ANALISIS DE DATOS SENSIBLES DE UNA ORGANIZACIÓN

1. **Incentivación y Clasificación de datos sensibles**
    a. **Datos por Departamento**

RECURSOS HUMANOS		
Tipo de Dato	**Descripción**	**Clasificación**
Nombre, DNI, y dirección de empleados (PII)	Información personal identificable (PII)	● **Alta**
HC médico y ausencias por salud	Información de salud y desempeño	● **Alta**
Información de nóminas y cuentas bancarias	Datos financieros personales	● **Alta**
Evaluaciones de desempeño y sanciones	Datos internos de gestión	● **Media**
Registro de capacitación y certificaciones	Documentación Legal	● **Baja**

FINANZAS		
Tipo de Dato	**Descripción**	**Clasificación**
Estados financieros corporativos	Balance, flujo de caja	● **Alta**
Detalles de cuentas bancarias y transferencias	Información financiera crítica	● **Alta**
Registro de nómina de empleados	Transacciones sobre pagos, beneficios y deducciones	● **Alta**
Proyecciones presupuestarias y estrategias de inversión	Planificación financiera futura para decisiones estratégicas	● **Media**
Informes de auditoría interna/externa	Evaluaciones de cumplimiento financiero control interno	● **Media**

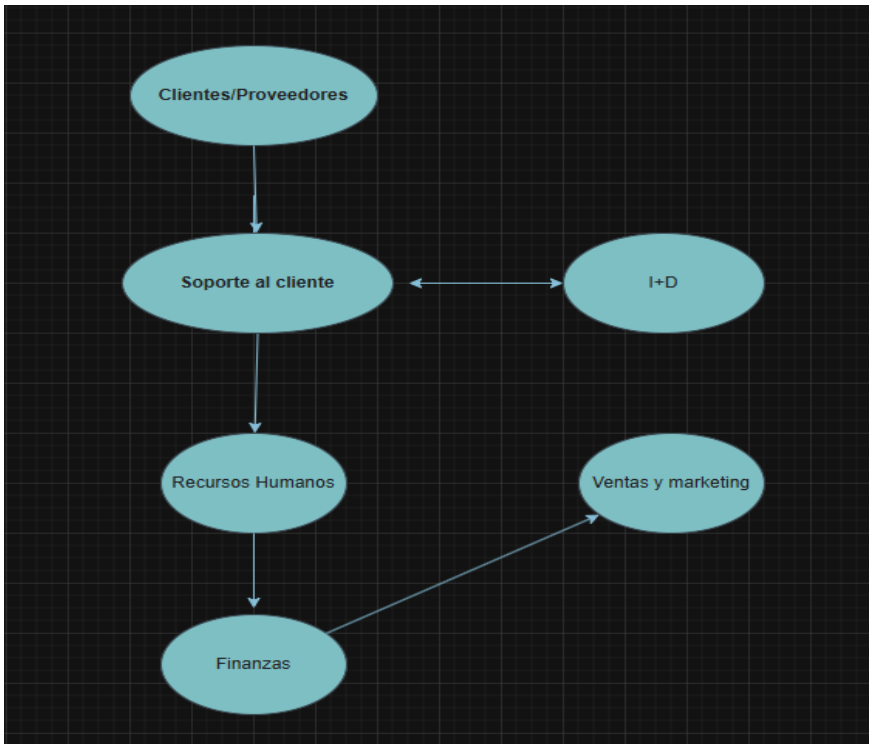
INVESTIGACIÓN Y DESARROLLO		
Tipo de Dato	**Descripción**	**Clasificación**
Código fuente propietario	Activo crítico que constituye el núcleo de los productos desarrollados	● **Alta**
Diseño de Arquitectura de software	Estructuras técnicas que detallan el funcionamiento de software	● **Alta**
Documentación Técnica de proyectos internos	Manuales, especificaciones y detalles operativos de los sistemas en desarrollo	● **Media**
Reportes de pruebas y QA	Resultados de controles de calidad sobre versiones de software	● **Media**
Feedback técnico confidencial de clientes	Comentarios e información sensible proporcionada por clientes durante el desarrollo	● **Alta**

SOPORTE AL CLIENTE		
Tipo de Dato	**Descripción**	**Clasificación**
Datos de contacto de clientes (nombre, correo, teléfono)	Información de identificación personal de clientes para soporte	● **Alta**
Historial de Tickets de soporte+	Registro de solicitudes, problemas y soluciones proporcionadas a los clientes	● **Media**
Grabaciones de llamadas/chat	Archivos multimedia que pueden contener información sensible durante la atención	● **Media**
Credenciales temporales o accesos brindados	Información que puede otorgar acceso temporal a sistemas o entornos de producción	● **Alta**
Comentarios o reclamos recibidos	Opiniones generales de los clientes que no contienen datos personales	● **Baja**

VENTAS Y MARKETING		
Tipo de Dato	**Descripción**	**Clasificación**
Bases de datos prospectos/clientes (emails, empresa, teléfono)	Información recolectada para contacto comercial y ventas	**Media**
Información de contratos de clientes	Detalles legales y financieros sobre acuerdos comerciales con clientes	**Alta**
Estrategias y campañas de marketing	Planes internos para promocionar productos y captar mercado	**Baja**
Análisis de mercado y posicionamiento competitivo	Información sobre tendencias, competencia y segmentación del público objetivo	**Media**
Métricas de conversión y resultados	Estadísticas sobre la efectividad de iniciativas de marketing	**Baja**

2. Mapeo de Flujo de datos y puntos de riesgo

a. Flujo de Información



Fuente: Elaboración Propia

b. Puntos de Riesgo Identificados y controles DLP

Puntos de Riesgo	Riesgo Potencial	Control DLP sugeridos
Envío de PII o archivos financieros	**Filtración accidental o intencional de datos**	**Filtro DLP por contenido + Cifrado automático**
Acceso sin control a carpetas compartidas	**Acceso no autorizado a datos críticos**	**Control de acceso basado en rol (RBAC) + Monitoreo**
Feedback Técnico no cifrado desde clientes hacia I+D	**Exposición de propiedad intelectual**	**Uso obligatorio de VPN + TSL + canal autenticado**

3. Informe Resumido

Resumen Ejecutivo

Este informe identifica los principales datos sensibles manejados por TechCorp Inc., los flujos de información interna y externa, y los puntos donde existe riesgo de fuga de datos. A través de la clasificación de datos por nivel de sensibilidad, se identificaron los departamentos más críticos (I+D, Finanzas y Soporte). Se proponen controles básicos de prevención de pérdida de datos (DLP), como cifrado automático, control de accesos y monitoreo de carpetas compartidas, para reducir riesgos potenciales de filtraciones.