Introducción a DLP

La Prevención de Pérdida de Datos (DLP) es un conjunto de estrategias y herramientas que ayudan a proteger la información sensible de una organización. Su objetivo principal es que solo el personal autorizado pueda acceder a los datos, evitando que se pierdan, se filtren o caigan en manos equivocadas. Es importante porque protege la información personal, financiera y de la empresa, además de ayudar a cumplir con leyes como GDPR, HIPAA o PCI-DSS.

Clasificación de Datos

Para organizar y proteger mejor los datos, se pueden dividir en tres categorías:

Datos Públicos: Información que puede compartirse sin problemas (por ejemplo, folletos, información de la web).

Datos Internos: Información interna de la empresa que no debe salir de ella (por ejemplo, procedimientos internos, correos internos).

Datos Sensibles: Información crítica o privada que requiere máxima protección (por ejemplo, números de tarjetas, datos de empleados, secretos comerciales).

Acceso y Control

Se aplicará el principio del menor privilegio, lo que significa que cada empleado solo puede acceder a la información que necesita para trabajar.

Flujo de revisión de permisos:

Los jefes de departamento revisan quién necesita acceso a qué información.

Solo se aprueba acceso a datos sensibles si hay una justificación clara.

Revisiones cada 6 meses para asegurar que nadie tenga más permisos de los necesarios.

Monitoreo y Auditoría

Para detectar actividades sospechosas, se aplicarán herramientas de monitoreo y auditoría, como sistemas DLP y registros de acceso (logs).

Se revisarán acciones como:

Copiar archivos sensibles a USB o la nube.

Enviar información confidencial por correo.

Se harán auditorías periódicas para comprobar que las políticas se cumplen.

Prevención de Filtraciones

Para evitar que los datos se filtren:

Cifrado de datos: Tanto los datos en reposo (discos, servidores) como los datos en movimiento (correo, transferencias).

Bloqueo de dispositivos externos: USB, discos duros y almacenamiento personal no autorizado.

Controles de aplicaciones: Solo software autorizado puede acceder a los datos sensibles.

Educación y Concientización

El personal recibirá capacitación sobre:

Qué son los datos sensibles y por qué deben protegerse.

Cómo aplicar las políticas DLP en su día a día.

Qué hacer si detectan un posible riesgo o filtración.

Caso práctico

El Caso Equifax mostró cómo una falta de DLP puede exponer millones de datos personales.
Si hubieran clasificado sus datos correctamente, aplicado controles de acceso y cifrado, y monitoreado el uso de los datos, podrían haber evitado la filtración o detectado el problema antes.