



# **Análisis de Datos Sensibles en una Organización Ficticia**

**Ramón Tirado Fernández**

# Índice

- 1. Introducción ..... 1
- 2. Identificación y Clasificación de Datos Sensibles..... 1
  - 2.1. Datos por Departamento ..... 1
  - 2.2. Políticas de TechCorp Relacionadas .....2
- 3. Mapeo de Flujos de Datos y Puntos de Riesgo .....3
  - 3.1. Diagrama de Flujo .....3
  - 3.2. Puntos de Riesgo y Controles DLP .....3
- 4. Recomendaciones.....4
- 5. Conclusión.....4



# 1. Introducción

TechCorp Inc. es una empresa de desarrollo de software con 200 empleados que maneja información crítica en áreas como finanzas, atención médica y comercio electrónico. Este informe identifica los datos sensibles en cada departamento, clasifica su nivel de riesgo, mapea los flujos de datos y propone controles de Prevención de Pérdida de Datos (DLP) para mitigar vulnerabilidades.

## 2. Identificación y Clasificación de Datos Sensibles

### 2.1. Datos por Departamento

Departamento	Datos Sensibles Identificados	Clasificación	Razón de Sensibilidad
Recursos Humanos	<ul style="list-style-type: none"><li>- Datos personales de empleados (PII)</li><li>- Registros de nóminas y beneficios</li></ul>	<div><div></div>Alta</div>	Incluye información privada protegida por leyes laborales.
	<ul style="list-style-type: none"><li>- Evaluaciones de desempeño</li></ul>	<div><div></div>Media</div>	Confidenciales, pero no críticas para la seguridad.
Finanzas	<ul style="list-style-type: none"><li>- Estados financieros</li><li>- Datos bancarios</li></ul>	<div><div></div>Alta</div>	Críticos para la competitividad y cumplimiento legal.
I+D	<ul style="list-style-type: none"><li>- Código fuente y patentes</li></ul>	<div><div></div>Alta</div>	Propiedad intelectual clave para la empresa.
	<ul style="list-style-type: none"><li>- Feedback de clientes no anonimizado</li></ul>	<div><div></div>Media</div>	Puede contener PII o información comercial.

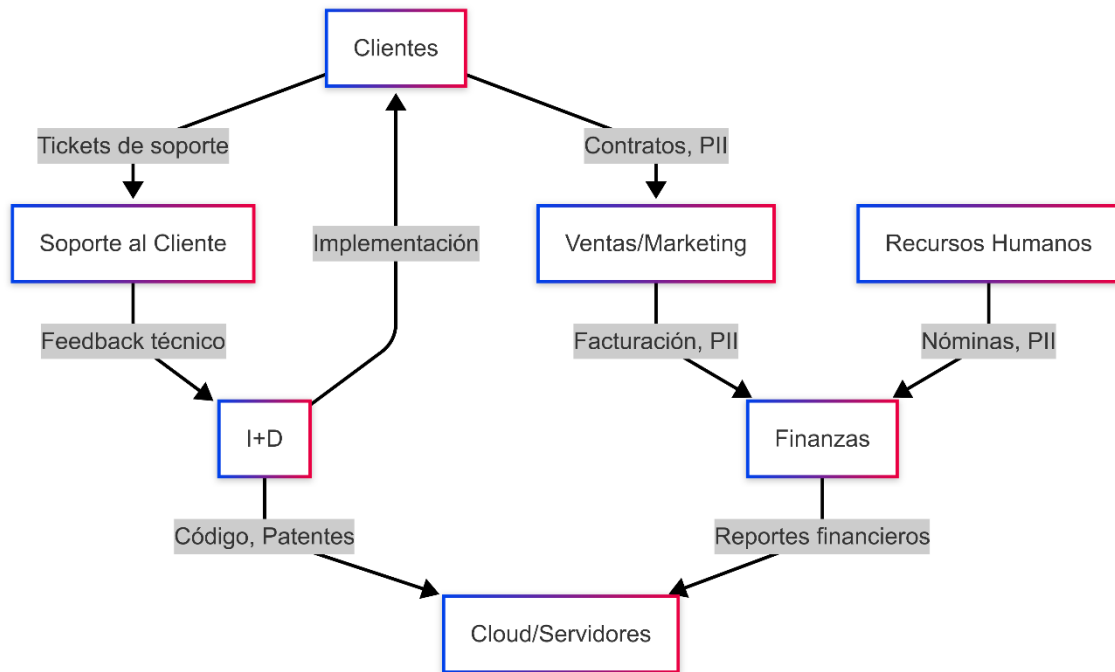
Departamento	Datos Sensibles Identificados	Clasificación	Razón de Sensibilidad
Soporte al Cliente	- Credenciales de clientes	 Alta	Riesgo de suplantación o brechas de seguridad.
	- Tickets con PII	 Media	Datos personales en registros de soporte.
Ventas y Marketing	- Bases de datos de clientes (PII)	 Alta	Protegidos por GDPR.
	- Estrategias de precios no publicadas	 Media	Sensibles comercialmente.

## 2.2. Políticas de TechCorp Relacionadas

- Política de Protección de Datos: Cumple con GDPR para PII.
- Infraestructura de TI: Usa cloud seguro y cifrado (mencionado en el PDF).
- Código de Conducta: Regula el manejo de información confidencial.

## 3. Mapeo de Flujos de Datos y Puntos de Riesgo

### 3.1. Diagrama de Flujo



- Clientes → Ventas/Marketing: Envío de PII (contratos, datos de contacto).
- Soporte al Cliente → I+D: Tickets con feedback sensible.
- HR → Finanzas: Transferencia de nóminas y datos bancarios.
- I+D → Cloud: Almacenamiento de código fuente y documentación técnica.

### 3.2. Puntos de Riesgo y Controles DLP

Punto de Riesgo	Riesgo	Control DLP Sugerido
Correos con PII entre Ventas y Finanzas	Filtración de datos personales.	Cifrado automático en emails con términos clave ("contrato", "cliente").
Repositorios de código en la nube	Acceso no autorizado a IP.	Autenticación MFA y segmentación de redes.
Tickets de soporte con credenciales	Exposición en chats internos.	Bloquear mensajes con patrones de credenciales (ej. regex en Slack/Microsoft Teams).

## 4. Recomendaciones

A. Priorizar protección en:

- Código fuente (I+D) y PII (HR, Ventas).
- Comunicaciones internas con datos financieros.

B. Implementar:

- Cifrado integral para datos en tránsito y almacenados.

C. Capacitación Monitoreo proactivo:

- Uso de herramientas DLP para detectar fugas en tiempo real en GDPR para HR y Soporte al Cliente.

## 5. Conclusión

TechCorp Inc. maneja datos altamente sensibles, especialmente en Finanzas, I+D y Ventas. Los mayores riesgos están en la transferencia no cifrada de PII y el almacenamiento de código en la nube. La implementación de controles DLP basados en cifrado, MFA y monitoreo de comunicaciones reducirá significativamente las vulnerabilidades, alineándose con las políticas existentes de la empresa.