CONFIDENCIAL

FINTRIXS PAY

Due Diligence

ÍNDICE MAESTRO — PAQUETE DE DUE DILIGENCE PARA BANCO SPONSOR AGREGADOR

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

1. Objetivo del paquete

Este paquete consolida la documentación regulatoria, de cumplimiento, de protección de datos personales y de ciberseguridad que Fintrixs S.A.S. entrega al Banco Sponsor Agregador como soporte de los dos formularios de Due Diligence diligenciados:

- **DUE DILIGENCE CT AGREGADORES DE ADQUIRENCIA — Versión 5.0** (aplicable a Fintrixs como agregador de adquirencia PayFac).
- **DUE DILIGENCE CENTRALIZACIÓN TESORERÍA / PAGOS — Versión 5.0** (aplicable a Fintrixs como TPP/TRD integrado al ecosistema del banco).

La documentación cubre las seis áreas de evaluación del banco: SARLAFT, Protección de Datos Personales, Ciberseguridad y Seguridad de la Información, Riesgo Operacional y Gestión del Fraude, Anticorrupción, y Continuidad del Negocio.

2. Arquitectura de alto nivel de Fintrixs Pay

Fintrixs Pay es una plataforma de pagos construida sobre un monorepo de aproximadamente 15 microservicios NestJS (TypeScript) y un frontend Vue 3. La plataforma cumple con:

- **PCI DSS v4.0** — scope delimitado a los servicios `card-vault-service` y `tokenization-service`; el resto de servicios opera con tokens (no PANs).
- **Ley 1581 de 2012** — protección de datos personales conforme al marco colombiano.
- **Circular Externa 007 de 2018 SFC** — requerimientos mínimos de ciberseguridad.
- **Circular Externa 008 de 2018 SFC** — protección de la información de consumidores financieros en pasarelas de pago.
- **Circular Externa 005 de 2019 SFC** — uso de servicios de computación en la nube.
- **Circular Externa 002 de 2024 SIC** — tratamiento de datos personales en sistemas de IA.
- **NIST Cybersecurity Framework**, **OWASP ASVS/Top 10**, **ISO/IEC 27001** (en proceso de alineación).

3. Estructura del paquete

Carpeta	Contenido	Área del DD que soporta
`01_Datos_Generales/`	Información corporativa, composición accionaria, certificados	INICIO - DATOS GENERALES
`02_SARLAFT/`	Manual SARLAFT, procedimientos KYC y de conocimiento de contrapartes	SARLAFT
`03_Proteccion_Datos_Personales/`	Política v2.1 (publicada), procedimientos y protocolos de privacidad	PROTECCIÓN DE DATOS PERSONALES
`04_Ciberseguridad_SI/`	Política de ciberseguridad, gestión de vulnerabilidades, pentesting, arquitectura de seguridad	CIBERSEGURIDAD Y SI
`05_Riesgo_Operacional_Fraude/`	Metodología de riesgos, matriz, política de prevención de fraude	RIESGO OPERACIONAL Y FRAUDE
`06_Anticorrupcion/`	Código de ética, política anticorrupción, canal de denuncias	ANTICORRUPCIÓN
`07_Continuidad_Negocio/`	Plan de continuidad (BCP), plan de recuperación (DRP)	CIBERSEGURIDAD Y SI (ítem BCM)
`08_Respuestas_Cuestionario/`	Respuestas textuales estructuradas a ambos cuestionarios de DD	Soporte transversal
`09_Anexos_Tecnicos/`	Diagrama de red, flujo de datos, inventario de activos, tokenización	Ciberseguridad y PDP

4. Mapa de documentos por pregunta del Due Diligence

4.1. SARLAFT (DD Agregadores y DD Tesorería)

# Pregunta DD	Documento entregado
P1–P8. Programa LAFT, Oficial de Cumplimiento, listas sancionatorias	`02_SARLAFT/02.1_Manual_SARLAFT_Fintrixs.md`
Debida diligencia a contrapartes	`02_SARLAFT/02.2_Procedimiento_Conocimiento_Contrapartes.md`

4.2. Protección de Datos Personales (DD Agregadores P1–P22 / DD Tesorería P1–P22)

# Pregunta DD	Documento entregado
P2. Política de Tratamiento de Datos Personales	`03_Proteccion_Datos_Personales/03.0_Politica_Tratamiento_Datos_Fintrixs_v2.pdf`
P8. Procedimiento de recolección, uso, circulación y supresión	`03.1_Procedimiento_Ciclo_Vida_Datos.md`
P9–P10. Autorización y revocatoria	`03.2_Procedimiento_Autorizacion_Revocacion.md`
P11. PQRs en protección de datos	`03.3_Procedimiento_PQRs.md`
P12. Protocolo de incidentes de seguridad de datos	`03.4_Protocolo_Incidentes_Datos.md`
P7. Acuerdos de confidencialidad	`03.5_Acuerdo_Confidencialidad_Modelo.md`
P22.1–22.4. IA y tratamiento de datos personales (Circular 002/2024 SIC)	`03.6_Gobierno_IA_Datos_Personales.md`

4.3. Ciberseguridad y SI (DD Agregadores P1–P7 / DD Tesorería P1–P11)

# Pregunta DD	Documento entregado
P1. Estándares (ISO 27001, PCI DSS, NIST, OWASP, CSA, ITIL)	`04_Ciberseguridad_SI/04.2_Marco_Referencia_Estandares.md`
P2. Regulaciones nacionales (Circ. 005/2019, 007/2018, 008/2018 SFC; Ley 1581)	`04.2_Marco_Referencia_Estandares.md` (sección 3)
P3. Política de Ciberseguridad y SI aprobada por directivos	`04.1_Politica_Ciberseguridad_Seguridad_Informacion.md`
P3. Proceso de gestión de vulnerabilidades e incidentes	`04.3_Proceso_Gestion_Vulnerabilidades_Incidentes.md`
P3. Informe de hacking ético / pentesting	`04.4_Informe_Ethical_Hacking_Resumen_Ejecutivo.md`
P4. Prácticas en pasarela propia (MFA, RBAC, mTLS, cifrado, WAF, 3DS)	`04.5_Controles_Tecnicos_Pasarela.md`
P6. Controles en back-end e integraciones	`04.6_Arquitectura_Seguridad_Backend.md`
P7–P8. App móvil y web (anti-ing inversa, SSL pinning, CSRF, DoS)	`04.7_Controles_Aplicaciones_Web_Movil.md`

4.4. Riesgo Operacional y Fraude

# Pregunta DD	Documento entregado
P1. Metodología de gestión de riesgos	`05_Riesgo_Operacional_Fraude/05.1_Metodologia_Gestion_Riesgos.md`
P3–P7. Controles de detección de errores y fraude	`05.2_Politica_Prevencion_Deteccion_Fraude.md`
P8. 3D Secure y tokenización	`05.3_Autenticacion_3DS_Tokenizacion.md`
Matriz de riesgos y controles	`05.4_Matriz_Riesgos_Controles.md`

4.5. Anticorrupción

# Pregunta DD	Documento entregado
P4. Declaración de cero tolerancia	`06_Anticorrupcion/06.1_Politica_Anticorrupcion.md`
P5–P10. Regalos, remuneraciones, funcionarios públicos	`06.1_Politica_Anticorrupcion.md`
P16–P17. Canal ético	`06.3_Canal_Etico_Denuncias.md`
Código de ética y conducta	`06.2_Codigo_Etica_Conducta.md`

4.6. Continuidad del negocio

# Pregunta DD	Documento entregado
P18–P19 Agregadores / Módulo 7 Tesorería — BCP/DRP, RTO/RPO, pruebas	`07_Continuidad_Negocio/07.1_Plan_Continuidad_Negocio.md`
Procedimiento operativo de respuesta a incidentes críticos	`07_Continuidad_Negocio/07.2_Runbook_Respuesta_Incidentes.md`

4.7. Respuestas estructuradas a los cuestionarios

# Cuestionario	Documento entregado
DD Agregadores de Adquirencia (Versión 5.0)	`08_Respuestas_Cuestionario/08.1_Respuestas_Cuestionario_Agregadores.md`
DD Centralización Tesorería / TPP-TRD (Versión 5.0)	`08_Respuestas_Cuestionario/08.2_Respuestas_Cuestionario_Tesoreria_TPP.md`

4.8. Anexos técnicos (soporte transversal)

Anexo	Documento entregado
Arquitectura técnica general (diagrama lógico + microservicios)	`09_Anexos_Tecnicos/09.1_Arquitectura_Tecnica_Fintrixs_Pay.md`
Flujo de datos PCI (DFD) y mapeo PCI DSS v4.0	`09_Anexos_Tecnicos/09.2_Flujo_Datos_PCI_DFD.md`
Inventario de activos de información	`09_Anexos_Tecnicos/09.3_Inventario_Activos_Informacion.md`
Mapa de cumplimiento normativo → controles → evidencia	`09_Anexos_Tecnicos/09.4_Mapa_Controles_Normativos.md`

5. Convenciones de uso

Los documentos se presentan en formato Markdown (`.md`) para facilitar su revisión y conversión. La política de Tratamiento de Datos Personales se entrega en su formato oficial PDF (versión firmada y publicada). Todos los documentos llevan un encabezado con versión, fecha de emisión, aprobación y vigencia, y son de uso exclusivo en el marco del proceso de afiliación con el banco sponsor.

6. Declaración de veracidad

Todo el contenido de este paquete es de responsabilidad de Fintrixs S.A.S. y refleja el estado de la Compañía a la fecha de emisión (16 de abril de 2026). Fintrixs se compromete a notificar al banco sponsor cualquier cambio material en los controles, políticas o procedimientos aquí descritos durante la vigencia de la relación comercial.

Juan Carlos Traslaviña Abaunza — Representante Legal Suplente / COO **Gabriel Ureña Chacón** — CEO / CTO — Responsable de la integración tecnológica