CONFIDENCIAL

FINTRIXS PAY

Continuidad del negocio

07.1 — PLAN DE CONTINUIDAD DEL NEGOCIO (BCP)

CÓDIGO	BCM-001
VERSIÓN	1.0 — 16 de abril de 2026
APROBADO POR	Representante Legal
VIGENCIA	24 meses (revisión anual + pruebas semestrales)

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

07.1 — PLAN DE CONTINUIDAD DEL NEGOCIO (BCP) · Código: BCM-001 · Versión: 1.0 — 16 de abril de 2026 · FINTRIXS S.A.S.

1. Objetivo

Garantizar la continuidad de los servicios críticos de Fintrixs Pay ante eventos disruptivos (fallas tecnológicas, ciber-ataques, indisponibilidad de proveedores, eventos físicos) minimizando el impacto en los clientes, subcomercios y contrapartes financieras.

2. Alcance

Aplica a:

- Servicios transaccionales de `payments-api` y `tokenization-service`.
- Servicios adyacentes críticos: `auth-service`, `card-vault-service`, `webhooks-service`.
- Servicios de soporte: `admin-audit-service`, `realtime-gateway`.
- Integraciones externas: Credibanco (adquirencia/3DS), proveedores cloud (AWS), Kafka, bases de datos.
- Recursos humanos clave (plan de sucesión).

3. Análisis de impacto al negocio (BIA)

3.1. Clasificación de procesos críticos

Proceso	Tier	RTO	RPO	Impacto de indisponibilidad
Procesamiento transaccional (autorización)	T0	≤ 1 h	≤ 5 min	Pérdida de ingresos + sanción contractual
Tokenización / Detokenización	T0	≤ 1 h	≤ 5 min	Bloqueo de pagos
Autenticación 3DS 2.2	T0	≤ 2 h	≤ 15 min	Incremento de fraude / rechazos
Reconciliación y liquidación	T1	≤ 4 h	≤ 30 min	Retraso en payout a subcomercios
Webhooks y notificaciones	T1	≤ 4 h	≤ 15 min	Desalineación con subcomercios
Onboarding / KYB	T2	≤ 24 h	≤ 1 h	Retraso en altas
Portal administrativo	T2	≤ 8 h	≤ 1 h	Degradación operativa interna
Reporting regulatorio	T2	≤ 24 h	≤ 1 h	Impacto regulatorio si sostenido

3.2. Umbrales regulatorios

- Reporte a **SFC** por indisponibilidad: **inmediato** si supera 60 minutos continuos (Circular 007).
- Reporte a **SIC** por incidente con afectación de datos: **15 días hábiles** (Ley 1581).
- Aviso a **banco sponsor**: **dentro de la primera hora** con escalamiento al siguiente nivel cada 30 minutos.

4. Estrategias de continuidad

4.1. Alta disponibilidad (HA)

- Despliegue multi-AZ en AWS `us-east-1` (zonas a, b, c).
- Load balancers (ALB + NLB) con health checks y failover automático.
- Kafka (MSK) con tres brokers, replication factor ≥ 3.
- PostgreSQL RDS con réplica de lectura síncrona multi-AZ.

- Frontend distribuido en CloudFront con caching multi-edge.

4.2. Disaster recovery (DR)

- Región DR: AWS `us-west-2` (estrategia **warm standby**).
- Replicación asíncrona de PostgreSQL (lag ≤ 30 s).
- Snapshots diarios con cross-region copy.
- Backups lógicos (pg_dump) diarios + backups transaccionales (WAL archiving).
- Imágenes de contenedor en ECR multi-región.
- IaC (Terraform) permite reconstrucción completa en DR.

4.3. Estrategia 3-2-1 de backups

- **3 copias** de los datos críticos.
- **2 tipos de medios** distintos (RDS snapshots + almacenamiento S3 con Object Lock).
- **1 copia off-site** (cross-region).
- Pruebas mensuales de restauración en entorno aislado.

4.4. Proveedores críticos

Proveedor	Mitigación
AWS	Multi-AZ + DR multi-región; plan de reversibilidad a otro IaaS (Azure/GCP)
Credibanco	Comunicación dedicada + contingencia vía canal alterno a Visa
Kafka (MSK)	Consumidor con buffer local + reintento con backoff
Proveedor DNS	DNS secundario configurado
KMS (AWS)	Llaves replicadas cross-region

5. Plan de recuperación ante desastres (DRP)

5.1. Escenarios cubiertos

- **E1:** Indisponibilidad de una AZ — failover automático.
- **E2:** Indisponibilidad de toda la región primaria — failover manual a DR en ≤ 4 h.
- **E3:** Compromiso de datos / ransomware — aislamiento + restauración desde backup limpio.
- **E4:** Falla total de proveedor cloud — ejecución del plan de reversibilidad.
- **E5:** Falla de Credibanco — transacciones en cola + notificación masiva a subcomercios.

5.2. Procedimiento (escenario E2)

1. Detección por monitoreo (CloudWatch + alertas multi-canal).
2. Activación del DR Manager por parte del Comité de Crisis.
3. Declaración formal de desastre; activación de runbook `RUN-DR-001`.
4. Promoción de réplicas en región DR (RDS, S3, MSK).
5. Actualización de DNS hacia endpoints DR (Route53 health checks).
6. Validación de servicios críticos (smoke tests).
7. Comunicación a usuarios, subcomercios, banco sponsor, SFC.
8. Operación en DR hasta restauración de la región primaria.
9. Failback planificado (fuera de ventana transaccional).
10. Post-mortem obligatorio y actualización del plan.

6. Comité de Crisis

Rol	Responsable	Suplente
Líder de Crisis	Representante Legal	CTO
Comunicación externa	Asesor Legal	Representante Legal
Técnico	CTO	Líder de DevOps
Operaciones	Líder de Operaciones	Coordinador SRE
Cumplimiento	Asesor de Cumplimiento	Asesor Legal

- Reunión inicial dentro de los **15 minutos** posteriores a la declaración.
- Centro de Comando Virtual (WarRoom en Slack + conferencia).
- Bitácora obligatoria con timestamps y decisiones.

7. Comunicación

7.1. Internos

- Canales de Slack dedicados (`#incident-response`, `#war-room`).
- Llamadas telefónicas al Comité de Crisis.
- Escalamiento automático vía PagerDuty / Opsgenie.

7.2. Externos

- Subcomercios: banner en dashboard + email + webhook status.
- Clientes finales: status page pública (`status.fintrixs.com`).
- Banco sponsor: notificación formal por canal acordado contractualmente.
- Regulador: cuando aplique, vía canal oficial.
- Prensa / opinión pública: vocería centralizada en el Representante Legal.

8. Pruebas del plan

8.1. Cronograma

Tipo de prueba	Frecuencia	Alcance
Tabletop	Trimestral	Validación procedimental con stakeholders
Simulacro técnico (failover AZ)	Semestral	Ejecución real sin impacto al usuario
Simulacro DR (región completa)	Anual	Failover completo a región DR
Prueba de restore de backups	Mensual	Validación de integridad

8.2. Métricas de éxito

- RTO alcanzado ≤ meta definida.
- RPO observado ≤ meta definida.
- Cero pérdida de datos críticos.
- Comunicación completa a stakeholders en ≤ 30 minutos.
- Post-mortem dentro de los 5 días hábiles.

9. Plan de sucesión (continuidad de personal)

- **Documentación** de runbooks y procedimientos críticos.
- **Redundancia** mínima 2x en roles clave (no hay "bus factor = 1").
- **Cross-training** entre áreas.
- **Consultores externos** en retainer para capacidades específicas.
- **Manuales de emergencia** que permitan operación asistida por un tercero.

10. Estado de madurez al corte del DD

Elemento	Estado
BCP documentado	SÍ (este documento)
BIA con RTO/RPO	SÍ
DR en región secundaria	En preparación (target: T+3 meses desde go-live)
Backups 3-2-1	SÍ
Pruebas de restore	SÍ, mensuales desde 2025
Simulacro DR completo	PENDIENTE (programado Q3 2026)
Tabletop exercise	SÍ, trimestral
Plan de sucesión	Parcial (pendiente depth ≥ 2 en algunos roles)

11. Brechas y plan de cierre

Brecha	Criticidad	Remediación	Plazo
Simulacro DR completo aún no ejecutado	Media	Ejecución programada	Q3 2026
Certificación ISO 22301	Baja	Exploración tras estabilización operativa	2027
Redundancia de personal 2x en SRE	Media	Contratación en curso	Q2 2026

12. Revisión y aprobación

- **Revisión anual** obligatoria.
- **Revisión extraordinaria** tras:
- Cambio material de arquitectura.
- Incidente disruptivo.
- Cambio regulatorio.
- Cambio en proveedores críticos.
- **Aprobación** del Representante Legal y del Comité de Riesgos.