitorear el acceso, copia, envío y almacenamiento de datos sensibles.
- **Reglas de auditoría:**
    - Registro detallado de accesos a datos sensibles.
    - Auditorías mensuales para identificar patrones anómalos de comportamiento.
    - Reportes automáticos de incidentes al equipo de ciberseguridad.

Prevención de Filtraciones

Las medidas para evitar la fuga de información incluirán:

- **Cifrado de datos sensibles** en tránsito y en reposo (protocolos TLS, AES-256).
- **Bloqueo de dispositivos externos no autorizados** (USB, discos duros externos).
- **Políticas de correo electrónico seguro**, restringiendo el envío de información crítica fuera de la red corporativa.
- Implementación de **herramientas DLP** que analicen el contenido y eviten transmisiones no autorizadas de datos.

Educación y Concientización

La seguridad de la información depende en gran medida de la conducta de los empleados. Para ello se implementarán programas de formación:

- **Capacitaciones trimestrales** en ciberseguridad y uso correcto de las políticas DLP.
- **Campañas de concientización** sobre riesgos como phishing, ingeniería social y manejo indebido de datos.
- **Simulaciones y pruebas prácticas** para evaluar el nivel de cumplimiento y reacción del personal ante incidentes.
- Creación de un **manual de buenas prácticas** accesible a todos los colaboradores.

Implementación de Políticas de Restricción de Dispositivos USB

Para aplicar restricciones de uso de dispositivos USB en la VM con Windows, primero se habilitó el acceso a estos dispositivos en VirtualBox mediante tres pasos básicos:

1. **Instalación del Extension Pack** desde la sección de extensiones de VirtualBox.
2. **Activación del soporte USB 2.0/3.0** en la configuración de la máquina virtual.
3. **Conexión y asignación del dispositivo USB** al iniciar la VM desde el menú *Dispositivos > USB*.

Esta configuración permite gestionar los USB en la VM, requisito previo para implementar políticas de restricción alineadas con las estrategias de **Data Loss Prevention (DLP)**.

Restricción de Acceso a Dispositivos USB

Como parte de la implementación de políticas de **Data Loss Prevention (DLP)** en la máquina virtual Windows, se aplicaron directivas de grupo para restringir el uso de dispositivos de almacenamiento extraíble.

Estas políticas impiden tanto la **lectura** como la **escritura** en memorias USB, evitando que los usuarios puedan copiar información confidencial de la organización hacia dispositivos externos o introducir archivos no autorizados desde ellos.

La efectividad de la política se comprobó conectando un dispositivo USB a la VM: al intentar acceder a la unidad, el sistema mostró el mensaje de error **“Acceso denegado”**, confirmando que la restricción fue aplicada con éxito.

(Se adjuntan capturas de evidencia del proceso y el resultado final).

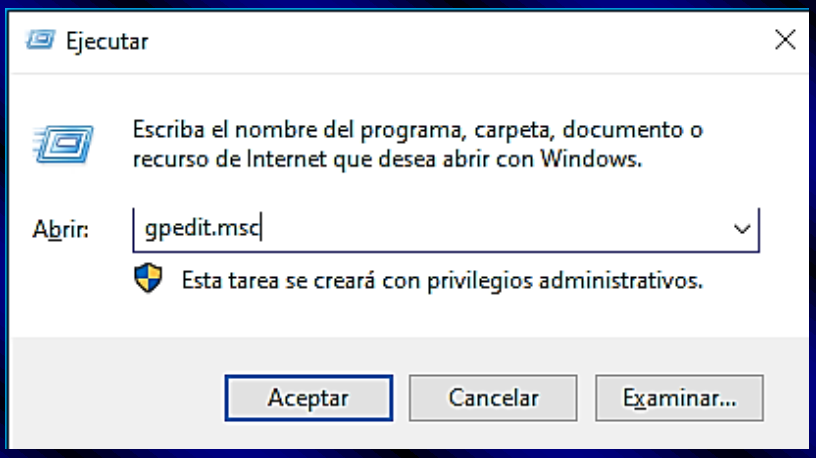

Figura 1. Apertura del Editor de directivas de grupo local en Windows.

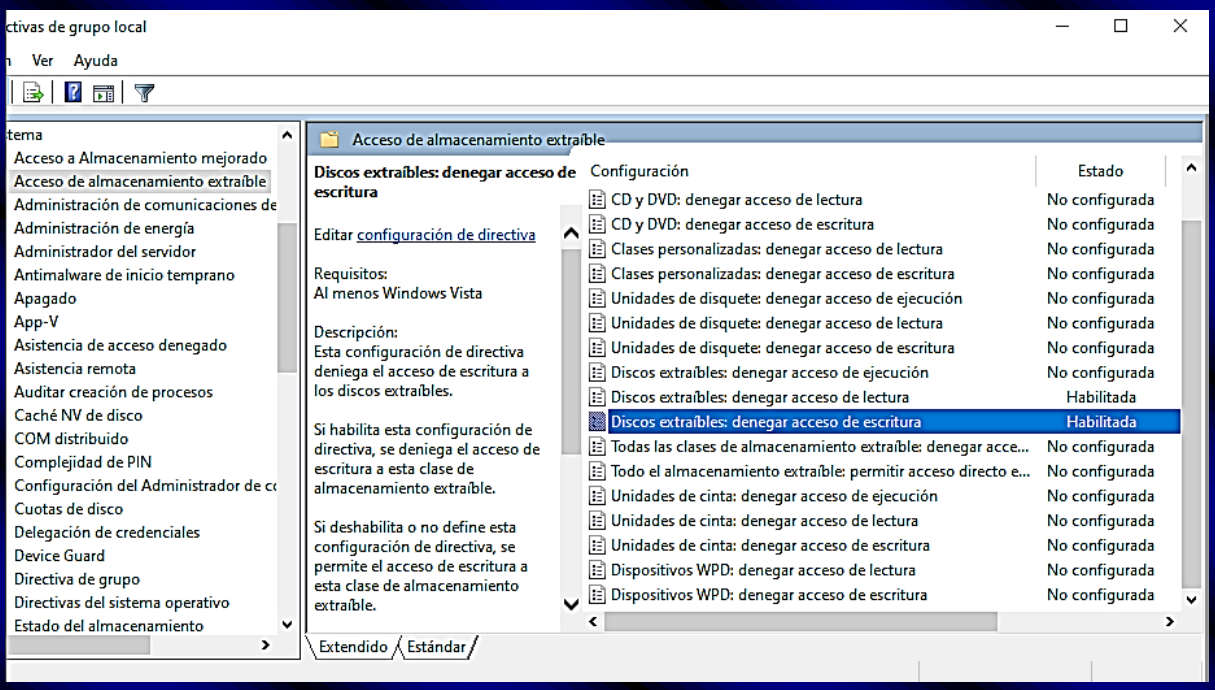

Figura 2. Configuración de la directiva “Discos extraíbles: denegar acceso de escritura”.

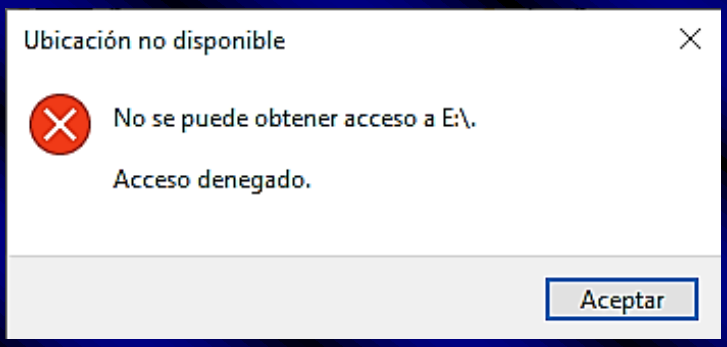

Figura 3. Evidencia de restricción aplicada: intento de acceso a la memoria USB bloqueado.