CONFIDENCIAL

FINTRIXS PAY

Protección de datos personales

03.6 — GOBIERNO DE INTELIGENCIA ARTIFICIAL Y TRATAMIENTO DE DATOS PERSONALES

CÓDIGO	PDP-006
VERSIÓN	1.0 — 16 de abril de 2026
APROBADO POR	DPO / CTO
VIGENCIA	12 meses (revisión obligatoria anual por evolución normativa)

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

03.6 — GOBIERNO DE INTELIGENCIA ARTIFICIAL Y TRATAMIENTO DE DATOS PERSONALES · Código: PDP-006 · Versión: 1.0 — 16 de abril de 2026 · FINTRIXS S.A.S.

1. Objetivo

Establecer lineamientos para el uso responsable de sistemas analíticos y de Inteligencia Artificial (IA) que involucren el tratamiento de datos personales, conforme a:

- Circular Externa 002 de 2024 SIC — lineamientos para el tratamiento de datos personales en sistemas de IA.
- Principios de la OCDE para la administración responsable de IA confiable.
- Ley 1581 de 2012, Decreto 1377 de 2013, Ley 2300 de 2023.
- Buenas prácticas NIST AI RMF 1.0.

2. Alcance

Aplica a cualquier sistema analítico o de IA utilizado por Fintrixs para:

- Prevención y detección de fraude transaccional.
- Análisis de comportamiento de pagos.
- Evaluación de riesgo en onboarding de comercios.
- Motores de recomendación y personalización.
- Generación de alertas y scoring.

3. Principios aplicados (OCDE)

1. **Crecimiento inclusivo, desarrollo sostenible y bienestar.**
2. **Respeto al estado de derecho, derechos humanos y valores democráticos.**
3. **Transparencia y explicabilidad.**
4. **Robustez, seguridad y resiliencia.**
5. **Rendición de cuentas.**

4. Principios de PDP aplicados a IA

- **Idoneidad:** los datos son pertinentes al objetivo del modelo.
- **Necesidad:** se usa el volumen mínimo de datos para el propósito.
- **Razonabilidad:** los resultados no generan decisiones arbitrarias.
- **Proporcionalidad:** el impacto del tratamiento es acorde al fin.

5. Ciclo de vida del modelo

5.1. Diseño

- Identificación de la finalidad y base de legitimación.
- Análisis previo de impacto de privacidad (PIA/DPIA) **obligatorio** para modelos que traten datos personales (pendiente de formalización para todos los modelos actuales; hoja de ruta de implementación en Q2/Q3 2026).
- Selección de fuentes de datos con autorización vigente.
- Eliminación / seudonimización de campos no esenciales.

5.2. Desarrollo y entrenamiento

- Ambientes segregados para entrenamiento (nunca con datos productivos en crudo).
- Datos sintéticos o seudonimizados cuando sea posible.
- Registros de linaje de datos (data lineage).
- Firma del dataset (hash SHA-256).

5.3. Validación

- Evaluación de sesgo, equidad y explicabilidad.
- Pruebas adversariales.
- Umbrales mínimos de precisión, recall y fairness.

5.4. Despliegue

- Control de versiones del modelo (MLOps).
- Registro en el catálogo interno de modelos.
- Monitoreo en producción (drift de datos y de concepto).
- Alertas automáticas ante degradación.

5.5. Mantenimiento y retiro

- Revisión del modelo al menos cada 6 meses.
- Retraining documentado.
- Retiro formal y supresión de artefactos cuando el modelo queda obsoleto.

6. Gobierno de modelo

Rol	Responsabilidad
Comité de Datos e IA	Aprobación de nuevos modelos con tratamiento de datos personales
Data Owner	Autoriza el uso de datos para un modelo específico
Model Owner	Responsable del desempeño del modelo
DPO	Supervisa cumplimiento normativo de privacidad
CISO	Supervisa controles de seguridad del modelo

7. Transparencia frente al titular

- Se informa al titular cuando una decisión automatizada tiene impacto sobre él (ej. rechazo transaccional por motor de fraude).
- El titular puede solicitar revisión humana de la decisión.
- La política de privacidad v2.1 describe los usos analíticos y la posibilidad de oponerse a la toma de decisiones automatizadas.

8. Riesgo de modelo

Fintrixs está implementando una metodología formal de gestión del riesgo de modelo, inspirada en la Guía de Supervisión de Riesgo de Modelo de la SFC, que incluye:

- Clasificación de modelos por criticidad.
- Inventario centralizado.
- Validación independiente de modelos críticos.
- Controles compensatorios (límites, revisiones humanas).

Estado: en definición; cronograma de implementación dentro de los 6 meses siguientes al inicio de operaciones comerciales con el banco.

9. Auditoría y trazabilidad

- Cada decisión relevante del modelo queda trazada en `admin-audit-service` con metadatos (versión del modelo, features clave, score, resultado).
- Los registros permiten reproducir la decisión ante un reclamo o una auditoría regulatoria.

10. Hoja de ruta

Ítem	Plazo
Formalización de DPIA para todos los modelos con datos personales	Q2 2026
Implementación de la metodología de riesgo de modelo	Q3 2026
Auditoría externa de fairness en modelos antifraude	Q4 2026
Publicación de informe anual de IA responsable	Q1 2027