INFORME CONFIDENCIAL – PERFIL DE CLIENTES Y DATOS DE CONTACTO

Empresa: DataTrust Solutions S.L.
Departamento: Seguridad de la Información
Clasificación: CONFIDENCIAL
Fecha: 07/12/2025
Responsable del informe: Departamento de Cumplimiento y Riesgos

---

1. Objetivo del informe

El objetivo de este documento es recopilar información identificativa y financiera de una muestra de clientes, con el fin de evaluar riesgos asociados al tratamiento de datos sensibles y probar los controles internos de protección de la información según la normativa vigente (RGPD e ISO/IEC 27001).

---

2. Datos de la muestra analizada

Nota: Todos los datos mostrados son *ficticios* y generados únicamente para fines de simulación.

Registro 1

- **Nombre completo:** Javier Morales Sánchez
- **DNI:** 12345678A
- **Email:** j.morales@example-corp.com
- **Teléfono:** +34 612 345 678
- **IBAN:** ES91 2100 0418 4502 0005 1332
- **Tarjeta bancaria:** 4111 1111 1111 1111

Registro 2

- **Nombre completo:** Laura Peña Rodríguez
- **DNI:** 87654321B
- **Email:** laura.pena@demo-mail.org
- **Teléfono:** +34 699 234 567
- **IBAN:** ES76 1465 0100 9456 7890 1234
- **Tarjeta bancaria:** 5500 0000 0000 0004

Registro 3

- **Nombre completo:** Carlos Gómez Navarro

- **DNI:** 45678912C
- **Email:** c.gomez@testingbusiness.net
- **Teléfono:** +34 622 987 654
- **IBAN:** ES45 0049 1500 1234 5678 9012
- **Tarjeta bancaria:** 3400 000000 00009

---

3. Riesgos identificados

Durante la simulación se identifican los siguientes riesgos potenciales:

- Exposición de datos sensibles en ficheros no cifrados.
- Almacenamiento de IBAN y tarjetas sin tokenización.
- Ausencia de mascarado en sistemas de reporting.
- Riesgo de fuga de información por accesos no auditados.

---

4. Recomendaciones

Se recomienda:

- Aplicar **cifrado en reposo y en tránsito**.
- Implantar técnicas de **data masking** en entornos de pruebas.
- Activar **DLP (Data Loss Prevention)** para correos y endpoints.
- Revisar las políticas de accesos privilegiados.

---

5. Conclusión

Los datos sensibles requieren controles técnicos y organizativos robustos. Esta simulación ha demostrado la necesidad de reforzar las medidas de protección para evitar sanciones regulatorias y daños reputacionales.