CONFIDENCIAL

FINTRIXS PAY

Continuidad del negocio

07.2 — RUNBOOK OPERATIVO DE RESPUESTA A INCIDENTES CRÍTICOS

CÓDIGO	BCM-002
VERSIÓN	1.0 — 16 de abril de 2026
APROBADO POR	Representante Legal
VIGENCIA	—

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

07.2 — RUNBOOK OPERATIVO DE RESPUESTA A INCIDENTES CRÍTICOS · Código: BCM-002 · Versión: 1.0 — 16 de abril de 2026 · FINTRIXS S.A.S.

1. Propósito

Guía operacional de referencia rápida durante un incidente disruptivo o ciberataque. Complementa el BCP (07.1) con pasos accionables.

2. Severidades

Sev	Definición	Objetivo de respuesta
SEV-1	Pérdida total o parcial del servicio transaccional	Respuesta en ≤ 5 min; restauración ≤ 1 h
SEV-2	Degradación severa de servicio secundario o amenaza activa	Respuesta ≤ 15 min; restauración ≤ 4 h
SEV-3	Problema limitado sin impacto transaccional	Respuesta ≤ 1 h; restauración ≤ 24 h
SEV-4	Anomalía sin impacto de negocio	Respuesta ≤ 8 h; cierre en sprint

3. Roles durante un incidente

- **Incident Commander (IC):** coordina. Un solo IC en cualquier momento.
- **Communications Lead:** comunicación interna y externa.
- **Operations Lead:** ejecución técnica.
- **Scribe:** bitácora en canal `#incident-<id>`.
- **Subject Matter Experts (SMEs):** según necesidad.

4. Flujo estándar (SEV-1 / SEV-2)

1. **Detección** — monitoreo automático (CloudWatch, Prometheus, Grafana) o reporte humano.
2. **Declaración** — IC abre canal `#incident-<id>` y page a Comité de Crisis.
3. **Triage** — identificación de alcance, impacto, hipótesis inicial.
4. **Contención** — aislar sistemas comprometidos, activar circuit breakers, limitar tráfico si aplica.
5. **Comunicación inicial** — subcomercios + banco sponsor + regulador cuando aplique.
6. **Investigación** — logs (`@fintrix/logging` + SIEM), trazas de correlación, análisis forense preliminar.
7. **Remediación** — rollback, hotfix, failover según corresponda.
8. **Verificación** — smoke tests, métricas de negocio estables, ausencia de alertas.

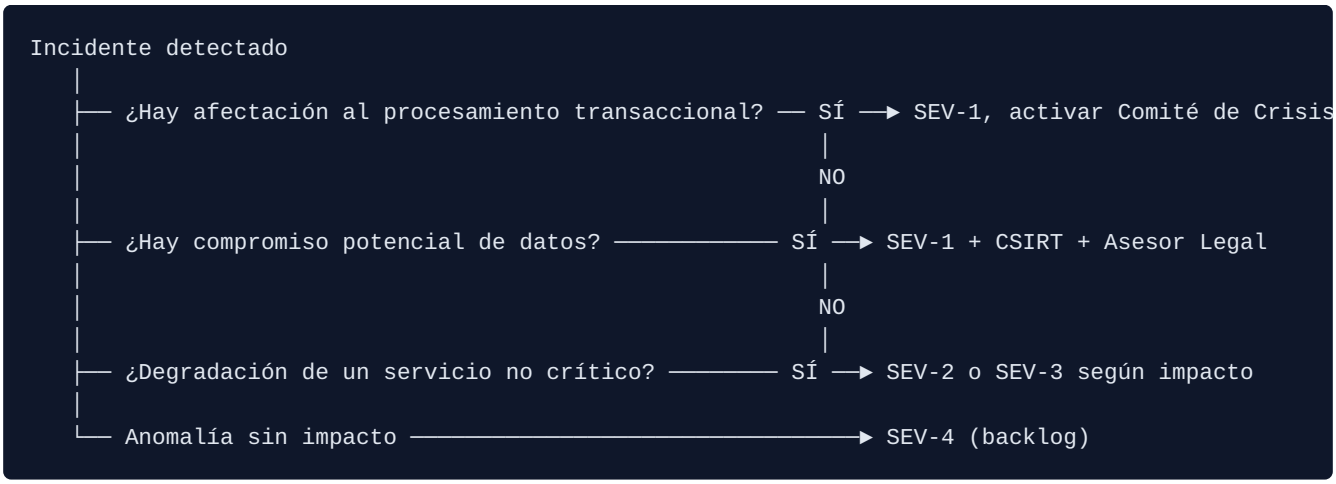
9. **Recuperación** — restablecimiento de tráfico al 100%.
10. **Post-mortem** — documento publicado ≤ 5 días hábiles (blameless).

5. Runbooks específicos (índice)

- `RUN-DR-001` — Failover a región DR.
- `RUN-DB-001` — Rotación / promoción de réplica PostgreSQL.
- `RUN-KAFKA-001` — Rebalanceo de consumidores / reemplazo de broker.
- `RUN-VAULT-001` — Aislamiento del `card-vault-service`.
- `RUN-FRAUD-001` — Activación de reglas antifraude reforzadas.
- `RUN-AUTH-001` — Rotación de llaves JWT y secretos KMS.
- `RUN-API-001` — Throttling / circuit breaker en Kong.
- `RUN-CRED-001` — Contingencia ante falla de Credibanco.

> *Los runbooks detallados residen en el repositorio interno `runbooks/` y se entregan bajo NDA.*

6. Árbol de decisión para escalamiento



7. Plantillas de comunicación

7.1. Aviso inicial a banco sponsor (interno)

> *Asunto: [INCIDENTE] Fintrixs Pay — Estimados, reportamos un incidente clasificado como iniciado a las . Impacto observado: . Plan de acción: . Próxima actualización en 30 minutos.*

7.2. Status page público

> *Estamos investigando una degradación en el servicio de . Los equipos están activos. Actualizaremos cada 15 minutos.*

8. Checklist post-incidente

- [ ] Incidente cerrado en la herramienta de tickets.
- [ ] Bitácora y evidencias archivadas.
- [ ] Post-mortem publicado.
- [ ] Acciones correctivas abiertas en backlog con dueño y fecha.
- [ ] Comunicación final a banco sponsor.
- [ ] Reporte regulatorio presentado (cuando aplique).
- [ ] Matriz de riesgos (05.4) actualizada si corresponde.
- [ ] Lecciones aprendidas socializadas a todo el equipo.