Implementación de Políticas de Seguridad DLP

2 de Junio del 2025

Visión general

Introducción al Data Loss Prevention (DLP)

La Prevención de Pérdida de Datos (DLP, por sus siglas en inglés) es un conjunto de estrategias y herramientas diseñadas para detectar, monitorear y proteger datos sensibles dentro de una organización, evitando su exposición, pérdida o acceso no autorizado. Su objetivo principal es garantizar que la información crítica no sea compartida de forma indebida fuera de los límites corporativos, ya sea de manera accidental o maliciosa.

DLP juega un papel crucial en la protección de la información confidencial, el cumplimiento normativo (como GDPR, HIPAA, o la LOPI), y la defensa contra amenazas internas. Al implementar políticas de DLP robustas, una empresa puede reducir significativamente el riesgo de fugas de datos, proteger la propiedad intelectual y mantener la confianza de sus clientes y socios.

Objetivos

1. Clasificación de Datos
2. Acceso y Control
3. Monitoreo y Auditoría
4. Prevención de Filtraciones
5. Educación y Concientización

Clasificación de Datos

Para una correcta implementación de DLP, la organización clasifica sus datos según su nivel de sensibilidad y criticidad. Las siguientes categorías serán utilizadas:

- **Datos Públicos:**

  Información que puede ser divulgada al público sin causar daño a la organización. Ejemplos incluyen comunicados de prensa, contenidos de la página web pública, información institucional general.

  ○

- **Datos Internos:**

  Información destinada únicamente para uso dentro de la organización. No debe ser divulgada externamente sin autorización. Ejemplos: organigramas, manuales de operación, reportes internos sin información sensible.

  ○

- **Datos Sensibles (Confidenciales):**

  Información crítica cuya divulgación no autorizada podría causar perjuicio legal, financiero o de reputación. Ejemplos: datos personales de clientes o empleados, información financiera no divulgada, propiedad intelectual, credenciales de acceso.

  ○

Acceso y Control

Basado en el principio del menor privilegio, el acceso a la información estará limitado estrictamente a aquellos usuarios que lo requieran para desempeñar sus funciones.

- **Asignación de permisos:**

  Cada empleado tendrá acceso solo a los datos necesarios según su rol. El acceso será gestionado por el equipo de TI y aprobado por el jefe de departamento correspondiente.

- **Revisión de permisos:**

  Se realizarán auditorías trimestrales de acceso a datos sensibles.El equipo de Seguridad de la Información será responsable de coordinar estas revisiones.Los responsables de cada departamento deberán validar que los accesos otorgados siguen siendo necesarios.

- **Desactivación automática de accesos:**

  Accesos a datos sensibles se revocarán automáticamente cuando un empleado cambie de puesto o salga de la empresa, mediante integración con el sistema de gestión de identidades (IAM).

Monitoreo y Auditoría

Toda actividad relacionada con datos sensibles será registrada y monitoreada activamente para identificar usos indebidos o patrones anómalos.

Herramientas utilizadas:

- DLP Endpoint Solutions: Para monitorear transferencias de datos desde estaciones de trabajo, USB, correo electrónico o servicios en la nube.
- SIEM (Security Information and Event Management): Para correlacionar eventos y generar alertas en tiempo real ante actividades sospechosas.
- Logs centralizados: Se mantendrá un historial de acceso, modificación y transferencia de datos confidenciales por un período mínimo de 12 meses.

Alertas automáticas:

Se generarán alertas en tiempo real si:

- Se intenta enviar datos sensibles por correo no corporativo.
- Se copian archivos confidenciales a dispositivos externos sin autorización.
- Se detecta movimiento inusual de grandes volúmenes de datos.

Prevención de Filtraciones

Se implementarán las siguientes medidas técnicas para prevenir la filtración de datos sensibles:

- Cifrado de datos:

  Cifrado en reposo: Toda la información sensible almacenada en servidores y dispositivos será cifrada (AES-256 como estándar).

  Cifrado en tránsito: Se exigirá el uso de protocolos seguros (como TLS 1.3) para la transmisión de datos.

- Control de dispositivos:
  1. Políticas de restricción de USB y dispositivos extraíbles.
  2. Software DLP instalado en estaciones de trabajo para bloquear acciones no autorizadas.
- Bloqueo de canales no seguros:
  1. Se limitará el uso de servicios de almacenamiento en la nube no aprobados.
  2. Restricción del uso de clientes de correo no corporativos.

Educación y Concientización

La capacitación del personal es un componente clave de cualquier política de seguridad.

Programa de formación continua:

Todos los empleados deberán completar una capacitación inicial en seguridad de la información y protección de datos dentro de sus primeros 30 días laborales.

Se realizarán sesiones semestrales de actualización y campañas de concientización.

Simulacros de fuga de datos:

Periódicamente se llevarán a cabo ejercicios simulados de filtración para evaluar la respuesta de los equipos y la eficacia de las medidas de protección.

Política de seguridad firmada: Cada empleado firmará una declaración de conocimiento y compromiso con la política de DLP de la empresa.

Políticas de restricción de USB y dispositivos extraíbles.

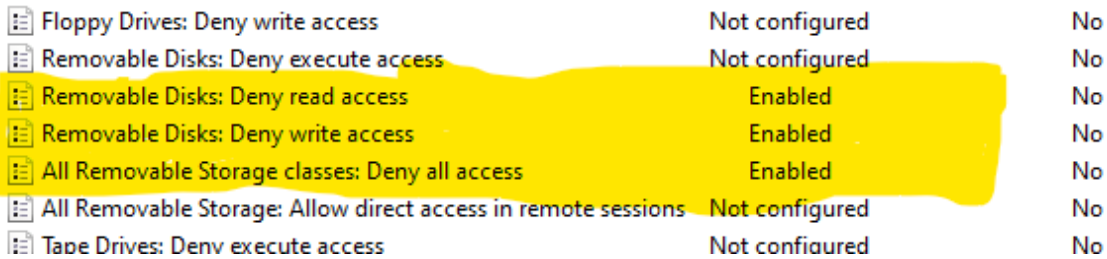
Aquí implementaremos una política de restricción de uso de USB y dispositivos extraíbles.

Metodología.

Abrimos el editor de políticas de grupo y luego vamos a Configuración del equipo > Plantillas administrativas > Sistema > Acceso de almacenamiento removible.

Aqui habilitamos las siguientes políticas:

- Todas las clases de almacenamiento extraíble: Denegar todo acceso
- Unidades de disco extraíbles: Denegar lectura
- Unidades de disco extraíbles: Denegar escritura



Esto nos da como resultado, que se deniega el acceso a la hora de conectar cualquier extraíble a la máquina.