COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Sesión 41
Foro del Sistema de Finanzas Abiertas (FSFA)

Comisión para el Mercado Financiero

Julio 2026

COMISIÓN
PARA EL MERCADO
FINANCIERO

Agenda

1 Presentaciones miembros GC: coherencia regulatoria **en materia de protección de datos personales (continuación)**

2 Presentaciones miembros GC: coherencia regulatoria en **materia de ciberseguridad y fraude**

COMISIÓN
PARA EL MERCADO
FINANCIERO

Agenda

1 Presentaciones miembros GC: coherencia regulatoria **en materia de protección de datos personales (continuación)**

COMISIÓN
PARA EL MERCADO
FINANCIERO

Asociación de Aseguradores de Chile, Asociación Gremial - Asociación de Aseguradores de Chile A.G. (AACH)

Asociación de Aseguradores de Chile

Coherencia entre *finanzas abiertas*, protección de datos y ciberseguridad

Hacia un marco articulado entre la Ley N° 21.521 (Ley Fintec) y la NCG N° 514, la Ley N° 21.719 de protección de datos y la Ley N° 21.663 (Ley Marco de Ciberseguridad), con atención específica al sector asegurador como participante del Sistema.

Ley N° 21.521 · NCG N° 514 Ley N° 21.719 Ley N° 21.663

TESIS CENTRAL

La coherencia entre el SFA, la Ley N° 21.719 y la Ley N° 21.663 no es una aspiración de buena técnica legislativa: es una *condición de funcionamiento* del sistema.

Sin articulación expresa, los mismos datos, los mismos titulares y las mismas instituciones quedarán sujetos a estándares de consentimiento, derechos ejercibles, deberes de ciberseguridad y autoridades fiscalizadoras que no fueron diseñados para coexistir. El resultado no es solo inseguridad jurídica para la industria: es fricción para el ejercicio efectivo de derechos por parte de los titulares.

Tres regímenes sobre el mismo dato

FINANZAS ABIERTAS

Ley N° 21.521 · NCG N° 514

El cliente habilita la circulación de su información. Consentimiento **expreso, específico por finalidad y revocable** mediante panel de control, con prohibición de *dark patterns*.

PROTECCIÓN DE DATOS

Ley N° 21.719 · 1 dic 2026

Reemplaza a la Ley N° 19.628 y crea la Agencia. Derechos de **acceso, rectificación, supresión, oposición, portabilidad y bloqueo.**

CIBERSEGURIDAD

Ley N° 21.663 · vigente 2024

Crea la ANCI y obliga a **operadores de importancia vital** —categoría que puede comprender a participantes del SFA— a gestión de riesgo y notificación de incidentes.

Los tres hacen del control del titular sobre su información el eje de la confianza digital. Por eso la incoherencia no se queda en la técnica legislativa: se traslada a la experiencia del titular y a la carga de cumplimiento de la industria.

DIAGNÓSTICO

Ámbitos prioritarios de coordinación

01	Tres autoridades fiscalizadoras	CMF, Agencia de Datos y ANCI, sin ventanilla única
02	Consentimiento	El modelo RAR-GM/FAPI frente a la ley N°21.719
03	Decisiones automatizadas	Suscripción y tarificación sobre datos de riesgo
04	Ciberseguridad: triple reporte	NCG 514, Ley 21.663 y Ley 21.719 ante un mismo incidente

01 Tres autoridades normativas y fiscalizadoras

Desde diciembre de 2026 habrá competencia simultánea de tres autoridades sobre cualquier participante del SFA.

AUTORIDAD	ÁMBITO	NORMA HABILITANTE
CMF	Supervisión prudencial y de conducta; fiscalización del SFA para todos sus participantes.	Ley 21.521 · DFL 251 · NCG 514
Agencia de Protección de Datos	Cumplimiento de la Ley N° 21.719 por todos los responsables de tratamiento.	Ley 21.719
Agencia Nacional de Ciberseguridad	Ciberseguridad de operadores de importancia vital y servicios esenciales.	Ley 21.663

Ante una brecha que exponga datos de salud de asegurados, un mismo incidente podría gatillar **reporte a la CMF en 30 minutos, notificación a la ANCI y notificación a la Agencia de Datos y a los titulares** —con plazos, formatos y destinatarios divergentes, sin protocolo de ventanilla única ni autoridad líder.

02

Consentimiento

- Ley N° 21.719

LO QUE YA RESUELVE

La NCG N° 514 anticipa el estándar de la Ley N° 21.719: consentimiento expreso, específico por finalidad, revocable y sin *dark patterns*. La consulta de 2025 incorporó la "finalidad" en la estructura RAR/FAPI del sistema.

LA BRECHA CONCRETA

El consentimiento "expreso y específico" previsto en el SFA podría no satisfacer, por sí solo, los requisitos del consentimiento establecidos en la Ley N°21.719. La interpretación y aplicación práctica de dichos requisitos dependerá de los criterios, instrucciones y demás pronunciamientos que, en el futuro, emita la Agencia de Protección de Datos Personales.

03

Decisiones automatizadas

Suscripción y tarificación dependen, estructuralmente, de modelos de riesgo. El SFA los alimenta con más datos y más actores.

EL EFECTO DEL SFA

El Sistema no solo multiplica los actores que pueden alimentar modelos de evaluación de riesgo, sino que además enriquece el insumo – más datos, transversales y con historia- volviendo la decisión automatizada más potente.

LA BRECHA

El artículos 8 de la Ley N° 21.719 reconoce el derecho a no quedar sujeto a decisiones basadas únicamente en tratamiento automatizado, y a obtener explicación, intervención humana y revisión.

04 Ciberseguridad: triple reporte

Un mismo evento —una brecha que exponga datos de salud compartidos por el SFA— activa simultáneamente tres marcos de notificación, con plazos, formatos y estándares de diligencia potencialmente divergentes.

SECTORIAL · CMF

NCG N° 514, Sección III.B

30 min

Reporte de incidentes a la CMF. Exige FAPI 2.0, mTLS, TLS 1.3 y certificados con validación extendida.

GENERAL · ANCI

Ley N° 21.663

OIV

Notificación obligatoria a la ANCI para participantes que califiquen como operadores de importancia vital.

DATOS · AGENCIA PDP

Ley N° 21.719

+ titulares

Reporte de vulneraciones que afecten datos personales a la Agencia, y a los titulares afectados en el caso que dichas vulneraciones se refieran, entre otras, datos relativos a obligaciones de carácter financiero, bancario o comercial.

El resultado: triple reporte y triple fiscalización ante un mismo hecho, **sin mecanismo de ventanilla única.**

EL ARGUMENTO

Articulación, *no jerarquía*

La regla "ley especial sobre ley general" está disponible como criterio residual —pero es insuficiente como política regulatoria frente a tres marcos que protegen intereses complementarios.

EL ARGUMENTO

Por qué la jerarquía no basta

I Intereses complementarios, no contrapuestos

Finanzas abiertas, protección de datos y ciberseguridad son facetas de una misma política de confianza digital. La prevalencia automática desatiende esa complementariedad.

II No resuelve lo operativo

Definir qué norma prevalece no elimina los paneles de consentimiento distintos para el titular, ni el triple reporte ante un mismo incidente para la industria.

III La articulación ya es posible

El artículo 24 de la Ley N° 21.521 constituye un precedente de coordinación normativa dentro del propio SFA que demuestra que el legislador ya optó por la articulación deliberada en un punto de contacto, al mencionar que el intercambio dentro del SFA, con consentimiento del cliente, no constituye violación de los deberes de confidencialidad, reserva o secreto que pesan sobre las instituciones participantes. El mismo criterio puede extenderse.

IV Debido proceso y proporcionalidad

Tres autoridades con competencia concurrente sobre un mismo hecho exigen coordinación que evite la duplicidad de procedimientos y la incertidumbre sobre el estándar de diligencia.

Propuestas

- Convenio CMF–Agencia–ANCI: Celebrar un convenio interinstitucional que establezca mecanismos de coordinación entre las tres autoridades, designe una autoridad líder según la materia, defina criterios de derivación y habilite una ventanilla única de contacto para los participantes del SFA.

- Criterio interpretativo conjunto CMF–Agencia PDP: Que otorgue certeza respecto de cuándo el consentimiento obtenido conforme a la Ley N°21.521 y la NCG N°514 satisface los requisitos de la Ley N°21.719, evitando duplicidades innecesarias y eventuales sanciones.

- Guía sectorial sobre decisiones automatizadas: Criterios para la aplicación del artículo 8° bis de la Ley N°21.719 en los procesos de suscripción y tarificación de seguros apoyados en el SFA, precisando estándares de transparencia, explicabilidad, intervención humana significativa y limitación de la finalidad del tratamiento.

- Protocolo unificado de incidentes, con la CMF como punto de entrada vía Reporte de Incidentes Operacionales (RIO): Implementar/Formalizar un protocolo de notificación que permita canalizar, a través del RIO de la CMF, un único reporte de incidentes que satisfaga simultáneamente las obligaciones de comunicación previstas en la Ley N°21.663 y en la Ley N°21.719, estableciendo mecanismos de derivación interna entre las autoridades competentes y evitando reportes duplicados frente a un mismo incidente.

GRACIAS

ASOCIACIÓN DE ASEGURADORES DE CHILE

Hacia un marco articulado entre las finanzas abiertas, la protección de datos y la ciberseguridad.

COMISIÓN
PARA EL MERCADO
FINANCIERO

Asociación Gremial de Empresas de Innovación Financiera de Chile A.G. (FinteChile)

Foro del Sistema de Finanzas Abiertas

FinteChile

Puntos de Fintechile para Foro SFA con tema ”Coherencia Regulatoria”

Junio 2026

www.fintechile.org

Contenidos

1. Ambigüedad en el concepto de consentimiento bajo SFA
2. Operaciones Desconocidas en SFA

Ambigüedad en el consentimiento

Posición Fintechile

Existe una falta de claridad regulatoria en torno a dos manifestaciones de voluntad que son conceptualmente distintas, pero que en la práctica - y en cierta medida por disposiciones de las NCG aplicables - se están confundiendo:

- el consentimiento para **acceder a datos financieros o iniciar pagos** bajo el Sistema de Finanzas Abiertas, y
- el consentimiento para **tratar los datos personales una vez que estos ya han sido obtenidos.**

La Ley Fintech establece expresamente que el consentimiento en el SFA tiene un alcance limitado, pues únicamente habilita el **acceso** a información o la ejecución de pagos, y que su revocación solo impide futuras consultas o transacciones, sin afectar el tratamiento de los datos previamente obtenidos. Sin embargo, la NCG 569 genera una ambigüedad terminológica, al vincular el consentimiento SFA con el "tratamiento, cesión o intercambio de datos" en su regulación del consentimiento y del panel de control, lo que tiende a unificar de manera equívoca ambos planos en la práctica, en lugar de separarlos. Además, la norma establece que, una vez revocado el consentimiento, el PSBI/PSIP debe interrumpir el acceso y "borrar los datos del usuario", lo que contradice el legítimo tratamiento de datos previamente obtenidos, sin que dicha obligación de eliminación tenga sustento alguno en la Ley Fintec, contraviniendo derechos adquiridos tanto de los proveedores como de los usuarios.

Esta configuración genera incertidumbre sobre el régimen aplicable y, en la práctica, puede llevar a los actores del mercado a evitar el SFA y operar fuera de él, accediendo a datos por otras vías menos supervisadas.

Ambigüedad en el consentimiento: Propuesta

Posición Fintechile

Para abordar este problema, FinteChile **propone introducir una aclaración normativa** expresa que delimite con precisión ambos tipos de consentimiento y sus efectos.

En particular, se plantea reafirmar que el consentimiento SFA **es autónomo y se restringe exclusivamente a habilitar el acceso a datos o la iniciación de pagos (tal como expresamente se señala en la Ley Fintec Art. 24),** mientras que el tratamiento posterior de esos datos debe regirse por la normativa general aplicable (ya sea la normativa de protección de datos para personas naturales o las reglas generales del derecho para otro tipo de datos).
Asimismo, se sugiere explicitar que la revocación del consentimiento en el SFA solo tiene efectos hacia el futuro, interrumpiendo nuevos accesos, sin invalidar el tratamiento de la información ya obtenida, siempre que este cuente con una base de licitud independiente (tal como expresamente se señala en la Ley Fintec). Así, se debe corregir la NCG 569 vigente, la cual:

- vincula el consentimiento SFA con el tratamiento de datos, y
- exige la eliminación de datos al revocar el consentimiento, lo que implica un efecto retroactivo relevante.

Se propone revisar la redacción de la NCG 514 (modificada por la 569) para no extralimitar el alcance del consentimiento bajo el SFA conforme se determina expresamente en la Ley Fintec, eliminando las ambigüedades indicadas y evitando que esta afecte el tratamiento previamente lícito de los datos.
Con ello, se busca otorgar mayor certeza jurídica, incentivar la participación dentro del perímetro regulado del SFA y fortalecer un ecosistema de finanzas abiertas más transparente, competitivo y supervisado.

Operaciones Desconocidas en SFA

Posición Fintechile

La Ley N.º 20.009 **protege a los usuarios frente a operaciones desconocidas mediante la restitución temprana de fondos** por parte del emisor mientras se investigan las responsabilidades. Este principio debe mantenerse.

Sin embargo, el desarrollo del Sistema de Finanzas Abiertas (SFA) **incorpora nuevos participantes en la cadena de pagos y distribuye entre ellos funciones de iniciación, autenticación y ejecución de transacciones**, lo que exige revisar la arquitectura de la ley para que la asignación final de costos cubra toda la cadena de pago, y no sólo la relación entre usuario, emisor e iniciador.

Actualmente, la ley continúa concentrando la responsabilidad económica inicial en el emisor y no establece mecanismos equivalentes para determinar, con la misma claridad, la **responsabilidad de los demás participantes que pudieron estar en mejor posición para prevenir, detectar o acreditar el fraude.**

Esta situación genera una asimetría regulatoria y puede producir incentivos insuficientes para una adecuada gestión de riesgos por parte de todos los intervinientes de la cadena de pagos.

Operaciones Desconocidas en SFA: Propuesta

Posición Fintechile

FinteChile propone revisar la Ley Antifraude para **incorporar criterios de asignación de responsabilidad aplicables a todos los participantes de la cadena de pagos**, manteniendo intacta la protección del usuario.

La normativa debiera facultar a la autoridad para **definir causales, estándares probatorios, procedimientos de controversia y mecanismos de atribución de responsabilidades y costos entre los distintos intervinientes**.

Este cambio no busca debilitar la protección al usuario ni trasladar automáticamente el fraude al comercio. Busca una regla de coherencia: **quien está en mejor posición para prevenir, autenticar, trazar, detener o probar una operación debe asumir la responsabilidad correspondiente**. Así, el SFA quedaría alineado con los incentivos de seguridad que ya existen en los sistemas de tarjetas, evitando arbitrajes regulatorios entre medios de pago y fortaleciendo la confianza en pagos abiertos, interoperables y competitivos.

La Ley Antifraude debe ajustarse para el contexto del Sistema de Finanzas Abiertas (SFA), de manera que la responsabilidad por operaciones desconocidas pueda distribuirse entre todos los participantes de la cadena de pagos según quién estaba en mejor posición para prevenir, controlar o demostrar el fraude.

COMISIÓN
PARA EL MERCADO
FINANCIERO

Agenda

2 Presentaciones miembros GC: coherencia regulatoria en **materia de ciberseguridad y fraude**

COMISIÓN
PARA EL MERCADO
FINANCIERO

Asociación de Bancos e Instituciones Financieras de Chile A.G (ABIF)

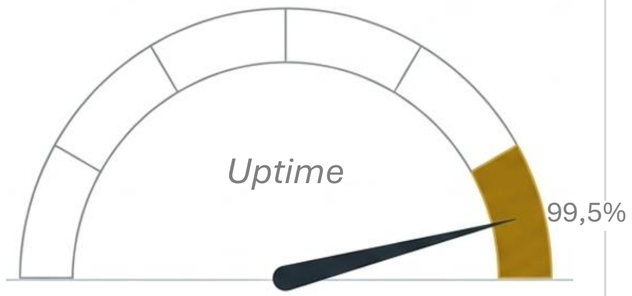
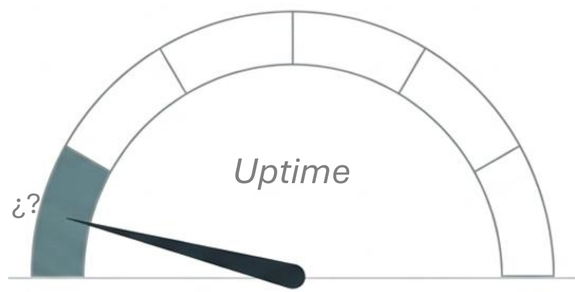
Sistema de Finanzas Abiertas

Coherencia Regulatoria – Ciberseguridad y Fraude

Asociación de Bancos de Chile – ABIF

Julio de 2026

Requisitos Operacionales SFA No Equivalentes (NCG N°569)

	Emisores (IPC)	Iniciadores de Pago (PSIP)
Disponibilidad		
	• ***Uptime*** diario de 95% y mensual de 99,5% para pagos. • Exige **tiempos de respuesta** de 0,8 seg. para pagos.	• **Sin exigencias** de *uptime* ni de rendimiento para PSIP en un **flujo sincrónico** de cara al usuario.
Reportería	• **Reportes obligatorios** de: disponibilidad, rendimientos, límites (TPS / TPM) y errores en respuesta de APIs.	• **Sin exigencias** de reportería que valide una experiencia de usuario adecuada.
Mantenciones	• **Restricciones a mantenciones** (tabla 6 de NCG N°569).	• **Sin restricciones.**

Tipo de Mantención	Tiempo de aviso (previo a ejecución)	Plazo máximo de extensión	Frecuencia máxima permitida
Correctiva	48 horas	4 horas	Mensual
Preventiva	7 días	8 horas	Mensual
Evolutiva / Actualización	14 días	12 horas	Mensual
Urgente	4 horas	2 horas	Mensual

⚠ La ausencia de métricas de rendimiento para PSIP **dificulta encontrar la causa raíz frente a potenciales fallas que puedan sufrir las personas** al utilizar el SFA.

Requisitos de Ciberseguridad SFA No Equivalentes

	Bancos (IPC)	Iniciadores de Pago (PSIP)
Monitoreo	• Deben monitorear continuamente **patrones de las transacciones** para detectar fraudes (RAN 1-7). • Implementar un marco de gobierno corporativo para la **gestión del riesgo tecnológico y de ciberseguridad** (RAN 20-10), siendo una de las tareas identificar y **mitigar riesgos de ingeniería social** en el proceso de Autenticación Reforzada de Clientes (ARC).	• **No hay un requisito de monitoreo en la capa de presentación** del PSIP/PSBI (app, web). El riesgo es que se presente un monto alterado, un beneficiario distinto o datos manipulados, entre otros (NCG N°569). *La ausencia de regulación en la capa de presentación del PSIP **crea un punto ciego que el banco no puede cubrir** desde su posición en el flujo transaccional.*
Herramientas de correlación de eventos	• Los bancos deben **implementar herramientas de seguimiento y correlación de eventos,** a objeto de detectar otros incidentes, identificar vulnerabilidades de la infraestructura física y virtual comprometida, *modus operandi* de los eventuales ataques, entre otros (RAN 20-8).	• El PSIP debe implementar **medidas de ciberseguridad** (NCG N°514), **pero no se contemplan herramientas de seguimiento y correlación de eventos** para detectar *modus operandi* de eventuales ataques.
Dualidad regulatoria	• Ante un incidente significativo de ciberseguridad los **bancos deben gestionar e informar a la CMF y a la ANCI,** mientras estas entidades no acuerden una norma conjunta de carácter general.	• PSIP no están por defecto declarados OIV, por lo cual **no tienen obligación de reportar a la ANCI.**

Fraudes Transaccionales No Equivalentes

	Sistemas de Pagos en Chile	SFA: Iniciación de Pagos
Arquitectura legal, contractual y técnica	• En Chile, la **CMF y el Banco Central establecen lineamientos** mínimos que deben cumplir las instituciones que participen del proceso de pago. • Las relaciones de conexión se determinan mediante **contratos bilaterales voluntarios entre las partes.**	• **El SFA no cuenta con una arquitectura contractual y técnica** para complementar los elementos que la regulación no establece frente a una **interconexión obligatoria** (condicionada al Directorio). Este punto fue discutido en el Foro del SFA y **ratificado por la Universidad Adolfo Ibáñez** que actuaba como Equipo de Soporte (Entregable 4.5, sep-2025).
Asignación respon-sabilidades fraudes	• El **emisor tiene una responsabilidad objetiva,** con un estándar de responsabilidad de culpa grave o dolo. • Hay presunciones específicas de culpa grave o dolo. • **Hay una sede judicial** (JPL) donde se resuelve. • Los bancos deben cumplir requisitos de autenticación (NCG 538)	• **La Ley de Fraudes establece que el PSIP resarcirá al emisor** si este es responsable de la operación desconocida (Art. 5) y que también debe demostrar que la operación fue autorizada dentro de su ámbito de competencia (Art. 4). • Sin embargo, **no existen definiciones de plazos ni mecanismos** para determinar la responsabilidad del PSIP frente a una operación desconocida, **ni menos requisitos de autenticación**.

Prevención (LA / FT) y Gestión de Proveedores No Equivalentes

	Banco / IPI-IPC	Fintech / PSBI-PSIP
Prevención Lavado de Activos (LA) / Financiamiento del Terrorismo (FT)	• Bancos deben contar con: **Oficial de Cumplimiento independiente** y de alta jerarquía; **Comités dedicados** (ej. Comité de Auditoría, Comité de Activos y Pasivos –ALCO- y Comité de alto nivel para LA/FT); **Auditoría interna independiente** que verifica la eficacia del marco de gobierno, de control y de riesgos como tercera línea de defensa; y revisiones de **Auditoría externa** cuando revelen debilidades importantes (RAN 1-13).	• Circular N°62 UAF: Empresas pequeñas pueden asignar como **Oficial de Cumplimiento a socio, administrador o ejecutivo.** • NCG N°502: Entidades con menos de 100 clientes activos (asesoría crediticia, enrutamiento de órdenes) o menos de 100 clientes activos/100.000 seguidores (asesoría de inversión) pueden **eximirse del cumplimiento de políticas internas, función de gestión de riesgos,** y –en el caso de asesoría crediticia– también función de **auditoría interna.** • NCG N°514: **En el momento del registro exige un documento de políticas de gestión** para PSBI y PSIP. • Ley N°19.913 (UAF): **No incorpora a PSBI como sujetos obligados** (contarán con 24 meses de información transaccional agregada).
Gestión de proveedores	• RAN 20-7 establece la **gestión de proveedores críticos durante todo el ciclo de vida** de estos. • Bancos **mantienen la responsabilidad** respecto de procesos externalizados (ej. casos que contemplen el tratamiento o almacenamiento de información de clientes). • En consulta una actualización a la RAN 20-7, que incluye la supervisión de **subproveedores** (cuartas partes o proveedores de proveedores).	• PSBI tienen obligaciones de resguardo de la información (NCG N°514), pero **no contemplan un marco de gestión y supervisión** del ciclo de vida de proveedores equivalente a la RAN 20-7. • **Tampoco mantienen la responsabilidad final** respecto de procesos externalizados, ni regula la cadena de subcontratistas.

Otras Asimetrías Relacionadas No Equivalentes

	Banco / IPI-IPC	Fintech / PSBI-PSIP
Requisitos para inicio de operaciones	LGB: Accionistas **solidariamente responsables**; Revisión por **tres años** del plan de negocio; Requisitos para controladores de **solvencia, idoneidad comercial, conducta y no inhabilidades** (sin antecedentes penales, concursales ni regulatorios graves; sin haber dirigido entidades en liquidación ni registrar protestos relevantes).	Ley Fintech (RPSF): No se establece responsabilidad solidaria de controladores; Se exige **síntesis del plan de negocios** (sin revisión posterior); Requisitos de **no inhabilidades más acotados que las bancarias** (infracciones graves de Ley Fintech y conductas constitutivas de delito bajo leyes específicas para la P. Jurídica o controladores).
Requisitos prudenciales	• AGF (NCG N°526): **[<50 clientes] exento** capital mínimo, garantías y ratio de capital. Luego **capital mínimo desde UF 5.000; garantías UF 10.000 por fondo,** ratio de capital 3% de APR. • Corredoras (NCG N°562): **[<500 clientes] exento** capital mínimo, garantías y ratio de capital. Luego **capital mínimo desde UF 5.000; garantías UF 6.000, ratio de capital** 3% de APR. • **Bancarias responden con totalidad** patrimonio efectivo.	• RPSF –Intermediación y Custodia (NCG N°502): **[<500 clientes] exento** capital mínimo y garantías; **[<5000 clientes] exento** ratio de capital. Luego **capital mínimo desde UF 1.000,** ratio de capital 3% APR. **Garantías se incluyen en patrimonio ajustado,** no se exigen separadas. • RPSF –Enrutamiento de órdenes (NCG N°502): **[<500 clientes] exento** capital mínimo y garantías. Luego **capital mínimo y garantías de UF 500; sin requerimientos** de ratio de capital.

Asimetrías Ley Fintech / NCG N°569 / Portal

1. Especificaciones del Portal del Desarrollador sin respaldo en NCG N°514/N°569 o Ley Fintech.

- Documentación técnica OpenAPI (*swagger*) establece que los **PSIP son responsables de la definición de la estructura de pagos recurrentes de monto variable –ej. monto, límite y frecuencia de cada iteración de pago.**
    - Lo anterior tiene implicancias operativas y de elementos para **determinar las responsabilidades frente a potenciales fraudes.**
- **No existe mención en las normas (NCG N°514 o N°569) respecto de estas definiciones.**

2. API de Confirmación de Fondos

- NCG N°569 y Portal del Desarrollador **incorporan la obligación para los IPI e IPC** de desarrollar una API que valide los fondos disponibles de los clientes.
- Esta API **no es necesaria para cumplir los requerimientos de compartir información y ejecutar órdenes de pagos** de la Ley Fintech (SFA). En efecto, el informe normativo de la NCG N°569 **la declara opcional para PSBI y PSIP.**

banca

asociación de bancos

COMISIÓN
PARA EL MERCADO
FINANCIERO

Asociación Gremial de la Industria del Retail Financiero A.G. - Retail Financiero A.G.

Asociación
Retail
Financiero

Convergencia y coherencia regulatoria entre Ley Fintec y Leyde Fraudes No. 20.009

Santiago, 08 de Julio de 2026

Evolución de las Pérdidas por Fraude Externo (2022 - 2026)

Análisis de la trayectoria y proyección de las pérdidas por fraude reportadas por la industria.

ACUMULADO HISTÓRICO

Entre 2022 y marzo de 2026 las pérdidas acumulan:

US$990 millones

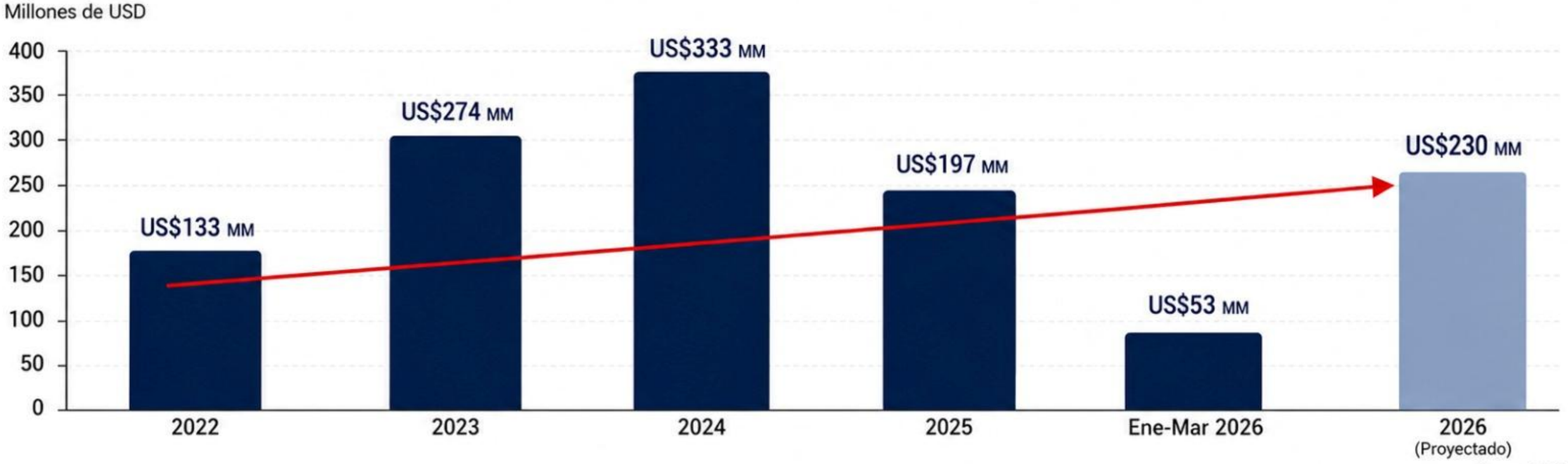
equivalentes a más de **$883.160 millones**

PROYECCIÓN 2026

Manteniendo el ritmo observado durante enero-marzo de 2026:

US$230 millones

equivalentes a más de **$205.160 millones** estimados para 2026



Fuente: CMF

Cifras en millones de dólares (USD)

Cifras en millones de pesos (MM$) al tipo de cambio promedio anual

Millonario fraude informático afecta a plataforma de pagos, pérdidas llegan a $1.070 millones

RS por RoadShow — 8 de julio de 2026

Monnet Pagos en Línea de Chile sufrió 214 transferencias no autorizadas entre el 1 y el 10 de junio, en un ataque que la empresa atribuye a una operación organizada para desviar fondos desde su plataforma.

La fintech aseguró que los responsables cambiaron de estrategia cada vez que reforzó sus sistemas de seguridad, utilizando distintos mecanismos para mantener el acceso.

Cuerpos Normativos Convergentes

1

Ley de Fraudes No. 20.009

Regula principalmente el régimen de responsabilidad frente al fraude en medios de pago y transacciones electrónicas.

2

Ley Fintec No. 21.521

Crea un nuevo ecosistema financiero tecnológico, basado en finanzas abiertas, datos, interoperabilidad, iniciación de pagos y nuevos prestadores de servicios financieros.

La pregunta a responder si la Ley No. 20.009 aplica, ¿si está diseñada para hacerse cargo del nuevo ecosistema Fintech?

Perímetros de cada Ley

Alcance de la Ley No. 20.009

Fue concebida como un régimen de limitación de responsabilidad frente al fraude en medios de pago y transacciones electrónicas, en un contexto de sistema financiero tradicional bajo el M4P.

Alcance de la Ley Fintech No. 21.521

Crea una arquitectura amplia:

1. finanzas abiertas,
2. iniciación de pagos
3. proveedores de información
4. Custodia
5. Intermediación
6. asesoría.
7. enrutamiento de órdenes
8. plataformas de financiamiento colectivo
9. sistemas alternativos de transacción
10. activos financieros virtuales.

¿Que fraudes cubre la ley No. 20.009?

La Ley No. 20.009 podría cubrir ciertos fraudes Fintech cuando se materializan como pagos o transferencias no autorizadas, pero **no regula integralmente los fraudes propios del nuevo ecosistema Fintech**.

Asociación Retail Financiero

Dos leyes, con racionales regulatorios diferentes

La siguiente tabla sintetiza las diferencias estructurales entre ambos regímenes normativos, evidenciando que responden a lógicas, objetos y diseños fundamentalmente distintos.

Dimensión	Ley No. 20.009	Ley Fintech No. 21.521
Objeto	Fraude en medios de pago y transacciones electrónicas	Servicios financieros tecnológicos
Lógica	Usuario /emisor	Multiplicidad de actores
Régimen	Restitutivo ex post	Habilitante, operacional y de supervisión
Foco	Cargos, abonos, giros y transferencias	Datos, APIs, consentimiento, órdenes, instrumentos y servicios, etc
Diseño	Pensada desde el sistema tradicional de pagos en el M4P	Diseñada para finanzas abiertas e innovación financiera

Nota: La Ley No. 20.009 protege frente al fraude en pagos; la Ley Fintech contienen riesgos que exceden el pago.

Perímetro de Ley No. 20.009

Medios de pago

Extravío, hurto, robo o fraude de tarjetas de pago.

Transacciones electrónicas

Fraudes en transacciones electrónicas; cargos, abonos o giros de dinero y transferencias electrónicas.

Operaciones no autorizadas

Operaciones realizadas por medios electrónicos no autorizadas por el usuario.

Restitución y carga probatoria

Restitución de fondos o cancelación de cargos; carga de la prueba respecto de la autorización de la operación.

Iniciación de pagos

Pagos o transferencias electrónicas iniciadas mediante proveedores de servicios de iniciación de pagos.

Extremamos la interpretación: Ley 20.009 sí podría alcanzar ciertos eventos Fintech, pero solo cuando se trata de una operación de pago no autorizada. (problema de temporalidad en la dictación de la ley)

Del modelo de cuatro partes a un ecosistema multiples actores

Modelo tradicional de pagos

La operación se explica por la interacción lineal entre cuatro actores:

1. **Emisor**
2. **Marcas**
3. **Adquirente / Operador**
4. **Comercio / Cliente**

Ecosistema Fintec multiples actores

Aparecen nuevos intervinientes que distribuyen la cadena de responsabilidad:

1. **Proveedor de iniciación de pagos**
2. **Institución proveedora de cuentas**
3. **Proveedor de servicios basados en información**
4. **Plataforma de financiamiento colectivo**
5. **Sistema alternativo de transacción**
6. **Intermediario de instrumentos financieros**
7. **Custodio**
8. **Asesor de inversión / crediticio**
9. **Proveedor tecnológico / API**

Nota: La cadena de responsabilidad deja de ser lineal y pasa a ser distribuida.

Asociación Retail Financiero

El consumidor interpretará que todo fraude Fintech esta protegido por la Ley No. 20.009

Existe una brecha entre la cobertura jurídica y la expectativa del cliente. Esta asimetría puedes ser fuente de conflicto regulatorio, judicial y reputacional.

Perspectiva jurídica / regulatoria	Perspectiva del cliente
La Ley No. 20.009 cubre fraudes en medios de pago y transacciones electrónicas	*"Me defraudaron usando una plataforma financiera digital."*
La Ley Fintec regula servicios financieros tecnológicos más amplios	*"Es mi plata; alguien del sistema financiero debe responder."*
No todo fraude Fintec es una operación de pago no autorizada	*"Si hubo fraude digital, debería aplicar la ley de fraudes."*
Puede haber fraude de datos, custodia, asesoría, órdenes, inversión o criptoactivos	*"No voy a distinguir entre iniciador, emisor, custodio, plataforma o proveedor tecnológico."*
La responsabilidad puede estar distribuida entre varios actores	*"Yo contraté un servicio financiero; no me corresponde perseguir a cada interviniente."*

OJO: La expectativa del cliente será más amplia que la cobertura jurídica efectiva.

Fricciones regulatorias, judiciales y reputacionales

La brecha normativa no es un problema abstracto. Se traduce en consecuencias concretas y previsibles para el sistema financiero, los reguladores y los tribunales.

Reclamos masivos.

Reclamos de clientes bajo la Ley No. 20.009 por fraudes que no encuadran en su ámbito de aplicación.

Presión reputacional

Sobre emisores y entidades tradicionales que quedan expuestos a responsabilidades que podrían corresponden a actores Fintech.

Conflictos entre actores

Entre emisores, iniciadores, plataformas, custodios y proveedores tecnológicos sobre quién debe responder.

Incertidumbre probatoria

Sobre carga de la prueba y sobre quién debe restituir al usuario afectado.

Judicialización

Ante juzgados de policía local y tribunales civiles, sin reglas claras de competencia ni de responsabilidad.

Arbitraje regulatorio

Entre actores Fintec y actores tradicionales que operan bajo regímenes distintos para riesgos equivalentes.

Intervención reactiva

Intervención regulatoria reactiva ante incidentes que pudieron haberse anticipado normativamente.

Pérdida de confianza

Debilitamiento de la confianza en el Sistema de Finanzas Abiertas y en el ecosistema Fintech en general.

Mensaje clave: La falta de claridad normativa trasladará el conflicto al cliente, al SFA, y a los tribunales.

Asociación Retail Financiero

Lo que falta: una regla de convergencia

- **Coordinación de responsabilidad frente al cliente**
- **Derecho de repetición entre intervinientes**
- **Carga de la prueba distribuida**
- **Trazabilidad de instrucciones**
- **Evidencia tecnológica y conservación de registros**
- **Deberes de prevención**
- **Estándares de autenticación y consentimiento**
- **Respuesta frente a incidentes**

Nota: Existe una brecha entre el diseño de la Ley Fintec y la arquitectura restitutiva de la Ley No. 20.009.

Ambas leyes tienen un ámbito legítimo y necesario, y que la solución no es reemplazar una por otra, sino coordinarlas mediante una regla de convergencia.

Asociación Retail Financiero

Ajustes normativos que se proponen.

01

Mantener la Ley No. 20.009 como régimen matriz

Preservar su rol como estatuto de fraude en pagos y transacciones electrónicas, haciendo ajustes al ámbito aplicación original.

02

Ajustar la Ley Fintech

Incorporar un estatuto especial de prevención, gestión y responsabilidad por fraude Fintech no transaccional, adaptado a los nuevos servicios y sujetos.

03

Incorporar una norma puente

Que coordine ambas leyes, establezca reglas de prelación y evite vacíos, duplicidades y fricciones entre regímenes.

04

Establecer deberes operacionales

Pronunciamiento de la CMF sobre el alcance de la Ley No. 20.009 frente a proveedores de iniciación de pagos; y Trazabilidad, evidencia, autenticación, consentimiento, alertas, cooperación antifraude y responsabilidad entre intervinientes de la cadena Fintech.

05

Proteger al cliente / consumidor de la complejidad

Evitar que el cliente deba identificar qué actor de la cadena causó el fraude para poder ejercer sus derechos.

Opcionalmente: Dejar todo refundido en Ley No. 20.009 para fraude en pagos y para fraude del ecosistema del SFA.

Asociación Retail Financiero

COMISIÓN
PARA EL MERCADO
FINANCIERO

Cooperativas de Ahorro y Crédito Asociación Gremial - COOPERA A.G.

Coopera - Foro consultivo

Coherencia regulatoria

Ciberseguridad y Fraude

COOPERA
Cooperativas de Ahorro y Crédito Asociadas

Jueves 09 julio 2026

Coherencia regulatoria

1. Duplicidad de reportes de incidentes de seguridad

Una misma contingencia operacional o de ciberseguridad puede activar simultáneamente obligaciones de reporte ante distintas autoridades.

Norma	Destinatario	Plazo
NCG 569	CMF	30 Minutos desde el incidente
Ley 21.663	CSIRT Nacional (ANCI)	3 horas (alerta temprana)
Ley 20.010 – I12	CMF	Mensual
LPDP	APDP	-

Una entidad financiera que sea simultáneamente participante del Sistema de Finanzas Abiertas y Prestador de Servicios Esenciales u Operador de Importancia Vital, debe preparar dos reportes distintos, dirigidos a autoridades diferentes y bajo estándares distintos, precisamente durante la etapa más crítica de un incidente.

Aunque la Ley de Ciberseguridad contempla el desarrollo de una futura "ventanilla única", dicho mecanismo aún requiere implementación normativa.

Riesgo práctico
- Duplicación de cargas administrativas
- Riesgo de inconsistencias entre reportes
- Utilización de recursos críticos en obligaciones administrativas en vez de contención del incidente

2. Superposición de autoridades regulatorias

La Ley Marco de Ciberseguridad establece que la autoridad sectorial será la encargada de la fiscalización cuando las sanciones tengan tenido efectos "al menos equivalentes" a la dictada por la Agencia, pero **dicha equivalencia deberá definirse mediante regulación posterior creada en conjunto**.

Actualmente no existe un criterio objetivo que permita determinar:
- Cuando una norma CMF desplaza una exigencia ANCI;
- Cuando ambas deben cumplirse simultáneamente.

Se tiene el entendimiento de la priorización legal, por lo que queremos validar la coherencia regulatoria

Coherencia regulatoria

3. Ambigüedad sobre el tratamiento de direcciones IP

La Ley Marco de Ciberseguridad establece expresamente que, para sus efectos, una dirección IP no constituye dato personal.

En cambio, el régimen del Sistema de Finanzas Abiertas remite a la normativa sobre protección de datos personales, donde determinados identificadores técnicos pueden ser considerados datos personales dependiendo del contexto.

Problema
Un mismo incidente podría recibir tratamientos regulatorios distintos según la autoridad competente.

4. Responsabilidad frente al fraude

La incorporación de nuevos actores genera una cadena de responsabilidad considerablemente más compleja.

Ley de Fraudes: El emisor debe:
- Restituir rápidamente los fondos;
- Probar la autorización de la operación.

Cuando interviene un PSIP, éste debe demostrar que la orden fue correctamente autorizada dentro de su ámbito de competencia.

Problema: Existe una asimetría temporal. El banco debe devolver inmediatamente el dinero al usuario. Posteriormente deberá intentar recuperar esos fondos del PSIP mediante:
- Ejecución de garantías
- Negociación
- Litigios

La Ley no establece un procedimiento expedito para dicho resarcimiento. El riesgo económico recae inicialmente sobre la institución financiera, aun cuando el responsable del incidente sea un tercero.

Coherencia regulatoria

5. Conservación de registros versus eliminación de datos

Sistema de Finanzas Abiertas
Cuando un usuario revoca el consentimiento:
- Debe interrumpirse inmediatamente el acceso
- Deben eliminarse los datos del usuario

Otras obligaciones regulatorias
Las entidades deben conservar registros durante varios años para efectos de: Auditoría, Supervisión CMF, Investigación de fraude y eventuales litigios.
La normativa no distingue claramente entre:
- Datos personales
- Registros de auditoría
- Evidencia técnica

Existe incertidumbre respecto de la conservación de evidencia, registros de auditoría y antecedentes forenses cuando se revoca un consentimiento o expira una base legal de tratamiento

6. Diferencias en los calendarios de implementación

La implementación del Sistema de Finanzas Abiertas es gradual. Mientras tanto, otras obligaciones regulatorias (seguridad, fraudes, continuidad operacional) son plenamente exigibles desde el inicio.

Oportunidad
Basado en la experiencia en el proceso de la Ley fintec y de Finanzas Abiertas para la elaboración de NCG, sería beneficioso replicar el proceso colaborativo para futuras implementación Normativas en términos de gradualidad y proporcionalidad.

7. Diferentes frecuencias de reportes regulatorios

Las entidades deben informar estadísticas de fraude con distintas periodicidades. Por ejemplo:
- Reportes trimestrales a la CMF;
- Publicaciones semestrales al público.

Consecuencia: Se generan procesos paralelos de consolidación de información con distintos cortes temporales, incrementando costos de cumplimiento.

Conclusiones

El principal desafío regulatorio no reside en que las tres leyes persigan objetivos incompatibles. Por el contrario, todas buscan fortalecer la confianza en el ecosistema financiero digital mediante mayores estándares de seguridad, resiliencia y protección del consumidor.

Sin embargo, **la coordinación entre estos cuerpos normativos todavía presenta vacíos relevantes**. Las principales tensiones provienen de la coexistencia de múltiples autoridades competentes, obligaciones de reporte concurrentes, estándares técnicos parcialmente distintos y reglas de responsabilidad que no siempre dialogan entre sí.

Desde una perspectiva de política regulatoria, las materias que aparecen como prioritarias para futuras precisiones normativas son:

1. Armonizar los plazos y canales de reporte de incidentes;
2. Definir criterios claros de equivalencia entre la regulación de la CMF y la ANCI;
3. Precisar la distribución de responsabilidades entre emisores, PSIP y otros participantes del Sistema de Finanzas Abiertas;
4. Compatibilizar las obligaciones de eliminación de datos con los deberes de conservación de evidencia;
5. Establecer procedimientos coordinados para el resarcimiento entre participantes del ecosistema financiero.

En definitiva, el éxito del Sistema de Finanzas Abiertas dependerá no solo de la sofisticación de sus estándares tecnológicos, sino también de la capacidad del marco regulatorio para ofrecer reglas coherentes, previsibles y coordinadas entre las distintas autoridades sectoriales.

Coopera - Foro consultivo

Coherencia regulatoria

COOPERA
Cooperativas de Ahorro y Crédito Asociadas

Jueves 09 julio 2026

COMISIÓN
PARA EL MERCADO
FINANCIERO

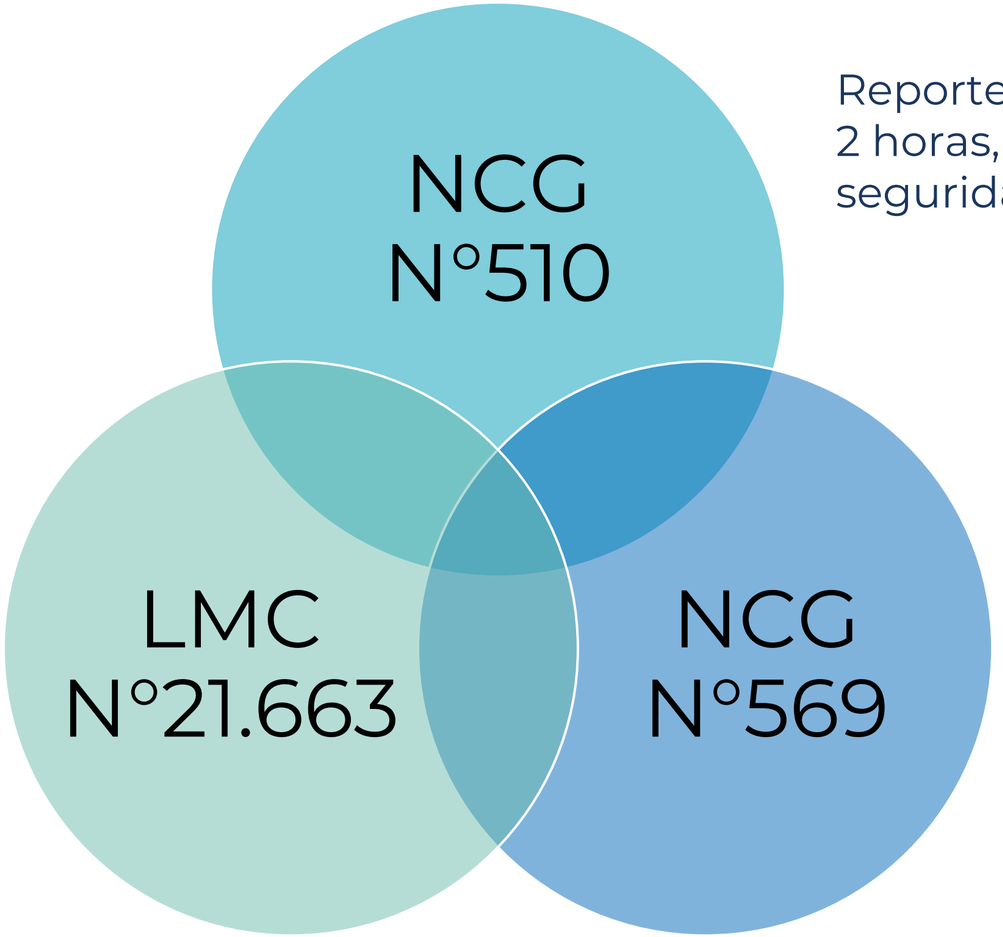
Asociación de Fondos Mutuos de Chile A.G.

Fondos Mutuos AG

Foro SFA, CMF

09 de julio 2026

Ciberseguridad: AGF sujetas a tres regímenes:



Reporte de incidentes a CMF en 2 horas, estándares de seguridad y continuidad

Reporte a CSIRT en 3 horas; ANCI puede dictar estándares técnicos y fiscalizar

RIO específico; facultad CMF para suspender participantes y definir medidas preventivas inmediatas

I. Duplicidad de estándares técnicos

Propuestas:

1. Dictar norma CMF-ANCI para declarar equivalencia de estándares (Art. 26 LMC)

2. Reconocimiento de estándares SFA, cumplen con NCG N°510 y ANCI

3. Estándares ANCI N/A a supervisados CMF en materias ya reguladas (art. 26 inc. 3°LMC)

II. Duplicidad continuidad de negocios

Propuestas:

1. Reconocer mecanismo alternativo conforme a plan de continuidad NCG N°510

2. Establecer que planes de Continuidad bajo NCG N°510 y 569, satisfacen obligaciones LMC, evitando doble revisión CMF - ANCI

3. Procedimiento de auto desconexión y reactivación (NCG N°569), es el único aplicable a AGF, sin interferencia de ANCI

III. Duplicidad reporte de incidentes

NCG N°510

Reporte a la CMF en 2 horas

NCG N°569 (SFA – RIO)

Reporte a la CMF a través de l RIO, con variables de afectación SFA, detalle de medidas de denegación y desconexión

LMC – art. 9°

Reporte CSIRT en plazo de 3 horas, reporte de actualización en 24horas si es operador de importancia vital, o en 72 horas en otros casos,; más informe en 15 días

Plazos y criterios no coincidentes: riesgo de doble sanción

III. Duplicidad reporte de incidentes

Propuestas:

Ventanilla única

Ventanilla única del art. 9° LMC: el RIO ante la CMF (modulo SFA incluido), sirve simultáneamente como alerta temprana al CSIRT Nacional

Criterios coordinados

Establecer criterios de calificación coordinados entre NCG N°510, 569 y la taxonomía LMC

Reconocimiento de notificación

Reconocer que la notificación vía RIO-SFA, cuando comprenda información equivalente a la LMC, satisfice la obligación de reporte ante el CSIRT

IV. Fiscalización CMF y ANCI

Se requiere: garantizar certeza jurídica

1

Norma conjunta CMF-ANCI

Ejercer potestad del art. 26 LMC y establecer a la CMF como autoridad sectorial prevalente

2

Impedir sanciones paralelas

Establecer mecanismo que evite sanciones paralelas sobre los mismos hechos

3

Competencias CMF

Reconocer que las medidas de suspensión, desconexión y reactivación de participantes del SFA son competencia exclusiva de la CMF

Coherencia SFA y normativa de Fraude

Se requiere:

1

Clarificar responsabilidad de las IPI

´Posterior a la Entrega de datos, una IPI no responderá por los daños que su mal uso pueda causar, siendo esto responsabilidad del PSBI o PSIP

2

Reconocer mecanismos suficientes

Aclarar que revocación de consentimiento en panel de control constituye medida de seguridad suficiente para efectos de la Ley N°20.009

3

Establecer estándar de monitoreo de fraude específico para el SFA

Definir requerimientos mínimos en materia de detección de operaciones anómalas, identificación de patrones de fraude y establecimiento de límites en canales digitales

COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Sesión 41
Foro del Sistema de Finanzas Abiertas (FSFA)

Comisión para el Mercado Financiero

Julio 2026