POLÍTICAS DE SEGURIDAD - DATA LOSS PREVENTION (DLP)

Kevin Pitti – 4Geeks Academy

Introducción al Data Loss Prevention (DLP)

Hoy en día, las empresas manejan muchísima información todos los días, desde datos de clientes y empleados hasta documentos internos importantes. Si esa información llega a perderse o cae en manos equivocadas, puede causar muchos problemas: pérdidas de dinero, daño a la imagen de la empresa o incluso problemas legales.

Para evitar eso, existe algo llamado DLP, que en español significa Prevención de Pérdida de Datos. En palabras simples, el DLP es un conjunto de reglas, herramientas y buenas prácticas que nos ayudan a proteger la información más importante de la empresa. Su objetivo principal es evitar que esos datos se compartan por accidente o que alguien sin autorización acceda a ellos.

Con estas políticas, buscamos no solo proteger los datos sensibles, sino también enseñar a todas las personas dentro de la empresa cómo manejar correctamente la información, creando así un ambiente más seguro y responsable para todos.

Clasificación de Datos

Para poder proteger adecuadamente la información, lo primero que debemos hacer es **clasificar los datos** en función de su sensibilidad. Esta clasificación nos permitirá aplicar diferentes niveles de seguridad dependiendo del tipo de información.

Nuestra organización usará la siguiente clasificación:

- **Datos Públicos**: Información que puede ser compartida sin restricciones. Ejemplos: contenido del sitio web, comunicados de prensa, horarios de atención.
- **Datos Internos**: Información que es de uso exclusivo dentro de la empresa, pero que no causaría un daño grave si se filtrara. Ejemplos: políticas internas, procedimientos operativos, manuales técnicos.
- **Datos Sensibles**: Información confidencial que puede causar daño financiero, legal o reputacional si se ve comprometida. Ejemplos: datos de clientes, estados financieros, credenciales de acceso, secretos comerciales.

Acceso y Control de Datos

Siguiendo el **principio del menor privilegio**, cada empleado o colaborador solo tendrá acceso a los datos que necesita para hacer su trabajo. Esto minimiza el riesgo de acceso no autorizado o filtraciones accidentales.

Políticas de acceso:

- Todos los nuevos accesos deben ser solicitados por un supervisor y aprobados por el departamento de TI o Seguridad de la Información.
- Los accesos serán revisados cada **tres meses** para verificar si aún son necesarios.
- Los roles involucrados en la revisión de permisos son:
    - **Jefe de Departamento**: revisa y justifica los accesos de su equipo.
    - **Equipo de TI / Seguridad**: valida y aplica los cambios necesarios.

Además, cualquier cambio de puesto o salida de personal deberá incluir una revisión inmediata de sus accesos.

Monitoreo y Auditoría

Para garantizar que se cumplan las políticas de seguridad, es fundamental contar con un sistema de **monitoreo y auditoría continua**.

Herramientas utilizadas:

- **SIEM (Ejemplo: Wazuh)**: Nos permite recopilar y analizar eventos del sistema, detectar comportamientos anómalos y generar alertas en tiempo real.
- **Herramienta de DLP (Ejemplo: Symantec DLP, Microsoft Purview)**: Estas soluciones ayudan a identificar, monitorear y proteger datos sensibles, incluso cuando están en movimiento (como en correos electrónicos o dispositivos USB).

Se realizarán **auditorías trimestrales** para revisar el acceso a los datos sensibles y detectar actividades sospechosas. Además, cualquier intento de copiar o enviar datos sensibles fuera de la red será registrado y revisado por el equipo de seguridad.

Prevención de Filtraciones

Para evitar que los datos sensibles salgan de la empresa, se aplicarán las siguientes medidas:

- **Cifrado de datos**: Todos los datos sensibles serán cifrados tanto en tránsito (cuando viajan por la red) como en reposo (cuando están almacenados en discos o servidores).
- **Bloqueo de dispositivos USB no autorizados**.
- **Control del tráfico de red**: mediante firewalls y proxies se bloqueará el envío no autorizado de archivos fuera de la organización.
- **Uso de herramientas DLP** para bloquear automáticamente correos electrónicos o transferencias que contengan información confidencial no permitida.

Estas medidas serán reforzadas constantemente con revisiones técnicas y actualizaciones de las herramientas de seguridad.

Educación y Concientización

La tecnología por sí sola no es suficiente si los empleados no están capacitados. Por eso, uno de los pilares fundamentales de esta política es la **educación y concientización** del personal.

Plan de capacitación:

- **Charlas mensuales** sobre seguridad de la información.
- **Simulacros de ataques de ingeniería social** como el phishing, para que el personal aprenda a identificarlos.
- **Manuales y recursos accesibles** con las políticas DLP y buenas prácticas.
- Evaluaciones periódicas para reforzar los conocimientos.

La idea es crear una cultura de seguridad en la organización, donde cada colaborador entienda que **la protección de los datos es responsabilidad de todos**.

Conclusión

Con estas políticas de DLP buscamos proteger uno de los activos más importantes de la organización: la información. Aplicando controles técnicos, procesos claros y capacitando al personal, reducimos al mínimo los riesgos de pérdida o filtración de datos sensibles. Este plan no solo cumple con buenas prácticas internacionales, sino que también refuerza la confianza de nuestros clientes, empleados y socios comerciales.