TechCorp Inc.

POLITICA DE PREVENCION DE PERDIDAS DE DATOS (DLP)

1. INTRODUCCION

La Prevención de Pérdida de Datos (DLP) es un conjunto de políticas, procedimientos y tecnologías implementadas para detectar y prevenir la fuga, filtración o pérdida no autorizada de datos sensibles desde los sistemas de la organización.

En TechCorp Inc., esta política busca establecer los lineamientos para proteger información crítica, minimizando los riesgos asociados al mal uso, exposición o pérdida de datos

2. OBJETIVO

El objetivo principal de esta política es:

- Proteger la información confidencial y sensible de la organización.
- Prevenir la fuga de información a través de diferentes canales, como correo electrónico, dispositivos extraíbles, servicios en la nube e impresión.
- Detectar y responder a las fugas de información de manera oportuna.
- Cumplir con las leyes, regulaciones y estándares de seguridad aplicables.
- Concienciar a los empleados sobre la importancia de la protección de la información.

3. ALCANCE

Esta política se aplica a todos los empleados, contratistas, consultores y cualquier otra persona que tenga acceso a la información de TechCorp Inc. Aplica a toda la información confidencial y sensible, incluyendo:

- Datos de clientes
- Datos de empleados
- Información financiera
- Propiedad intelectual
- Información de salud
- Información estratégica

4. DEFINICIONES

- **Fuga de información:** La divulgación no autorizada de información confidencial o sensible fuera de la organización.
- **Información confidencial:** Información que, si se divulga sin autorización, podría causar un daño significativo a la organización o a terceros.
- **Información sensible**: Información que requiere un grado de protección especial, aunque su divulgación no cause un daño significativo.

5. RESPONSABILDIADES

- **Alta Dirección:** Es responsable de aprobar y apoyar esta política.
- **Departamento de Seguridad de la Información:** Es responsable de desarrollar, implementar y mantener esta política.
- **Propietarios de la Información:** Son responsables de clasificar y proteger la información bajo su control.
- **Todos los Empleados:** Son responsables de cumplir con esta política y de proteger la información de la organización.

6. DIRECTRICES

A. Clasificación de Datos

Todos los datos tratados por la organización deben ser clasificados en función de su sensibilidad y el impacto que causaría su exposición o pérdida. Las categorías establecidas son:

- **Datos Sensibles:** Información crítica cuyo acceso, modificación o pérdida no autorizada podría generar un impacto significativo legal, financiero o reputacional. Incluye:
  - ✓ Datos personales y currículums del personal.
  - ✓ Datos financieros (nómina, presupuestos, inversiones).
  - ✓ Información confidencial de clientes.
  - ✓ Propiedad intelectual y código fuente.

- **Datos Internos:** Información accesible solo al personal autorizado de TechCorp. Su divulgación no autorizada podría causar daño operativo o reputacional. Ejemplos: organigramas, manuales internos, datos de contacto interno.
- **Datos Públicos:** Información que puede ser divulgada sin restricciones. Ejemplos: información institucional publicada en el sitio web, campañas de marketing, comunicados oficiales.

B. Control de Acceso a la información

TechCorp Inc. aplica el **principio del menor privilegio**, garantizando que cada usuario tenga acceso únicamente a los datos necesarios para cumplir sus funciones.

- El acceso a los datos será gestionado por el área de Seguridad de la Información, en conjunto con los responsables de cada departamento.
- Toda solicitud de acceso debe pasar por una revisión formal y ser autorizada por un supervisor o responsable de área.
- El acceso a datos sensibles requerirá doble validación y será revisado de forma semestral.
- Se llevarán registros de todas las asignaciones y revocaciones de permisos.
- Se utilizarán controles de autenticación fuerte (MFA) para acceder a sistemas con datos sensibles.

C. Prevención de Filtraciones

Se adoptarán mecanismos técnicos y organizativos para prevenir fugas de información:

- Cifrado obligatorio de datos sensibles, tanto en tránsito como en reposo.
- Bloqueo automático de dispositivos extraíbles en puestos de trabajo donde no sean requeridos.
- Políticas de uso aceptable que prohíban el envío de información sensible a correos personales o plataformas no autorizadas.
- Restricción de impresión de documentos clasificados sin autorización previa.
- No se debe proporcionar información confidencial o sensible a plataformas de IA sin autorización.

D. Prevención de Filtraciones

Para proteger la información sensible y detectar actividades anómalas, se implementará un sistema de monitoreo continuo y auditoría periódica, que incluirá:

- Herramientas DLP para controlar la transferencia de datos vía correo electrónico, dispositivos USB, servicios en la nube y navegación web.

- Sistemas SIEM para correlacionar eventos y detectar posibles incidentes de seguridad.
- Auditorías internas semestrales para revisar los accesos, movimientos y manipulaciones de información crítica.
- Generación de reportes automáticos sobre actividades sospechosas, que serán evaluados por el equipo de seguridad de la información.

E. Educación y Concientización

La protección de los datos es responsabilidad de todos los colaboradores. Para fomentar una cultura de seguridad, se implementará un programa continuo de capacitación y concientización, que incluye:

- Charlas periódicas sobre buenas prácticas de seguridad de la información.
- Simulacros y pruebas de respuesta ante incidentes.
- Módulos de formación obligatoria para nuevos ingresos y renovaciones anuales.
- Difusión de alertas y comunicados ante riesgos emergentes (phishing, ransomware, etc.).