TechCorp Inc.

Análisis de datos sensibles

Joel González.

En el siguiente proyecto se lleva acabo un análisis de la organización TechCorp Inc. Se detectarán los departamentos que la comprenden, el flujo de información que hay entre ellos y los riesgos que hay al tener tráfico de información de unos departamentos a otros.

1- Identificando y clasificando datos sensibles.

A) Recursos Humanos (RH)

Funciones: Contratación, rendimiento, relaciones laborales y capacitación.

Posibles Datos Sensibles:

1. Nombres completos y direcciones de los empleados.
2. Números de identificación personal.
3. Datos de las nóminas.
4. Registro de desempeño y evaluaciones.
5. Registros médicos de los empleados.

Clasificación según el riesgo de los datos que se manejan.

- Nombres y direcciones**:** **Media**
- ID personal**:** **Alta**
- Nomina: **Alta**
- Evaluaciones del personal: **Media**
- Registros médicos: **Alta**

B) Finanzas

Funciones: Presupuestos, nóminas, transacciones, inversiones.

Posibles datos sensibles.

1. Detalles de cuentas bancarias.
2. Tarjetas de crédito de clientes.
3. Registros de nóminas.
4. Análisis financieros internos.
5. Reportes de auditoría.

Clasificación según el riesgo de los datos que se manejan

- Cuentas bancarias: **ALTA.**
- Tarjetas de crédito: **ALTA.**
- Nomina: **ALTA.**

- Análisis financieros: **Media.**
- Auditorias: **Media.**

C) Investigación y desarrollo.

Funciones: Diseño de software, propiedad intelectual, feedback de clientes.

Posibles datos sensibles.

1. Código fuente propio.
2. Prototipos de software.
3. Resultados de pruebas de seguridad.
4. Datos confidenciales de clientes para pruebas.
5. Documentación técnica interna.

Clasificación según el riesgo de los datos que se manejan

- Código fuente: **Alta.**
- Prototipos: **Alta.**
- Pruebas de seguridad: **Alta.**
- Datos de clientes: **Alta.**
- Documentación interna: **Media.**

D) Soporte al cliente.

Funciones: Tickets, consultas, feedback.

Posibles datos sensibles.

1. Historia de tickets con datos de clientes.
2. Correos electrónicos de clientes.
3. Conversaciones grabadas.
4. Detalles de problemas técnicos.
5. Encuestas de satisfacción.

Clasificación según el riesgo de los datos que se manejan

- Historial de tickets: **Media.**
- Correos: **Media.**
- Grabaciones: **Alta.**
- Problemas técnicos: **Media.**
- Encuestas: **Baja.**

E) Ventas y Marketing.

Funciones: Clientes potenciales, análisis de mercado.

Posibles datos sensibles.

1. Información de clientes potenciales.
2. Contratos y acuerdos.
3. Estrategias de mercado.
4. Base de datos de clientes.
5. Estadísticas de campañas.

Clasificación según el riesgo de los datos que se manejan

- Clientes potenciales: **Media.**
- Contratos: **Alta.**
- Estrategias de mercado: **Media.**
- Base de datos de clientes: **Alta**
- Estadística: **Baja.**

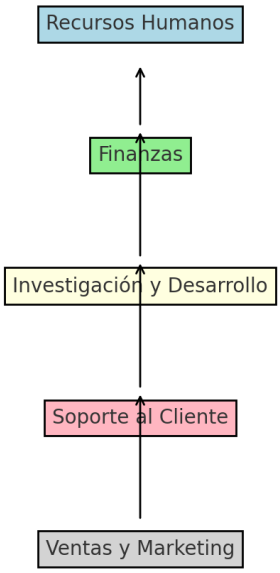
2-Diagrama de Flujo de Datos y Puntos de Riesgo

Flujo general:

- HR envía datos de nómina a Finanzas por correo interno.
- Finanzas usa servidores locales y nube para almacenar registros.
- I+D comparte prototipos con Soporte para pruebas.
- Soporte gestiona datos de clientes vía chat/correo.
- Ventas recibe datos de clientes y coordina con Finanzas para facturación.

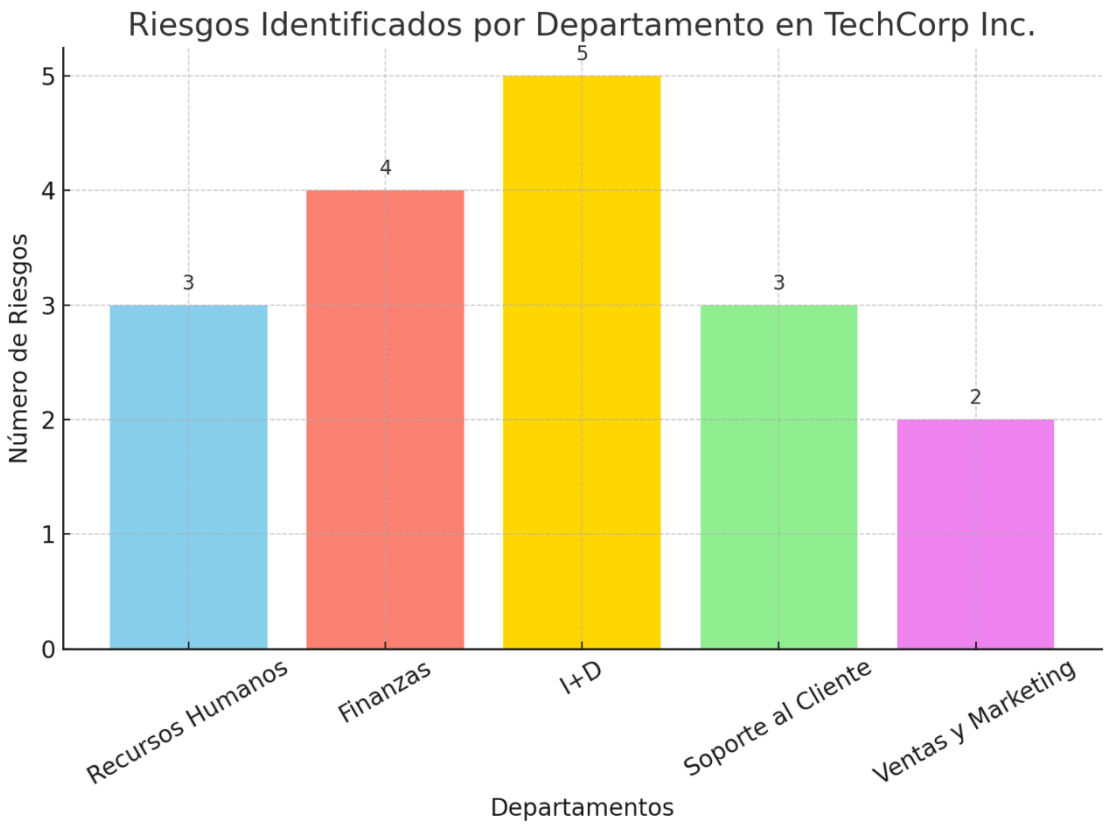
Canales: correo electrónico, unidades compartidas, almacenamiento en la nube.

Diagrama



Puntos de Riesgo Identificados:

1. **Correos electrónicos con adjuntos de nómina** → riesgo de envío a destinatario incorrecto.
   Control sugerido: cifrado de correos y verificación de destinatarios.
2. **Acceso a prototipos de software en nube** → riesgo de acceso no autorizado.
   Control sugerido: autenticación multifactor (MFA) y permisos mínimos.
3. **Unidades compartidas de tickets de Soporte** → riesgo de acceso no autorizado por empleados de otros departamentos.
   Control sugerido: segmentar carpetas y aplicar control de acceso basado en roles.



Resumen de datos sensibles por departamento y su nivel de sensibilidad.

Departamento	Tipo de Dato Sensible	Nivel de Sensibilidad
Recursos Humanos	Nombres completos y direcciones	**Media**
Recursos Humanos	Números de identificación personal (ID)	**Alta**
Recursos Humanos	Datos de nómina y salarios	**Alta**
Recursos Humanos	Evaluaciones de desempeño	**Media**
Recursos Humanos	Registros médicos	**Alta**
Finanzas	Detalles de cuentas bancarias	**Alta**

Departamento	Tipo de Dato Sensible	Nivel de Sensibilidad
Finanzas	Tarjetas de crédito	**Alta**
Finanzas	Registros de nómina	**Alta**
Finanzas	Análisis financieros internos	**Media**
Finanzas	Reportes de auditoría	**Media**
Investigación y Desarrollo	Código fuente propietario	**Alta**
Investigación y Desarrollo	Prototipos de software	**Alta**
Investigación y Desarrollo	Resultados de pruebas de seguridad	**Alta**
Investigación y Desarrollo	Datos confidenciales de clientes	**Alta**
Investigación y Desarrollo	Documentación técnica interna	**Media**
Soporte al Cliente	Historial de tickets	**Media**
Soporte al Cliente	Correos electrónicos de clientes	**Media**
Soporte al Cliente	Conversaciones grabadas	**Alta**
Soporte al Cliente	Detalles de problemas técnicos	**Media**
Soporte al Cliente	Encuestas de satisfacción	**Baja**
Ventas y Marketing	Información de clientes potenciales	**Media**
Ventas y Marketing	Contratos y acuerdos	**Alta**
Ventas y Marketing	Estrategias de mercado	**Media**
Ventas y Marketing	Base de datos de clientes	**Alta**

Departamento	Tipo de Dato Sensible	Nivel de Sensibilidad
Ventas y Marketing	Estadísticas de campañas	**Baja**

Conclusión

El análisis realizado a **TechCorp Inc.** Nos permitió identificar tipos de datos sensibles que maneja cada departamento, clasificar su nivel de sensibilidad y rastrear los principales flujos de información dentro de la empresa.
El resultado muestra que áreas como Finanzas e Investigación y Desarrollo manejan información de nivel confidencial, lo que implica mayores riesgos si no se gestionan de forma adecuada.

También, se identificaron puntos críticos en los canales de comunicación y almacenamiento que requieren controles específicos para prevenir fugas de datos y accesos no autorizados.

Este proyecto resalta la importancia de tener una buena gestión de los datos, controles de seguridad bien aplicados y estándares como GDPR y una cultura de organización que nos permita la protección de la información.

Recomendaciones Generales

Fortalecer Políticas de Seguridad:
Revisar y actualizar regularmente las políticas de protección de datos para garantizar el cumplimiento de las normativas vigentes.

Implementar Controles de Acceso Basados en Roles:
Limitar el acceso a datos sensibles solo a los empleados que realmente los necesiten para sus funciones.

Usar Cifrado y Autenticación Fuerte:
Asegurar el cifrado de correos electrónicos, archivos y bases de datos.
Activar la autenticación multifactor para todos los accesos críticos.

Capacitar al Personal:
Brindar capacitaciones sobre buenas prácticas de seguridad de la información y detección de amenazas.

Monitoreo y Auditorías:
Implementar herramientas de monitoreo de red y auditorías para detectar y responder rápidamente a posibles problemas de seguridad.

Revisar Proveedores y Servicios en la Nube:
Verificar que los servicios en la nube usados por TechCorp cumplan con estándares de seguridad robustos.