Identificación y Clasificación de Datos Sensibles

1. Recursos Humanos (HR) 👯

- **Datos sensibles manejados**:
    1. Información Personal Identificable (PII) de empleados (nombre, dirección, teléfono).
    2. Historial laboral y evaluaciones de rendimiento.
    3. Datos médicos y de salud relacionados con beneficios.
    4. Información de contacto de emergencia.
    5. Detalles de compensación y beneficios.
- **Clasificación**:
    - **Alta**: PII, datos médicos y de salud.
    - **Media**: Historial laboral, evaluaciones de rendimiento.
    - **Baja**: Información de contacto de emergencia.

2. Finanzas 💰

- **Datos sensibles manejados**:
    1. Información de nómina y salarios de empleados.
    2. Registros de transacciones financieras y bancarias.
    3. Información de impuestos de la empresa.
    4. Detalles de inversión y planificación financiera.
    5. Informes financieros y presupuestos.
- **Clasificación**:
    - **Alta**: Nómina, transacciones bancarias, impuestos.
    - **Media**: Planificación financiera, informes presupuestarios.
    - **Baja**: N/A.

3. Investigación y Desarrollo (I+D) 🧪

- **Datos sensibles manejados**:
    1. Propiedad intelectual (patentes, diseños de software).
    2. Información técnica sobre productos en desarrollo.
    3. Investigación de mercado y análisis de necesidades de clientes.

4. Estrategias de innovación y mejora.
5. Documentación de pruebas y prototipos.

- **Clasificación**:
  - **Alta**: Propiedad intelectual, documentación técnica.
  - **Media**: Investigación de mercado.
  - **Baja**: Documentación de pruebas.

4. Soporte al Cliente 🎧

- **Datos sensibles manejados**:
  1. Información personal de clientes (nombre, email).
  2. Registros de tickets de servicio.
  3. Historial de interacciones y soporte recibido.
  4. Información sobre problemas técnicos reportados.
  5. Comentarios y retroalimentación de clientes.
- **Clasificación**:
  - **Alta**: Información personal de clientes.
  - **Media**: Registros de tickets, historial de soporte.
  - **Baja**: Comentarios y retroalimentación.

5. Ventas y Marketing 📈

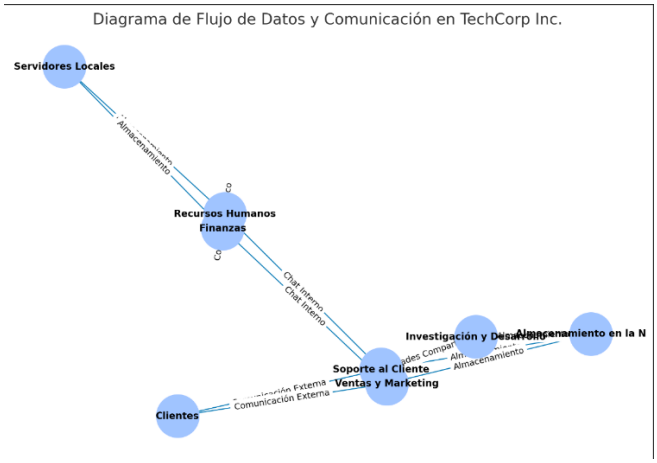
- **Datos sensibles manejados**:
  1. Información de prospectos y clientes.
  2. Estrategias de ventas y campañas de marketing.
  3. Datos de mercado y análisis de la competencia.
  4. Historial de ventas y transacciones con clientes.
  5. Datos de contacto y preferencias de clientes.
- **Clasificación**:
  - **Alta**: Información de clientes y prospectos.
  - **Media**: Estrategias de ventas y marketing.
  - **Baja**: Datos de mercado y competencia.

Esta clasificación utiliza los estándares de privacidad y protección de datos descritos, considerando la sensibilidad de cada tipo de dato en función de su impacto potencial en la empresa y en la privacidad de empleados y clientes.

a) Diagrama de Flujo de Datos

La siguiente imagen es un diagrama que ilustra:

1. **Canales de Comunicación**:
    - Comunicación interna entre departamentos mediante correo electrónico, chat y unidades compartidas.
    - Comunicación externa con clientes y proveedores.
2. **Ubicaciones de Almacenamiento**:
    - Servidores locales y almacenamiento en la nube.



b) Puntos de Riesgo Identificados

1. **Correo Electrónico entre Recursos Humanos y Finanzas**:
    - **Riesgo**: Los datos sensibles, como detalles de nómina o PII, pueden ser interceptados o enviados accidentalmente a destinatarios incorrectos.
2. **Unidades Compartidas entre Investigación y Desarrollo y Soporte al Cliente**:
    - **Riesgo**: Exposición potencial de propiedad intelectual y datos técnicos debido a permisos de acceso inadecuados o a la falta de controles de acceso.
3. **Comunicación Externa entre Soporte al Cliente y Clientes**:

- **Riesgo**: La información de clientes y el historial de soporte pueden filtrarse o verse comprometidos por ataques de phishing o interceptación durante la comunicación.

c) Controles de DLP para Mitigar los Riesgos

1. **Correo Electrónico Interno (Recursos Humanos y Finanzas)**:
   - **Control DLP**: Implementar un cifrado de correo electrónico para proteger la transmisión de datos sensibles. Añadir también advertencias de contenido sensible y verificación de destinatarios.
2. **Unidades Compartidas (Investigación y Desarrollo y Soporte al Cliente)**:
   - **Control DLP**: Configurar permisos de acceso estrictos y realizar auditorías regulares. Implementar monitoreo de actividad en archivos para detectar accesos no autorizados y movimientos de datos inusuales.
3. **Comunicación Externa (Soporte al Cliente y Clientes)**:
   - **Control DLP**: Emplear cifrado de extremo a extremo y autenticación multifactor para asegurar el acceso de clientes a los sistemas. Supervisar la salida de datos mediante controles de filtrado y prevenir la transmisión de información sensible sin autorización.

   Estos controles ayudarán a reducir el riesgo de exposición de datos sensibles dentro de los flujos de datos de TechCorp.

Informe de Análisis

1. Identificación de Datos Sensibles por Departamento 📋

Cada departamento en TechCorp maneja distintos tipos de datos sensibles que requieren niveles de protección específicos. A continuación, se muestra un desglose de los datos sensibles identificados en cada área clave:

- **Recursos Humanos**:
    - **Información Personal Identificable (PII)**: Nombres, direcciones, números de teléfono y otros datos que pueden identificar a un empleado.
    - **Historial laboral y evaluaciones de rendimiento**: Registros de desempeño de los empleados, ascensos y evaluaciones periódicas.
    - **Datos médicos y de salud**: Información sobre beneficios de salud, discapacidades, entre otros.
    - **Información de contacto de emergencia**: Datos de contacto de familiares o contactos de emergencia.
    - **Detalles de compensación y beneficios**: Salarios, bonificaciones y detalles sobre beneficios adicionales.
- **Finanzas**:
    - **Información de nómina y salarios**: Detalles de la compensación de los empleados.
    - **Registros de transacciones financieras y bancarias**: Cuentas y transferencias, tanto internas como de clientes.
    - **Información de impuestos de la empresa**: Declaraciones fiscales y obligaciones tributarias.
    - **Detalles de inversión y planificación financiera**: Estrategias de inversión, análisis de riesgo y planificación presupuestaria.
    - **Informes financieros y presupuestos**: Proyecciones y reportes económicos para la toma de decisiones.
- **Investigación y Desarrollo (I+D)**:
    - **Propiedad intelectual**: Patentes, secretos comerciales y diseños únicos.
    - **Información técnica sobre productos**: Detalles técnicos de los productos en desarrollo.
    - **Investigación de mercado**: Análisis de mercado para determinar oportunidades de innovación.

    - **Estrategias de innovación y mejora**: Enfoques para mantener la competitividad de TechCorp.
    - **Documentación de pruebas y prototipos**: Resultados de pruebas de productos y prototipos preliminares.
- **Soporte al Cliente**:
    - **Información personal de clientes**: Datos de clientes como nombres, direcciones y números de teléfono.
    - **Registros de tickets de servicio**: Detalles sobre incidencias reportadas por los clientes.
    - **Historial de interacciones y soporte**: Resumen de interacciones pasadas y soluciones proporcionadas.
    - **Información sobre problemas técnicos reportados**: Detalles técnicos de los problemas enfrentados por los clientes.
    - **Comentarios y retroalimentación**: Opiniones y sugerencias que pueden ayudar a mejorar los productos y servicios.
- **Ventas y Marketing**:
    - **Información de prospectos y clientes**: Datos básicos y preferencias de compra.
    - **Estrategias de ventas y campañas de marketing**: Planes para promover productos y atraer clientes.
    - **Datos de mercado y análisis de la competencia**: Información sobre tendencias del mercado y actividades de competidores.
    - **Historial de ventas y transacciones**: Registros de ventas con clientes actuales y anteriores.
    - **Datos de contacto y preferencias de clientes**: Preferencias de los clientes en cuanto a productos y comunicación.

---

2. Clasificación de Datos Sensibles

La clasificación de los datos se realiza según su nivel de sensibilidad:

- **Alta Sensibilidad** : Información extremadamente sensible que, en caso de exposición, podría tener graves consecuencias para la empresa.
    - Ejemplos: Información personal identificable (PII), datos médicos, información de nómina, registros financieros, propiedad intelectual.

- **Sensibilidad Media** : Información sensible que requiere protección significativa, ya que su exposición podría afectar a la empresa.
    - Ejemplos: Historial laboral, evaluaciones de rendimiento, investigación de mercado, registros de soporte al cliente.
- **Baja Sensibilidad** : Información menos sensible, pero que aún debe protegerse para evitar posibles filtraciones.
    - Ejemplos: Información de contacto de emergencia, comentarios y retroalimentación de clientes, datos de análisis de mercado.

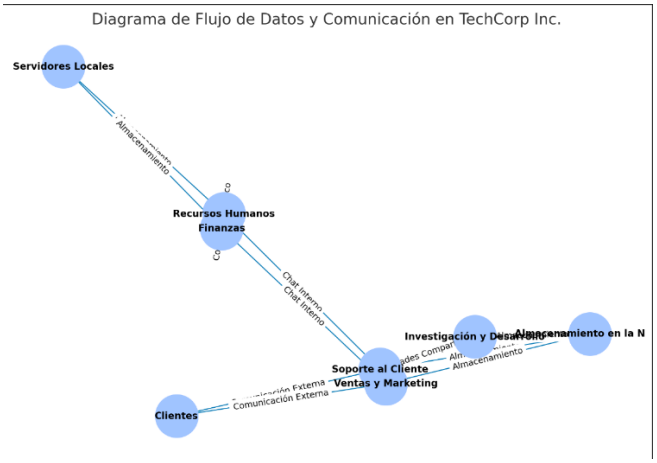
Departamento	Tipo de Dato	Clasificación de Sensibilidad
Recursos Humanos	PII de empleados	Alta
Recursos Humanos	Historial laboral	Media
Recursos Humanos	Datos médicos y de salud	Alta
Recursos Humanos	Contacto de emergencia	Baja
Recursos Humanos	Compensación y beneficios	Alta
Finanzas	Nómina y salarios	Alta
Finanzas	Transacciones financieras	Alta
Finanzas	Impuestos	Alta
Finanzas	Inversiones	Media
Finanzas	Informes financieros	Media
Investigación y Desarrollo	Propiedad intelectual	Alta
Investigación y Desarrollo	Información técnica	Alta
Investigación y Desarrollo	Investigación de mercado	Media
Investigación y Desarrollo	Estrategias de innovación	Media
Investigación y Desarrollo	Documentación de pruebas	Baja
Soporte al Cliente	PII de clientes	Alta
Soporte al Cliente	Registros de tickets	Media
Soporte al Cliente	Historial de soporte	Media
Soporte al Cliente	Problemas técnicos	Media
Soporte al Cliente	Comentarios y retroalimentación	Baja
Ventas y Marketing	Datos de prospectos	Alta
Ventas y Marketing	Estrategias de ventas	Media
Ventas y Marketing	Análisis de competencia	Media
Ventas y Marketing	Historial de ventas	Media
Ventas y Marketing	Preferencias de clientes	Baja

---

3. Diagrama de Flujo de Datos

El diagrama siguiente muestra cómo fluye la información entre los departamentos y las ubicaciones de almacenamiento (servidores locales y almacenamiento en la nube), así como los principales canales de comunicación:

![Diagrama de flujo de datos](Adjuntar aquí el diagrama generado que muestra los flujos de información entre departamentos y almacenamiento.)



---

4. Puntos de Riesgo y Controles de Prevención de Pérdida de Datos (DLP) Sugeridos 🚨

Punto de Riesgo 1: **Correo Electrónico Interno entre Recursos Humanos y Finanzas**

- **Riesgo**: Los correos electrónicos que contienen información sensible, como detalles de nómina, pueden ser interceptados o enviados accidentalmente a destinatarios incorrectos, exponiendo datos críticos de los empleados.
- **Control DLP Sugerido**: Implementar cifrado de correo electrónico para proteger la transmisión de datos. Agregar advertencias de contenido sensible y verificación de destinatarios para reducir el riesgo de errores de envío.

Punto de Riesgo 2: **Unidades Compartidas entre Investigación y Desarrollo y Soporte al Cliente**

- **Riesgo**: La propiedad intelectual, así como documentos técnicos, podrían exponerse debido a permisos de acceso inadecuados o cambios de configuración en las unidades compartidas.
- **Control DLP Sugerido**: Configurar permisos basados en roles y realizar auditorías periódicas de acceso. Implementar monitoreo de actividad en archivos sensibles para detectar intentos de acceso no autorizados y movimientos de datos inusuales.

Punto de Riesgo 3: **Comunicación Externa entre Soporte al Cliente y Clientes**

- **Riesgo**: La información de clientes puede verse comprometida por ataques de phishing o interceptaciones durante las interacciones con el equipo de Soporte.
- **Control DLP Sugerido**: Implementar cifrado de extremo a extremo para comunicaciones externas y emplear autenticación multifactor para los clientes que acceden a portales o sistemas de soporte. Establecer un monitoreo y control de datos de salida para prevenir el envío de información no autorizada.