COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Informe Normativo:

NORMAS SOBRE MEDIDAS SEGURIDAD Y AUTENTICACIÓN DE OPERACIONES SOMETIDAS A LA LEY N°20.009

Abril 2025

www.CMFChile.cl

Índice Informe Normativo

I. INTRODUCCIÓN

Con fecha 30 de mayo de 2024 se publicó en el Diario Oficial la Ley N°21.673 en virtud de la cual se "adoptan medidas para combatir el sobreendeudamiento", a través de la incorporación de una serie de modificaciones a diversos cuerpos legales. En particular, conforme con el artículo 4° de la referida ley, se introducen modificaciones de naturaleza tanto sustantiva como procedimental a la Ley N°20.009 que "*estable el régimen de responsabilidad de los titulares o usuarios de tarjetas de pago y transacciones electrónicas, en caso de extravío, hurto, robo y fraude*", disponiéndose el ejercicio de facultades instructivas de esta Comisión en determinados aspectos necesarios para la adecuada implementación de los cambios legales respectivos.

Esta Comisión, con fecha 29 de noviembre de 2024 dictó la Norma de Carácter General N°523, que contiene instrucciones para el envío de solicitudes y resoluciones judiciales asociadas a los procedimientos judiciales de la Ley N°20.009, en ejercicio de lo dispuesto en el artículo 5 quáter de dicho cuerpo legal.

A su turno, con fecha 17 de diciembre de 2024 fue publicado en el Diario Oficial el Decreto Exento N°435 del Ministerio de Hacienda, suscrito de forma conjunta con el Ministerio de Economía, Fomento y Turismo, que determina los umbrales de restitución aplicables conforme lo dispone el artículo 5° de la ya referida Ley N°20.009.

Teniendo en consideración las disposiciones de normativa secundaria y reglamentaria antes indicadas, la presente propuesta normativa, de conformidad con lo dispuesto en el inciso noveno del artículo 4 de la Ley N°20.009, desarrolla las instrucciones que deberán someterse los emisores de tarjetas de pago y demás prestadores financieros de sistemas de transacciones electrónicas, en lo que respecta a los sistemas de autenticación de transacciones, incluyendo las operaciones que deberán de forma obligatoria someterse a esquemas de autenticación reforzada de clientes ("ARC").

II. OBJETIVOS DE LA PROPUESTA NORMATIVA.

Conforme se indica en el inciso noveno del artículo 4 de la Ley N°20.009, esta Comisión, mediante la dictación de una norma de carácter general, establecerá "*estándares mínimos de seguridad, registro y autenticación. A través de la referida norma de carácter general, la Comisión determinará los supuestos de uso y transacciones en que resulte obligatorio por parte del emisor el uso de autenticación reforzada*".

A su turno, y acto seguido, el inciso décimo del referido artículo indica que *para estos efectos, se entenderá por autenticación el procedimiento que permita al emisor comprobar la identidad del usuario o la validez de la utilización de un medio de pago, incluida la utilización de credenciales de seguridad personalizadas del usuario, y por autenticación reforzada, la utilización de al menos dos factores de autenticación, sea de conocimiento, posesión o inherencia, diferentes e independientes entre sí, para el acceso o utilización de los medios de pago, cuentas o sistemas similares que permitan efectuar pagos o transacciones electrónicas".*

Consecuente, es deber de esta Comisión impartir normativa secundaria que regule para los diversos medios de pago y emisores que da cuenta los artículos 1° y 2° de la Ley N°20.009, en cuanto se encuentren previamente sometidos a su perímetro regulatorio, en los siguientes aspectos:

1. Estándares mínimos sobre seguridad, registro y autenticación de transacciones.
2. Estándares asociados a la autenticación reforzada de clientes.
3. Determinación de supuestos de uso y transacciones que resulte obligatorio el uso de ARC por parte del respectivo emisor.

III. RECOMENDACIONES Y EXPERIENCIA INTERNACIONAL

Se consideró principalmente la Directiva Europea (PSD2).

Es la directiva vigente que regula pagos en la unión europea, vigente desde 2018. En este cuerpo legal se incluye la posibilidad de que los bancos puedan prestar servicios de terceros, regula el funcionamiento de servicios de iniciación de pagos y los servicios de información de cuentas.

Para estos fines introduce nuevos requisitos de seguridad, entre ellos la autenticación reforzada de clientes (ARC). Establece la necesidad de contar con dos factores de autenticación en operaciones que antes no lo requerían. Lo anterior se traduce por ejemplo en el remplazo de las tarjetas de coordenadas, o la exención de requisitos de seguridad en operaciones de bajo riesgo.

IV. PROPUESTA NORMATIVA

Esta Comisión, en uso de las facultades que le confieren los artículos 1, 3, 5 en sus numerales 1, 8 y 18, y 20 en su numeral 3 del Decreto Ley N°3.538, el artículo 4 de la Ley N°20.009, y lo acordado por el Consejo de la Comisión en Sesión Extraordinaria/Ordinaria N°XXXX de XXX de XXX de 2025, ha estimado

pertinente impartir las siguientes instrucciones relativas a estándares mínimos de seguridad y de autenticación a los bancos, sociedades de apoyo al giro, empresas emisoras de tarjetas de pago y cooperativas de ahorro y crédito fiscalizadas por esta Comisión.

1. Disposiciones Generales

Objeto y ámbito de aplicación

La presente Norma de Carácter General establece los estándares mínimos de seguridad, registro y autenticación aplicables a los emisores de medios de pago y prestadores de servicios financieros (en adelante, "Emisores" conforme con lo dispuesto en el artículo 2° de la Ley N°20.009) sujetos a la fiscalización de la Comisión para el Mercado Financiero (en adelante, "la Comisión"). Asimismo, determina los supuestos de uso y transacciones en los cuales es obligatorio implementar mecanismos de autenticación reforzada.

Definiciones

Para los efectos de la presente norma, se entenderá por:

1. **Autenticación**: Procedimiento que permita al emisor comprobar la identidad del usuario o la validez de la utilización de un medio de pago, incluida la utilización de credenciales de seguridad personalizadas del usuario
2. **Autenticación reforzada de cliente o ARC**: Procedimiento de autenticación basado en la utilización de al menos dos factores de autenticación independientes y diferentes entre sí (de dos categorías diferentes) con características de seguridad adecuada[1][2], para el acceso, contratación o utilización de los medios de pago, cuentas o sistemas similares que permitan efectuar pagos o transacciones electrónicas[3]. Los factores de autenticación deben pertenecer a las siguientes categorías:

[1] véase Art 5 Reglamento delegado 2018/398 de la Comisión Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32018R0389

[2] véase como ejemplo la discusión de NIST sobre la seguridad de las contraseñas. https://pages.nist.gov/800-63-4/sp800-63b/passwords/

[3] Véase la guía del NIST en draft sobre Identidad Digital. https://pages.nist.gov/800-63-4/

a) **Conocimiento**: Algo que solo el usuario conoce (por ejemplo, contraseñas o números de identificación personal o PIN).

b) **Posesión**: Algo que solo el usuario posee (por ejemplo, un dispositivo *token* o un mensaje enviado a un dispositivo confiable previamente registrado).

c) **Inherencia**: Algo que el usuario es (por ejemplo, biometría facial, huella dactilar, o datos biométricos conductuales, tales como ritmo de tecleo o dinámica de uso del dispositivo).

3. **Código de Autenticación:** Elemento informático de carácter único y diferenciable, generado como resultado de la aplicación exitosa de los respectivos factores o elementos de autenticación empleados en el marco de un procedimiento de autenticación de transacciones, incluyendo ARC, que permiten al Emisor generar o cursar la orden de pago respectiva.

2. Estándares Mínimos de Seguridad y Registro

Requisitos generales

Los Emisores deben velar por la integridad, confidencialidad y disponibilidad de los sistemas de pago, en los componentes y elementos de infraestructura de los cuales estos participan, mediante la implementación de medidas de seguridad adecuadas, incluyendo:

- Mecanismos de cifrado y protección de datos sensibles.
- Registros auditables y trazables de todas las transacciones y eventos de autenticación, incluyendo los intentos o peticiones fallidas con los respectivos códigos de error o información de depuración.
- Monitoreo continuo de patrones de transacciones para detectar posibles fraudes.
- Implementación de medidas que aseguren la independencia y diferenciación de los factores de autenticación utilizados.
- Medidas de protección para el almacenamiento y transmisión de los respectivos códigos de autenticación, muy especialmente cuando estos tienen como orígenes dispositivos capaces de múltiples funciones y operaciones (p.ej. teléfonos inteligentes). Será obligación de los Emisores disponer medidas adecuadas en materia de caducidad y expiración de códigos de autenticación ante eventos tales como recurrencia de eventos fallidos o transcurso de tiempo razonable de vida útil.

Criterios de robustez, independencia y diferenciación de factores

Los Emisores deberán garantizar que:

- Los factores de autenticación empleados sean inherentemente distintos en su naturaleza y no dependan de un mismo canal o dispositivo para su generación y validación. En caso de que los factores de autenticación se suministren al cliente a través de un mismo dispositivo, como en el caso de la interacción de biometría de plataformas móviles y claves de un solo uso a números telefónicos (p. ej. SMS OTP), deberán disponer las medidas lógicas y operativas necesarias para que la vulneración de uno de los factores no comprometa la confiabilidad y seguridad del otro.
- Las medidas de autenticación no sean reutilizables ni predecibles, evitando el uso de mecanismos estáticos.
- Los dispositivos utilizados para la autenticación reforzada posean mecanismos de detección de manipulación o clonación.
- Los factores categorizados como de posesión contienen elementos que impiden o repudian el uso de terceros o la replicación de estos o de los datos incorporados en este.
- Los dispositivos confiables han sido registrados bajo procedimientos rigurosos que garantizan la acreditación de titularidad y posesión.
- Los elementos basados en conocimiento consideran medidas que permiten su actualización, cambio, bloqueo o reemplazo ante diversas hipótesis que impliquen el potencial de compromiso de la respectiva pieza de información. Adicionalmente, los Emisores deberán establecer exigencias de actualización, longitud y complejidad de claves de forma que los usuarios no eludan estas restricciones de forma contraproducente.
- Los emisores conocen y se ha interiorizado adecuadamente acerca del funcionamiento interno y nivel de confianza de los factores categorizados como inherencia que éste haya implementado, tanto aquellos que se encuentren bajo su control o gestión directa, como aquellos en que la verificación biométrica resulta delegada a terceros, siendo siempre y en todo caso el Emisor el responsable sobre los mecanismos que ha dispuesto para ser utilizados por sus usuarios y clientes.

3. Supuestos de Uso de Autenticación Reforzada de Clientes

Casos de aplicación obligatoria ARC

El uso de autenticación reforzada es obligatorio en los siguientes casos:

- Acceso a plataformas de banca en línea o sus similares (personas y empresas) y aplicaciones móviles que permitan la gestión de pagos y de todas aquellas transacciones establecidas como casos de aplicación en esta sección.
- Solicitudes de modificación de datos personales o credenciales de autenticación del cliente. Validación de dispositivos de confianza.
- Solicitudes de incorporación de destinatarios frecuentes o enrolamiento de comercios u otra de clase de beneficiarios para pagos recurrentes.
- Gestión de pagos o transacciones que impliquen movimiento de fondos presentes o futuros de manera electrónica, incluyendo la contratación de servicios.
- Cualquier acción que pueda generar un fraude en el pago, como el caso de operaciones consideradas atípicas dentro del comportamiento del usuario.

Excepciones

Se exceptúa la obligación de autenticación reforzada en los siguientes casos:

- Operaciones de pago de bajo monto o importe, que por su nivel de riesgo sea considerado aceptable en las políticas de riesgo de los emisores. Este monto no puede superar los 20 mil pesos o su equivalente en moneda extranjera por cada transacción y 80 mil como importe acumulado diario total.
- Pagos recurrentes a beneficiarios particulares por montos y periodicidad predefinidos por el usuario, tales como pagos automáticos de servicios transferencias de fondos programadas, siempre que hayan sido validados previamente, al momento de originarse la recurrencia o suscribirse el respectivo plan de pagos, mediante ARC conforme se indica en el subtítulo precedente.
- Autenticaciones realizadas en dispositivos de confianza previamente registrados por el usuario y validados mediante ARC.

- Transacciones realizadas en terminales desatendidos de servicios de estacionamientos, transporte y máquinas expendedoras.
- Transferencias de fondos e importes de crédito entre cuentas del mismo titular en los respectivos Emisores, distintas de la contratación o cancelación de productos.

4. Responsabilidad y Sanciones

Responsabilidad de los Emisores

Conforme lo dispone el inciso final del artículo 4 de la Ley N°20.009, los emisores serán responsables de los perjuicios causados a los usuarios por incumplimiento de los estándares de seguridad, registro y autenticación establecidos en la presente norma.

Supervisión y sanciones

La Comisión fiscalizará el cumplimiento de la presente norma y podrá imponer sanciones a quienes infrinjan los deberes en esta indicados, conforme con las reglas establecidas en el Título III del DL N°3.538, de 1980.

V. EVALUACIÓN DE IMPACTO

Si bien el costo de implementar las medidas establecidas en esta norma pudiera ser alto, permiten robustecer la seguridad de las transacciones financieras y, por ende, la confianza de los usuarios en el sistema.

Adicionalmente, la existencia de medidas de seguridad, registro y autenticación robusta permiten disminuir las sospechas de autofraude, lo que facilita la interacción entre entidades financieras y sus clientes.

En la actualidad, las instituciones emisoras utilizan una gran diversidad de mecanismos de autenticación en las transacciones de sus clientes, con distintos grados de seguridad y complejidad. Por ejemplo, utilizan mecanismos de autenticación biométrica, principalmente de manera complementaria o para el ingreso ciertas soluciones; autenticación por capas y en algunos casos medidas de seguridad adicionales basadas en comportamiento.

Esta diversidad en la aplicación de soluciones, su profundidad y uso, además, se aplica para la definición de capas de seguridad o autenticación diferenciada,

dependiendo de los casos de uso, periodicidad, canales de atención y tipo de usuarios. Y la mayoría de las instituciones implementan múltiples métodos de autenticación en conjunto.

El objetivo de esta norma es establecer estándares mínimos en el uso de mecanismos de seguridad y su uso.

VI. PLAZO DE IMPLEMENTACIÓN

La presente propuesta normativa entrará en vigor el XXXXX 2025. Las instituciones deberán ajustar sus procedimientos y medidas de seguridad y autenticación asociadas a medios de pago y transacciones electrónicas dentro del plazo de 1 año desde dictada la presente norma, debiendo informar a la Comisión en un plazo no superior a 90 días desde su entrada en vigor, el respectivo plan de adecuación de sus procedimientos y sistemas, incluyendo definición de hitos, plazos y elementos físicos y lógicos involucrados o impactados.

VII. REFERENCIAS

- Guía de Identidad Digital, NIST en draft. https://pages.nist.gov/800-63-4/
- PSD2. DIRECTIVA (UE) sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n o 1093/2010 y se deroga la Directiva 2007/64/CE. 25 de noviembre 2015. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32015L2366
- PSD3. Propuesta relativa a los servicios de pago y los servicios de dinero electrónico en el mercado interior y por la que se modifica la Directiva 98/26/CE y se derogan las Directivas (UE) 2015/2366 y 2009/110/CE. 28 de junio 2023. https://eur-lex.europa.eu/resource.html?uri=cellar:e09b163c-1687-11ee-806b-01aa75ed71a1.0007.02/DOC_1&format=PDF
- Q&A. EBA aclara la aplicación de fuertes requisitos de autenticación del cliente a carteras digitales. 31 de enero de 2023. https://www.eba.europa.eu/publications-and-media/press-releases/eba-clarifies-application-strong-customer-authentication
- Reglamento delegado 2018/389 (RTS SCA) https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32018R0389

COMISIÓN
PARA EL MERCADO
FINANCIERO

Regulador y Supervisor Financiero de Chile

www.cmfchile.cl