100 años de regulación y supervisión bancaria

COMISIÓN PARA EL MERCADO FINANCIERO

Reunión de Gerentes de la ABIF

Avances en implementación regulatoria: SFA y Ley de Fraudes

Solange Berstein J.
Presidenta, Comisión para el Mercado Financiero

Agosto 2025

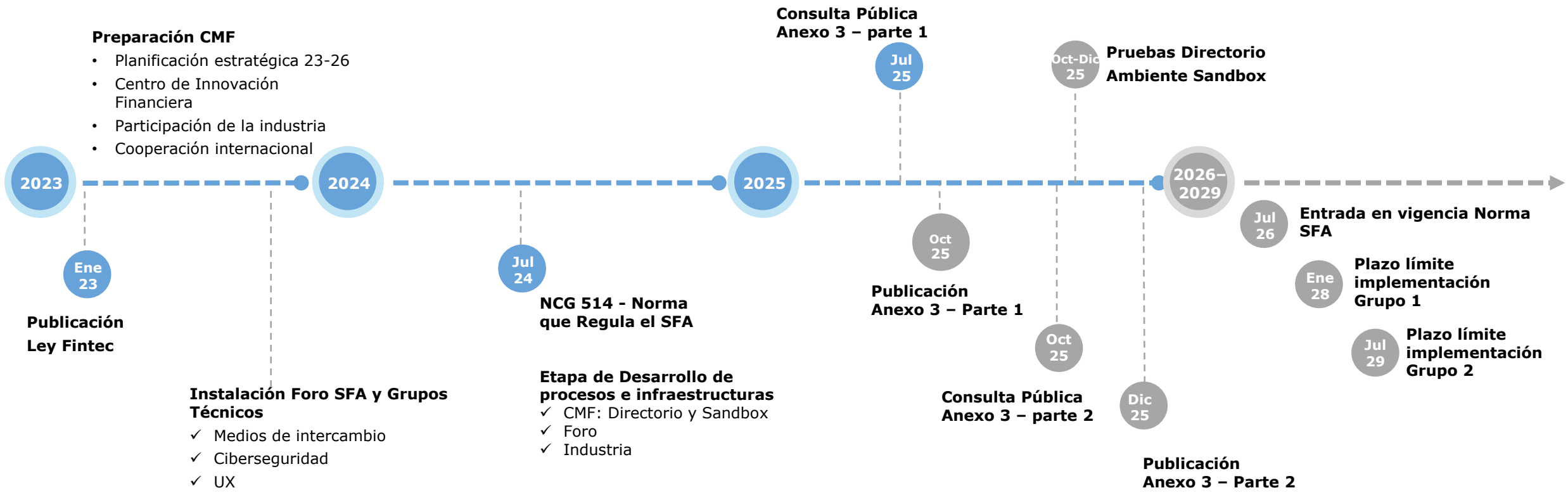
COMISIÓN PARA EL MERCADO FINANCIERO

100 años de regulación y supervisión bancaria

Sistema de Finanzas Abiertas

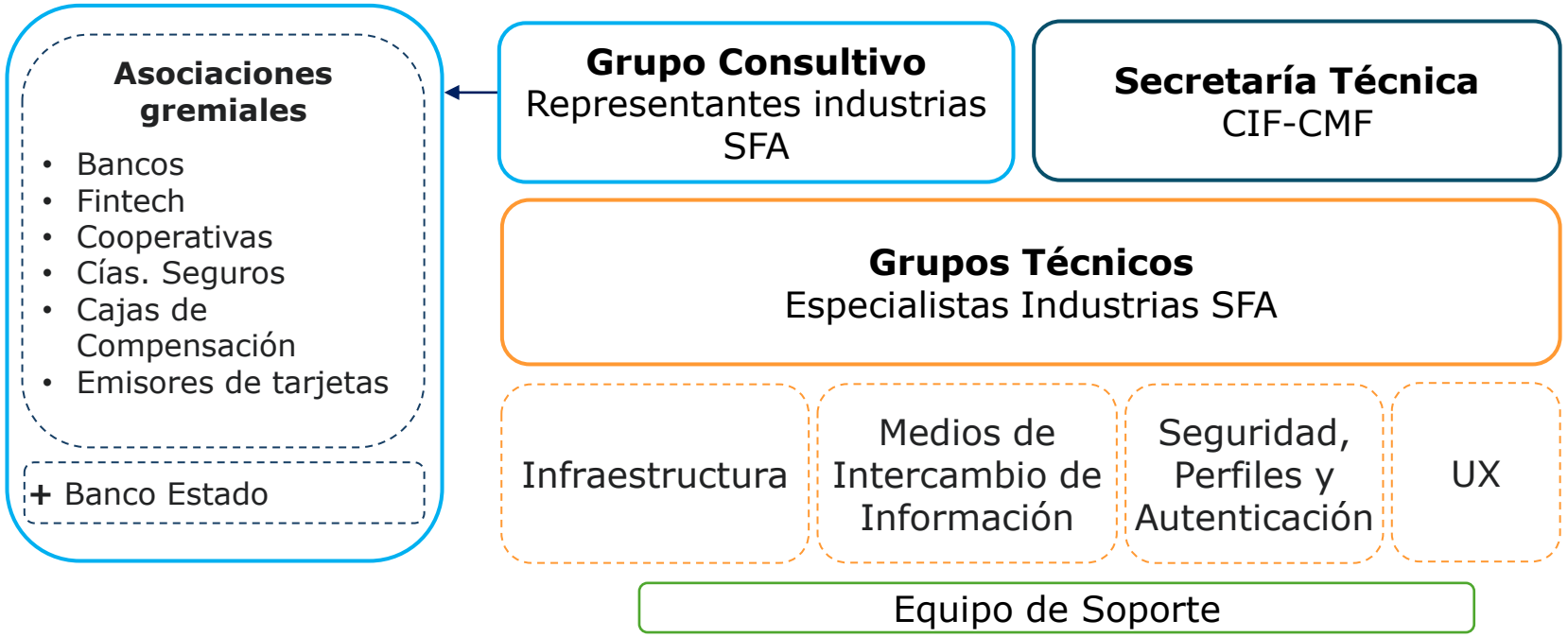
Desde publicada la Ley Fintec hemos trabajado fuertemente en su implementación

Sistema de Finanzas Abiertas



El trabajo del Foro del Sistema de Finanzas Abiertas ha sido clave para recoger las propuestas del mercado

Instancia consultiva, colaborativa y no vinculante a la CMF, cuyo objetivo es cooperar en el análisis y discusión de las materias y propuestas relativas al Sistema de Finanzas Abiertas, con el objeto de lograr un funcionamiento adecuado de este sistema.



El trabajo del Foro del Sistema de Finanzas Abiertas ha sido clave para recoger las propuestas del mercado

Se han recibido cinco entregables incrementales, con las materias que cubren los flujos de intercambio de información para personas naturales y jurídicas.

Las materias de Iniciación de Pagos serán abordadas en un entregable separado (entregado primera parte).

(*) N° de sesiones de los grupos

Entregable	Materia	Fecha
Etapa 0	Términos y Condiciones, y Canales de Atención	14-08-2024
Etapa 1	Información Persona Natural e información pública	17-10-2024
Etapa 2	Persona Natural	05-12-2024
Etapa 3	Flujos de solicitud de información de Datos Públicos, de Persona Natural y de Persona Jurídica	30-01-2025
Etapa 3.5	Cierre Flujos de Solicitud de Información de Datos Públicos, Persona Natural y Persona Jurídica	14-04-2025
Etapa 4	Iniciación de Pagos	24-07-2025

Se cumplió el hito de emitir la norma: NCG Nº514 - Regula la implementación del SFA

Secciones de la norma

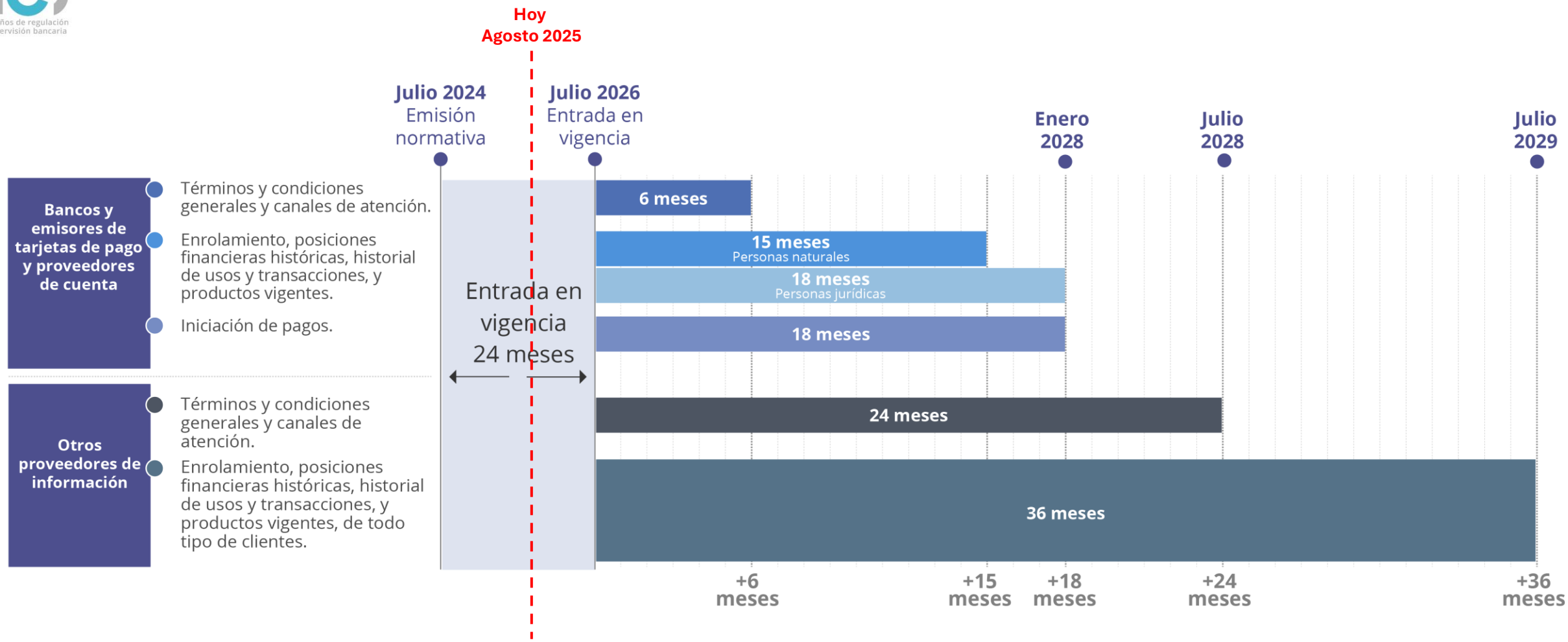
- Perímetro del Sistema de Finanzas Abiertas — I
- Funcionamiento del Sistema — II
- Seguridad y Resguardos del Sistema — III
- Información del Sistema — IV
- Otras Disposiciones — V

Anexos normativos

- 01 Variables para conjuntos de información del SFA
- 02 Productos del SFA
- 03 Anexo Técnico
- 04 Especificaciones técnicas para la distribución de costos

Estos Anexos serán desarrollado por la CMF durante el período para la entrada en vigencia de la norma.

Se estableció un calendario de implementación gradual en un horizonte de 5 años



Algunos elementos a destacar para resguardar el intercambio seguro y la interoperabilidad del SFA

Perímetro

Establece alcance y requisitos de participación en el SFA

Datos registrales de la sociedad, legales, plan de negocios, organigramas, gestión consentimiento, de datos personales, políticas de gestión, certificados perfiles seguridad, pruebas funcionales.

Medios de Intercambio de Información

APIs estandarizadas y con alta disponibilidad.

Incorporación de un mecanismo alternativo ante contingencias.

Datos

Define la taxonomía y conjunto de datos a compartir en el SFA

Información sin consentimiento (*T&C, Canales de atención)* y con consentimiento (*Identificación y registro*; *Condiciones comerciales y transacciones; e Iniciación de Pagos)*

Consentimiento

Establece la forma en que se deberá manifestar la voluntad.

Se establece el deber de los participantes de proveer un panel de control para que usuarios gestionen sus consentimientos.

Seguridad y resguardos

Gestión de riesgo, control interno, estándares de seguridad, ciberseguridad, continuidad del negocio, autenticación y verificación, interoperabilidad, entre otros.

Con el input del Foro se elabora Anexo 3, actualmente en consulta pública - Principales contenidos

Anexo 3

Infraestructura y Funcionamiento
Funcionamiento e informaciones del Directorio -
Existencia de múltiples marcas -
API del directorio -
Continuidad del Directorio -

Requerimientos de Seguridad
Perfil de seguridad FAPI 2.0 -
Certificación de OIDF -

Certificados Digitales de Identidad
Autoridades Certificadoras -
Certificados Digitales -
Validación de Firmas -
Registro Dinámico de Clientes -

Ambiente de Pruebas de la CMF y Certificados Funcionales
Pruebas funcionales IPI en ambiente CMF (Directorio)–
Pruebas funcionales PSBI en ambiente CMF –
Pruebas funcionales IPI y PSBI en ambiente no CMF -
Hitos para participar en Directorio y Sandbox -

Intercambio de Información
- Especificaciones, disponibilidad y rendimiento de APIs
- TPM y TPS
- Mecanismo alternativo
- Pruebas de calidad, marcha blanca y mantenciones
- Mecanismo de monitoreo

Consentimiento
- Generación y administración del consentimiento (RAR+GM)
- Autenticación del cliente por parte de la IPI

Portal Web de Desarrolladores
- Documentación Técnica
- Recursos para Desarrolladores
- Soporte y Comunidad
- Actualizaciones del Portal

Reportes
- Rep. de Incidentes Operacionales (RIO)
- Rep. de mantenciones
- Rep. de calidad de la información
- Rep. de disponibilidad y rendimiento
- Rep. de estado de actividad en el SFA para IPI y PSBI

Implementación de Mecanismo Alternativo (MA)

Las IPI/IPC deben implementar el MA de entrega de información, será **réplica funcional de la API Principal (MP)** y deberá cumplir con los requisitos de seguridad, interoperabilidad y especificaciones técnicas asociados.

El MA deberá

- Activarse cuando el mecanismo principal y su contingencia no estén disponibles.
- Ubicado de forma que no comparta los mismos riesgos que el MP y su contingencia.
- Aplican medidas de seguridad de RAN 20-7 de la Comisión.
- Tener su propio servidor de autorización (Sincronizado con el servidor de autorización del MP)
- Velar por el cumplimiento de FAPI 2.0 e identificadores de clientes OAuth (client_id).
- Las IPI serán responsables de establecer los mecanismos más adecuados dada su infraestructura, tales como acceso directo a *cores* de negocios, acceso a API intermedias, acceso a portales de información de clientes, entre otros.

- ELEMENTOS ATENUADOS DE EXIGIBILIDAD RESPECTO AL MP

Disponibilidad

- 90% diaria
- 95% mensual
- Base de cálculo diario de 24 horas
- Tiempo máximo de procesamiento: 5.000 milisegundos.

Actualización

- Hasta 60 minutos en promedio con respecto al mecanismo principal.

Generación y Administración del Consentimiento en línea con estándares internacionales

- La forma en que se generará y administrará el consentimiento en el SFA será mediante **Rich Authorization Requests (RAR) y Grant Management (GM) respectivamente. Para RAR la referencia es el RFC 9396.**

- PSBI/PSIP deben verificar y validar que quien otorgue el consentimiento (**mandato-PJ**) esté debidamente facultado para autorizar transmisión de datos o iniciación de pagos.
- IPI/IPC deberán cursar requerimientos de información con la sola autenticación del PSBI/PSIP y del usuario que se les indique.

- Consentimiento debe contener: tipo de información para la que autoriza, servicio que desea prestar, institución, período o frecuencia y finalidad, que debe ser clara y detallada.
- IPI/IPC pueden ofrecer en su interfaz selección de productos a los cuales acotar el intercambio o tratamiento.

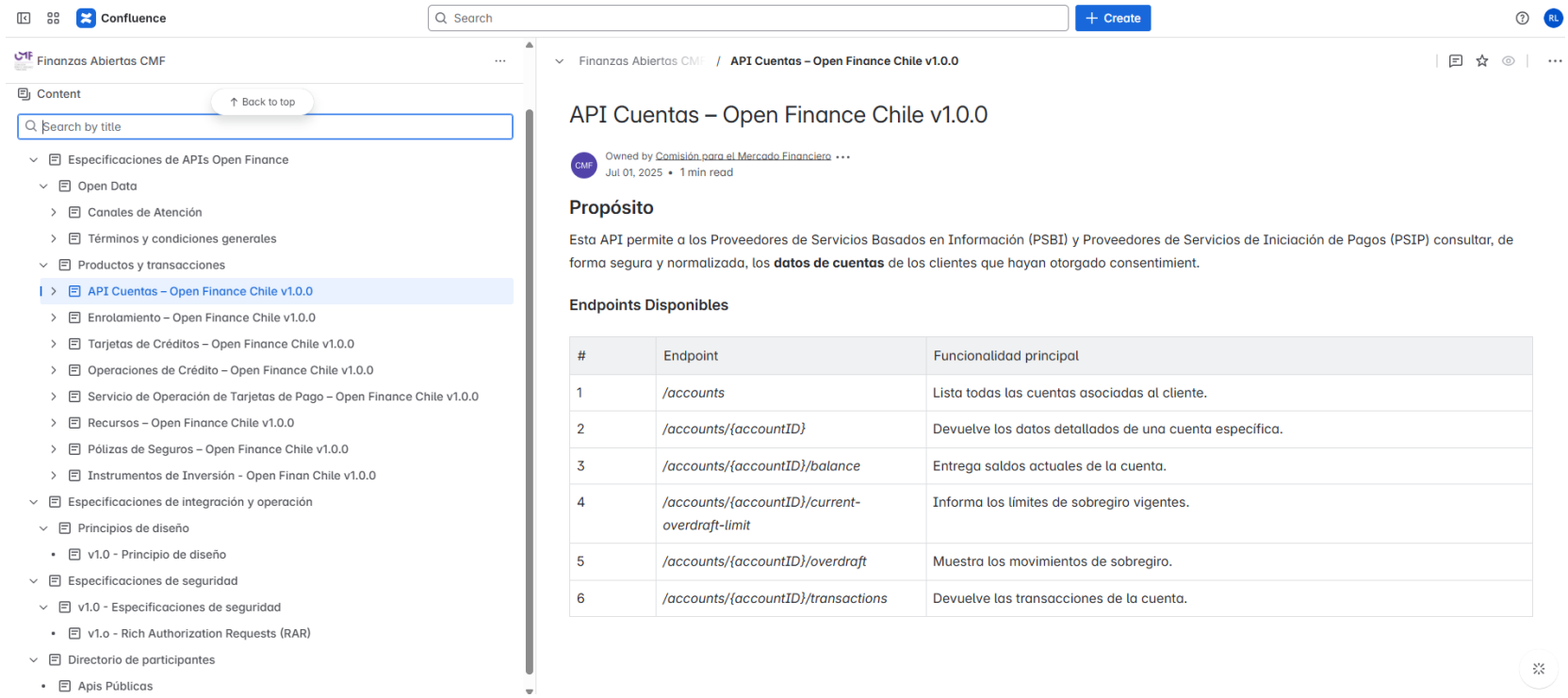
Los elementos técnicos de la Norma se publican en el Portal Desarrollador, para facilitar acceso a especificaciones técnicas a equipos de desarrollo de Participantes

Principales Contenidos

- **Documentación Técnica**
  - Estándares de desarrollos
  - Especificaciones de las API
  - Flujos de información/conexión

- **Operación**
  - Actores del SFA en Chile
  - Principios de Diseño
  - Modelos de gobierno

- **Soporte y Comunidad**
  - Q&A
  - Contacto de soporte técnico
  - Comunidad
  - Alertas en tiempo real



Los elementos técnicos de la Norma se publican en el Portal Desarrollador, para facilitar acceso a especificaciones técnicas a equipos de desarrollo de Participantes

Principales Contenidos

- **Documentación Técnica**
  - Estándares de desarrollos
  - Especificaciones de las API
  - Flujos de información/conexión
- **Operación**
  - Actores del SFA en Chile
  - Principios de Diseño
  - Modelos de gobierno
- **Soporte y Comunidad**
  - Q&A
  - Contacto de soporte técnico
  - Comunidad
  - Alertas en tiempo real

Application Programming Interfaces (APIs)

- **APIs Open Finances**
  - API Cuentas
  - Enrolamiento
  - Tarjetas de Crédito
  - Operaciones de Crédito
  - Servicio de Operación de Tarjetas de Pago
  - Recursos
  - Pólizas de seguros
  - Instrumentos de inversión
- **Directorio de Participantes**
  - APIs Públicas

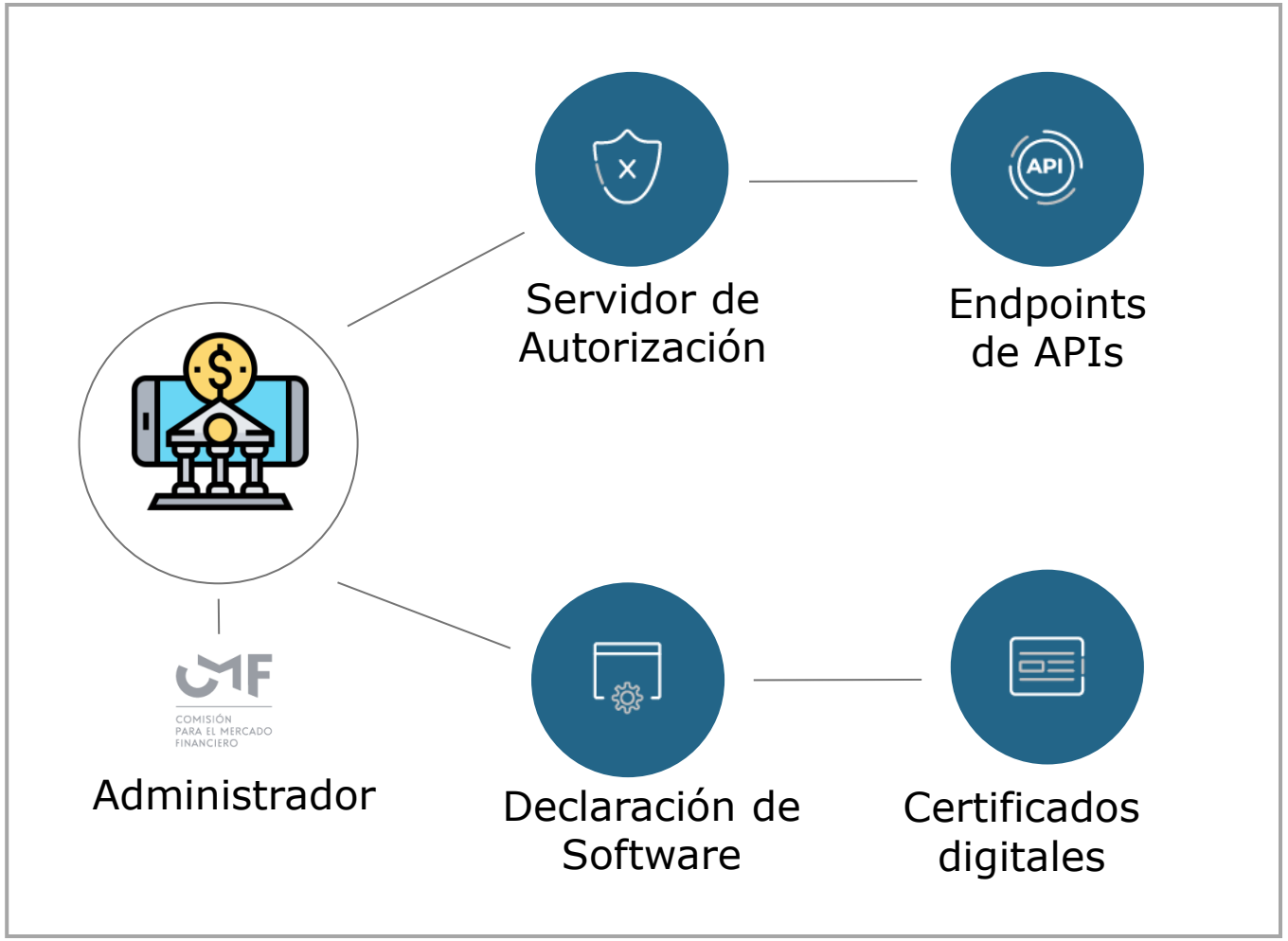
Especificaciones

- **Open Data**
  - Canales de Atención
  - Términos y condiciones generales
- **Integración y operación**
  - Principios de Diseño
- **Seguridad**
  - Seguridad y privacidad
  - Rich Authorization Requests (RAR)

Directorio de Participantes del SFA será gestionado por la CMF

→ Es un **registro centralizado** y regulado que identifica y organiza a las entidades que participan en el SFA.

→ Permite la **búsqueda, consulta y actualización de los participantes** habilitados en el SFA, incluyendo sus datos de registro, autorización, roles y perfiles, recursos de API, certificados digitales, entre otros.



El Sandbox Tecnológico se establece como el Ambiente de Pruebas, incluirá el Directorio y todas las APIs del SFA

Información Relevante:

- Acceso autorizado por la CMF (proceso de solicitud).
- Cumple con dos funciones:
  - ✓ Área de pruebas para procesos de certificación que deberán realizar los certificadores externos, y
  - ✓ Área para testeo de nuevos modelos de negocios de PSBI/PSIP.

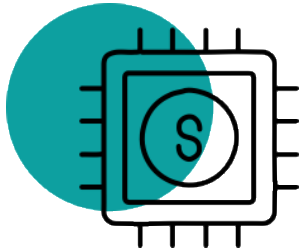
Hitos para participar del Directorio y Sandbox:

- Las IPI podrán participar del Sandbox desde que presentan su solicitud de inscripción en nómina como IPI.
- Los PSBI requerirán haber entregado los antecedentes solicitados por norma (1.2 y 1.2), previo a la incorporación a las pruebas funcionales en el Sandbox.

Requisitos para Entidades Certificadoras:

- Experiencia de al menos 3 años realizando pruebas tecnológicas
- Experiencia en APIs
- Experiencia en Ciberseguridad

	IPIs	PSBI
Dentro de Ambiente CMF	• Actualizar información en el Directorio (cambios de estados e información general). • Descarga del Directorio de prueba local. • Uso del sistema de mensajería en AP (ej: simular informar uso de mantenciones programadas).	• Uso de Directorio • Registro de Clientes de las PSBI en las IPI • Flujos de datos de términos y condiciones de las IPIs • Flujo de consentimiento • Obtención de datos personales de clientes
Fuera de Ambiente CMF	• Validación de Endpoints TyCs / Canales de Atención / Consumo de datos. • Simulación de registro de PSBI. • Flujo de entrega de Access token a PSBI en nombre de un usuario real. • Validación de Access token emitido para consultar información. • Pruebas funcionales Panel de Control. • Pruebas de Mecanismo Alternativo.	• Realización de pruebas sobre los paneles de control de consentimiento.



Ley de Fraudes

La evolución de los medios de pago y sus riesgos, ha llevado a ajustar el marco legal aplicable

- Limita responsabilidad de los usuarios post-aviso.
- Considera solo fraudes con tarjeta presente

- Incluye fraudes electrónicos y medios de pago en general
- Cambia el estándar probatorio a culpa grave o dolo

- Otorgar mayores herramientas para investigar casos con indicios de autofraude, negligencia, o comportamiento oportunista

La Ley 21.763 otorga mayores herramientas para detectar casos de autofraude, negligencia y comportamientos oportunistas

	Anterior a la modificación	Posterior a la modificación
Antigüedad de operaciones que pueden reclamarse (días)	120	60
Plazo para recibir el reintegro de los fondos (días hábiles)	5	10-15
Requiere declaración jurada	No	Sí
Requiere denuncia formal	No	Sí
Umbral, de restitución de fondos	Legalmente, en 35 UF	A través de reglamento de Mindha, actualmente en 35 UF.
Garantía de restitución de fondos	Debe restituir al menos el monto hasta el umbral, sin perjuicio de poder iniciar acciones judiciales.	Si la entidad tiene antecedentes de dolo o culpa grave, puede suspender el pago, lo que luego debe ser confirmada por JPL

Implementación se encuentra en proceso

- **Fijación de umbrales (Art. 5 Ley 20.009)**
  Reglamento Min. Hacienda, Min Economía, previa consulta a la CMF; Revisión anual.
  Diciembre 2024: Se mantuvo el umbral de UF 35

- **Repositorio de sentencias (Art. 5 quáter Ley 20.009)**
  NCG 523 de fecha 29/11/2024
  Vigencia: Reporte mensual a partir de los primeros 5 días hábiles del mes de julio de 2025

- **Norma de fijación de estándares (Art. 4 Ley 20.009)**
  NCG 538 de fecha 17/06/2025
  Vigencia: 1 agosto de 2025, excepto en lo relacionado a casos de uso obligatorio de autenticación reforzada, cuya vigencia es desde julio de 2026

- **Información para fines de fiscalización y estadísticas (Art. 11 Ley 20.009)**
  Modificación Archivo Normativo E24
  NCG 539 de fecha 30/06/2025

Cambio significativo en solicitudes de restitución, afectando tanto a usuarios como a instituciones financieras

Drástica reducción de solicitudes de restitución

- Caída sustancial en el número y montos reclamados post-ley.
- Las nuevas exigencias (declaración jurada, denuncia formal, menor plazo) han desincentivado conductas oportunistas.

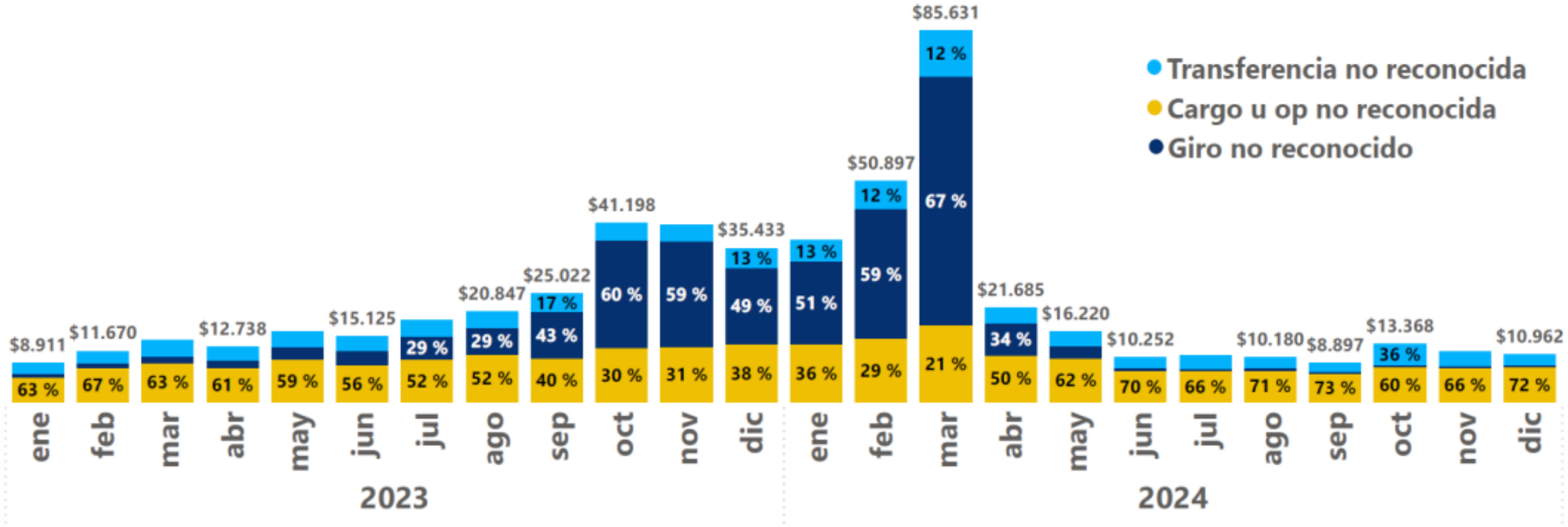
Cambio en el perfil de las solicitudes: monto y tipo de operación

- Las solicitudes se concentran en operaciones de mayor monto promedio.
- Solicitudes de restitución por giros no reconocido de cajeros automáticos dejan de ser preponderantes tras ley.
- Los montos asociados a usuarios reincidentes caen.

Sin embargo, los reclamos de clientes a CMF tras solicitudes de restitución han aumentado.

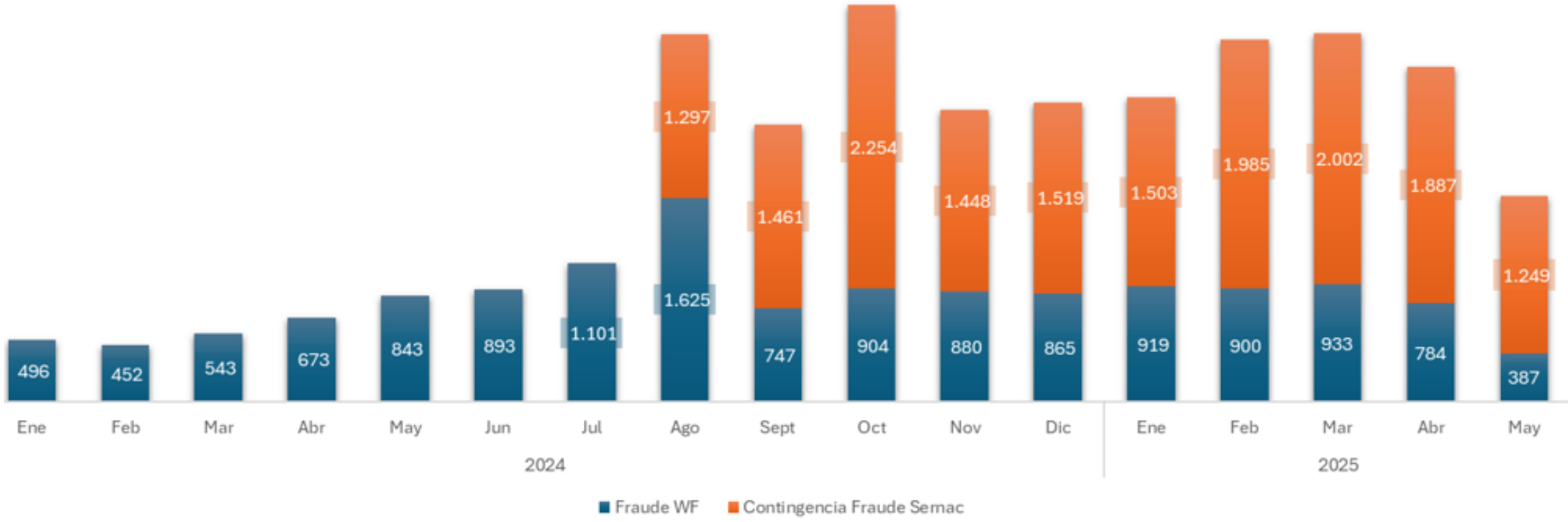
Caída importante de reclamos por fraude, en particular giros no reconocidos de cajeros automáticos

Solicitudes de restitución por mes: Montos impugnados por tipo de operación
(millones de pesos)



Fuente: CMF

Por otro lado, los reclamos de clientes a CMF tras solicitudes han aumentado



Fuente: CMF

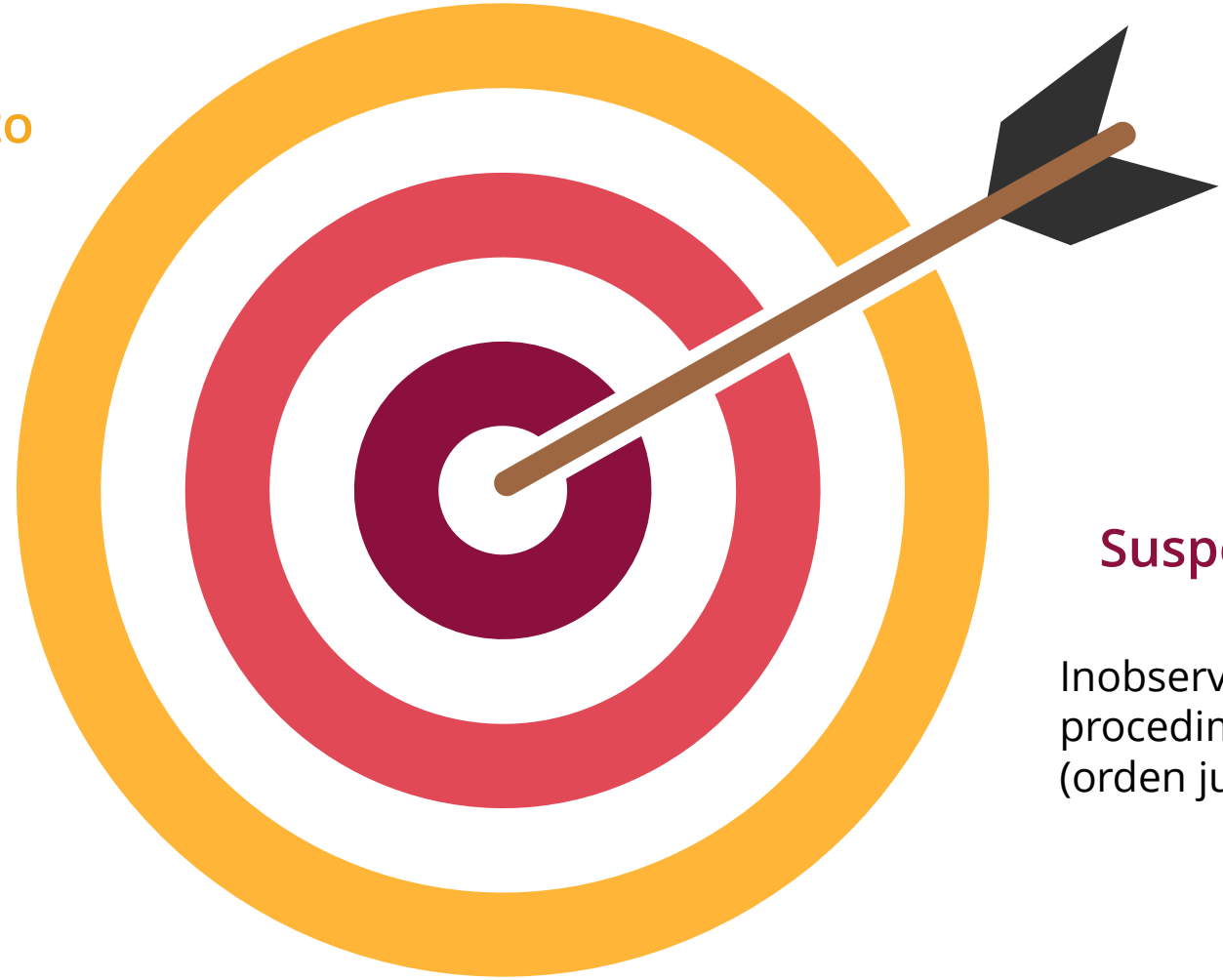
Reclamaciones: Principales focos de supervisión

Gestiónde desconocimiento de operaciones

Rechazos por aspectos formales: plazos aviso, declaración jurada, denuncia judicial

Restitución

Cumplimiento oportuno deber de conducta IFIS: Abono normativo o inicio de acciones legales.



Suspensión

Inobservancia del procedimiento legal (orden judicial)

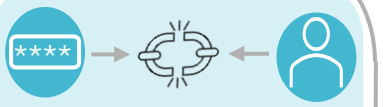
NCG 538: Medidas de seguridad, registro y autenticación de operaciones sometidas a la ley N°20.009

Objetivo: Cumplir con lo dispuesto en la Ley 20.009, en la que se establece que la Comisión determinará los supuestos de uso y transacciones en que resulte obligatorio por parte del emisor el uso de autenticación reforzada de clientes (ARC).

Definición de Autenticación Reforzada de Clientes (ARC): Procedimiento de autenticación basado en la utilización de al menos dos factores independientes y de diferentes categorías, entre 3 dimensiones:

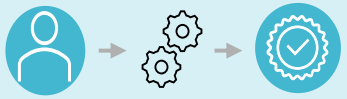
* La ARC con un factor de inherencia, podrá usarse como presunción de dolo o culpa grave. Si solo incluye factores de posesión y conocimiento, se puede usar como base de presunción judicial.

NCG 538: Robustez, independencia y diferenciación. Los emisores deben garantizar:



Los factores de autenticación sean **independientes**, de modo que la vulneración de uno de los factores **no comprometa** la **confiabilidad** y **seguridad** del otro.

Los elementos basados en **conocimiento** consideran medidas que permiten su **bloqueo** y **restablecimiento,** ante un potencial compromiso de la respectiva pieza de información.

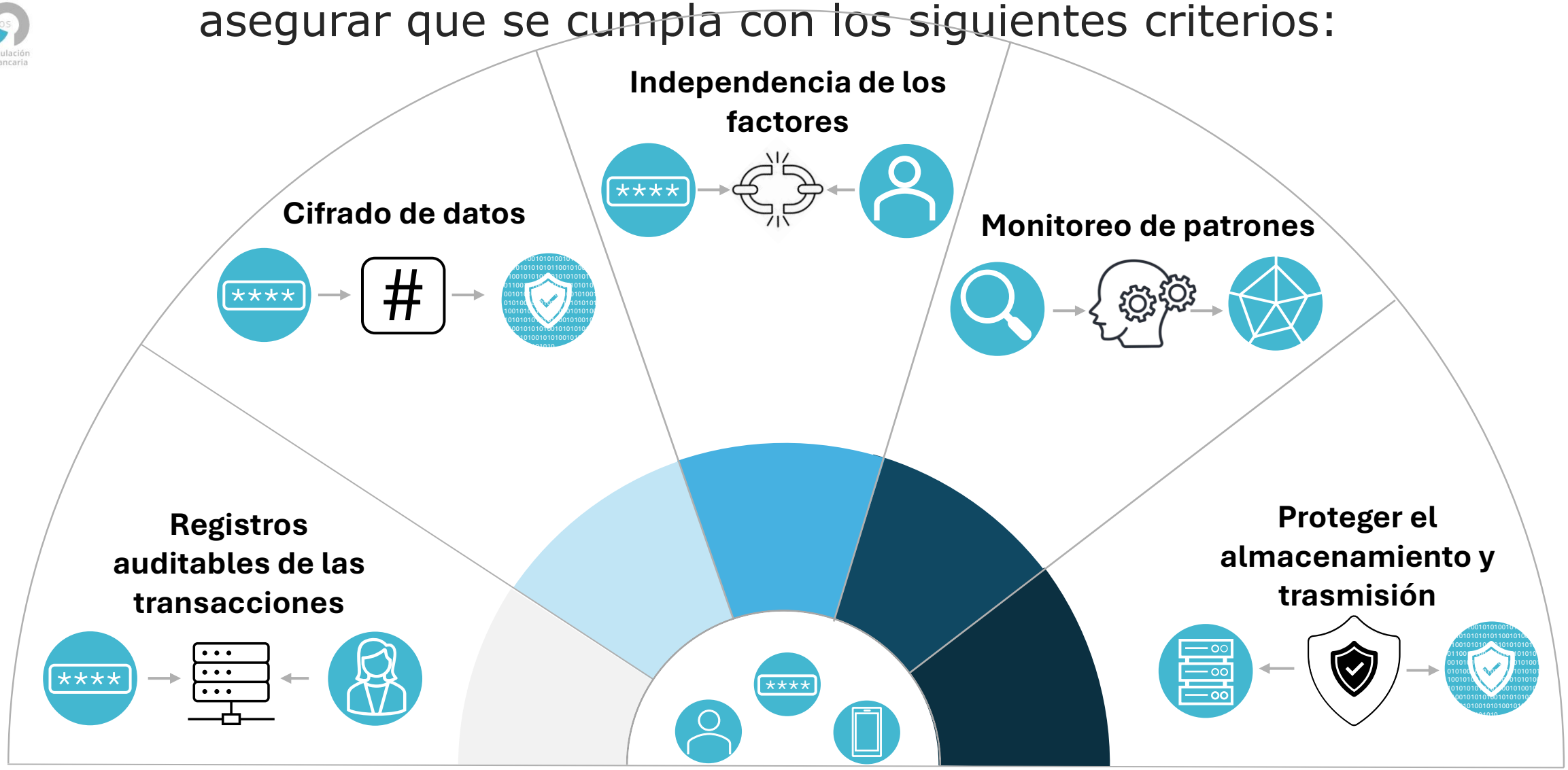


Respecto de **inherencia,** conocen y se han interiorizado adecuadamente acerca del **funcionamiento interno** y **nivel de confianza** de los factores implementados.

Los **dispositivos** que se **proporcionan** para la autenticación reforzada **deben poseer mecanismos** de detección de **manipulación** o **clonación**.

Se debe eliminar el uso de mecanismos que incorporen **conjuntos** de **datos impresos** utilizados para la autenticación.

NCG 538: Requisitos generales. Los emisores deben asegurar que se cumpla con los siguientes criterios:



NCG 538: Casos de aplicación obligatoria de ARC

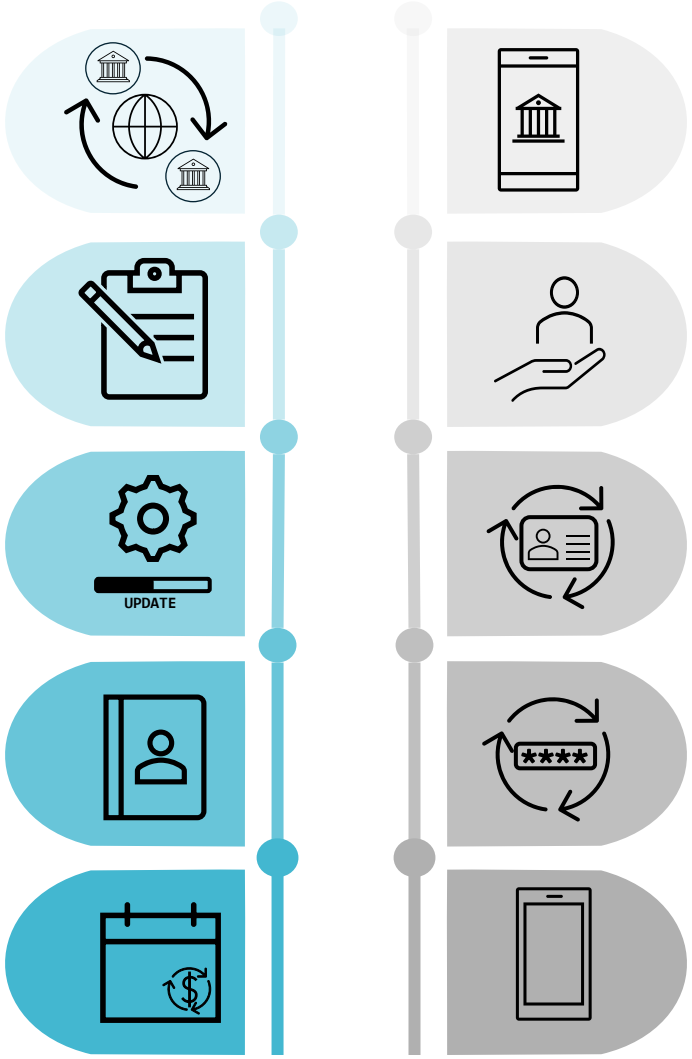
TRANSFERENCIA ELECTRÓNICA DE FONDOS

01. Solicitudes

02. Modificaciones

03. Información asociada a destinatarios

04. Pagos recurrentes



PLATAFORMAS DIGITALES

05. Proceso de incorporación del cliente

06. Modificación de datos personales

07. Modificación de claves de autenticación

08. Incorporación de dispositivo de confianza y su reemplazo o eliminación

COMISIÓN PARA EL MERCADO FINANCIERO

100 años de regulación y supervisión bancaria

Palabras finales

Palabras finales

- En SFA , hemos avanzado de acuerdo con el calendario publicado.

- Aún existen desafíos que ir abordando desde la CMF y con los participantes del SFA:
  - Avances en emisión de normativa complementaria del SFA: Anexo 3 y 4, normas de información para supervisión, monitoreo continuo y análisis de participantes del SFA.
  - Pruebas del Sandbox Tecnológico y el Directorio.
  - Cumplimiento de requerimientos de APIs regulatorias, requisitos de seguridad, certificaciones, entre otros, por parte de los participantes.
  - Potenciar el trabajo del Foro del SFA y el ecosistema financiero para construir un SFA robusto, interoperable y valioso para los usuarios.
  - Comunicar de manera efectiva los beneficios del SFA a los usuarios finales, empoderarlos en el uso de sus datos y fomentar decisiones financieras informadas.

- Las cifras indican que los casos de **fraude** han disminuido. Esperamos que Ley y su normativa permita disminuir aún más los casos.

- Con todo, la educación que entregan los proveedores a los clientes sobre estos temas es condición necesaria para avanzar en el buen uso de los medios de pagos.

100 años de regulación y supervisión bancaria

COMISIÓN PARA EL MERCADO FINANCIERO

Reunión de Gerentes de la ABIF

Avances en implementación regulatoria: SFA y Ley de Fraudes

Solange Berstein J.
Presidenta, Comisión para el Mercado Financiero

Agosto 2025

NCG 538: Preguntas (1)

Q ¿Cuál es la responsabilidad de los usuarios respecto de esta normativa?

A Respecto a la gestión de seguridad: usar claves seguras, mantener sus claves, datos y otros factores de autenticación actualizados, eliminar dispositivos de confianza que ya no usa, no compartir claves ni otros factores de verificación con terceros, usar dispositivos de confianza seguros.

Q ¿Qué es un dispositivo de confianza?

A Es un dispositivo electrónico reconocido por el propio usuario ante el emisor como tal y debe haber cumplido con un proceso de enrolamiento a través de ARC.

NCG 538: Preguntas (2)

Q ¿La **NCG 538** dispone algún criterio respecto a las contraseñas incluidas en el factor de conocimiento?

A La norma define que todo lo relacionado con contraseñas como exigencias de **actualización**, **longitud**, **complejidad**, **reutilización** y **previsibilidad** de claves, serán los emisores quienes deban establecer exigencias, siempre considerando que estas no sean contraproducentes para velar por la seguridad de éstas.

Q ¿Se considera la tarjeta de coordenadas un conjunto de datos impresos?

A Sí.

NCG 538: Preguntas (3)

Q ¿Se podrá realizar ARC en casos no considerados obligatorios?

A La norma considera que el emisor **siempre podrá utilizar ARC** en cualquier operación que lo **considere necesario**, en línea con su marco de gestión de riesgos. Lo anterior le permitiría utilizar lo dispuesto en el literal h) del articulo 5ter de la ley N°20.009.

Q ¿Los *log* que se generan en el proceso de autenticación, pueden ser considerados como códigos de autenticación?

A No pueden ser considerados, ya que tienen una funcionalidad diferente, los *log* tienen una **naturaleza de registro**, en cambio los códigos de autorización en su mayoría encriptados, tienen una naturaleza de **validación de la operación**. En general los códigos de autenticación tienen **informacion de la operación** básica, como la fecha de la operación o la cuenta de destino y el monto en el caso de transferencias. Estos además tienen una **duración y alcance limitado**.

NCG 538: Preguntas (4)

Q ¿Qué es un mecanismo que detecte la manipulación o clonación de un dispositivo utilizado para ARC?

A La norma define que todo dispositivo entregado por el emisor tendrá que contar un mecanismo que detecte si este ha sido manipulado o clonado. Lo anterior considera mecanismos preventivos ante manipulaciones y de validación que los dispositivos realmente sean aquellos que fueron entregados por el emisor y no corresponda a un reemplazo.

Q ¿Cuál es el plazo de implementación de la norma?

A La presente norma entre en vigor a partir del **1 de agosto de 2025**, excepto respecto de los casos de ARC obligatoria, cuya vigencia comenzará el **1 de julio de 2026**.