4GeeksAcademy

Análisis de Datos Sensibles en una Organización Ficticia

1. Identificar y Clasificar Datos Sensibles

A y B) Datos Sensibles por Departamento

- **Recursos Humanos (RRHH):**

  1. Nombre de los empleados, posibles candidatos al acceso para el puesto de trabajo, datos privados como nombres, direcciones, identificaciones.

  2. Historial de los trabajadores como los distintos trabajos y tiempo de duración en la empresas y en las que estuvo trabajando.

  3. Datos económicos y de la cantidad salarial de cada uno de los empleados.

  4. Información personal de los empleados de carácter único como datos bancarios, expediente médico y características únicas del contrato.

  5. Datos de los motivos y reportes que se le hace a cada personal de la empresa, en caso de filtrarse puede crear muchos conflictos internos.

- **Finanzas:**

  1. Detalles bancarios como número de cuentas, movimientos y transacciones realizadas.

  2. Información de los destinos de movimientos de dinero como inversiones, compra y venta.

  3. Información económica dentro de la empresa la cantidad total disponible de dinero que hay y acceso a más datos de este tipo.

  4. Datos de las distintas cuentas a pagar y cobrar.

  5. Cuentas financieras de los socios y de los clientes.

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

  1. Códigos fuentes, algoritmos, software único de la empresa.

  2. Historial del desarrollo de cada uno de los productos.

3. Especificaciones técnicas de los productos propios de la empresa.

4. Proyectos y planes a futuro que tiene planeado la empresa.

5. Especificaciones técnicas de los productos trabajados en conjunto con diferentes empresas.

- **Soporte al Cliente:**

1. Datos de carácter personal de cada uno de los distintos clientes (PII).

2. Consulta e historial de cada uno de los clientes hechos hacia el grupo de soporte.

3. Información sensible que puede haber en cada uno de los tickets o consultas que pueden poner en riesgo a la empresa y cliente.

4. Los credenciales de los clientes pueden ser robados al ser compartidos de manera personal con el soporte del cliente.

5. Información específica de los productos que hacen los clientes revelando el nicho de ventas de la empresa.

- **Ventas y Marketing:**

1. Bases de datos de los clientes.

2. Diferentes estrategias de mercadotecnia y campañas de marketing.

3. Informe de las ventas realizadas además del análisis del mercado actual.

4. Bonus, contratos y acuerdos realizados tanto con empresas como con clientes.

5. Preferencia de las compras de los clientes.

C) Clasificación de Datos según Sensiblidad.

- **Alto:**

- PII tanto de los empleados, clientes y empresas.

- Información de los propios productos y colaboraciones con empresas.

- Datos económicos, bancarios y movimientos de las transacciones.

- **Medio:**

    - Informes financieros y mercadotecnia.

    - Datos de los productos más vendidos y el feedback de los clientes hacia estos.

    - Estrategias de marketing, campañas y colaboraciones.

- **Bajo:**

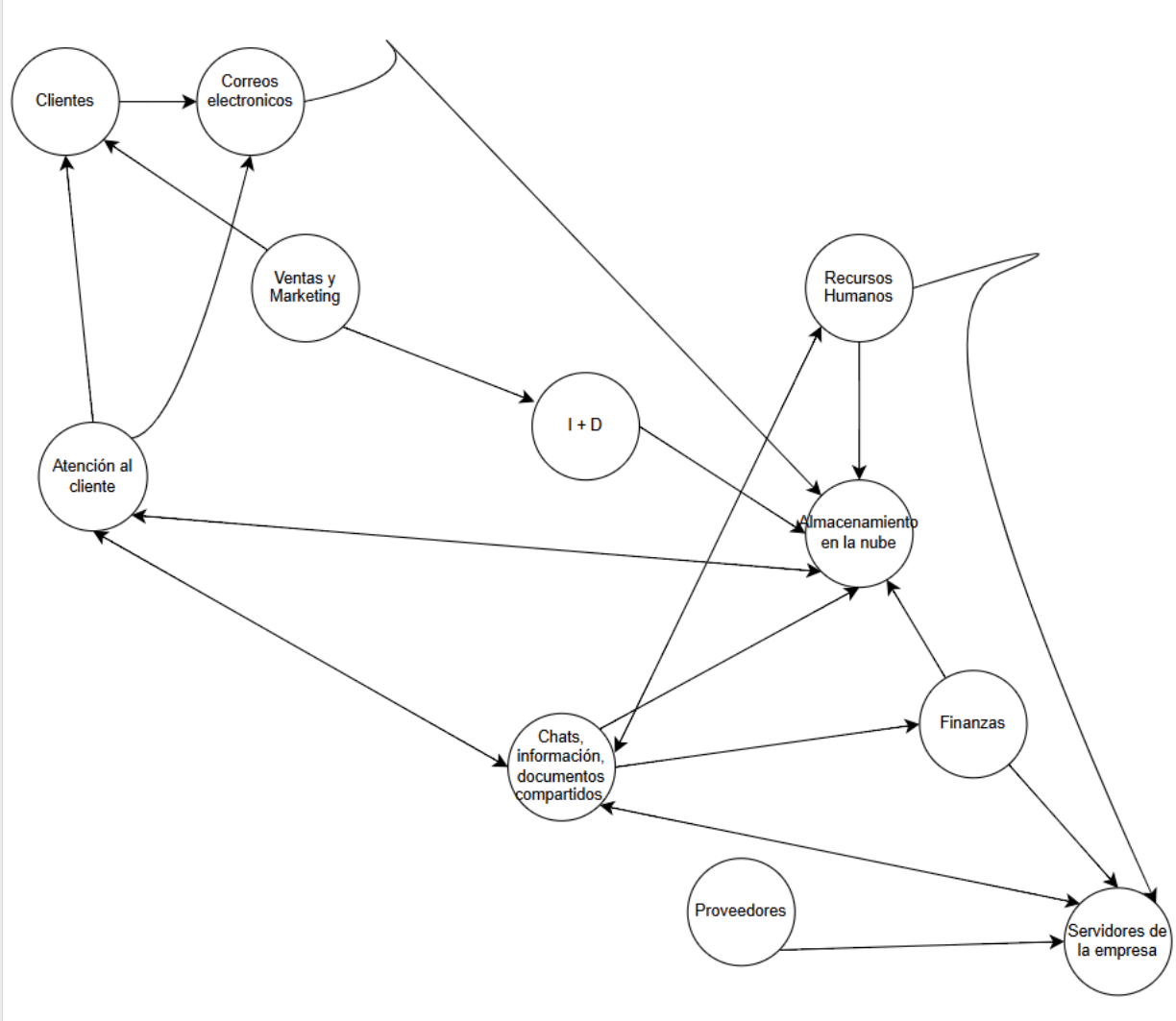
    - Detalles de carácter general de los productos.

    - Historial de compra de los clientes de manera más generalizada(No innovadoras por ellos).

    - Especificaciones técnicas de productos ya lanzados al mercado.

2. Mapear los Flujos y Datos y los Puntos de Riesgo

Diagrama



Identificación de posibles riesgos en el flujo de datos sensibles.

1.- A la hota de transmitir datos de carácter importante mediante correo electrónico sin estar cifrado:

Riesgo: Cabe la posibilidad de la intercepción de estos correos vulnerando la privacidad de estos.

2.- Acceso no autorizado a datos privados y únicos de la empresa.

Riesgo: Podrían poner en riesgo severo a la empresa y la reputación de esta a la hora de manejar los datos de los clientes.

3.- Compartir información de carácter sensible a través de plataformas de comunicación como las redes sociales.

Riesgo: Podrían filtrarse diferentes credenciales únicas que podrían derivar a nuevas brechas de seguridad además de filtración de productos o cosas únicas de la empresa.

Control básico de DLP (Prevención de Pérdida de Datos)

Para poder evitar que estos problemas lleguen a suceder se implementará una serie de controles para evitar que esto suceda o llegará.

1. Clasificación de todos los datos sensibles y de carácter más único mediantes herramientas especializadas, donde se clasificara los permisos de los trabajadores para cada uno de estos solo tengan acceso a sus necesidades y requisitos.
2. Monitorización constante de lo que sucede y de las actividades tanto internas por parte de los empleados como ajena a esta para evitar acciones sospechosas.
3. Formación continua y educación para los empleados para que estos están al tanto de las nuevas posibilidades de fraudes y cómo gestionar los datos de la empresa y seguridad.