CONFIDENCIAL

FINTRIXS PAY

Protección de datos personales

03.4 — PROTOCOLO DE GESTIÓN DE INCIDENTES DE SEGURIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

CÓDIGO	PDP-004
VERSIÓN	1.0 — 16 de abril de 2026
APROBADO POR	DPO / CISO / Representante Legal
VIGENCIA	24 meses

FINTRIXS S.A.S. · NIT 901.994.194-3
Paquete de Due Diligence — Banco Sponsor Agregador
Emitido el 16 de abril de 2026 — Versión 1.0 del paquete

03.4 — PROTOCOLO DE GESTIÓN DE INCIDENTES DE SEGURIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES · Código: PDP-004 · Versión: 1.0 — 16 de abril de 2026 · FINTRIXS S.A.S.

1. Objetivo

Establecer las acciones de identificación, contención, análisis, erradicación, recuperación, notificación y lecciones aprendidas frente a incidentes de seguridad que afecten datos personales, en línea con:

- Ley 1581 de 2012 y Decreto 1377 de 2013.
- Circular Externa 02 de 2015 de la SIC (reporte al RNBD).
- Circular Externa 007 de 2018 de la SFC.
- NIST SP 800-61r2 y SP 800-53.
- PCI DSS v4.0, Requisito 12.10.

2. Definiciones

- **Incidente de seguridad:** evento que compromete la confidencialidad, integridad o disponibilidad de datos personales.
- **Brecha de datos:** incidente materializado con acceso, pérdida o divulgación no autorizada.
- **Tiempo de detección (MTTD), tiempo de respuesta (MTTR), tiempo de notificación (MTTN).**

3. Roles y comité de respuesta (CSIRT)

Rol	Responsable
Líder del CSIRT	CISO (CTO)
Oficial de Privacidad	DPO
Líder técnico	Líder de Plataforma
Comunicaciones	Gerencia / Legal
Legal	Apoderado / Firma externa
Enlace con banco sponsor	COO

4. Fases del protocolo

4.1. Identificación

Fuentes de detección:

- Alertas del SIEM corporativo (eventos de `@fintrixs/logging`, Kafka, WAF, IDS/IPS).
- Monitoreo de integridad (FIM) y DLP.
- Alertas de `admin-audit-service`.
- Reportes internos (empleados) o externos (titulares, aliados, autoridades).

4.2. Contención

- Aislamiento del activo afectado (quarantine).
- Bloqueo de credenciales y revocación de tokens.
- Corte de conexiones externas si procede.
- Snapshot forense de la evidencia (discos, logs, memoria).

4.3. Análisis

- Triage inicial por el CSIRT (≤ 1 hora desde la detección para incidentes altos).
- Determinación del alcance (cantidad de titulares, tipos de datos, sistemas involucrados).
- Evaluación de criticidad (matriz de severidad).

4.4. Erradicación y recuperación

- Eliminación de la causa raíz (patching, rotación de llaves, reconstrucción).
- Restauración desde backups validados.
- Endurecimiento adicional.

4.5. Notificación

Destinatario	Umbral	Plazo
Titular afectado	Cualquier brecha con riesgo para sus derechos	≤ 72 horas
SIC (RNBD)	Incidentes que afecten la información registrada	≤ 15 días hábiles (Circular Externa 02/2015)
Banco sponsor	Incidentes con impacto potencial al ecosistema del banco	≤ 24 horas
Red adquirente (Credibanco / Visa)	Incidentes que afecten datos de tarjeta	Según PCI DSS Req. 12.10 + acuerdo con la red
Autoridades adicionales (UIAF, Fiscalía)	Según naturaleza del incidente	Según ley aplicable

4.6. Lecciones aprendidas

- Post-mortem en máximo 15 días desde el cierre.
- Actualización de runbooks, matriz de riesgos y políticas.
- Comunicación interna y formación focalizada.

5. Matriz de severidad

Severidad	Criterios	SLA detección-contención
Crítica (S1)	Brecha confirmada de datos sensibles o > 1.000 titulares	15 min detección / 1 h contención
Alta (S2)	Brecha potencial / acceso no autorizado / datos de entre 100 y 1.000 titulares	1 h / 4 h
Media (S3)	Intento no exitoso o brecha < 100 titulares sin datos sensibles	4 h / 24 h
Baja (S4)	Eventos sospechosos sin impacto confirmado	24 h / 72 h

6. Runbooks técnicos

- RB-001 Exposición de PAN.
- RB-002 Compromiso de credenciales o tokens.

- RB-003 Ransomware o malware en entorno corporativo.
- RB-004 Exfiltración detectada por DLP.
- RB-005 Acceso no autorizado en base de datos con RLS.

7. Evidencia y cadena de custodia

- Preservación de evidencias digitales con hash SHA-256.
- Custodia documentada en `admin-audit-service` con sello de tiempo.
- Almacenamiento seguro mínimo 5 años.

8. Comunicación con los titulares

En notificación al titular se incluye: naturaleza del incidente, tipos de datos comprometidos, medidas tomadas, riesgos potenciales, recomendaciones, canal de contacto del DPO.

9. Pruebas del protocolo

- Simulacro de respuesta a incidentes al menos **una vez al año**.
- Revisión de runbooks tras cualquier incidente S1/S2.
- Integración con ejercicios de pentest.