CONFIDENCIAL

FINTRIXS PAY

Anexos técnicos

09.4 — MAPA DE CUMPLIMIENTO NORMATIVO → CONTROLES → EVIDENCIA

CÓDIGO	ANX-004
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

09.4 — MAPA DE CUMPLIMIENTO NORMATIVO → CONTROLES → EVIDENCIA · Código: ANX-004 · Versión: 1.0 — 16 de abril de 2026 · FINTRIXS S.A.S.

1. Regulación colombiana — protección del consumidor y datos personales

Norma	Exigencia	Control Fintrixs	Evidencia
Ley 1581/2012 + Decreto 1377/2013	Tratamiento de datos con finalidad, autorización, derechos	PTDP v2.1	**03.0**
Ley 1581/2012	Procedimientos de consulta, reclamo, revocación	PQR + autorización	**03.2**, **03.3**
Ley 1581/2012 art. 17, 18	DPO designado	Rol DPO asignado	**03.0** y org. en **01.1**
Ley 2300/2023	Canales de atención y "no molestar"	Honrado en `email-service` y campañas	**03.0** secc. 12
Circular SIC 002/2024	Gobernanza de IA con datos personales	Política IA	**03.6**
Decreto 1074/2015 (compilatorio)	Registro RNBD	Inscripción programada	**03.1**

2. Regulación financiera — SFC

Norma	Exigencia	Control	Evidencia
Circular 007/2018 SFC	Requerimientos mínimos de ciberseguridad	Política CSI, CSIRT, reportes, controles técnicos	**04.1**, **04.3**, **04.5**
Circular 005/2019 SFC	Seguridad y calidad en manejo de información del consumidor financiero	Cifrado, autenticación, RLS, auditoría	**04.5**, **04.6**
Circular 008/2018 SFC	Continuidad del negocio	BCP/DRP	**07.1**, **07.2**
Circular 029/2014 (CBJ)	Protección al consumidor financiero	Canales de atención, información clara	**03.3**

3. Regulación anti-LA/FT

Norma	Exigencia	Control	Evidencia
Circular 007/2018 SFC (SARLAFT)	Sistema de administración de LAFT	Manual SARLAFT, Oficial de Cumplimiento, monitoreo, ROS	**02.1**, **02.2**
Circular 100-000005/2014 Supersociedades	SAGRILAFT	Adopción parcial (debajo de umbrales obligatorios)	**02.1**
Resolución UIAF 212/2009	Reportes ROS	Estructura definida; activación con go-live	**02.1** secc. 8
Ley 1121/2006	Obligaciones anti-lavado	Consulta listas sancionatorias, KYC/KYB	**02.2**

4. Regulación anticorrupción

Norma	Exigencia	Control	Evidencia
Ley 1778/2016	Responsabilidad por soborno transnacional	Política anticorrupción, debida diligencia a terceros	**06.1**
Ley 2195/2022	Lucha contra la corrupción	Cláusulas contractuales, capacitación	**06.1**
Circular 100-000011/2021 Supersociedades (PTEE)	Programa de transparencia (aplica por umbrales)	Marco equivalente voluntario	**06.1**, **06.2**, **06.3**

5. Estándares internacionales adoptados

Estándar	Adopción	Evidencia
PCI DSS v4.0	Implementado ~95%; QSA en contratación	**04.5**, **04.6**, **05.3**, **09.2**
NIST CSF	Identify, Protect, Detect, Respond, Recover mapeados	**04.2**
ISO 27001/27002	Marco de referencia; certificación exploratoria	**04.2**
ISO 22301	Adopción parcial (BCP)	**07.1**
OWASP ASVS / SAMM	Desarrollo seguro	**04.2**, **04.5**
CSA CCM	Controles cloud	**04.2**
ITIL 4	Gestión de servicios	**04.3**
CIS Controls	Hardening y baseline	**04.2**

6. Regulación laboral y corporativa (pertinente al DD)

Norma	Exigencia	Control
Código Sustantivo del Trabajo	Contratación regular	Procesos de talento documentados
Ley 1010/2006	Prevención de acoso laboral	**06.2** secc. 5.7
Ley 222/1995 + 1258/2008	Gobierno corporativo SAS	Estatutos vigentes

7. Lista de brechas reconocidas (declaración transparente)

#	Brecha	Estado	Fecha objetivo
1	Oficial de Cumplimiento dedicado	Pendiente de designación formal	Pre-go-live con sponsor
2	Certificación PCI DSS v4.0	En proceso (~95%)	Q3 2026
3	Registro RNBD	Programado	Mes en curso
4	Simulacro DR completo	Programado	Q3 2026
5	Pólizas de RC profesional y cibernética	Cotización	Pre-go-live
6	Publicación pública de políticas	En preparación	Inicio de operaciones con sponsor
7	Redundancia 2x en algunos roles SRE	Contratación en curso	Q2 2026
8	Certificación ISO 27001 formal	Exploratorio	2027
9	Certificación ISO 22301 formal	Exploratorio	2027

8. Governance

Este mapa se revisa **trimestralmente** en el Comité de Riesgos y se actualiza ante cambios regulatorios o materiales. La aprobación corresponde al Representante Legal.