



PROCESO: ÉTICA Y CUMPLIMIENTO

POLÍTICA ANTIFRAUDE

Vigente desde: 04 Nov de 2024

Versión: 01

1. Declaración de compromiso

Fintra mantiene una posición de tolerancia cero frente al fraude, interno o externo. La confianza de nuestros clientes, aliados, empresas convenio y entidades públicas es nuestro principal activo, y protegerla es responsabilidad de todos.

La Junta Directiva y la Alta Dirección se comprometen a promover una cultura ética y a mantener controles efectivos para prevenir, detectar y responder al fraude en todas las líneas de negocio.

2. Objetivo

Establecer el marco de actuación para la prevención, detección, investigación, respuesta y recuperación frente a eventos de fraude que afecten a Fintra, a sus clientes o a sus grupos de interés.

3. Alcance

Aplica a accionistas, Junta Directiva, Alta Dirección, colaboradores, practicantes, contratistas, proveedores, aliados, corresponsales, empresas convenio y demás terceros relacionados con Fintra, en todos los procesos, canales (digitales y presenciales) y regionales.

4. Marco normativo de referencia

Norma / estándar	Contenido relevante
Código Penal (Ley 599 de 2000)	Estafa, abuso de confianza, falsedad documental, hurto por medios informáticos, administración desleal, entre otros.
Ley 1273 de 2009	Delitos informáticos y protección de la información y los datos.
Ley 1474 de 2011 y Ley 2195 de 2022	Prevención de la corrupción y medidas de transparencia empresarial.
Ley 1581 de 2012	Protección de datos personales.
Ley 1527 de 2012 y Ley 1902 de 2018	Marco de la libranza y régimen de operadores de libranza.
Capítulo X Circular Básica Jurídica — Superintendencia de Sociedades (SAGRILAFI)	Autocontrol y gestión del riesgo de LA/FT/FPADM, en lo aplicable.
Estándares de referencia	Marco COSO de control interno; ACFE — Guía de gestión del riesgo de fraude; ISO 31000.

La Dirección Jurídica verificará periódicamente la vigencia de estas normas y su aplicabilidad según la naturaleza jurídica y el régimen de supervisión de Fintra.

5. Definiciones

- **Evento de fraude:** hecho materializado o intento de fraude detectado.
- **Fraude:** acto u omisión intencional, realizado mediante engaño, ocultamiento o abuso de confianza, para obtener un beneficio indebido para sí o para un tercero, o causar un perjuicio a Fintra o a terceros.
- **Fraude externo:** cometido por clientes, solicitantes, proveedores u otros terceros.
- **Fraude interno:** cometido por colaboradores, directivos o administradores, solos o en complicidad con terceros.
- **Señal de alerta:** hecho, comportamiento o situación atípica que puede indicar un posible fraude.
- **Suplantación de identidad:** uso de la identidad de otra persona para acceder a productos o servicios.

6. Principios

- **Tolerancia cero:** todo indicio de fraude será investigado, sin importar el cargo o monto.
- **Prevención primero:** los controles se diseñan desde la creación de productos y procesos.
- **Responsabilidad compartida:** cada colaborador es la primera línea de defensa.
- **Confidencialidad y debido proceso** en las investigaciones.
- **No represalias** contra quien reporte de buena fe como se encuentra estipulado en la Política de Protección al denunciante.

7. Tipologías de fraude relevantes para Fintra

7.1 Microcrédito

- Suplantación de identidad y uso de documentos falsos o adulterados en solicitudes digitales.
- Negocios ficticios, inflados o prestados para simular capacidad de pago.
- Visitas de campo no realizadas o con información alterada.
- Colusión entre asesor y solicitante; créditos "testaferro".

7.2 Libranza Privada (Nómina)

- Empresas convenio ficticias o de fachada; empleados inexistentes o certificados laborales falsos.

- Alteración de desprendibles de nómina o certificaciones de ingresos.
- Retención o desvío por parte del empleador de los descuentos efectuados y no girados a Fintra.

7.3 Libranza Pública

- Suplantación de pensionados, docentes o servidores públicos; documentos de pagaduría falsificados.
- Captación de clientes por intermediarios no autorizados con cobros indebidos.
- Manipulación de cupos o de la aplicación de descuentos.

7.4 Fraude interno y transversal

- Desvío o apropiación de recursos de desembolsos o recaudos.
- Manipulación de datos en sistemas o en el DW (modificación de estados de mora, reestructuraciones no autorizadas, condonaciones indebidas).
- Fraude en compras: sobrecostos, proveedores ficticios, facturación duplicada.
- Manipulación de reportes financieros o de indicadores de gestión.
- Fraude cibernético: phishing, vishing, toma de cuentas, accesos no autorizados y fuga de información de clientes.
- Uso indebido de información confidencial o de datos personales.

8. Marco de gestión del riesgo de fraude

8.1 Prevención

- Código de Ética y Conducta y declaración de conflictos de interés.
- Selección y verificación de antecedentes del personal, con énfasis en cargos críticos.
- Validación de identidad robusta: validación documental y consultas en centrales de riesgo y listas restrictivas.
- Verificación de existencia, solidez y vigencia del convenio con el empleador o la entidad pública.
- Segregación de funciones entre originación, análisis, aprobación, desembolso y recaudo.
- Gestión de accesos por perfil y mínimo privilegio; registro y revisión de logs.
- Debida diligencia a todas las contrapartes con la que se desea tener alguna relación contractual.

8.2 Respuesta

- Investigación liderada por el Oficial de Cumplimiento y/o Auditoría Interna con apoyo de Jurídica y Tecnología.
- Preservación de evidencia física y digital con cadena de custodia.
- Denuncia ante autoridades competentes y acciones de recuperación de activos cuando proceda.
- Lecciones aprendidas y ajuste de controles.

9. Señales de alerta

Ámbito	Ejemplos de señales de alerta
Solicitudes	Documentos con inconsistencias, datos de contacto compartidos entre varios solicitantes, prisa inusual por el desembolso.
Colaboradores	Estilo de vida no acorde con ingresos, resistencia a tomar vacaciones o a rotar funciones, concentración atípica de créditos en mora temprana.
Proveedores	Facturas sin soporte, cuentas bancarias a nombre de terceros, vínculos con colaboradores.
Tecnología	Accesos fuera de horario, cambios masivos de datos, intentos de acceso fallidos reiterados.

10. Roles y responsabilidades

Rol	Responsabilidades
Junta Directiva	Aprobar la política
Presidencia y Alta Dirección	Promover la cultura antifraude; asegurar recursos y controles.
Oficial de Cumplimiento / Gestión de Riesgos	Evaluar el riesgo de fraude; administrar la matriz de riesgos; coordinar investigaciones y reportes.
Comité de Ética	Analizar casos y recomendar medidas disciplinarias.
Auditoría Interna	Evaluar la eficacia de los controles; realizar auditorías e investigaciones.
Tecnología y Seguridad de la Información	Proteger sistemas y datos; monitorear eventos de ciberseguridad.
Gerentes de línea y regionales	Aplicar y supervisar controles operativos; escalar alertas.
Todos los colaboradores	Cumplir la política, estar atentos a señales de alerta y reportar oportunamente.

11. Canales de reporte

Cualquier sospecha o hecho de fraude debe reportarse de inmediato, de forma confidencial y, si se desea, anónima, por medio de:

- **Línea ética:** eticaycumplimiento@fintra.co
- **Formulario web anónimo:** fintra.co/lineaetica/
- **Contacto directo con el Oficial de Cumplimiento:** 301 315 7006

Los colaboradores no deben realizar investigaciones por su cuenta, confrontar a los presuntos responsables ni divulgar la información reportada. Fintra protege a quien reporte de buena fe contra cualquier represalia.

12. Investigación y régimen sancionatorio

- Toda denuncia será registrada, evaluada y, si procede, investigada en los plazos definidos en el procedimiento de investigación.
- Las sanciones para colaboradores se aplicarán conforme al Reglamento Interno de Trabajo, incluida la terminación del contrato con justa causa.
- Para terceros: terminación de la relación contractual, inclusión en listas internas de exclusión y acciones legales.
- Fintra ejercerá las acciones penales, civiles y de recuperación de recursos que correspondan.

Nota: toda decisión sobre sanciones, reportes a autoridades o temas regulatorios debe ser validada por un responsable humano autorizado.

13. Capacitación y cultura

- Inducción y capacitación anual obligatoria en prevención del fraude.
- Programas específicos para fuerza comercial, analistas de crédito, operaciones, tesorería y cobranza.
- Campañas de educación financiera y prevención de fraude dirigidas a clientes (suplantación, falsos intermediarios, phishing).

14. Monitoreo, actualización y vigencia

El Oficial de Cumplimiento presentará informes a la Junta Directiva anualmente. La política se revisará como mínimo cada tres años o ante cambios normativos, organizacionales, tecnológicos o del perfil de riesgo.

CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Cambios Efectuados al Documento
01	04/11/2024	- Creación del documento.

ELABORADO POR
Roxana Perea

REVISADO POR
Melissa Díaz Yacomelo

APROBADO POR
Catherine Desmoineaux

Analista SIG	Oficial de Cumplimiento	Gerente
--------------	-------------------------	---------