CONFIDENCIAL

FINTRIXS PAY

Respuestas al cuestionario de Due Diligence

08.1 — RESPUESTAS ESTRUCTURADAS AL CUESTIONARIO DE DD — AGREGADORES

CÓDIGO	—
VERSIÓN	—
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

Sección A — Información corporativa

P1. Razón social, NIT y constitución. Fintrixs S.A.S., NIT 901.994.194-3, sociedad por acciones simplificada constituida en Colombia. Ver **01.1 Información Corporativa**.

P2. Representante Legal y apoderados. Gabriel López Aponte, C.C. 1014199115 de Bogotá. Ver **01.1**.

P3. Estructura accionaria. Sociedad con un único accionista. No hay beneficiario final que supere el 5% con vinculación PEP. Detalle en **01.1**.

P4. Sede y operación. Domicilio en Bogotá D.C. Operación 100% digital. Infraestructura productiva en AWS `us-east-1` (ver anexo técnico **09.1**).

Sección B — SARLAFT

P5. ¿Cuenta con un sistema SARLAFT? Sí. Manual formalizado en **02.1 Manual SARLAFT**. Metodología de riesgo LAFT/FT/FPADM basada en la Circular 007 de 2018 (SFC) y referencia a Circular 100-000005 de 2014 (Supersociedades). Fintrixs no alcanza aún los umbrales que obligan al SAGRILAFT formal, pero adopta los elementos aplicables.

P6. Oficial de Cumplimiento. Función asignada al Representante Legal durante la fase pre-operativa. Se nombrará un Oficial de Cumplimiento dedicado **antes** del inicio de operaciones con el banco sponsor. Hoja de vida y certificación UIAF se anexarán en el paquete de nominación.

P7. Procedimiento KYC/KYB y consulta de listas. Descrito en **02.2 Procedimiento Conocimiento de Contrapartes**. Se consultan listas OFAC, ONU, INTERPOL, UE, PEP y listas internas. El `onboarding-service` integra estos controles con trazabilidad en `admin-audit-service`.

Sección C — Protección de datos personales

P8. Política de Tratamiento de Datos Personales (PTDP). Anexa en **03.0 Política_Tratamiento_Datos_Fintrixs_v2.pdf** (vigente, v2.1, 26 páginas).

P9. Registro en RNBD. Inscripción ante la SIC programada para el mes en curso. Plan en **03.1**.

P10. Procedimientos de autorización, revocación y PQR. Documentos **03.2** y **03.3**. Dentro de tiempos legales (15 días hábiles para consultas, 15 para reclamos).

P11. Protocolo de incidentes. 03.4. Reporte a SIC dentro de 15 días hábiles; registro nacional en RNBD.

P12. Uso de IA con datos personales. Gobernanza descrita en **03.6** conforme a **Circular 002 de 2024 de la SIC**. Los modelos de IA usados son proveídos por terceros certificados (sin entrenamiento propio sobre datos sensibles).

Sección D — Ciberseguridad y Seguridad de la Información

P13. Política de ciberseguridad. 04.1. Alineada con Circular 007/2018 de la SFC, NIST CSF e ISO 27001. Roles: Representante Legal, CTO, CSIRT, DPO.

P14. Estándares de referencia. 04.2. NIST CSF, ISO 27001/27002, PCI DSS v4.0, OWASP ASVS/SAMM, CIS Controls, CSA CCM, ITIL.

P15. Gestión de vulnerabilidades e incidentes. 04.3. SLA de remediación por severidad; CSIRT con procedimientos documentados; reporte obligatorio al regulador.

P16. Ethical hacking. 04.4. Resumen ejecutivo del último ejercicio; pruebas anuales + por release mayor. Sin hallazgos críticos abiertos al corte.

P17. Controles técnicos de la pasarela. 04.5. mTLS, JWT RS256, RBAC, RLS, WAF, tokenización, cifrado AES-256, KMS, SIEM, DLP.

P18. Arquitectura de seguridad backend. 04.6. Mapea cada microservicio a sus controles (payments-api, auth-service, tokenization-service, card-vault-service, etc.).

P19. Controles en aplicaciones web y móviles. 04.7. SSL pinning en móvil, CSP estricto en web, hardening del frontend, integridad del bundle.

Sección E — Riesgo operacional y fraude

P20. Metodología de gestión de riesgos. 05.1. Basada en ISO 31000, ISO 27005, NIST SP 800-30. Matriz en **05.4**.

P21. Prevención y detección de fraude. 05.2. Scoring transaccional, reglas de velocidad, 3DS 2.2, colaboración con emisor.

P22. 3D Secure y tokenización. 05.3. 3DS 2.2 vía Credibanco + Visa Secure. Tokenización híbrida (red + interna). Certificación PCI DSS v4.0 al ~95%.

P23. Matriz de riesgos y controles. 05.4. 18 riesgos identificados, ninguno con residual "Alto" o "Extremo" al corte.

Sección F — Anticorrupción y ética

P24. Política anticorrupción. 06.1. Tolerancia cero. Adopción voluntaria de un marco equivalente a PTEE.

P25. Código de ética. 06.2. Aplica a empleados, contratistas, proveedores, aliados y subcomercios.

P26. Canal ético de denuncias. 06.3. Multicanal, anónimo, confidencial, con política de no represalias.

Sección G — Continuidad del negocio

P27. Plan de continuidad (BCP). 07.1. RTO ≤ 1h para servicios T0. Multi-AZ + DR en región secundaria (warm standby).

P28. Plan de recuperación ante desastres (DRP). 07.1, sección 5. Escenarios E1–E5 cubiertos. Pruebas semestrales.

P29. Runbook operativo. 07.2. Procedimiento de respuesta a incidentes con severidades y árbol de decisión.

Sección H — Infraestructura y arquitectura

P30. Arquitectura de microservicios. ~15 microservicios NestJS + frontend Vue 3. Ver diagrama en **09.1**.

P31. Infraestructura cloud. AWS `us-east-1` (primaria), `us-west-2` (DR). Kubernetes (EKS), Kafka (MSK), PostgreSQL (RDS con Multi-AZ).

P32. Proveedores críticos. AWS (IaaS), Credibanco (adquirencia/3DS), Confluent/MSK (Kafka), auditor QSA (en contratación).

P33. Segregación de ambientes. Dev, Staging, Prod. Cuentas AWS separadas. Network policies y RLS en DB.

Sección I — Marco regulatorio y relaciones con terceros

P34. Licencias y habilitaciones. Fintrixs S.A.S. opera como **agregador** / **facilitador de pagos**. La liquidación y el procesamiento transaccional se realizan a través del **banco sponsor** y de la **red Credibanco (Visa)**. No se requiere licencia bancaria directa.

P35. Modalidad de integración con la red. MID independiente por subcomercio cuando el volumen lo justifica; agregación para volúmenes menores. Detalle técnico en **09.1**.

P36. Contratos con subcomercios. Incluyen cláusulas de cumplimiento, auditoría, protección de datos, anticorrupción, terminación por incumplimiento y tratamiento de datos personales conforme a Ley 1581.

P37. Contratos con proveedores. Incluyen NDAs, DPAs (cuando aplique), cláusulas anticorrupción, SLAs y derecho de auditoría.

Sección J — Estado financiero y operativo

P38. Estado financiero. Detalle en anexo financiero separado (entrega bajo NDA con firma del Representante Legal).

P39. Pólizas de seguro. Póliza de responsabilidad civil profesional en cotización. Se entregará al inicio de operación con el banco sponsor.

P40. Volumetría proyectada. Proyección en escenarios base / medio / alto. Entrega bajo NDA.

Resumen de brechas explícitamente declaradas

1. **Oficial de Cumplimiento dedicado** — pendiente, se nombrará antes del go-live.
2. **Certificación PCI DSS v4.0** — en curso, ~95% de avance, QSA en contratación.
3. **Registro RNBD** — programado mes en curso.
4. **Simulacro DR completo** — programado Q3 2026.
5. **Pólizas de RC profesional** — en cotización.
6. **Publicación pública** de políticas (anticorrupción, canal ético) — al inicio formal de operaciones.

Todas las brechas están acompañadas de un plan de cierre con fecha objetivo.