INFORME DE POLÍTICAS DE SEGURIDAD DLP

Proyecto: Implementación de Control de Acceso y Prevención de Fuga de Datos

Fecha de Ejecución: Febrero 2026

Elaborado por: Jose Rodriguez

ÍNDICE

1. Introducción

La información es uno de los activos más valiosos de la organización. La falta de controles adecuados puede derivar en brechas de seguridad masivas, sanciones financieras y daños reputacionales. Este documento establece la política oficial de Prevención de Pérdida de Datos (DLP), diseñada bajo el Principio del Menor Privilegio (PoLP), para garantizar que los datos sensibles sean accedidos, utilizados y transmitidos únicamente por personal autorizado.

2. Clasificación de Datos

Para aplicar controles proporcionales al riesgo, la información se categoriza en tres niveles de sensibilidad:

- **Nivel 1 - Documentos Públicos:** Información destinada a la difusión general (ej. material de marketing, comunicados de prensa). No requiere restricciones de acceso.
- **Nivel 2 - Documentos Internos:** Datos para uso exclusivo de empleados (ej. manuales de procesos, organigramas). Requiere autenticación corporativa.
- **Nivel 3 - Documentos Sensibles:** Información crítica (ej. PII, datos financieros, contratos legales, secretos comerciales). El acceso está restringido a niveles directivos o roles específicos bajo estricta necesidad.

3. Principio del Menor Privilegio (PoLP)

La organización adoptará el Principio de menor privilegio como base de su seguridad. Esto implica:

- **Acceso por Necesidad:** Los permisos se otorgan basándose exclusivamente en las funciones del puesto de trabajo.
- **Revisión de Accesos:** Los privilegios de acceso serán auditados trimestralmente para revocar permisos innecesarios o de empleados que hayan cambiado de rol.

4. Controles en Almacenamiento en la Nube (Google Drive)

Siguiendo los estándares de seguridad de la infraestructura cloud, se aplican las siguientes restricciones:

- **Deshabilitación de Enlaces Públicos:** La opción "Cualquier persona con el enlace" queda desactivada por defecto para documentos de Nivel 2 y 3.
- **Compartición Controlada:** El acceso externo solo se permitirá a socios aprobados bajo permisos de "Solo Lectura", inhabilitando las opciones de descarga, impresión o copia.
- **Etiquetado Automático:** Los archivos con contenido sensible (ej. números de tarjeta o SSN) recibirán etiquetas automáticas de "Confidencial".

5. Controles de Endpoints y Dispositivos Físicos

Para mitigar la fuga de datos a través de medios físicos:

- **Restricción de Dispositivos USB:** Se bloquea el uso de unidades de almacenamiento extraíbles en todas las estaciones de trabajo, salvo excepciones autorizadas por el equipo de seguridad para casos de uso específicos.
- Cifrado de Datos en Reposo: Todos los equipos de la empresa deben tener activo el cifrado de disco (BitLocker, FileVault o LUKS) para proteger la información en caso de robo o pérdida del hardware.

6. Gestión de Excepciones y Cumplimiento

- Proceso de Excepción: Cualquier desviación de esta política debe ser solicitada formalmente, revisada por el gerente de DLP y documentada con una fecha de expiración.
- Cumplimiento Normativo: Estas políticas se alinean con marcos legales como el RGPD (protección de datos personales) y PCI-DSS (seguridad de datos financieros).
- Monitoreo: Se mantendrán registros de auditoría (logs) de todos los intentos de acceso y transferencias de archivos sensibles.

7. Educación y Concientización

El factor humano es la primera línea de defensa.

- Capacitación Trimestral: Todo el personal debe completar módulos de formación sobre manejo seguro de información y riesgos de ingeniería social.
- Reporte de Incidentes: Se incentiva la notificación inmediata de cualquier fuga accidental de datos sin temor a represalias, para activar los protocolos de mitigación.

8. Conclusión

La implementación de esta política de DLP y el cumplimiento estricto del Principio del Menor Privilegio permiten a la organización proteger su propiedad intelectual y la privacidad de sus clientes. La seguridad es una responsabilidad compartida que garantiza la continuidad y la integridad de nuestras operaciones.