**Proyecto: Análisis de Datos Sensibles en TechCorp Inc.**

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

**a) Datos Sensibles por Departamento**

* **Recursos Humanos (HR)**
  1. Información Personal Identificable (PII) de empleados (nombres, direcciones, números de seguro social).
  2. Historial laboral y evaluación de desempeño.
  3. Datos de nómina y cuentas bancarias.
  4. Registros médicos de empleados (beneficios de salud).
  5. Contratos laborales y documentos de relaciones laborales.
* **Finanzas**
  1. Información financiera de la empresa (estados financieros, balances).
  2. Detalles de nómina de empleados.
  3. Información sobre inversiones y estrategias financieras.
  4. Datos de cuentas bancarias y transacciones.
  5. Facturas y recibos de clientes y proveedores.
* **Investigación y Desarrollo (I+D)**
  1. Propiedad intelectual (código fuente, algoritmos).
  2. Documentación de diseño y desarrollo de software.
  3. Planes de productos futuros.
  4. Información técnica sensible de los clientes.
  5. Datos de prueba y rendimiento de los productos.
* **Soporte al Cliente**
  1. Información de contacto de los clientes.
  2. Historial de interacción de los clientes con el soporte.
  3. Tickets de soporte con detalles técnicos.
  4. Datos de acceso a los sistemas de los clientes.
  5. Información de retroalimentación y encuestas de satisfacción.
* **Ventas y Marketing**
  1. Datos de clientes potenciales (nombres, correos electrónicos, números de teléfono).
  2. Estrategias de marketing y campañas de publicidad.
  3. Contratos y acuerdos con clientes.
  4. Datos de rendimiento de ventas.
  5. Información sobre el análisis de mercado y competidores.

**b) Clasificación de Datos**

| **Departamento** | **Tipo de Dato** | **Clasificación** |
| --- | --- | --- |
| **Recursos Humanos** | Información Personal Identificable (PII) | Alta |
|  | Historial laboral y evaluaciones | Media |
|  | Datos de nómina | Alta |
|  | Registros médicos | Alta |
|  | Contratos laborales | Media |
| **Finanzas** | Información financiera de la empresa | Alta |
|  | Detalles de nómina de empleados | Alta |
|  | Información sobre inversiones | Alta |
|  | Datos de cuentas bancarias | Alta |
|  | Facturas y recibos | Media |
| **Investigación y Desarrollo (I+D)** | Propiedad intelectual | Alta |
|  | Documentación de diseño y desarrollo | Alta |
|  | Planes de productos futuros | Alta |
|  | Información técnica de clientes | Media |
|  | Datos de prueba y rendimiento | Media |
| **Soporte al Cliente** | Información de contacto de los clientes | Media |
|  | Historial de interacción con el soporte | Baja |
|  | Tickets de soporte con detalles técnicos | Media |
|  | Datos de acceso a sistemas | Alta |
|  | Información de retroalimentación | Baja |
| **Ventas y Marketing** | Datos de clientes potenciales | Media |
|  | Estrategias de marketing | Media |
|  | Contratos y acuerdos | Alta |
|  | Datos de rendimiento de ventas | Baja |
|  | Información de análisis de mercado y competidores | Media |

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

**a) Diagrama de Flujo de Datos**

El flujo de datos entre los departamentos sigue varios canales internos y externos:

* **Canales Internos**: Comunicación por correo electrónico y chat entre departamentos (Recursos Humanos, Finanzas, I+D, etc.) para compartir datos relacionados con proyectos, pagos, y recursos humanos.
* **Canales Externos**: Interacciones de ventas y soporte con clientes a través de correo electrónico, sistemas de tickets y almacenamiento de datos en la nube para colaboración con clientes y proveedores.
* **Almacenamiento**: TechCorp utiliza tanto almacenamiento en la nube (para facilitar trabajo remoto y escalabilidad) como servidores locales (para datos sensibles como nóminas y propiedad intelectual).

**b) Puntos de Riesgo Identificados**

1. **Correo Electrónico Interno**: Riesgo de exposición de PII o propiedad intelectual en correos no cifrados o enviados por error a destinatarios incorrectos.
2. **Acceso a la Nube**: Posibles brechas de seguridad si las credenciales de empleados no están correctamente gestionadas, lo que puede permitir acceso no autorizado.
3. **Sistemas de Soporte al Cliente**: Datos técnicos y de acceso de clientes podrían ser expuestos si no se implementan controles de seguridad adecuados en los sistemas de tickets.

**c) Controles de DLP Sugeridos**

1. **Cifrado de Correos Electrónicos**: Implementar cifrado de extremo a extremo en las comunicaciones internas que incluyan datos sensibles.
2. **Autenticación Multifactor (MFA)**: Implementar MFA para todas las cuentas de empleados que acceden a la nube y los sistemas de desarrollo.
3. **Seguridad en Sistemas de Soporte**: Implementar control de acceso basado en roles y cifrado en los sistemas de soporte para limitar el acceso a datos técnicos críticos.

A diagram of a data flow

Description automatically generated

**Informe del Análisis**

TechCorp Inc. maneja una amplia variedad de datos sensibles que son críticos para la operación y éxito de la empresa, incluyendo datos personales, financieros y propiedad intelectual. A través del análisis realizado, se identificaron riesgos significativos en los flujos de datos, especialmente en las comunicaciones internas, el acceso a la infraestructura en la nube y los sistemas de soporte al cliente.

Para mitigar estos riesgos, es esencial implementar controles de seguridad adicionales como el cifrado de correos electrónicos, autenticación multifactor para accesos a la nube y mejorar los controles de acceso en los sistemas de soporte. Estas medidas ayudarán a proteger la integridad de los datos y asegurar el cumplimiento de normativas como el GDPR, salvaguardando la reputación de la empresa y fortaleciendo la confianza de los clientes.

Al aplicar estas recomendaciones, TechCorp puede reducir considerablemente los puntos de exposición de datos sensibles, mejorar la seguridad operativa y continuar su crecimiento como líder en el desarrollo de software, garantizando al mismo tiempo la protección de sus activos más valiosos.

**Lista de Tipos de Datos Sensibles por Departamento**

* Recursos Humanos: PII, nómina, historial laboral.
* Finanzas: Información financiera, nómina, cuentas bancarias.
* I+D: Propiedad intelectual, documentación de desarrollo.
* Soporte al Cliente: Información de contacto, datos técnicos de acceso.
* Ventas y Marketing: Contratos, estrategias de marketing.

**Clasificación de Datos**: Los datos sensibles más críticos están relacionados con PII, finanzas y propiedad intelectual, todos clasificados como de alta sensibilidad.

**Puntos de Riesgo**:

1. Correo interno sin cifrado.
2. Acceso no seguro a la nube.
3. Sistemas de soporte sin controles de seguridad robustos.

**Controles de DLP Sugeridos**: Cifrado de correos, autenticación multifactor y control de acceso a sistemas críticos.