Implementar Políticas de Seguridad DLP a dispositivos de almacenamiento externo

---

Realizado por: Arturo Martín-Vegue González

Para: 4Geeks Academy

Prevención de Pérdida de Datos (DLP)

En una organización es importante establecer políticas *DLP* para detectar o prevenir la filtración de datos sensibles.

Las políticas *DLP* consiste en establecer medidas de prevención y actuación en el manejo de información en una organización, ya sea a través de medidas de seguridad informáticas o estableciendo procedimientos para que los trabajadores traten de manera adecuada la información que manejan. Ninguna organización está exenta de peligro y hay que ser siempre cautelosos con la información y hacer un uso adecuado de la misma.

Clasificación de Datos

En este documento se clasificarán los datos en función de la sensibilidad y lo que podría suponer a una persona u organización que se pudiesen filtrar.

- Datos Sensibles: Información personal o corporativa que en caso de filtración, supondría daños graves (financieros, reputacionales o legales) a los afectados, véase:
  - Datos fiscales, financieros, identificación personal (PII), propiedad intelectual (PI), historiales médicos y credenciales.
- Datos Uso Interno: Información corporativa no destinada al público, cuya filtración causaría un impacto moderado en la organización:
  - Comunicaciones internas generales, organigramas, guías de estilo, procedimientos de empleados (sin detalles de seguridad).
- Datos Públicos: Información destinada a ser divulgada necesaria para la actividad comercial:
  - NIF de la organización, ubicación de las instalaciones, catálogo de productos, servicios, políticas de privacidad.

Acceso y Control

Para la correcta aplicación de las medidas de prevención (*DLP*), el uso de los sistemas, el control de acceso y el manejo de información, deben estar correctamente definidos en las políticas de la empresa. Garantizar la confidencialidad e integridad de los datos debe ser una prioridad fundamental para la continuidad del negocio.

1. Política de Mínimo Privilegio (PoLP)

Para ello, el acceso a los recursos de información se regirá bajo el principio del menor privilegio. Esto implica que:

- Los usuarios tendrán acceso únicamente a los datos y sistemas estrictamente necesarios para desempeñar sus funciones laborales actuales.
- Cualquier solicitud de acceso adicional deberá ser justificada por una necesidad de negocio y aprobada temporal o permanentemente.
- Se implementará un modelo RBAC (Role-Based Access Control): Los permisos se asignan al "cargo" (Rol), no a la persona, asegurando la estandarización.

2. Flujo de Revisión de Permisos

Para garantizar que los privilegios no se acumulen de forma innecesaria, se establece el siguiente flujo de auditoría:

- Frecuencia: Las revisiones se realizarán de forma trimestral.
- Roles Responsables:
  - Data Owner (Responsable del Departamento): Es quien valida si sus empleados siguen necesitando los accesos actuales.
  - Administrador de Seguridad (IT): Genera los informes de acceso y ejecuta las revocaciones.
- Procedimiento:
  1. Generación: IT envía al Data Owner un listado con los accesos actuales de su equipo.
  2. Validación: El Data Owner marca los accesos como "Mantener" o "Revocar" según la función actual del empleado.
  3. Ejecución: IT elimina los permisos marcados como "Revocar" en un plazo máximo de 48h.
  4. Registro: El resultado de la revisión se archiva como evidencia de cumplimiento (auditoría).

Monitoreo y Auditoría

Para garantizar la efectividad de las políticas *DLP*, se establece un sistema de vigilancia continua y registro de eventos. El objetivo no es solo bloquear, sino obtener visibilidad sobre cómo fluyen los datos dentro de la organización.

1. Reglas de Monitoreo de Datos Sensibles

Se configuran reglas de detección basadas en el contenido y el contexto para los datos clasificados previamente como "Sensibles" o "Internos":

- **Movimiento Lateral y Exfiltración**: Se generará una alerta crítica cuando se intenten copiar archivos con etiquetas de sensibilidad hacia dispositivos de almacenamiento (USB), servicios de almacenamiento en la nube no corporativos (Google Drive personal, Dropbox).
- **Ofuscación de Datos**: Se monitoreará el cambio de extensiones de archivo (ej: renombrar passwords.xlsx a fondo_de_pantalla.jpg) y el cifrado de archivos por herramientas no autorizadas.
- **Anomalías de Volumen**: Alerta ante la copia o descarga masiva de información en periodos cortos de tiempo.

2. Herramientas de Monitoreo y Gestión

Se implementará una arquitectura híbrida compuesta por agentes en el endpoint y un sistema de detección y respuesta central (SIEM):

- **Agente Endpoint**: Se desplegará un agente en todos los puestos de trabajo (Wazuh). Este agente es responsable de la **inspección de contenido** en tiempo real y el bloque de puertos USB si no se cumplen los requisitos de cifrado.
- **SIEM (Security Information and Event Manager**: Se utilizará **Wazuh** para centralizar los logs.
  - El agente enviará los logs al SIEM.
  - El SIEM se encargará de contrastar la información con otros logs (Firewall, Directorio Activo) para dar contexto (ej: "El usuario que copió el USB acababa de fallar 3 veces su contraseña").

3. Política de Auditoría y Trazabilidad

Para cumplir con normativas legales y facilitar el análisis forense en caso de incidente:

- **Las 4 condiciones del Log**: Todo registro de auditoría deberá responder a: **Quién** (Usuario), **Qué** (Acción y Dato afectado), **Cuándo** (Timestamp) y **Dónde** (Dispositivo y destino).
- **Retención:** Los logs de actividad DLP se almacenarán en un servidor seguro e inmutable por un periodo mínimo de **12 meses**.
- **Revisión:** Se realizarán auditorías aleatorias mensuales sobre los logs de "falsos positivos" para ajustar la sensibilidad de las reglas y no entorpecer el trabajo legítimo.

Prevención de Filtraciones

Más allá de la detección, se establecen mecanismos de **bloqueo activo** y protección criptográfica para impedir la fuga de información *antes* de que ocurra.

1. Cifrado de Dispositivos y Datos

El cifrado es la última línea de defensa: si el dispositivo se pierde o se roba, los datos deben ser ilegibles.

- **Cifrado de Disco Completo:** Todos los portátiles y estaciones de trabajo corporativos tendrán activado el cifrado de disco (ej: *BitLocker* en Windows o *FileVault* en macOS) con claves gestionadas centralizadamente.
- **Cifrado de Medios Extraíbles:** Se forzará, mediante política de grupo (GPO) o agentes, el cifrado obligatorio de cualquier dispositivo USB conectado. Si un usuario intenta copiar un archivo corporativo a un USB personal no cifrado, el sistema denegará la operación y solicitará formatear y cifrar el dispositivo primero.

Educación y Concienciación

La tecnología por sí sola no basta. Si los empleados no conocen los riesgos, las herramientas de seguridad fallarán. El objetivo de este apartado es asegurar que todo el equipo entienda qué se puede hacer y qué no.

1. Formación desde el primer día

La seguridad será parte obligatoria de la bienvenida a la empresa:

- **Al entrar:** Antes de empezar a trabajar, a cada empleado se le explicarán las normas básicas (qué datos son sensibles, por qué no usar USBs personales, etc.) de forma sencilla.
- **Durante el año:** No sirve de nada dar una charla de 3 horas una vez al año que todo el mundo olvida. En su lugar, se enviarán recordatorios breves y consejos prácticos cada mes para mantener la seguridad fresca en la memoria de todos.

2. Simulacros y Pruebas Prácticas

La mejor forma de aprender es practicando. Se realizarán pruebas sorpresa para ver si están preparados:

- **Correos de prueba:** Se enviarán correos falsos (simulando ser un banco o un proveedor) para ver quién o quiénes necesitan refuerzo en la formación.
- **El objetivo es concienciar**: Si alguien falla, se le explicará como detectarlo la próxima vez.

3. Saber a quién preguntar

A veces surgen dudas, "¿Puedo enviar este archivo?", "¿Este USB es seguro?".

- Se creará un canal de comunicación directo para que cualquier empleado pregunte al equipo de seguridad antes de cometer un error.

Conclusiones

La implementación de una estrategia de **Prevención de Pérdida de Datos (DLP)** en dispositivos de almacenamiento externo no debe entenderse únicamente como una barrera tecnológica o una lista de prohibiciones. Como se ha desarrollado en este documento, se trata de un enfoque integral que combina **tecnología** (cifrado y bloqueo), **procesos** (clasificación y revisión de permisos) y, fundamentalmente, **personas** (concienciación).

En definitiva, proteger la información no es solo una cuestión de cumplimiento técnico, sino una garantía para mantener la confianza de los clientes y la reputación de la organización.