Manual DLP

1. Introducción al Data Loss Prevention (DLP)

El **Data Loss Prevention (DLP)** es un conjunto de prácticas y tecnologías que permiten a las organizaciones prevenir la pérdida, filtración o acceso no autorizado a datos confidenciales. DLP asegura que la información sensible se mantenga protegida, tanto cuando está almacenada como en tránsito, y ayuda a prevenir la exposición accidental o malintencionada.

La importancia de DLP dentro de una organización radica en su capacidad para proteger los activos de datos más valiosos, incluidos aquellos que contienen información financiera, datos personales de empleados o clientes, propiedad intelectual y otros datos críticos. Un sistema robusto de DLP permite no solo proteger la integridad y confidencialidad de los datos, sino también cumplir con normativas y regulaciones de protección de datos, como el GDPR, HIPAA o PCI-DSS.

2. Clasificación de datos

Para implementar una estrategia efectiva de DLP, es fundamental que la organización clasifique sus datos en función de su sensibilidad y criticidad. Esta clasificación ayudará a identificar qué datos requieren mayores niveles de protección y cómo se deben gestionar dentro del entorno empresarial. A continuación se definen tres categorías de clasificación de datos:

- **Datos Públicos:** Esta categoría incluye la información que es accesible por el público en general y cuya divulgación no representa un riesgo para la organización. Ejemplos incluyen comunicados de prensa, publicaciones en redes sociales o información corporativa pública.

- **Datos Internos:** Información restringida al personal de la organización y que no debe ser divulgada fuera de la empresa sin autorización. La divulgación accidental o intencionada de estos datos podría generar daños reputacionales menores. Ejemplos incluyen políticas internas, procedimientos operativos y comunicaciones internas.

- **Datos Sensibles:** Información crítica que, si se expone o pierde, puede causar daños significativos a la organización, sus clientes o empleados. Esta información incluye datos financieros, información personal identificable (PII), propiedad intelectual, y credenciales de acceso. Estos datos requieren los más altos niveles de protección.

3. Acceso y Control

Basado en el **principio del menor privilegio**, el acceso a los datos sensibles se otorga únicamente a aquellos empleados que lo necesiten para desempeñar sus funciones. Esto implica restringir los permisos y accesos de manera que los usuarios solo tengan acceso a

los datos estrictamente necesarios. La revisión de permisos será un proceso recurrente para garantizar que los accesos se mantengan alineados con las funciones laborales de los empleados.

- **Responsables de revisión de permisos:**
    - **Departamento de TI:** Supervisará y realizará ajustes en los niveles de acceso a los sistemas y datos sensibles.
    - **Gerentes de Área:** Revisarán periódicamente los accesos de sus equipos para asegurar que cumplen con el principio del menor privilegio.
    - **Oficial de Seguridad de la Información (CISO):** Revisará los procesos y controles de acceso para garantizar el cumplimiento de las políticas de seguridad.

El flujo de revisión de permisos se llevará a cabo trimestralmente, donde cada gerente de área revisará y validará los accesos de su equipo, y el departamento de TI realizará ajustes según sea necesario.

4. Monitoreo y Auditoría

Es crucial implementar un sistema de monitoreo continuo y auditoría para detectar posibles violaciones de seguridad o usos indebidos de los datos sensibles. Se establecerán políticas específicas para la supervisión de los flujos de datos y las actividades relacionadas con la manipulación de información clasificada.

Las herramientas de monitoreo y auditoría que se utilizarán incluyen:

- **Soluciones SIEM (Security Information and Event Management):** Estas herramientas integran registros de eventos de seguridad de diferentes fuentes, detectan actividades anómalas y generan alertas en tiempo real.
- **Herramientas DLP:** Soluciones específicas de DLP monitorearán el flujo de información dentro y fuera de la red de la organización para prevenir la salida no autorizada de datos sensibles. Estas herramientas también permitirán bloquear o cifrar los datos que se consideren riesgosos para la filtración.

Los logs de actividad y las auditorías de acceso serán revisados mensualmente por el equipo de TI y se realizará un análisis de incidentes ante cualquier actividad sospechosa detectada.

5. Prevención de Filtraciones

Para prevenir la filtración de datos sensibles, se aplicarán las siguientes medidas tecnológicas:

- **Cifrado de datos:** Los datos sensibles se cifrarán tanto en reposo como en tránsito. Esto incluye correos electrónicos, documentos almacenados en servidores locales o en la nube, y cualquier tipo de transferencia de datos a través de redes públicas o internas.

- **Herramientas DLP:** Las soluciones de DLP se configurarán para identificar patrones de datos sensibles (como números de tarjetas de crédito o identificaciones personales) y bloquear su transferencia no autorizada a través de correos electrónicos, impresoras o dispositivos externos.

- **Control de dispositivos externos:** Se implementarán restricciones sobre el uso de dispositivos de almacenamiento externos (como USB) y se configurarán para cifrar automáticamente los datos que se copien a dichos dispositivos.

6. Educación y Concientización

Un componente esencial de la política de DLP es la capacitación continua de todo el personal sobre los riesgos de seguridad de la información y las mejores prácticas para proteger los datos. Se implementarán los siguientes programas de educación y concientización:

- **Capacitaciones regulares:** Se ofrecerán capacitaciones obligatorias semestrales a todos los empleados para que comprendan las políticas de seguridad y las tecnologías utilizadas para proteger los datos sensibles.

- **Simulaciones de phishing:** Se realizarán simulaciones de ataques de phishing para capacitar a los empleados sobre cómo detectar y reaccionar ante correos electrónicos sospechosos.

- **Materiales de concientización:** Se distribuirán regularmente boletines informativos y se colocarán recordatorios visuales en áreas comunes sobre la importancia de proteger los datos confidenciales y reportar cualquier actividad sospechosa.