COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Informe Normativo:

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

Septiembre 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 modificaciones a diversos cuerpos legales.

En particular, conforme con el artículo 4° de la referida ley, se introdujeron modificaciones de naturaleza tanto sustantiva como procedimental a la Ley N°20.009, la cual "*establece 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 algunos 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.

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 determinó 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 la 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 a las 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 (en adelante, "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, debe establecer "*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*".

En el inciso décimo del referido artículo se 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.

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

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

III. MARCO NORMATIVO

- **Ley N°20.009**, que establece un régimen de limitación de responsabilidad para titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude. En su art. 4, inciso 9 señala: *"La Comisión para el Mercado Financiero, mediante 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."*

- **Ley N°21.673**, publicada el 30.05.2024, señala que lo dispuesto en los incisos noveno, décimo y final, del art. 4 de la ley N°20.009, comenzará a regir al momento de la publicación de las referidas normas de carácter general por parte de la Comisión para el Mercado Financiero, las que deberán ser dictadas dentro de los doce meses siguientes a la publicación de dicha ley.

- **Capítulo 8-41 de la RAN** sobre Tarjetas de Pago, en su numeral 4.2 donde se establecen los requisitos mínimos de transferencia electrónica de fondos para Cuentas con Provisión de Fondos.

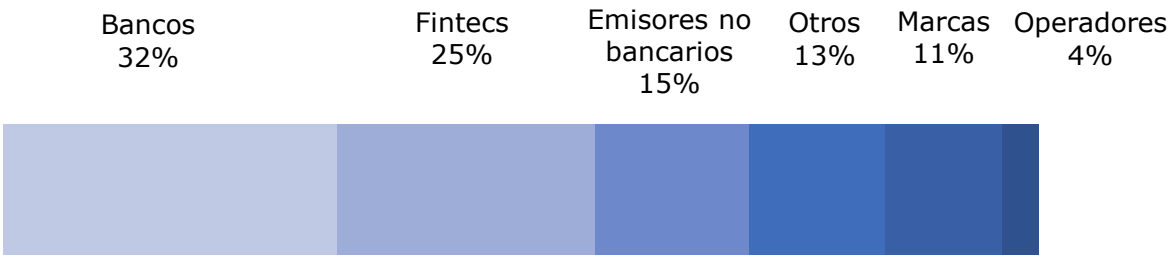
- **Capítulo 1-7 de la RAN** relativo a Transferencia Electrónica de Fondos, establece los requisitos mínimos que deben cumplir los sistemas utilizados, entre los cuales se encuentran requisitos de seguridad que garanticen que las operaciones sólo puedan ser realizadas por personas debidamente autorizadas para ello.

- **Circular N°1 de Emisores No Bancarios de Tarjetas de Pago**, numeral 2.3.4, Medidas de resguardo operacional. Respecto de las transacciones, señala que las tecnologías que se implementen deben contar con métodos robustos de autenticación y sistemas de prevención de fraudes.

IV. CONTRIBUCIONES AL PROCESO CONSULTIVO[1]

Entre el 14 de abril y el 5 de mayo de 2025 esta Comisión sometió a consulta pública una propuesta normativa que regulaba las medidas de seguridad y autenticación de operaciones bajo la Ley 20.009.

En este proceso se recibieron cerca de 260 comentarios, enviados por 27 representantes de entidades provenientes de diferentes industrias, incluyendo a bancos, emisores de tarjetas de pagos no bancarias, distintos representantes de Fintec, operadores de tarjetas de pagos, redes de pago internacionales, diversos estudios jurídicos, asociaciones gremiales, entre otros. Su participación estuvo distribuida de acuerdo con la siguiente figura:



Fuente: Elaboración CMF

El número de comentarios asociados a aspectos generales de la propuesta normativa, estándares mínimos de seguridad y casos de uso de ARC, mostraron un nivel de participación similar entre ellos.

Por otra parte, el mayor número de observaciones recibidas se refirió a materias de responsabilidad y sanciones.

El contenido de los comentarios se puede agrupar en los siguientes temas:

i. Entregar mayor nivel de precisión en la descripción de definiciones de algunos términos, conceptos y procesos utilizados en la norma, cuyas interpretaciones podrían ser variadas y escapar del objetivo, especialmente en lo referido a los factores de autenticación y dispositivos de confianza.

ii. Incorporar ejemplos de referencia para la aplicación de ARC.

iii. Definir el alcance de la norma respecto a las operaciones incluidas,

[1] Comentarios considerados en la publicación de la NCG 538 de fecha 17.06.2025.

estableciendo aquéllas que requieren obligatoriamente el uso de ARC.

iv. Incluir en el alcance de la norma a otros actores del proceso de pagos.

v. Señalar la relación entre la implementación de ARC y el Sistema de Finanzas Abiertas.

vi. Aclarar los posibles efectos en la implementación de la ley de fraudes.

vii. Inclusión de otras excepciones a la ARC.[2]

En consideración a los comentarios recibidos, se realizaron modificaciones al texto puesto en consulta pública, incluyendo las siguientes:

a. Se ajustaron algunas definiciones, de modo tal que se evitaran posibles ambigüedades que podían llevar a interpretaciones equívocas. En el caso de los factores de autenticación, se realizaron cambios en la redacción y se agregaron referencias a los tipos de elementos que pueden ser considerados en una u otra categoría, de forma de cumplir con la necesidad de tener dos factores diferentes e independientes. En relación con los dispositivos de confianza, se realizó una definición.

b. Se simplificó la forma de definir los casos de exigencia obligatoria del uso de ARC, cambiando el enfoque desde una aplicación general, con excepciones, hacia una acotada a ciertas funcionalidades. Con esto se resolvió la observación sobre una mayor cantidad de excepciones de ARC solicitadas.

c. Se estableció que el alcance de la norma aplica solo a emisores de pagos y prestadores de servicios financieros de pagos electrónicos, en los términos que define la ley N°20.009.

d. Se aclaró que los requisitos expuestos en la NCG en relación con la ARC tienen el carácter de obligatorio en los casos que se mencionan. Lo anterior no restringe a los emisores, que así lo decidan, a aplicar autenticación reforzada en otros casos de usos, en el entendido de que así se configuran marcos probatorios en procesos judiciales, tal como se

[2] Diversos comentarios apuntaron a ampliar el tipo de excepciones al uso de ARC, proponiendo una extensa lista con casos especiales. En respuesta a ello, se consideró mover la estructura de exigencias en el uso de ARC hacia una visión simplificada, es decir, tomando en cuenta casos de base y eliminando ambigüedades producidas por el formato presentado en la versión anterior.

señala en el artículo 4 de la ley N°21.673 numeral 5, literal h).

e. Se cambió el concepto de mecanismos estáticos de autenticación por el de conjuntos de datos impresos.[3] Cabe destacar que ambos conceptos restringen el uso de las tarjetas de coordenadas.

   En este sentido, es del caso señalar que la tarjeta de coordenadas como mecanismo de seguridad viene en retirada en varias jurisdicciones. Su uso no es válido para fines de autenticación en la Unión Europea y, además, no es utilizada en Estados Unidos y Canadá. Por su parte, países como Argentina, Perú y México han promovido desde hace algún tiempo el uso de tokens, apps móviles y biometría debido a su mayor seguridad, desplazando el uso de mecanismos impresos.

COMENTARIOS POSTERIORES[4]

La NCG 538 fue publicada el 17 de junio y su entrada en vigencia fue el 1 de agosto, con excepción de los casos obligatorios de ARC, los cuales comenzarían a ser exigibles el 1 julio de 2026.

Posterior a la entrada en vigencia de la NCG 538, se recibieron comentarios relativos a la eliminación de las tarjetas de coordenadas como mecanismo de autenticación. Dichos comentarios se centraban en las dificultades operativas que tendría su eliminación, en especial para algunos grupos específicos de la población, por lo cual se solicitaba una ampliación del plazo para la implementación.

Dado ello, con fecha 7 de agosto 2025 se publicó la NCG 544, en la cual se modificó la entrada en vigencia de la eliminación de mecanismos con conjuntos de datos impresos, postergándola hasta el 1 de agosto de 2026. Adicionalmente, se realizaron precisiones con el objetivo, por una parte, de clarificar que los casos de ARC obligatoria eran aplicables para las plataformas de todos los emisores (bancos y otras entidades) y, por otra, establecer que las disposiciones generales eran aplicables a servicios financieros de pagos electrónicos.

[3] Véase recuadro en sección V. RECOMENDACIONES Y EXPERIENCIA INTERNACIONAL.

[4] Comentarios considerados en publicación de NCG 544 de fecha 07.08.2025.

V. RECOMENDACIONES Y EXPERIENCIA INTERNACIONAL

En la elaboración normativa se consideraron diversas referencias internacionales relevantes en la esta materia. Principalmente, se tuvo en cuenta lo dispuesto en la Directiva Europea PSD2 y PSD3, así como estándares provenientes de otras jurisdicciones, tales como los definidos por el *National Institute of Standards and Technology* (NIST) del gobierno de Estados Unidos.

La Directiva Europea sobre servicios de pago, vigente desde 2018, contempla la posibilidad de que los bancos puedan prestar servicios de terceros y regula el funcionamiento de servicios de iniciación de pagos y servicios de información de cuentas. Para ello, introduce nuevos requisitos de seguridad, entre los que destaca el uso de ARC, con uso de al menos dos factores de autenticación categorizados como conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) e inherencia (algo que es el usuario), que deben ser independientes entre sí, vale decir, que la vulneración de uno no comprometa la fiabilidad de los demás.

Asimismo, esta Directiva ordena que los Estados miembros procuren que los proveedores de servicios de pago apliquen la autenticación reforzada de clientes obligatoriamente cuando el cliente acceda a su cuenta de pago en línea; inicie una operación de pago electrónico; o, realice por un canal remoto cualquier acción que pueda generar un riesgo de fraude en el pago u otros abusos.

Las recomendaciones de NIST indican explícitamente los tipos de validación permitidas con sus respectivas características y formas de mitigación de los riesgos, de acuerdo con situaciones de vulneraciones específicas como ataques asociados a robos de elementos de seguridad, *phishing*, ingeniería social, *endpoints* comprometidos, entre otros eventos. Respecto al uso de contraseñas, define el uso y requisitos mínimos de longitud, complejidad y forma de verificación. Además, NIST recomienda definir criterios sobre longitud y complejidad, de manera tal de no aumentar la frustración del usuario y la dificultad del uso de contraseñas.

ACERCA DE LAS TARJETAS DE COORDENADAS EN EL USO DE ARC

La *European Banking Authority* (EBA) señala que los servicios de pago ofrecidos electrónicamente deben prestarse con la adecuada protección, asegurando que quién hace uso del servicio es el usuario legítimo y está, por lo tanto, dando consentimiento a la transferencia de fondos y acceso a su información de cuenta, mediante un uso normal de sus credenciales de seguridad personalizadas utilizando ARC. Por otro lado, indican que los requisitos de seguridad de los factores categorizados como de "posesión", deberán estar sujetos a medidas destinadas *a* ***evitar la replicación.*** [5]

Respecto a los datos impresos en las tarjetas de pagos -como los son las tarjetas de coordenadas- y su consideración como factor de posesión, la autoridad europea en su *Regulatory Technical Standards* (RTS) de 2017 2015/2366[6], define diferencias entre dispositivos entregados a los clientes que pueden ser replicados por un tercero, como es el caso de los números disponibles en tarjetas de coordenadas, por sobre otro tipo de dispositivos como *token* criptográficos (*pinpass*). En el caso de las tarjetas de coordenadas, la posibilidad de obtener copias de las combinaciones numéricas, por ejemplo, a través de una foto o fotocopia, difiere de los *tokens* criptográficos que no son posibles de replicar. Aun cuando no es posible validar que el *token* está siendo usado por un tercero no autorizado, la existencia de una única copia del dispositivo lo hace menos vulnerable como mecanismo de autenticación.

[5] REGLAMENTO DELEGADO (UE) 2018/389 DE LA COMISIÓN de 27 de noviembre de 2017, Capítulo II, Artículo 7, número 2.

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R0389

VI. NORMATIVA PUBLICADA

REF.: NORMA SOBRE MEDIDAS SEGURIDAD Y AUTENTICACIÓN DE OPERACIONES SOMETIDAS A LA LEY N°20.009

NORMA DE CARÁCTER GENERAL N° 538

17 de junio de 2025.-

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, lo dispuesto en los nuevos incisos noveno y décimo el artículo 4 de la Ley N°20.009, y lo acordado por el Consejo de la Comisión en Sesión Ordinaria N°448 de 12 de junio 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.

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 los artículos 1° y 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 permite 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 de diferentes categorías. Las categorías por considerar son las siguientes:
   a) **Conocimiento**: Algo que solo el usuario conoce, así como las contraseñas o números de identificación personal o PIN.
   b) **Posesión:** Algo que solo el usuario posee, tal como un dispositivo token o hardware criptográfico portátil, un mensaje tipo OTP (One Time Password), la tarjeta de pago o un smartphone.
   c) **Inherencia**: Algo que el usuario es. Usualmente para este factor se utiliza la verificación biométrica, tal como huella dactilar, rostro, voz o datos conductuales. El uso de este factor debe tener como objetivo permitir distinguir inequívocamente al usuario y mitigar el riesgo de suplantación de identidad.

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.

4. **Dispositivo de Confianza:** 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.

Estándares Mínimos de Seguridad, Registro y Autenticación

Requisitos generales

Los Emisores, además de cumplir con la normativa vigente asociada a su calidad de emisor de medios de pago, 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, incluyendo lo siguiente:

- Implementación de medidas que aseguren la independencia de los factores de autenticación utilizados.
- Mecanismos de cifrado, protección y confidencialidad de los datos utilizados en el proceso de autenticación.
- 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.
- Medidas de protección para el almacenamiento y transmisión de los respectivos códigos de autenticación. Será obligación de los Emisores disponer de protocolos de caducidad y expiración de códigos de autenticación.

Criterios de robustez, independencia y diferenciación de factores

Los Emisores deberán garantizar que:

- 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. Adicionalmente, los Emisores deberán establecer exigencias de actualización, longitud, complejidad, reutilización y previsibilidad de claves de forma que los usuarios no eludan estas restricciones de forma contraproducente.
- En relación con la definición de inherencia, conocen y se han interiorizado adecuadamente acerca del funcionamiento interno y nivel de confianza de los factores implementados de esta categoría, tanto aquellos que se

encuentren bajo su control o gestión directa, como aquellos en que la verificación biométrica resulta delegada a terceros, siendo el Emisor, siempre y en todo caso, el responsable sobre los mecanismos que ha dispuesto para ser utilizados por sus usuarios y clientes.

- Los dispositivos que proporciona para la autenticación reforzada posean mecanismos de detección de manipulación o clonación.
- Eliminar el uso de mecanismos que incorporen conjuntos de datos impresos, utilizados para la autenticación.

Supuestos de Uso de Autenticación Reforzada de Clientes

El emisor siempre podrá utilizar ARC en cualquier operación o transacción en que lo considere necesario, lo cual deberá estar plasmado en su marco de gestión de riesgos y permitirá utilizar la presunción judicial señalada en la letra h) del artículo 5 ter de la Ley N°20.009.

Casos de aplicación obligatoria ARC:

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

- Gestión y realización de transferencias electrónicas de fondos. Esto implica el uso de ARC en todas las solicitudes y modificaciones que permitan la transacción, tales como la información asociada a destinatarios y contratación de pagos recurrentes, entre otros.
- Proceso de incorporación del cliente en las plataformas digitales del banco, incorporación y modificación de datos personales, modificación de claves de autenticación, incorporación de dispositivo de confianza y su reemplazo o eliminación.

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.

Vigencia

La presente norma entra 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.

REF.: MODIFICA NORMA DE CARÁCTER GENERAL N° 538 Y POSTERGA VIGENCIA DE ÉSTA COMO LO INDICA.

NORMA DE CARÁCTER GENERAL N° 544

Bancos, sociedades de apoyo al giro, empresas emisoras de tarjetas de pago y, cooperativas de ahorro y crédito.

7 de agosto de 2025.-

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; lo dispuesto en los nuevos incisos noveno y décimo el artículo 4 de la Ley N°20.009; y lo acordado por el Consejo de la Comisión en Sesión extraordinaria N°151 de 6 de agosto de 2025, ejecutado mediante Resolución Exenta N°7.869 de 7 de agosto de 2025, ha estimado pertinente impartir las siguientes instrucciones que modifican la Norma de Carácter General N°538, sobre estándares mínimos de seguridad y de autenticación, en los siguientes términos:

1. En el apartado "**Disposiciones Generales**", en el primer párrafo sobre "Objeto y ámbito de aplicación" se reemplaza la frase *"…aplicables a los emisores de medios de pago y prestadores de servicios financieros…"* por *"…aplicables a los emisores de medios de pago y prestadores de servicios financieros de pagos electrónicos…".*

2. En el apartado "**Casos de aplicación obligatoria ARC**", se reemplaza la palabra "*banco*" por "*emisor*".

3. Se modifica la **Vigencia**, reemplazando el texto por el siguiente:
   "La presente norma entra en vigor a partir del 1 de agosto de 2025, excepto los casos de ARC obligatoria y la exigencia de eliminación del uso de mecanismos que incorporen conjuntos de datos impresos utilizados para la autenticación, cuya vigencia comenzará el 1 de agosto de 2026."

NORMA DE CARÁCTER GENERAL N° 538 - CONSOLIDADA

REF.: NORMA SOBRE MEDIDAS SEGURIDAD Y AUTENTICACIÓN DE OPERACIONES SOMETIDAS A LA LEY N°20.009.

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, lo dispuesto en los nuevos incisos noveno y décimo el artículo 4 de la Ley N°20.009, lo acordado por el Consejo de la Comisión en Sesión Ordinaria N°448 de 12 de junio de 2025, y lo acordado por el Consejo de la Comisión en Sesión extraordinaria N°151 de 6 de agosto 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.

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 de pagos electrónicos (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 permite 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 de diferentes categorías. Las categorías a considerar son las siguientes:

a) **Conocimiento**: Algo que solo el usuario conoce, así como las contraseñas o números de identificación personal o PIN.

b) **Posesión:** Algo que solo el usuario posee, tal como un dispositivo token o hardware criptográfico portátil, un mensaje tipo OTP (One Time Password), la tarjeta de pago o un smartphone.

c) **Inherencia**: Algo que el usuario es. Usualmente para este factor se utiliza la verificación biométrica, tal como huella dactilar, rostro, voz o datos conductuales. El uso de este factor debe tener como objetivo permitir distinguir inequívocamente al usuario y mitigar el riesgo de suplantación de identidad.

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.

4. **Dispositivo de Confianza:** 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.

Estándares Mínimos de Seguridad, Registro y Autenticación

Requisitos generales

Los Emisores, además de cumplir con la normativa vigente asociada a su calidad de emisor de medios de pago, 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, incluyendo lo siguiente:

- Implementación de medidas que aseguren la independencia de los factores de autenticación utilizados.

- Mecanismos de cifrado, protección y confidencialidad de los datos utilizados en el proceso de autenticación.

- 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.

- Medidas de protección para el almacenamiento y transmisión de los respectivos códigos de autenticación. Será obligación de los Emisores disponer de protocolos de caducidad y expiración de códigos de autenticación.

Criterios de robustez, independencia y diferenciación de factores

Los Emisores deberán garantizar que:

- 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. Adicionalmente, los Emisores deberán establecer exigencias de actualización, longitud, complejidad, reutilización y previsibilidad de claves de forma que los usuarios no eludan estas restricciones de forma contraproducente.

- En relación con la definición de inherencia, conocen y se han interiorizado adecuadamente acerca del funcionamiento interno y nivel de confianza de los factores implementados de esta categoría, tanto aquellos que se encuentren bajo su control o gestión directa, como aquellos en que la verificación biométrica resulta delegada a terceros, siendo el Emisor, siempre y en todo caso, el responsable sobre los mecanismos que ha dispuesto para ser utilizados por sus usuarios y clientes.

- Los dispositivos que proporciona para la autenticación reforzada posean mecanismos de detección de manipulación o clonación.

- Eliminar el uso de mecanismos que incorporen conjuntos de datos impresos, utilizados para la autenticación.

Supuestos de Uso de Autenticación Reforzada de Clientes

El emisor siempre podrá utilizar ARC en cualquier operación o transacción en que lo considere necesario, lo cual deberá estar plasmado en su marco de gestión de riesgos y permitirá utilizar la presunción judicial señalada en la letra h) del artículo 5 ter de la Ley N°20.009.

Casos de aplicación obligatoria ARC:

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

- Gestión y realización de transferencias electrónicas de fondos. Esto implica el uso de ARC en todas las solicitudes y modificaciones que permitan la transacción, tales como la información asociada a destinatarios y contratación de pagos recurrentes, entre otros.

- Proceso de incorporación del cliente en las plataformas digitales del emisor[1], incorporación y modificación de datos personales, modificación de claves de autenticación, incorporación de dispositivo de confianza y su reemplazo o eliminación.

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.

Vigencia[2]

La presente norma entra en vigor a partir del 1 de agosto de 2025, excepto los casos de ARC obligatoria y la exigencia de eliminación del uso de mecanismos que incorporen conjuntos de datos impresos utilizados para la autenticación, cuya vigencia comenzará el 1 de agosto de 2026.

[1] Modificado por NCG N°544 de fecha 07.08.2025

[2] Se posterga plazo diferido mediante NCG N°544 de fecha 07.08.2025.

VII. EVALUACIÓN DE IMPACTO

Si bien el impacto en la implementación de las medidas establecidas en esta norma debería ser limitado para la mayoría de los sujetos obligados, considerando el amplio nivel de adopción de soluciones ya existentes, por el lado de los usuarios del sistema puede haber segmentos de la población para los cuales se generen mayores dificultades en la adopción de nuevos mecanismos de autenticación. [1]

Entre los mecanismos utilizados de manera previa a la emisión de esta normativa, se incluyen la autenticación biométrica, la evaluación de patrones de comportamiento, los requisitos de complejidad en las contraseñas, el uso de claves OTP y la preferencia por mecanismos de autenticación digitales en lugar de aquellos con datos impresos, como lo son las tarjetas de coordenadas.

La definición de las condiciones de ARC y de los casos de uso obligatorio, tendrán como consecuencia que las entidades eleven la seguridad de los dispositivos que utilizan para la autenticación de clientes. Si bien esto elevará el estándar de seguridad en las transacciones, también tendrá potencialmente un efecto en los costos de éstas.

Dichos costos dependerán tanto de las brechas iniciales de los distintos emisores, así como también de las políticas y/o lineamientos específicos de seguridad que cada uno de ellos defina.

Con todo, la eliminación de la tarjeta de coordenadas como mecanismo de autenticación significa un avance relevante para la seguridad de las transacciones. De acuerdo con la información que se tuvo en consideración para este proceso normativo, en la actualidad los emisores que aún mantienen un parque de tarjetas de coordenadas activas, cuentan además con un mecanismo de autenticación alternativo que se ajusta con el nuevo estándar, por lo cual los costos para los emisores podrían resultar no ser tan significativos.

Por su parte, respecto a los usuarios, la adopción de nuevos mecanismos que reemplacen las tarjetas de coordenadas podría significar mayores dificultades en segmentos con menores niveles de digitalización y/o con mayor dificultad o resistencia al cambio.

---

[1] Según los datos publicados en la Nota Técnica CMF 03/24, de oferta y demanda de servicios financieros, menos del 30% de los adultos mayores de 60 años usan el *smartphone* para hacer o recibir pagos, mientras que un 53% encuentra difícil o confuso hacer transacciones por internet.

Al respecto, cabe mencionar que alrededor del 15% de los titulares de cuentas bancarias corresponde a adultos mayores de 65 años. [2] De ellos, se estima que el 25% paga servicios online y el 28% realiza transferencias por internet.[3]

Para este grupo, de manera de minimizar el impacto, será fundamental que los emisores adopten un enfoque proactivo, informando claramente los mecanismos alternativos disponibles y acompañando a los clientes en su proceso de adaptación. Esto incluye brindar asistencia presencial, desarrollar campañas de educación en finanzas digitales, seguridad y uso de la Autenticación Reforzada de Clientes (ARC).

[2] Los clientes financieros titulares de cuentas bancarias ascienden a 22.241.182 personas naturales a diciembre de 2024.
[3] Fuente: Datos CMF.

VIII. 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