CONFIDENCIAL

FINTRIXS PAY

Respuestas al cuestionario de Due Diligence

08.2 — RESPUESTAS ESTRUCTURADAS AL CUESTIONARIO DE DD — TESORERÍA CENTRALIZADA / TPP-TRD

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

08.2 — RESPUESTAS ESTRUCTURADAS AL CUESTIONARIO DE DD — TESORERÍA CENTRALIZADA / TPP-TRD ·
Código: — · Versión: — · FINTRIXS S.A.S.

Módulo 1 — Información General de la Empresa

1. **Razón social / NIT:** Fintrixs S.A.S., NIT 901.994.194-3.
2. **Domicilio:** Bogotá D.C. — ver **01.1**.
3. **Representante Legal:** Gabriel López Aponte, C.C. 1014199115.
4. **Actividad económica:** Desarrollo de plataforma tecnológica de pagos (pasarela de pagos y agregador).
5. **Composición accionaria:** Ver **01.1**.
6. **Años de operación:** Constituida recientemente; pre-operacional en cuanto a procesamiento con banco sponsor.

Módulo 2 — Experiencia y relaciones bancarias

1. **Referencias bancarias:** Se entregan bajo NDA.
2. **Relaciones con otros bancos:** Cuenta corriente operativa. Sin otras relaciones de sponsorship activas.
3. **Antecedentes regulatorios:** Sin sanciones ni investigaciones en curso.

Módulo 3 — SARLAFT / Cumplimiento

1. **Sistema SARLAFT:** Ver **02.1**. Manual adoptado; Oficial de Cumplimiento a nombrar pre-go-live.
2. **KYC/KYB de contrapartes:** Ver **02.2**.
3. **Reporte a UIAF:** Estructura definida; reportes ROS se activarán con el inicio transaccional.
4. **Listas restrictivas consultadas:** OFAC, ONU, INTERPOL, UE, PEP, listas internas. Detalle en **02.2**.

Módulo 4 — Protección de Datos

1. **PTDP:** Documento **03.0** (26 páginas, v2.1).
2. **Inscripción RNBD:** Programada — ver **03.1**.
3. **DPO:** Rol asignado. Contacto en la política 03.0.
4. **Procedimientos del titular: 03.2** (autorización/revocación), **03.3** (PQR).
5. **Incidentes de seguridad de datos: 03.4**.

Módulo 5 — Ciberseguridad y TI

1. **Política de ciberseguridad: 04.1**.
2. **Gestión de incidentes: 04.3**.
3. **Pentest: 04.4** (último ejercicio concluido; sin hallazgos críticos abiertos).
4. **Controles técnicos: 04.5**.
5. **Arquitectura de seguridad: 04.6**.
6. **Aplicaciones web/móvil: 04.7**.
7. **Cifrado en reposo y tránsito:** AES-256 en reposo (KMS), TLS 1.2+/mTLS en tránsito.
8. **Gestión de accesos:** RBAC, MFA, JWT RS256, sesiones con revocación, auditoría en `admin-audit-service`.
9. **Segregación de funciones:** Matriz RACI por ambiente; separación entre quienes desarrollan, despliegan y auditan.

Módulo 6 — Riesgo Operacional

1. **Metodología de riesgos: 05.1** — ISO 31000, ISO 27005, NIST SP 800-30.
2. **Matriz de riesgos y controles: 05.4**.
3. **Riesgo de fraude: 05.2**.
4. **Tokenización y 3DS: 05.3**.

Módulo 7 — Continuidad del negocio

1. **BCP/DRP: 07.1**.
2. **RTO/RPO:** T0 → RTO ≤ 1h, RPO ≤ 5 min.
3. **Pruebas del plan:** Trimestrales (tabletop) + semestrales (técnicas) + anuales (DR completo).
4. **Runbook de respuesta: 07.2**.

Módulo 8 — Anticorrupción

1. **Política anticorrupción: 06.1**.
2. **Código de ética: 06.2**.
3. **Canal de denuncias: 06.3**.
4. **Capacitación:** Obligatoria en onboarding + refresco anual.

Módulo 9 — Infraestructura y Arquitectura

1. **Proveedores cloud:** AWS primaria (`us-east-1`), DR (`us-west-2`).

2. **Segmentación de red:** VPC con subnets públicas/privadas; CDE PCI aislado; network policies estrictas.
3. **Data residency:** Actualmente en US por requisitos de latencia y costo; análisis formal de transferencia internacional conforme a Ley 1581 (cláusulas contractuales tipo SIC).
4. **Monitoreo y alertas:** CloudWatch, Prometheus, Grafana, SIEM, PagerDuty.
5. **Gestión de llaves:** AWS KMS; rotación automatizada; llaves replicadas cross-region.

Módulo 10 — Modelo Operativo con el Banco Sponsor

1. **Flujo transaccional:** Subcomercio → Fintrixs Pay → Credibanco → red Visa → emisor → autorización.
2. **Liquidación:** A través del banco sponsor, con reconciliación T+N según contrato.
3. **Reportes al banco sponsor:** Reportes operativos y de cumplimiento con periodicidad acordada (típicamente diario/mensual).
4. **Capacidad de auditoría:** Fintrixs acepta auditorías del banco sponsor con preaviso razonable; derecho contractualmente previsto.

Módulo 11 — Aspectos específicos TPP-TRD / Tesorería centralizada

1. **Cuentas de recaudo y compensación:** Operadas en el banco sponsor; Fintrixs es el operador tecnológico del flujo.
2. **Conciliación automática:** `payments-api` ejecuta conciliación con archivos / endpoints del banco sponsor.
3. **Reporte de saldos:** Diario, con corte definido contractualmente.
4. **Manejo de devoluciones:** Proceso automatizado con trazabilidad punta a punta.
5. **Contingencia operativa:** Procedimientos manuales documentados en **07.2**.

Módulo 12 — Servicios de valor agregado

1. **Pagos recurrentes / tokenización de red:** Implementado.
2. **Disputas y contracargos:** Módulo en desarrollo; procedimiento documentado en runbook `RUN-DISPUTE-001` (entrega tras GA).
3. **Reportes para subcomercios:** Dashboard en Vue 3 + API GraphQL; exportación CSV/XLSX.

Módulo 13 — Relaciones con terceros

1. **Evaluación de proveedores críticos:** Proceso documentado; matriz de madurez aplicada.
2. **Contratos con cláusulas de cumplimiento:** Sí — PTDP, anticorrupción, auditoría.

3. **Subcontratación de funciones críticas:** No aplica en la capa regulatoria principal; ciertos servicios de infraestructura están en AWS.

Módulo 14 — Estado financiero

1. **Estados financieros:** Bajo NDA.
2. **Proyecciones financieras:** Bajo NDA.
3. **Pólizas de seguro:** En cotización (RC profesional + cibernética).

Módulo 15 — Estructura organizacional

1. **Organigrama:** Ver **01.1** (estructura resumida). Detallado bajo NDA.
2. **Roles de cumplimiento:** Representante Legal (RL), DPO, CISO, Oficial de Cumplimiento (a nombrar), Asesor Legal.
3. **Plan de talento:** Plan de contratación y sucesión documentado en **07.1**, sección 9.

Anexos asociados a este cuestionario

Anexo	Ubicación
Organigrama detallado	Bajo NDA
Estados financieros	Bajo NDA
Pólizas	En cotización
Referencias comerciales	Bajo NDA
Certificaciones (ISO/PCI)	En curso; se entregan al concluir

Declaración de veracidad

El Representante Legal declara que la información suministrada es veraz, completa y suficiente, y autoriza al banco sponsor a consultar centrales de información, listas restrictivas y referencias conforme a la normatividad vigente. Los documentos marcados como "Bajo NDA" se entregan mediante canal seguro una vez firmado el NDA correspondiente.