Sistema de Seguridad de la información (SGSI)

Fecha 15 Sep 2025
Autor:

COPYRIGHT

Historial de Cambios.

Fecha	Versión Documento	Descripción	Responsable del Cambio	Aprobado Por	Cargo Aprobador
15-09-25	1	Generación del Documento			
18-09-25	2	Cambios a la Política			

TABLA DE CONTENIDO

Contenido

1. Introducción

En **DARUPAY S.A.S**. la seguridad de la información es un pilar estratégico para garantizar la confidencialidad, integridad y disponibilidad (CIA) de los datos que procesamos como pasarela y orquestador de pagos.

Este procedimiento establece los lineamientos de implementación, operación y control de nuestro SGSI, siguiendo las mejores prácticas de ISO 27001:2022 y NIST CSF (Identify, Protect, Detect, Respond, Recover).

2. Objetivos

- Proteger los datos sensibles de clientes, proveedores y aliados.
- Garantizar la continuidad del negocio y la resiliencia operativa.
- Cumplir con las normativas nacionales (Ley 1581 de 2012, Habeas Data; SARLAFT/SAGRILAFT) e internacionales (ISO 27001, PCI DSS, NIST CSF).
- Prevenir incidentes de ciberseguridad y fraude electrónico.

3. Alcance

Este procedimiento aplica a:

- Todos los sistemas de información y datos administrados por DaruPay.
- Todos los empleados, contratistas, proveedores y aliados que accedan a información sensible.
- Los servicios ofrecidos: Transfiya, PayIN, Payout, PSE, conciliación y portal integrado.

4. Marco de Referencia

- ISO 27001:2022 – Sistema de Gestión de Seguridad de la Información.
- ISO 27002:2022 – Controles de seguridad de la información.
- NIST Cybersecurity Framework – Identify, Protect, Detect, Respond, Recover.
- PCI DSS – Seguridad de datos de tarjetas de pago.

5. Procedimiento del SGSI

5.1. Identificación

- Inventario de activos de información (sistemas, bases de datos, APIs).
- Clasificación de información (confidencial, interna, pública).
- Análisis de riesgos de seguridad (ISO 27005).
- Evaluación de amenazas y vulnerabilidades.

5.2. Protección

- Control de accesos: MFA, roles, mínimo privilegio.
- Encriptación: AES-256 en datos en reposo, TLS 1.3 en tránsito.
- Tokenización: en datos de tarjetas (cumplimiento PCI DSS).
- Concienciación y formación: capacitaciones anuales obligatorias.
- Seguridad perimetral: firewalls de próxima generación, WAF, IDS/IPS.

5.3. Detección

- Monitoreo continuo con SIEM (Security Information and Event Management).
- Detección de anomalías mediante reglas y machine learning.
- Alertas tempranas de fraudes y accesos no autorizados.
- Revisión de logs críticos (autenticación, transacciones, bases de datos).

5.4. Respuesta

- Procedimiento formal de Gestión de Incidentes.
- Equipo de respuesta a incidentes (CSIRT interno).
- Escalamiento inmediato al Oficial de Cumplimiento en caso de LA/FT.
- Comunicación a autoridades competentes (SFC, UIAF) en incidentes mayores.

5.5. Recuperación

- Planes de Continuidad del Negocio (BCP).
- Planes de Recuperación ante Desastres (DRP).
- Pruebas anuales de recuperación de infraestructura crítica.
- Revisión post-incidente y lecciones aprendidas.

6. Roles y Responsabilidades

- Junta Directiva: supervisa la estrategia de ciberseguridad.
- CISO: responsable del SGSI, implementación de controles ISO/NIST.
- Oficial de Cumplimiento: gestión de alertas vinculadas a LA/FT.
- Comité de Riesgos: análisis periódico de indicadores de seguridad.
- Todos los empleados: cumplimiento de políticas y reporte de incidentes.

7. Monitoreo y Métricas

- KPI/KRI:
  - % de incidentes detectados vs. reportados.
  - Disponibilidad de servicios (>99.9%).
  - Latencia promedio (<3 segundos).
  - Número de accesos no autorizados bloqueados.
- Auditorías internas y externas: anuales.
- Revisión de controles: continua y documentada.

8. Vigencia

Este procedimiento es aplicable desde la constitución de DaruPay S.A.S. y será revisado y actualizado anualmente o ante cambios regulatorios o tecnológicos.