Informe de Análisis de Seguridad de Datos en TechCorp Inc.

1. Tipos de Datos Sensibles por Departamento

A partir del análisis del documento proporcionado, se identificaron los siguientes tipos de datos sensibles manejados por los departamentos clave:

- **Recursos Humanos**:
  - Información Personal Identificable (PII)
  - Datos de contratación y evaluación del desempeño
  - Datos salariales
  - Registros de diversidad e inclusión
  - Documentos legales relacionados con el personal
- **Finanzas**:
  - Transacciones financieras
  - Información de presupuestos y nómina
  - Estrategias de inversión
  - Datos de análisis financiero
  - Contratos con clientes y proveedores
- **Investigación y Desarrollo (I+D)**:
  - Propiedad intelectual
  - Datos de investigación de mercado
  - Especificaciones técnicas de software
  - Planes de innovación tecnológica
  - Feedback de clientes
- **Soporte al Cliente**:
  - Registros de consultas de clientes
  - Datos técnicos de incidencias
  - Información de acceso a cuentas
  - Historial de soporte ofrecido
  - Encuestas de satisfacción
- **Ventas y Marketing**:
  - Datos de clientes potenciales
  - Estrategias de marketing
  - Contratos y acuerdos con clientes
  - Datos de mercado
  - Presupuestos de campañas

2. Clasificación de Datos Sensibles

Los datos sensibles fueron clasificados según su nivel de sensibilidad:

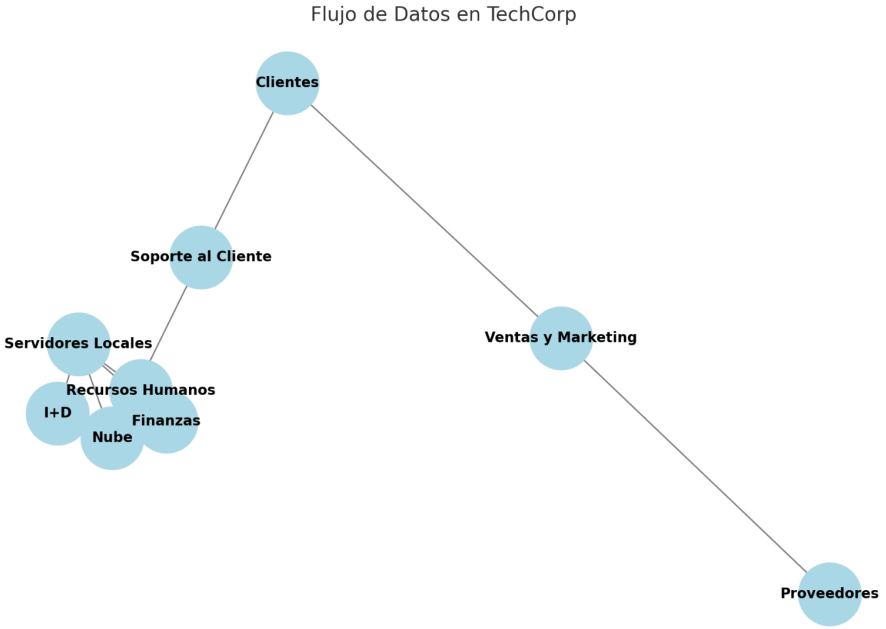
- **Alta Sensibilidad**: PII, Datos de contratación y evaluación del desempeño, Documentos legales relacionados con el personal, transacciones financieras, Información de presupuestos y nómina, Estrategias de inversión, propiedad intelectual, Especificaciones técnicas de software, Planes de innovación tecnológica, Registros de consulta de clientes, Datos técnicos de incidencias, Información de datos de acceso a cuentas, Contratos y acuerdos con clientes.
- **Media Sensibilidad**: Datos salariales, Registros de diversidad e inclusión, Datos de análisis financiero, Contratos con clientes y proveedores, Datos de investigación de mercado, Feedback de clientes, Historial de soporte ofrecido, datos técnicos, estrategias de marketing.
- **Baja Sensibilidad**: Información general de mercado y encuestas.

Recursos Humanos	- Información Personal Identificable (PII) - Datos de contratación y evaluación del desempeño - Datos salariales - Registros de diversidad e inclusión - Documentos legales relacionados con el personal	- Alta - Alta - Media - Media - Alta
Finanzas	- Transacciones financieras - Información de presupuestos y nómina - Estrategias de inversión - Datos de análisis financiero - Contratos con clientes y proveedores	- Alta - Alta - Alta - Media - Media
Investigación y Desarrollo	- Propiedad intelectual - Datos de investigación de mercado	- Alta - Media

	- Especificaciones técnicas de software - Planes de innovación tecnológica - Comentarios de clientes sobre productos	- Alta - Alta - Media
Soporte al Cliente	- Registros de consultas de clientes - Datos técnicos de incidencias - Información de acceso a cuentas - Historial de soporte ofrecido - Feedback y encuestas de satisfacción	- Alta - Alta - Alta - Media - Media
Ventas y Marketing	- Datos de clientes potenciales - Estrategias de marketing - Contratos y acuerdos con clientes - Datos de mercado - Presupuestos de campañas	- Media - Media - Alta - Media - Media

3. Diagrama de Flujo de Datos

El flujo de datos en TechCorp Inc. se visualizó mediante un diagrama que ilustra las conexiones entre los departamentos y los sistemas de almacenamiento (nube y servidores locales), así como las interacciones externas con clientes y proveedores.



4. Puntos de Riesgo y Controles DLP

Puntos de Riesgo Identificados:

1. **Configuración y accesos en la nube**:
    - Riesgo de configuraciones incorrectas y accesos no autorizados.
2. **Exposición de datos en Soporte al Cliente**:
    - Riesgo de fuga de datos sensibles durante interacciones.
3. **Transferencias entre departamentos y almacenamiento**:
    - Riesgo de pérdida o robo de datos sin encriptación.

Controles DLP Sugeridos:

1. **Para la nube**:
    - Cifrado extremo a extremo.
    - Permisos estrictos basados en roles.
2. **Para Soporte al Cliente**:
    - Capacitación en manejo seguro de datos.
    - Herramientas de monitoreo en tiempo real.
3. **Para transferencias de datos**:
    - Implementación de HTTPS/TLS.
    - Auditorías regulares para identificar vulnerabilidades.