Políticas de Seguridad para la Prevención de Pérdida de Datos (DLP)

Introducción al Data Loss Prevention (DLP)

La Prevención de Pérdida de Datos (DLP) es un conjunto de estrategias y herramientas utilizadas para asegurar que la información confidencial de una organización no se pierda, sea mal utilizada o accedida por personas no autorizadas. Las soluciones de DLP permiten identificar, monitorear y proteger los datos en uso, movimiento y reposo. Dentro de una organización, su aplicación es esencial para proteger propiedad intelectual, datos financieros, registros personales y otros activos digitales sensibles.

El presente documento establece las políticas de DLP de la organización, bajo el principio del menor privilegio, asegurando que sólo el personal autorizado tenga acceso a la información necesaria para el cumplimiento de sus funciones.

Clasificación de Datos

La clasificación de los datos permite establecer diferentes niveles de protección según su grado de sensibilidad. Para esta organización, los datos se dividen en tres categorías principales:

- **Datos Públicos**: Información general de la empresa que puede ser compartida con cualquier empleado e incluso con el público externo, sin implicaciones de seguridad.
- **Datos Internos**: Documentos administrativos, procedimientos y comunicados internos. Solo pueden ser accedidos por el personal autorizado dentro de la organización.
- **Datos Sensibles**: Información altamente confidencial como contratos, información financiera, datos de clientes o empleados. Su acceso está limitado a directivos o personal expresamente autorizado.

Acceso y Control

La asignación de permisos se realizará de forma que cada empleado tenga acceso únicamente a los datos estrictamente necesarios para realizar sus funciones:

- **Acceso Restringido**: Cada departamento tendrá acceso únicamente a las carpetas y documentos que requiera.
- **Revisión Periódica de Permisos**: Cada tres meses se revisarán los accesos para asegurar que solo el personal activo mantenga permisos adecuados.
- **Accesos Temporales**: Cuando se requiera acceso puntual a datos sensibles, éste será concedido mediante solicitud formal y revocado tras la finalización de la tarea.
- **Permisos de Edición**: Sólo los responsables directos podrán editar documentos sensibles; los demás tendrán acceso de solo lectura.

Monitoreo y Auditoría

Para garantizar el cumplimiento de las políticas, se implementarán mecanismos de supervisión:

- **Registro de Actividades**: Se registrarán las acciones realizadas sobre los documentos sensibles (visualización, edición, descargas y distribución).
- **Herramientas de Monitoreo**: Se utilizarán soluciones SIEM o DLP para obtener visibilidad sobre los accesos y posibles incidentes.
- **Alertas de Seguridad**: Se configurarán alertas automáticas para cualquier acción sospechosa (como compartir archivos sensibles con usuarios externos).
- **Auditorías Trimestrales**: Se realizarán auditorías cada tres meses para identificar desviaciones y ajustar las políticas si es necesario.

Prevención de Filtraciones

Las siguientes medidas técnicas se implementarán para evitar la fuga de información:

- **Cifrado de Datos**: Toda información sensible será cifrada tanto en movimiento como en reposo.
- **Control de Dispositivos USB**: Se restringirá el uso de dispositivos USB a través de GPOs o soluciones DLP, permitiendo sólo dispositivos autorizados.
- **Bloqueo de Compartición Pública**: Se deshabilitará la opción de compartir con "cualquier persona con el enlace" en los documentos clasificados como sensibles.
- **Etiquetado de Documentos**: Se usarán etiquetas de "Confidencial" y "Solo uso interno" para archivos sensibles, que activarán restricciones automáticas.

Educación y Concientización

La formación del personal es un componente fundamental de esta estrategia:

- **Capacitaciones Trimestrales**: Se organizarán sesiones obligatorias para repasar las políticas de seguridad y actualizaciones relevantes.
- **Material Educativo**: Se distribuirán boletines digitales, infografías y videos cortos con ejemplos prácticos.
- **Simulacros de Incidentes**: Se realizan ejercicios simulados para preparar al personal en caso de incidentes reales de seguridad.