fintrixs

EL CONTROL ES TUYO — LA TRANSPARENCIA NUESTRA

Política de Tratamiento de Datos Personales y Privacidad

FINTRIXS S.A.S. | NIT 901994194-3

Bogotá D.C., Colombia

Versión 2.1 | Vigencia: 1 de octubre de 2025

Última actualización: 16 de abril de 2026

CONTENIDO

DISPOSICIONES GENERALES

1. Identificación del Responsable del Tratamiento
2. Naturaleza de la Compañía y Actividad de Pasarela de Pagos
3. Objeto y Alcance de la Política
4. Definiciones
5. Marco Normativo Aplicable
6. Principios Rectores del Tratamiento

DATOS PERSONALES Y TRATAMIENTO

7. Tipología de Datos Tratados
8. Finalidades del Tratamiento
9. Autorización del Titular
10. Derechos de los Titulares
11. Procedimiento para Ejercer Derechos
12. Deberes de Fintrixs como Responsable

PASARELA DE PAGOS — TRATAMIENTO ESPECIAL DE DATOS

13. Datos Personales en la Operación de Pasarela de Pagos
14. Datos de Tarjetahabientes y Cumplimiento PCI DSS
15. Procesamiento de Transacciones y Flujo de Datos
16. Tokenización de Datos de Pago
17. Prevención de Fraude y Monitoreo Transaccional
18. Responsabilidades Compartidas: Comercio, Adquirente y Pasarela
19. Datos del Comercio Afiliado (Merchant Data)
20. Pagos Internacionales y Flujo Transfronterizo de Datos
21. Retención y Eliminación de Datos Transaccionales

TECNOLOGÍA, SEGURIDAD Y BLOCKCHAIN

22. Seguridad de la Información
23. Uso de Tecnología Blockchain y Protección de Datos
24. Analítica, Inteligencia Artificial y Automatización
25. Cookies y Tecnologías de Rastreo

TRANSFERENCIA, INCIDENTES Y DISPOSICIONES FINALES

26. Transferencia y Transmisión Internacional de Datos
27. Compartición de Información y Encargados del Tratamiento
28. Tratamiento de Datos de Menores de Edad
29. Gestión de Incidentes de Seguridad
30. Conservación y Supresión de Datos
31. Limitación de Responsabilidad
32. Oficial de Protección de Datos
33. Vigencia y Actualizaciones
34. Aceptación de la Política
35. Información de Contacto

1. IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO

FINTRIXS S.A.S. (en adelante **"Fintrixs"** o **"la Compañía"**), sociedad comercial constituida bajo las leyes de la República de Colombia, actúa como responsable del tratamiento de datos personales en los términos de la Ley 1581 de 2012 y sus decretos reglamentarios.

Campo	Detalle
Razón Social	FINTRIXS S.A.S.
NIT	901994194-3
Domicilio	Bogotá D.C., Colombia
Dirección	Cra 78 No. 17-55, Oficina 704
Correo electrónico	info@fintrixs.com
Teléfono	+57 302 318 4519
Sitio web	https://fintrixs.com

2. NATURALEZA DE LA COMPAÑÍA Y ACTIVIDAD DE PASARELA DE PAGOS

2.1. Naturaleza corporativa

Fintrixs es una compañía de base tecnológica enfocada en el desarrollo de infraestructura digital, soluciones SaaS, herramientas fintech y sistemas basados en tecnología blockchain. Integra pagos tradicionales con tecnología blockchain a través de un ecosistema DeFi, ofreciendo terminales POS, wallets criptográficas, tokenización FIAT (FINX), Mini Apps empresariales, ERP contable (CUENTYX) y pasarelas de pagos híbridas.

2.2. Actividad como pasarela de pagos

Fintrixs opera como **pasarela de pagos híbrida**, facilitando la intermediación tecnológica entre los comercios (merchants), los compradores (tarjetahabientes o pagadores), las redes de procesamiento (Visa a través de Credibanco), los bancos adquirentes, los bancos emisores y las redes blockchain (Hedera Hashgraph). En esta calidad, Fintrixs:

• Recibe, procesa, enruta y confirma instrucciones de pago originadas por compradores a favor de comercios.

• Captura y transmite datos de instrumentos de pago (tarjetas, tokens, wallets) de forma cifrada a los procesadores y redes correspondientes.

• Opera como agregador de pagos autorizado por el banco sponsor, canalizando las transacciones de los comercios afiliados a su ecosistema.

• Gestiona la conciliación, liquidación y dispersión de fondos a los comercios conforme a los acuerdos comerciales establecidos.

• Emite tarjetas Visa físicas y virtuales en articulación con el banco sponsor y la red Visa.

• Procesa pagos en blockchain mediante tokens FINX y USDC a través de la red Hedera Hashgraph.

2.3. Roles en el ecosistema de pagos

En el contexto del ecosistema de pagos, Fintrixs desempeña los siguientes roles de acuerdo con la operación:

Rol	Descripción	Relación con datos personales
Pasarela de pagos (Payment Gateway)	Captura y transmite los datos de la transacción de forma cifrada al procesador/adquirente.	Responsable y/o encargado del tratamiento de datos transaccionales.
Agregador de pagos (Payment Facilitator)	Permite a comercios procesar pagos bajo su cuenta maestra con el banco sponsor.	Responsable del tratamiento de datos de comercios y subcomercioantes.
Emisor de instrumentos (vía banco sponsor)	Gestiona la emisión de tarjetas Visa físicas y virtuales para usuarios del ecosistema.	Corresponsable junto al banco sponsor del tratamiento de datos de tarjetahabientes.
Operador de wallet y tokens	Administra las wallets MPC y la operación del token FINX en blockchain.	Responsable del tratamiento de datos vinculados a wallets y transacciones on-chain.

2.4. Declaración regulatoria

Fintrixs actúa como **proveedor de tecnología e infraestructura de pagos**, y no como entidad financiera vigilada por la Superintendencia Financiera de Colombia. La Compañía no capta, administra ni custodia recursos del público de forma directa. Las operaciones financieras se canalizan a través de bancos sponsor, entidades adquirentes y redes de pago debidamente autorizados y regulados. La emisión de tarjetas y el manejo de fondos se realiza siempre en

articulación con las entidades financieras correspondientes.

3. OBJETO Y ALCANCE DE LA POLÍTICA

3.1. Objeto

La presente Política tiene por objeto establecer los criterios, procedimientos y directrices que Fintrixs adoptará para la recolección, almacenamiento, uso, circulación, transferencia, transmisión, supresión y, en general, el tratamiento de datos personales de los titulares, en cumplimiento de la Constitución Política de Colombia, la Ley 1581 de 2012, las normas del estándar PCI DSS y la regulación aplicable al procesamiento de pagos.

3.2. Alcance

Esta política aplica a todas las bases de datos y/o archivos que contengan datos personales tratados por Fintrixs, incluyendo:

- Clientes corporativos (comercios afiliados al ecosistema de pagos).
- Tarjetahabientes y compradores que realicen transacciones a través de las plataformas de Fintrixs.
- Usuarios de las wallets, aplicaciones y servicios digitales de Fintrixs.
- Inversionistas y participantes de los protocolos FCRP y FCRPe.
- Proveedores, contratistas, procesadores y aliados comerciales.
- Empleados, colaboradores y candidatos.
- Visitantes de los sitios web, aplicaciones y plataformas.
- Bancos sponsor, entidades adquirentes y emisores involucrados en el flujo de pagos.
- Terceros relacionados con la operación de la Compañía.

4. DEFINICIONES

Para efectos de la presente política se adoptan las siguientes definiciones:

4.1. Definiciones de protección de datos (Ley 1581 de 2012)

Autorización: Consentimiento previo, expreso e informado del titular para el tratamiento de datos personales.

Base de datos: Conjunto organizado de datos personales que sea objeto de tratamiento.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato sensible: Dato que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación. Incluye datos biométricos, de salud, orientación política, convicciones religiosas, origen racial o étnico.

Dato público: Dato calificado como tal por la ley o la Constitución Política.

Dato privado: Dato que por su naturaleza íntima o reservada solo es relevante para el titular.

Encargado del tratamiento: Persona natural o jurídica que realice el tratamiento de datos personales por cuenta del responsable.

Responsable del tratamiento: Persona natural o jurídica que decida sobre la base de datos y/o el tratamiento de datos.

Titular: Persona natural cuyos datos personales sean objeto de tratamiento.

Tratamiento: Cualquier operación sobre datos personales: recolección, almacenamiento, uso, circulación o supresión.

Transferencia: Envío de información a otro responsable dentro o fuera del país.

Transmisión: Comunicación de datos al encargado por cuenta del responsable, dentro o fuera del territorio.

4.2. Definiciones del ecosistema de pagos

Pasarela de pagos (Payment Gateway): Plataforma tecnológica que captura, cifra, transmite y enruta datos de transacciones de pago entre el comercio, el comprador y las redes de procesamiento.

Tarjetahabiente (Cardholder): Persona natural o jurídica titular de una tarjeta de crédito o débito emitida por un banco emisor, que utiliza dicho instrumento para realizar pagos.

Comercio afiliado (Merchant): Persona natural o jurídica que acepta pagos a través de las plataformas de Fintrixs y tiene un acuerdo comercial vigente con la Compañía.

Banco adquirente (Acquirer): Entidad financiera que procesa las transacciones con tarjeta por cuenta del comercio afiliado.

Banco emisor (Issuer): Entidad financiera que emite la tarjeta de crédito o débito al tarjetahabiente.

Banco sponsor: Entidad financiera que respalda las operaciones de Fintrixs como agregador de pagos, permitiendo la emisión de tarjetas y el procesamiento de transacciones bajo su licencia.

PAN (Primary Account Number): Número principal de la cuenta de la tarjeta de pago.

PCI DSS: Payment Card Industry Data Security Standard. Estándar de seguridad de datos de la industria de tarjetas de pago, establecido por el PCI Security Standards Council.

Tokenización de pago: Proceso de sustitución del PAN por un valor alfanumérico no reversible (token de pago) que no puede ser utilizado fuera del contexto específico autorizado.

3D Secure (3DS): Protocolo de autenticación del tarjetahabiente que añade una capa adicional de seguridad en transacciones de comercio electrónico.

Credibanco: Red de pagos adquirente en Colombia que procesa transacciones Visa.

CVV/CVC: Código de verificación de la tarjeta. Dato de autenticación que no debe almacenarse tras la autorización.

4.3. Definiciones tecnológicas y blockchain

Blockchain: Tecnología de registro distribuido que almacena datos de forma inmutable y transparente en una red descentralizada.

Hedera Hashgraph: Red de registro distribuido de nivel empresarial utilizada por Fintrixs para la emisión de tokens y el procesamiento de transacciones blockchain.

Token FINX: Token operativo empresarial emitido por Fintrixs sobre Hedera, respaldado 1:1 por moneda FIAT en cuentas del banco sponsor.

Wallet MPC: Billetera digital basada en computación multipartita que divide la llave privada en fragmentos para mayor seguridad sin frases semilla.

HSM (Hardware Security Module): Módulo de seguridad de hardware utilizado para la protección de llaves criptográficas.

KYC (Know Your Customer): Proceso de verificación de identidad del cliente conforme a regulaciones de prevención de lavado de activos.

AML (Anti-Money Laundering): Procedimientos y controles para la prevención del lavado de activos y financiación del terrorismo.

Gasless / Relayer gasless: Mecanismo que permite al usuario realizar transacciones blockchain sin pagar directamente las comisiones de red (gas fees).

5. MARCO NORMATIVO APLICABLE

5.1. Legislación colombiana de protección de datos

• **Constitución Política de Colombia** — Artículos 15 y 20 (derecho a la intimidad y habeas data).

• **Ley Estatutaria 1581 de 2012** — Régimen General de Protección de Datos Personales.

• **Decreto 1377 de 2013** — Reglamentario parcial de la Ley 1581 de 2012.

• **Decreto 1074 de 2015** — Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.

• **Ley 1266 de 2008** — Habeas data en el ámbito financiero y comercial.

• **Circular Externa 002 de 2015 de la SIC** — Registro Nacional de Bases de Datos.

5.2. Normativa aplicable a pagos y servicios financieros

• **Ley 527 de 1999** — Comercio electrónico, firmas digitales y mensajes de datos.

• **Ley 1273 de 2009** — Delitos informáticos y protección de la información.

• **Ley 1735 de 2014** — Sociedades Especializadas en Depósitos y Pagos Electrónicos (SEDPE).

• **Decreto 1357 de 2018** — Actividades de financiación colaborativa y crowdfunding.

• **Circulares de la Superintendencia Financiera de Colombia** aplicables a la operación con bancos sponsor y redes de pago.

• **Regulación de Credibanco y Visa** sobre procesamiento de transacciones, prevención de fraude y manejo de disputas.

5.3. Estándares internacionales

• **PCI DSS v4.0** — Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago.

• **PCI PA-DSS** — Estándar de seguridad para aplicaciones de pago.

• **GDPR** — Reglamento General de Protección de Datos de la Unión Europea (principios de referencia).

• **ISO/IEC 27001** — Sistema de Gestión de Seguridad de la Información.

• **ISO 22301** — Continuidad del negocio.

• **Recomendaciones GAFI** — Prevención de lavado de activos y financiación del terrorismo.

• **EMVCo 3D Secure** — Especificaciones de autenticación de pagos.

6. PRINCIPIOS RECTORES DEL TRATAMIENTO

Fintrixs garantiza que todo tratamiento de datos personales se realizará conforme a los siguientes principios:

Legalidad: Tratamiento conforme a las disposiciones legales vigentes.

Finalidad: El tratamiento obedecerá a una finalidad legítima, informada previamente al titular.

Libertad: Tratamiento solo con consentimiento previo, expreso e informado, salvo excepciones legales.

Veracidad o calidad: La información será veraz, completa, exacta, actualizada y comprensible.

Transparencia: El titular podrá obtener en cualquier momento información sobre sus datos.

Acceso y circulación restringida: Los datos se sujetarán a los límites de su naturaleza y la ley.

Seguridad: Medidas técnicas, humanas y administrativas para proteger los registros.

Confidencialidad: Todas las personas que intervengan en el tratamiento garantizarán reserva.

Minimización de datos: Solo se recolectarán los datos estrictamente necesarios para las finalidades declaradas.

Responsabilidad demostrada (accountability): Fintrixs implementará mecanismos para demostrar el cumplimiento de sus obligaciones en materia de protección de datos.

7. TIPOLOGÍA DE DATOS TRATADOS

De acuerdo con la naturaleza de sus actividades, incluyendo la operación como pasarela de pagos, Fintrixs podrá recolectar y tratar las siguientes categorías de datos personales:

7.1. Datos de identificación personal

Nombres y apellidos, documento de identidad, fecha y lugar de nacimiento, nacionalidad, estado civil, fotografía, firma, datos biométricos (para KYC).

7.2. Datos de contacto

Dirección, correo electrónico, teléfono fijo y/o celular, perfiles de redes sociales proporcionados voluntariamente.

7.3. Datos financieros y de pago

Número de tarjeta (PAN) — tratado exclusivamente en tránsito conforme a PCI DSS, tipo de tarjeta (crédito/débito), fecha de vencimiento, nombre del tarjetahabiente grabado en la tarjeta, datos de cuenta bancaria (número, tipo, entidad), historial transaccional dentro del ecosistema, saldos en wallets y tokens, información tributaria y de facturación.

7.4. Datos del comercio afiliado

Razón social, NIT, representante legal, dirección comercial, categoría comercial (MCC), datos bancarios para dispersión, historial de ventas y transacciones, documentos de constitución y habilitación, información de cumplimiento KYC/KYB del comercio.

7.5. Datos tecnológicos y de navegación

Dirección IP, tipo de dispositivo y sistema operativo, geolocalización (autorizada), logs de actividad, cookies, huella digital del dispositivo (device fingerprint), datos de comportamiento digital.

7.6. Datos para autenticación y seguridad

Credenciales de acceso cifradas, fragmentos de llaves MPC, resultados de verificación 3D Secure, datos de autenticación biométrica.

7.7. Datos laborales

Información de empleo, cargo, experiencia profesional, información académica, referencias.

7.8. Datos sensibles

Fintrixs podrá tratar datos sensibles únicamente cuando sea estrictamente necesario, previa **autorización expresa y reforzada** del titular. El tratamiento de datos sensibles se realizará con medidas reforzadas de seguridad técnica y organizacional. Ninguna actividad de la Compañía estará condicionada a que el titular suministre datos sensibles.

> ***Importante — Datos de tarjeta (CHD):*** *Conforme al estándar PCI DSS, los datos de autenticación sensibles (CVV/CVC, datos de banda magnética, PIN/PIN block)* ***nunca son almacenados*** *por Fintrixs tras la autorización de la transacción. El PAN se trata exclusivamente de forma cifrada en tránsito y se tokeniza inmediatamente para cualquier referencia posterior.*

8. FINALIDADES DEL TRATAMIENTO

8.1. Finalidades de la operación de pasarela de pagos

- Captura, cifrado, transmisión y enrutamiento de instrucciones de pago entre compradores, comercios y redes de procesamiento.
- Autorización, procesamiento, compensación y liquidación de transacciones con tarjeta (Visa) y en blockchain.
- Conciliación de transacciones y dispersión de fondos a comercios afiliados.
- Emisión, gestión y administración de tarjetas Visa físicas y virtuales a través del banco sponsor.
- Procesamiento de pagos con código QR mediante tokens FINX y USDC.
- Operación de terminales POS Fintrixs con doble vía (Visa + Hedera).
- Gestión de contracargos, disputas y reversiones de transacciones.
- Detección, prevención e investigación de fraude en transacciones.
- Cumplimiento de reglas operativas de Visa, Credibanco y el banco sponsor.
- Generación de comprobantes de pago y facturación electrónica.

8.2. Finalidades generales

- Ejecución de relaciones contractuales y precontractuales.
- Prestación, administración y mejora de los servicios tecnológicos.
- Gestión de cuentas de usuario, comercios y empresas.
- Operación y administración del token FINX y las wallets MPC.
- Gestión de los protocolos FCRP y FCRPe de distribución de recompensas.
- Operación del ERP contable CUENTYX con conciliación automática.
- Desarrollo y operación de Mini Apps empresariales.

8.3. Finalidades de cumplimiento regulatorio

- Validación y verificación de identidad (KYC) de usuarios y comercios.
- Conocimiento del cliente empresarial (KYB — Know Your Business) para comercios afiliados.
- Prevención de lavado de activos, financiación del terrorismo y proliferación de armas (AML/CFT).
- Monitoreo transaccional y reporte de operaciones sospechosas.
- Cumplimiento de requerimientos de autoridades administrativas, judiciales y de control.
- Integración con la DIAN para facturación electrónica.
- Cumplimiento del estándar PCI DSS para protección de datos de tarjetas.

8.4. Finalidades analíticas y comerciales

- Analítica de datos para mejora continua de servicios y experiencia del usuario.
- Evaluación de comportamiento, perfilamiento y modelos de riesgo.
- Personalización de servicios y productos del ecosistema.
- Envío de comunicaciones informativas, operacionales y comerciales (previa autorización).

El titular podrá revocar en cualquier momento su autorización para finalidades comerciales y de mercadeo sin afectar el tratamiento necesario para la prestación de servicios o el cumplimiento regulatorio.

9. AUTORIZACIÓN DEL TITULAR

9.1. Obtención de la autorización

El tratamiento de datos personales se realizará previa autorización libre, expresa e informada del titular, obtenida por cualquier medio verificable: electrónico, escrito, verbal o conducta inequívoca.

9.2. Autorización en el contexto de pagos

En el contexto de la pasarela de pagos, la autorización para el tratamiento de datos transaccionales se entiende otorgada cuando:

- El tarjetahabiente ingresa voluntariamente los datos de su tarjeta en el formulario de pago de la plataforma o en el terminal POS.
- El usuario presenta su tarjeta física (chip, banda, NFC) en un terminal POS Fintrixs para realizar una transacción.
- El tarjetahabiente completa el proceso de autenticación 3D Secure autorizado por su banco emisor.
- El usuario realiza un pago mediante su Wallet Fintrixs escaneando un código QR.

• El comercio afiliado acepta los términos y condiciones del servicio de pasarela que incluyen la cláusula de tratamiento de datos.

9.3. Excepciones a la autorización

No se requerirá autorización conforme al artículo 10 de la Ley 1581 de 2012 cuando se trate de datos requeridos por entidades públicas, datos públicos, urgencias médicas, tratamiento autorizado por ley para fines históricos o estadísticos, datos del Registro Civil, o cumplimiento de obligaciones legales en materia de prevención de fraude y lavado de activos.

10. DERECHOS DE LOS TITULARES

Conforme al artículo 8 de la Ley 1581 de 2012, los titulares tienen los siguientes derechos:

• **Acceso o consulta:** Conocer y obtener gratuitamente sus datos personales tratados por Fintrixs.

• **Actualización:** Solicitar la actualización de datos desactualizados.

• **Rectificación:** Solicitar corrección de datos inexactos, incompletos o que induzcan a error.

• **Supresión:** Solicitar la eliminación de datos cuando no se respeten los principios legales o hayan dejado de ser necesarios.

• **Revocatoria:** Revocar la autorización para el tratamiento de datos.

• **Oposición:** Oponerse al tratamiento cuando existan motivos fundados.

• **Portabilidad:** Solicitar la entrega de datos en formato estructurado y de uso común.

• **Presentar quejas:** Acudir ante la Superintendencia de Industria y Comercio (SIC).

• **Ser informado:** Conocer el uso que se ha dado a sus datos personales.

> ***Limitación en el contexto de pagos:*** *El ejercicio de ciertos derechos (como supresión o revocatoria) podrá ser limitado cuando los datos sean necesarios para el cumplimiento de obligaciones legales, tributarias, de prevención de fraude o para la gestión de disputas y contracargos conforme a las reglas de las redes de pago. Fintrixs informará al titular sobre estas limitaciones.*

11. PROCEDIMIENTO PARA EJERCER DERECHOS

Las solicitudes deberán enviarse a **info@fintrixs.com** con el asunto "Datos Personales", incluyendo: nombre completo, documento de identidad, datos de contacto, descripción de la solicitud, documentos de soporte y poder si se actúa por apoderado.

Tipo de solicitud	Plazo de respuesta	Prórroga máxima

Consultas	10 días hábiles	5 días hábiles adicionales
Reclamos	15 días hábiles	8 días hábiles adicionales

12. DEBERES DE FINTRIXS COMO RESPONSABLE

En su calidad de responsable del tratamiento, Fintrixs se compromete a garantizar el ejercicio del habeas data, solicitar y conservar la autorización, informar sobre finalidades y derechos, conservar la información con medidas de seguridad adecuadas, mantener datos veraces y actualizados, tramitar consultas y reclamos en los plazos legales, y cumplir las instrucciones de la SIC.

13. DATOS PERSONALES EN LA OPERACIÓN DE PASARELA DE PAGOS

13.1. Categorías de datos tratados en el flujo de pago

En su operación como pasarela de pagos, Fintrixs trata las siguientes categorías de datos durante el ciclo de vida de una transacción:

Categoría de datos	Ejemplos	Momento del tratamiento
Datos del tarjetahabiente (Cardholder Data — CHD)	PAN (cifrado), nombre en la tarjeta, fecha de vencimiento	Captura → transmisión → tokenización (no almacenamiento del PAN)
Datos de autenticación sensibles (SAD)	CVV/CVC, PIN, datos de banda magnética/chip	Solo en tránsito, NUNCA almacenados
Datos de la transacción	Monto, moneda, fecha/hora, código de autorización, ID de transacción	Captura → procesamiento → almacenamiento (para conciliación)
Datos del comprador	Nombre, email, teléfono, dirección de envío (cuando aplique)	Captura → almacenamiento (según finalidad y retención)
Datos del comercio	Razón social, NIT, MCC, terminal ID, dirección	Registro → almacenamiento → conciliación

Datos de autenticación 3D Secure	Resultado de autenticación, ECI, XID/DS TransID	Flujo de autenticación → registro
Datos de dispositivo (antifraude)	Device fingerprint, IP, geolocalización, user agent	Captura en tiempo real → análisis antifraude

13.2. Base legal para el tratamiento de datos de pago

El tratamiento de datos personales en el contexto de la pasarela de pagos se fundamenta en:

- **Ejecución contractual:** Los datos son necesarios para procesar la transacción solicitada por el tarjetahabiente y el comercio.
- **Obligación legal:** El cumplimiento de normativa tributaria (facturación electrónica), prevención de lavado de activos (AML/CFT), y reglas de las redes de pago.
- **Interés legítimo:** La prevención de fraude y la seguridad de las transacciones constituyen un interés legítimo de Fintrixs, los comercios y los tarjetahabientes.
- **Consentimiento:** Para finalidades adicionales como comunicaciones comerciales o analítica no esencial.

14. DATOS DE TARJETAHABIENTES Y CUMPLIMIENTO PCI DSS

14.1. Compromiso con PCI DSS

Fintrixs se compromete a cumplir con el estándar **PCI DSS (Payment Card Industry Data Security Standard)** en su versión vigente para la protección de los datos de tarjetahabientes que transitan por sus sistemas. Este compromiso abarca todos los componentes, redes, servidores, aplicaciones y procesos involucrados en el almacenamiento, procesamiento o transmisión de datos de tarjetas de pago.

14.2. Entorno de datos de tarjetahabientes (CDE)

Fintrixs define, documenta y mantiene un entorno de datos de tarjetahabientes (Cardholder Data Environment — CDE) que incluye:

- Los sistemas y componentes que almacenan, procesan o transmiten datos de tarjetas.
- Los sistemas conectados al CDE o que podrían afectar su seguridad.
- Los procesos de negocio y flujos de datos que involucran datos de tarjetahabientes.

14.3. Controles PCI DSS implementados

Los controles implementados incluyen, sin limitarse a:

a) Protección de datos almacenados

- El PAN se almacena únicamente de forma tokenizada o cifrada con algoritmos robustos (AES-256).
- Los datos de autenticación sensibles (CVV/CVC, PIN, datos de banda/chip) **nunca se almacenan** tras la autorización.
- Se implementa truncamiento del PAN para visualización (primeros 6 y últimos 4 dígitos máximo).
- Las llaves criptográficas se protegen en módulos HSM y se rotan periódicamente.

b) Cifrado de datos en tránsito

- Todas las transmisiones de datos de tarjeta se realizan mediante TLS 1.2 o superior.
- Las conexiones con procesadores y redes de pago utilizan canales cifrados punto a punto.
- Se implementa cifrado en el punto de interacción (POI) en terminales POS.

c) Control de acceso y autenticación

- Acceso al CDE restringido bajo el principio de mínimo privilegio (need-to-know).
- Autenticación multifactor (MFA) obligatoria para acceso administrativo al CDE.
- Identificación única por usuario; prohibición de cuentas compartidas.
- Registro y monitoreo de todos los accesos a datos de tarjetahabientes.

d) Monitoreo y pruebas

- Registro de logs de auditoría para todos los accesos a componentes del CDE.
- Pruebas regulares de seguridad: escaneos de vulnerabilidades y pruebas de penetración.
- Monitoreo continuo de la integridad de archivos y configuraciones.
- Sistema de detección de intrusiones (IDS/IPS) en el perímetro del CDE.

14.4. Validación de cumplimiento

Fintrixs mantendrá su nivel de cumplimiento PCI DSS conforme al nivel que le corresponda según el volumen de transacciones procesadas. La validación podrá incluir la realización de Cuestionarios de Autoevaluación (SAQ), escaneos de seguridad por proveedores certificados (ASV — Approved Scanning Vendors), y/o auditorías realizadas por Evaluadores de Seguridad Cualificados (QSA — Qualified Security Assessors) según corresponda.

15. PROCESAMIENTO DE TRANSACCIONES Y FLUJO DE DATOS

15.1. Flujo de datos en pagos con tarjeta (Visa)

El procesamiento de una transacción con tarjeta a través de Fintrixs sigue el siguiente flujo de datos:

1. Captura: El tarjetahabiente ingresa sus datos en el checkout digital o presenta su tarjeta en el POS Fintrixs. Los datos se capturan y cifran inmediatamente en el punto de interacción.

2. Tokenización: Fintrixs reemplaza el PAN por un token de pago antes de transmitir los datos internamente.

3. Transmisión al procesador: Los datos cifrados se transmiten al adquirente (Credibanco) a través de canales seguros para solicitar la autorización.

4. Autorización: Credibanco enruta la solicitud a la red Visa, que a su vez la envía al banco emisor. El banco emisor autoriza o declina la transacción.

5. Respuesta: El resultado de la autorización se transmite de vuelta por el mismo canal seguro hasta el comercio y el tarjetahabiente.

6. Compensación y liquidación: Tras la autorización, se ejecutan los procesos de compensación entre adquirente y emisor, y la liquidación de fondos al comercio.

7. Eliminación de SAD: Inmediatamente después de la autorización, todos los datos de autenticación sensibles (CVV, PIN, datos de chip/banda) son eliminados de forma irreversible de los sistemas de Fintrixs.

15.2. Flujo de datos en pagos blockchain

En pagos realizados con tokens FINX o USDC a través de la red Hedera Hashgraph:

• El comprador inicia el pago desde su Wallet Fintrixs escaneando un código QR generado por el comercio o el POS.

• La transacción se firma criptográficamente mediante el esquema MPC de la wallet, sin que ninguna parte individual tenga acceso a la llave privada completa.

• La transacción se envía a la red Hedera a través del relayer gasless de Fintrixs, sin exponer datos personales del usuario en la blockchain.

• La red Hedera registra la transacción con identificadores pseudonimizados (direcciones de wallet), sin datos personales identificables.

• Fintrixs registra la correlación entre la transacción on-chain y los datos del usuario/comercio exclusivamente en bases de datos off-chain protegidas.

• Se genera automáticamente el asiento contable correspondiente en el ERP CUENTYX.

15.3. Autenticación 3D Secure

Para transacciones de comercio electrónico, Fintrixs implementa el protocolo **3D Secure (3DS)** que permite la autenticación del tarjetahabiente por parte de su banco emisor, añadiendo una capa adicional de seguridad. Los datos de autenticación 3DS se transmiten de forma cifrada y se almacenan únicamente con fines de resolución de disputas y contracargos, por el tiempo exigido por las reglas de la red.

16. TOKENIZACIÓN DE DATOS DE PAGO

16.1. Tokenización del PAN (tarjetas)

Fintrixs implementa **tokenización** como mecanismo principal para proteger los datos de tarjetas de pago. La tokenización reemplaza el número de tarjeta (PAN) por un valor alfanumérico único (token de pago) que no tiene valor fuera del contexto específico autorizado y no puede ser revertido para obtener el PAN original sin acceso al sistema de tokenización seguro.

Características de la tokenización implementada:

- Los tokens se generan de forma irreversible y son únicos por contexto (comercio, canal, dispositivo).
- El PAN original se almacena exclusivamente en un vault de tokenización cifrado con llaves protegidas en HSM.
- Los tokens se utilizan para todas las operaciones posteriores: conciliación, reportes, contracargos y referencias de transacciones.
- Los comercios afiliados reciben únicamente tokens, nunca el PAN completo.
- La detokenización (recuperación del PAN original) está restringida a procesos específicos que lo requieran y sujeta a controles de acceso estrictos.

16.2. Tokenización FIAT (Token FINX)

Además de la tokenización de datos de tarjeta, Fintrixs opera un sistema de **tokenización de moneda FIAT** mediante el token FINX, emitido sobre la red Hedera Hashgraph con respaldo 1:1 en cuentas del banco sponsor. En relación con la protección de datos:

- Las transacciones con FINX se registran en blockchain con direcciones pseudonimizadas, sin datos personales identificables.
- La vinculación entre una dirección de wallet y la identidad del titular se almacena exclusivamente en bases de datos off-chain protegidas.
- Los procesos de conversión FINX-FIAT requieren verificación de identidad (KYC) y se registran conforme a la normativa de prevención de lavado de activos.

17. PREVENCIÓN DE FRAUDE Y MONITOREO TRANSACCIONAL

17.1. Sistema antifraude

Fintrixs implementa un sistema integral de prevención y detección de fraude que incluye:

- Monitoreo en tiempo real de todas las transacciones procesadas.

- Motor de reglas y modelos de machine learning para detección de patrones anómalos.
- Análisis de velocidad transaccional (velocity checks): frecuencia, montos, geolocalización.
- Verificación de device fingerprint y análisis de comportamiento del dispositivo.
- Listas de control (negativas, de observación y positivas) para tarjetas, dispositivos, IPs y comercios.
- Integración con servicios externos de verificación de identidad y prevención de fraude.
- Implementación de 3D Secure para autenticación reforzada del tarjetahabiente.

17.2. Datos tratados para prevención de fraude

Para la prevención de fraude, Fintrixs podrá tratar datos adicionales incluyendo:

- Huella digital del dispositivo (device fingerprint), dirección IP y datos de geolocalización.
- Patrones de comportamiento transaccional del tarjetahabiente y del comercio.
- Historial de contracargos y disputas asociados al comercio o al instrumento de pago.
- Resultados de verificación de identidad y autenticación.
- Información compartida por redes de pago y consorcios antifraude.

17.3. Monitoreo AML/CFT

En cumplimiento de las normativas de prevención de lavado de activos y financiación del terrorismo, Fintrixs realizará monitoreo transaccional que incluye la identificación de operaciones inusuales o sospechosas, la verificación contra listas restrictivas nacionales e internacionales (OFAC, ONU, listas colombianas), y el reporte a las autoridades competentes (UIAF — Unidad de Información y Análisis Financiero) cuando corresponda. Este tratamiento se realiza en cumplimiento de obligaciones legales y no requiere autorización del titular.

18. RESPONSABILIDADES COMPARTIDAS: COMERCIO, ADQUIRENTE Y PASARELA

18.1. Modelo de responsabilidad compartida

En el ecosistema de pagos, las responsabilidades sobre la protección de datos personales se distribuyen entre los diferentes actores:

Actor	Responsabilidad principal sobre datos

Fintrixs (Pasarela/Agregador)	Protección de datos en tránsito durante el procesamiento. Tokenización. Cumplimiento PCI DSS. Prevención de fraude. Almacenamiento seguro de datos tokenizados y transaccionales.
Comercio afiliado	Protección de datos en su entorno antes de enviarlos a la pasarela. Cumplimiento de su propio nivel PCI DSS. Obtención del consentimiento de sus clientes.
Banco sponsor / Adquirente	Procesamiento de la transacción ante la red. Custodia de fondos. Emisión de tarjetas. Cumplimiento regulatorio ante la Superintendencia Financiera.
Red de pago (Visa/Credibanco)	Enrutamiento y autorización. Reglas operativas. Estándares de seguridad. Gestión del esquema de disputas.
Banco emisor	Autenticación del tarjetahabiente (3DS). Autorización/declinación de la transacción. Relación directa con el tarjetahabiente.

18.2. Obligaciones del comercio afiliado

Los comercios afiliados al ecosistema Fintrixs están obligados contractualmente a:

- Cumplir con la normativa de protección de datos personales en su interacción con los compradores.
- No almacenar datos de tarjeta (PAN completo, CVV, PIN) en sus sistemas, salvo que cuenten con certificación PCI DSS propia.
- Obtener el consentimiento de sus clientes para el tratamiento de datos cuando sea requerido.
- Implementar medidas de seguridad adecuadas en sus sistemas e infraestructura.
- Notificar a Fintrixs inmediatamente ante cualquier sospecha de compromiso de datos.
- Cooperar en la gestión de disputas, contracargos e investigaciones de fraude.

19. DATOS DEL COMERCIO AFILIADO (MERCHANT DATA)

Fintrixs recolecta y trata datos de los comercios afiliados a su ecosistema para las siguientes finalidades:

- Proceso de onboarding y verificación del comercio (KYB — Know Your Business): validación de documentos de constitución, representación legal, información tributaria y financiera.

• Evaluación de riesgo del comercio: análisis de la categoría comercial (MCC), historial de contracargos, volumen transaccional esperado y reputación.

• Gestión operativa: configuración de terminales POS, pasarela web, Mini Apps y parámetros de liquidación.

• Conciliación y liquidación: procesamiento de la dispersión de fondos al comercio conforme a los ciclos acordados.

• Cumplimiento regulatorio: monitoreo transaccional AML/CFT, reportes a autoridades, facturación electrónica.

• Operación del protocolo FCRPe: gestión del cashback compartido y las recompensas del ecosistema.

20. PAGOS INTERNACIONALES Y FLUJO TRANSFRONTERIZO DE DATOS

Cuando Fintrixs procese pagos internacionales o transacciones que involucren actores en diferentes jurisdicciones, los datos personales podrán fluir a través de fronteras conforme a las siguientes directrices:

• Las transacciones con tarjetas internacionales implican la transmisión de datos entre el banco emisor (posiblemente en otro país), la red Visa (infraestructura global) y Fintrixs/Credibanco en Colombia.

• Las transacciones blockchain son inherentemente transfronterizas, pero los datos personales identificables permanecen en las bases de datos off-chain de Fintrixs.

• Fintrixs garantizará que las transferencias internacionales de datos cumplan con las regulaciones colombianas y que los países destinatarios cuenten con niveles adecuados de protección o, en su defecto, se implementen salvaguardas contractuales.

• En su plan de expansión a México, Chile y Argentina, Fintrixs cumplirá adicionalmente con las normativas locales de protección de datos de cada jurisdicción.

21. RETENCIÓN Y ELIMINACIÓN DE DATOS TRANSACCIONALES

Tipo de dato	Período de retención	Fundamento
Datos de autenticación sensibles (CVV, PIN, chip)	CERO — eliminación inmediata tras autorización	PCI DSS Requisito 3.3

PAN tokenizado + datos de transacción	Hasta 18 meses operativos	Gestión de disputas y contracargos (reglas Visa)
Registros de transacciones con fines contables	Mínimo 5 años	Normativa tributaria colombiana (DIAN)
Registros de transacciones con fines AML/CFT	Mínimo 5 años desde el fin de la relación comercial	Normativa SARLAFT y recomendaciones GAFI
Datos de KYC/KYB del comercio	Duración de la relación + 5 años	Normativa AML/CFT y obligaciones contractuales
Logs de acceso al CDE	Mínimo 12 meses (3 meses disponibles inmediatamente)	PCI DSS Requisito 10.7
Datos de prevención de fraude	Hasta 7 años	Investigaciones y análisis de patrones

Una vez cumplidos los plazos de retención, los datos serán eliminados de forma segura conforme a procedimientos de borrado certificado, o anonimizados de manera irreversible para fines estadísticos.

22. SEGURIDAD DE LA INFORMACIÓN

22.1. Medidas técnicas

- Cifrado en tránsito (TLS 1.2+) y en reposo (AES-256).
- Infraestructura MPC para wallets — llave dividida en 3 fragmentos.
- Autenticación multifactor (MFA) para acceso a sistemas y plataformas.
- Módulos HSM para protección de llaves criptográficas.
- Firewalls, IDS/IPS y WAF (Web Application Firewall).
- Cifrado punto a punto (P2PE) en terminales POS.
- Segmentación de redes y aislamiento del CDE.
- Pruebas de penetración y escaneos de vulnerabilidades periódicos.
- Monitoreo continuo 24/7 de sistemas e infraestructura.

22.2. Medidas organizacionales

- Políticas internas de seguridad y protección de datos.

- Capacitación continua en seguridad y cumplimiento PCI DSS.
- Acuerdos de confidencialidad con todo el personal.
- Control de acceso basado en roles (RBAC) y principio de mínimo privilegio.
- Auditorías internas y externas periódicas.
- Plan de continuidad del negocio y recuperación ante desastres.
- Gestión formal de cambios en sistemas del CDE.

23. USO DE TECNOLOGÍA BLOCKCHAIN Y PROTECCIÓN DE DATOS

En relación con el uso de blockchain (Hedera Hashgraph), Fintrixs implementa:

- No se registran datos personales identificables directamente en redes blockchain. Las transacciones usan identificadores pseudonimizados (direcciones de wallet).
- Los datos personales y sensibles se almacenan exclusivamente off-chain con controles de acceso apropiados.
- Se emplean técnicas de hashing para referencias de datos almacenados on-chain.
- La wallet MPC garantiza que Fintrixs nunca tiene custodia total de las llaves privadas.
- El relayer gasless no expone datos personales del usuario final a la red.

24. ANALÍTICA, INTELIGENCIA ARTIFICIAL Y AUTOMATIZACIÓN

Fintrixs utiliza herramientas de IA, analítica avanzada y automatización para optimizar operaciones, mejorar la experiencia del usuario, fortalecer la seguridad y detectar fraude. Los titulares podrán solicitar información sobre decisiones automatizadas que les afecten y, cuando aplique, solicitar intervención humana.

25. COOKIES Y TECNOLOGÍAS DE RASTREO

Los sitios web y plataformas de Fintrixs utilizan cookies esenciales (funcionamiento y seguridad), de rendimiento (analítica de uso), funcionales (preferencias del usuario) y analíticas (estadísticas de navegación). El usuario podrá gestionar sus preferencias de cookies a través de la configuración del navegador o los mecanismos habilitados en las plataformas.

26. TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS

Los datos podrán ser transferidos o transmitidos dentro o fuera de Colombia a proveedores cloud, redes blockchain, redes de pago internacionales (Visa), proveedores de KYC/AML, y entidades financieras aliadas. Fintrixs garantizará niveles adecuados de protección e implementará salvaguardas contractuales cuando sea necesario.

27. COMPARTICIÓN DE INFORMACIÓN Y ENCARGADOS DEL TRATAMIENTO

La información podrá compartirse con proveedores tecnológicos, entidades financieras, procesadores de pago, redes de pago (Visa/Credibanco), autoridades competentes, auditores y asesores. Los encargados del tratamiento operarán bajo instrucciones de Fintrixs y conforme a acuerdos contractuales que garanticen confidencialidad, seguridad y limitación de uso.

28. TRATAMIENTO DE DATOS DE MENORES DE EDAD

Los servicios de Fintrixs están dirigidos exclusivamente a personas mayores de edad. No se recolectan intencionalmente datos de menores. Si se detecta la recolección de datos de un menor sin autorización del representante legal, se procederá a su eliminación inmediata.

29. GESTIÓN DE INCIDENTES DE SEGURIDAD

Ante incidentes de seguridad que comprometan datos personales o de pago, Fintrixs activará protocolos de detección y contención inmediata, evaluación de impacto, notificación a autoridades (SIC, banco sponsor, Visa/Credibanco según aplique), comunicación a titulares afectados cuando corresponda, remediación y documentación del incidente y lecciones aprendidas.

> *En el contexto de pagos, los incidentes que involucren datos de tarjetahabientes serán reportados adicionalmente a las redes de pago (Visa) y al banco sponsor/adquirente conforme a sus reglas operativas y plazos establecidos.*

30. CONSERVACIÓN Y SUPRESIÓN DE DATOS

Los datos personales se conservarán durante el tiempo necesario para cumplir las finalidades del tratamiento y las obligaciones legales aplicables. Los períodos específicos de retención de datos transaccionales se detallan en la Sección 21 de esta política. Una vez cumplidos los plazos, los datos serán eliminados de forma segura o anonimizados irreversiblemente.

31. LIMITACIÓN DE RESPONSABILIDAD

Fintrixs no será responsable por daños derivados de interrupciones del servicio, accesos no autorizados causados por negligencia del titular, fallos de servicios de terceros, información incorrecta proporcionada por el titular, decisiones del banco emisor sobre autorización/declinación de transacciones, contracargos derivados de disputas entre tarjetahabiente y comercio, o eventos de fuerza mayor. Lo anterior, sin perjuicio de la responsabilidad legal como responsable del tratamiento.

32. OFICIAL DE PROTECCIÓN DE DATOS

Fintrixs designará un Oficial de Protección de Datos responsable de supervisar el cumplimiento de esta política y la normativa vigente, atender solicitudes de titulares, coordinar la implementación de medidas de protección, servir de enlace con la SIC, realizar evaluaciones de impacto, y promover la cultura de protección de datos en la organización.

33. VIGENCIA Y ACTUALIZACIONES

La presente política entra en vigencia el **1 de octubre de 2025** y fue actualizada por última vez el **16 de abril de 2026**. Fintrixs podrá modificarla en cualquier momento, informando a través de sus canales oficiales. La versión vigente estará siempre disponible en **https://fintrixs.com**.

34. ACEPTACIÓN DE LA POLÍTICA

El uso de los servicios, plataformas, aplicaciones y productos de Fintrixs — incluyendo la realización de transacciones de pago a través de la pasarela — implica el conocimiento y aceptación de la presente Política. Al proporcionar datos personales, realizar transacciones o utilizar los servicios del ecosistema, el titular manifiesta su consentimiento libre, previo, expreso e informado para el tratamiento conforme a lo establecido en este documento.

35. INFORMACIÓN DE CONTACTO

Canal	Detalle
Correo electrónico	info@fintrixs.com
Teléfono	+57 302 318 4519

Dirección física	Cra 78 No. 17-55, Oficina 704, Bogotá D.C.
Sitio web	https://fintrixs.com
Horario de atención	Lunes a viernes, 8:00 a.m. - 6:00 p.m.

FINTRIXS S.A.S.
NIT 901994194-3

"El control es tuyo — La transparencia nuestra"