**1. Identificación y Clasificación de Datos Sensibles**

**a) Identificación de tipos de datos sensibles por departamento:**

**- Recursos Humanos (HR):**

- Datos sensibles: Información personal identificable (PII) de empleados, incluyendo nombres, direcciones y teléfonos, historial de empleo, información de nómina, evaluaciones de desempeño, y datos de salud.

**- Clasificación: Alta Sensibilidad (🔴).**

**- Finanzas:**

- Datos sensibles: Información financiera (balances y reportes), cuentas bancarias, números de tarjetas de crédito, presupuestos y proyecciones, información de transacciones y pagos.

**- Clasificación: Alta Sensibilidad (🔴).**

**- Investigación y Desarrollo (I+D):**

- Datos sensibles: Propiedad intelectual (códigos fuente y patentes), detalles de proyectos en desarrollo, documentación técnica, resultados de investigaciones, y estrategias de innovación.

- Clasificación: Alta Sensibilidad (🔴).

**- Soporte al Cliente:**

- Datos sensibles: Información de contacto y detalles de interacciones de clientes, tickets de soporte, credenciales de acceso (si se aplican), encuestas de satisfacción y detalles técnicos de sistemas de clientes.

- Clasificación: Media Sensibilidad (🟠).

**- Ventas y Marketing:**

- Datos sensibles: Datos de clientes potenciales y actuales, análisis de mercado, información de campañas de marketing, datos sobre comportamiento de clientes y proveedores.

**- Clasificación: Media Sensibilidad (🟠).**

**b) Clasificación de Sensibilidad de Datos:**

Cada tipo de dato se clasifica según la sensibilidad en alta, media o baja de acuerdo con su potencial impacto en la seguridad y privacidad de la empresa y sus clientes.

**2. Mapeo de Flujos de Datos y Puntos de Riesgo**

**a) Diagrama de flujo de datos:**

Los datos fluyen a través de distintos canales y ubicaciones en TechCorp Inc., lo cual incluye:

- Canales de comunicación interna: Correos electrónicos y chat corporativo.

- Comunicación externa: Interacciones con clientes y proveedores.

- Almacenamiento de datos: Servidores locales y en la nube, así como unidades compartidas.

**b) Puntos de riesgo identificados:**

- Correo electrónico: El intercambio de información no cifrada puede exponer datos financieros o PII de empleados.

- Unidades compartidas: Riesgo de acceso no autorizado a documentos de HR o Finanzas.

- CRM y plataformas de soporte: Posible fuga de datos de clientes si se gestionan sin seguridad adecuada.

**c) Controles básicos de DLP para mitigar riesgos:**

- Cifrado de correos electrónicos y archivos sensibles para evitar fugas.

- Control de acceso y auditoría en unidades compartidas.

- Monitoreo de actividad en plataformas de CRM para detectar accesos sospechosos o descargas masivas de datos.

**3. Informe de Resultados**

**El informe incluye:**

- Inventario de Datos Sensibles: Lista de datos por departamento.

- Clasificación de Sensibilidad de Datos: Resumen visual por nivel de riesgo.

- Diagrama de Flujo de Datos: Representación de canales y puntos de almacenamiento.

- Puntos de Riesgo y Controles DLP: Listado de riesgos y medidas recomendadas para cada punto crítico.