

Informe Normativo - Post Consulta Pública:
PUBLICACIÓN MODIFICACIÓN NCG N°538

Junio 2026

www.CMFChile.cl

Índice Informe Normativo

I. INTRODUCCIÓN	3
II. OBJETIVOS DE LA PROPUESTA NORMATIVA	4
III. MARCO NORMATIVO	4
IV. CONTRIBUCIONES AL PROCESO CONSULTIVO	5
V. RECOMENDACIONES Y EXPERIENCIA INTERNACIONAL	8
VI. PROPUESTA NORMATIVA POST CONSULTA	10
VII. EVALUACIÓN DE IMPACTO	12
VIII. REFERENCIAS	13

I. INTRODUCCIÓN

El 30 de mayo de 2024 se publicó la ley N°21.673, la cual introdujo ajustes significativos a la Ley N°20.009 (Ley) con el fin de fortalecer el régimen de responsabilidad asociado al uso de tarjetas de pago y transacciones electrónicas. Esta reforma responde al incremento sostenido de fraudes y operaciones no reconocidas en el sistema financiero, buscando equilibrar la protección a los usuarios con la necesidad de reducir el uso indebido del mecanismo de restitución inmediata de fondos.

Antes de estos cambios, el procedimiento permitía la restitución obligatoria de montos reclamados por hasta UF 35 en un plazo de cinco días hábiles, sin exigencias formales para presentar el reclamo. Este diseño generó un alto volumen de denuncias sin sustento suficiente, lo que produjo impactos financieros relevantes en diversas instituciones.

En este contexto, la ley N°21.673 otorgó nuevas facultades regulatorias a esta Comisión para dictar instrucciones que permitieran la correcta implementación del marco legal. En ejercicio de dichas atribuciones, en noviembre de 2024 se emitió la Norma de Carácter General N°523 (NCG N°523), referida al envío de solicitudes y resoluciones judiciales. Posteriormente, en diciembre de 2024, el Decreto Exento N°435 del Ministerio de Hacienda definió los umbrales de restitución aplicables.

A ello, se sumó la publicación, en junio de 2025, de la Norma de Carácter General N°538 (NCG N°538), que estableció estándares de seguridad y autenticación para transacciones electrónicas, incluyendo la eliminación de mecanismos basados en datos impresos, como lo son las tarjetas de coordenadas. Sin embargo, tras su dictación esta Comisión tomó conocimiento de dificultades operativas para su implementación, particularmente para segmentos de la población con menor nivel de digitalización. Estas inquietudes motivaron la modificación introducida en agosto de 2025, por la Norma de Carácter General N°544 (NCG N°544), que aplazó la eliminación de dichos mecanismos hasta el 1° de agosto de 2026.

Posteriormente, algunas instituciones manifestaron que existen grupos de clientes que sólo utilizan mecanismos con conjuntos de datos impresos para autenticarse y además presentan dificultad en la adaptación de nuevos mecanismos de autenticación, lo cual los dejaría fuera de los servicios que requieren este procedimiento. La presente propuesta normativa considera lo anterior, permitiendo que estos clientes puedan continuar realizando transferencias electrónicas y otros servicios que requieran Autenticación

reforzada de cliente (ARC), sin perder los beneficios que estos servicios financieros otorgan.

Si bien la utilización de mecanismos impresos durante los procesos de *onboarding* ha venido a la baja, se hace particular énfasis en que los emisores manifiesten en el periodo de consulta pública si advierten dificultades específicas en dicho ámbito.

II. OBJETIVOS DE LA PROPUESTA NORMATIVA

Con el propósito de cumplir lo establecido en la Ley, conforme se indica en el inciso noveno del artículo 4 de la Ley N°20.009, así como de facilitar la implementación de lo establecido en la NCG N°538, especialmente en lo referido a la eliminación de mecanismos con conjunto de datos impresos como mecanismo de autenticación, esta propuesta tiene como objetivo principal continuar colaborando con la inclusión financiera de grupos de clientes con dificultades en la adopción de nuevos medios de autenticación.

No obstante lo anterior, es necesario reiterar que el objetivo de la Ley y el mandato para esta norma, son los de establecer los mecanismos que permiten probar la titularidad de las operaciones y transacciones de los usuarios, con el fin de limitar su responsabilidad ante el fraude, y por ende, se hace necesario considerar el mantenimiento de los mecanismos de conjuntos impresos a determinados grupos de clientes, como una excepción extraordinaria que se otorgará solo en el momento de la emisión de esta normativa, incluso cuando en el futuro pudieran existir clientes que cumplan con los mismos criterios. La razón de esto radica en la necesidad de avanzar hacia procedimientos que incluyan mecanismos más seguros y robustos que protejan al cliente, y por ello, resulta imprescindible que las instituciones emisoras continúen avanzando hacia ese objetivo.

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 noveno señala: "*La Comisión para el Mercado Financiero, mediante norma de carácter general, establecerá estándares mínimos de*

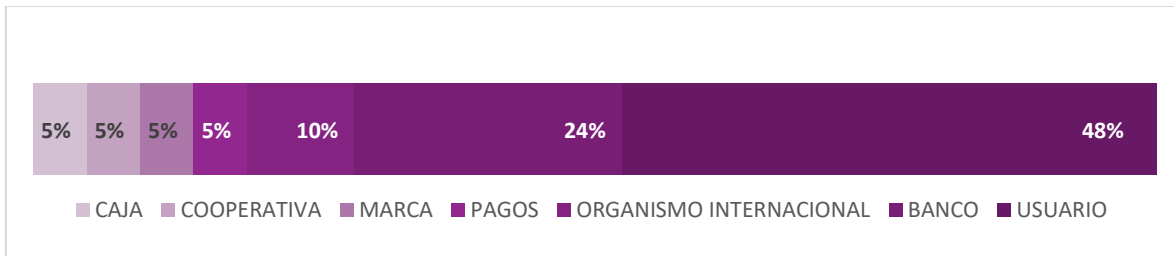
seguridad, registro y autenticación. A través de la referida norma de carácter general, la Comisión determinará los supuestos de uso y transacciones en que resulte obligatorio por parte del emisor el uso de autenticación reforzada.”

- **NCG N°538**, publicada el 17.06.2025, que regula las medidas de seguridad que deben aplicarse en las operaciones sometidas bajo la Ley N°20.009, señalando los casos de obligatoriedad de uso de Autenticación Reforzada de Clientes (ARC).
- **Capítulo 8-41 de la Recopilación Actualizada de Normas para bancos (RAN)** sobre Tarjetas de Pago, que en su numeral 4.2 establece los requisitos mínimos de transferencia electrónica de fondos para Cuentas con Provisión de Fondos.
- **Capítulo 1-7 de la RAN para bancos**, relativo a Transferencia Electrónica de Fondos, que establece los requisitos mínimos que deben cumplir los sistemas utilizados, entre los cuales se encuentran exigencias de seguridad que garanticen que las operaciones sólo puedan ser realizadas por personas debidamente autorizadas para ello.
- **Circular N°1 para Emisores No Bancarios de Tarjetas de Pago**, en su numeral 2.3.4 establece 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

Entre el 30 de marzo y el 4 de abril de 2026 esta Comisión sometió a consulta pública una propuesta normativa que modifica la N.C.G. N°538, exceptuando la eliminación del uso de mecanismos con conjuntos de datos impresos para autenticación a determinados clientes.

En este proceso se recibieron comentarios de un poco más de 20 personas naturales y jurídicas, cuya participación estuvo distribuida de la siguiente manera:



Fuente: Elaboración CMF

Los comentarios recibidos provenientes de distintos actores presentaron tanto similitudes como diferencias. Las materias más comentadas por categoría de participante, fueron las siguientes:

Las personas naturales señalaron estar de acuerdo con la posibilidad de exceptuar a clientes de la obligatoriedad de eliminar el uso de mecanismos con conjuntos de datos impresos para autenticar. Sin embargo, manifestaron sus aprensiones en relación con la limitación de los grupos que puedan excluirse, la pérdida del derecho de los clientes frente a los bancos para poder decidir los métodos de autenticación, así como la eventual discriminación percibida al permitir que sólo algunos clientes continúen usando tarjetas de coordenadas.

Asimismo, señalaron riesgos asociados a la vulnerabilidad en sus Dispositivos de Confianza frente a robos o ataques cibernéticos. También destacaron que la obsolescencia de sus smartphones y la imposibilidad de adquirir tecnología ad-hoc les impide aplicar los mecanismos de autenticación exigidos por algunas instituciones, generando situaciones de exclusión tecnológica. Frente a esto, algunos señalaron que, ante la eliminación de tarjetas de coordenadas, el banco debiese ofrecer alternativas de autenticación, como tokens físicos y permitir que el cliente pueda elegir.

Adicionalmente se mencionó el abandono digital por parte de algunos emisores, reflejado en la ausencia de campañas o instancias de acompañamiento para clientes con menores competencias digitales.

Por su parte, las entidades bancarias y no bancarias señalaron deficiencias en la definición de ciertos conceptos, solicitando mayor precisión en la definición de los criterios que se considerarán válidos para seleccionar a sus clientes en su lista de excepción. Indicaron que la falta de claridad puede generar disparidades entre emisores y dificultades en los procesos de auditorías. Asimismo, solicitaron definir con mayor exactitud el alcance de los “mejores esfuerzos” que deben realizar los emisores antes de clasificar a un cliente en la lista de excepción.

En línea con lo planteado por algunos clientes, algunas instituciones advirtieron que la imposibilidad de incorporar, con posterioridad a la entrada en vigencia de

la norma, a nuevos clientes que presenten las mismas dificultades que aquellos incluidos en la lista de excepción, podría contravenir lo dispuesto en la ley N°19.496¹, constituyendo eventualmente una forma de discriminación arbitraria. En ese contexto, propusieron que la normativa contemple la posibilidad de incorporar nuevos grupos en el futuro, siempre que cumplan con los mismos criterios establecidos.

Finalmente, organismos internacionales recomendaron incentivar el uso de mecanismos de autenticación resistentes al phishing -como passkeys o llaves físicas-, exigir a los bancos reportes semestrales acerca de nuevas tecnologías evaluadas para reducir progresivamente la población exenta del uso de autenticación reforzada y extender la aplicación de los estándares de la N.C.G. N°538 a todo tipo de transacciones de pago.

En consideración a los comentarios recibidos, se realizaron las siguientes acciones en la propuesta normativa:

Comentario	Origen	Tratamiento
Incorporar nuevos clientes a la lista de excepción	Usuarios y entidades bancarias	Se mantiene. Los clientes pueden ser incluidos en alguno (s) de los grupos solamente al momento de emisión de la normativa.
Poder de decisión de clientes sobre mecanismos de autenticación	Usuarios	Se deja igual.
Incompatibilidad u obsolescencia de dispositivo de confianza con el mecanismo de autenticación	Usuarios	Se permite que estos usuarios entren en la lista de excepción, o bien, el emisor deberá proporcionar token físico
Abandono digital de los emisores	Usuarios	Se exige a los emisores acompañar a los usuarios no digitalizados mediante campañas, capacitaciones y formas de asistencia.
Definir criterios de selección para la lista de excepción	Entidades bancarias	Se dan lineamientos para criterios.
Precisar el concepto de "mejores esfuerzos"	Entidades bancarias	Se elimina el concepto.

¹ Ley sobre protección de los derechos de los consumidores

Incentivar el uso de mecanismos resistentes al phishing	Internacional	Se evaluará en el tiempo.
Extender los estándares a todo tipo de transacciones de pago	Internacional	Se evaluará en el tiempo.
Incorporar excepciones de ARC en TEF de bajo riesgo	Bancos	Se incorpora la excepción para transferencias mismo RUT en mismo emisor.

V. RECOMENDACIONES Y EXPERIENCIA INTERNACIONAL

En la elaboración normativa se consideraron diversas referencias internacionales relevantes en la 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, que 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**.²

Respecto a los datos impresos en las tarjetas de pagos -como lo son las tarjetas de coordenadas- y su consideración como factor de posesión, la autoridad europea en su *Regulatory Technical Standards* (RTS) de 2017 2015/2366³, 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. 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.

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

³ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R0389>

VI. PROPUESTA NORMATIVA POST CONSULTA

**REF.: MODIFICA NCG 538 SOBRE
MEDIDAS SEGURIDAD Y
AUTENTICACIÓN DE
OPERACIONES SOMETIDAS A LA
LEY N°20.009.**

NORMA DE CARÁCTER GENERAL N° XXX

XX de xxxxxx de 2026.-

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 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°xxx de xx de xxxxxx de 2026, ejecutado mediante Resolución Exenta N°xxxxx de x de xxxxxx de 2026, 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:

En el título "Supuestos de Uso de Autenticación Reforzada de Clientes, se reemplaza el primer punto de los "**Casos de aplicación obligatoria ARC**", por lo siguiente:

- *"Gestión y realización de transferencias electrónicas de fondos, con excepción de aquéllas cuyas cuentas de origen y destino se encuentren asociados a un mismo RUT y se realicen en una misma institución emisora. Esto implica el uso de ARC en todas las solicitudes y modificaciones que permitan la transacción, tales como la información asociada a destinatarios y pagos recurrentes (en el momento de su contratación), entre otros."*

En el apartado "**Vigencia**", se sustituye dicho párrafo por el siguiente texto:

"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.

La utilización de ARC para los casos de uso obligatorio descritos en la presente norma no se extenderá a las operaciones efectuadas por aquellos clientes pertenecientes a grupos que podrán determinar los propios emisores, sobre la base de los siguientes criterios: ser adulto mayor⁴; presentar una condición de salud deteriorada o de discapacidad; tener dificultad para acceder a canales físicos de atención; presentar incompatibilidad o indisponibilidad de dispositivos de confianza con los mecanismos de autenticación que requiere la entidad.

Los clientes incluidos en aquellos grupos podrán seguir utilizando conjuntos de datos impresos para autenticarse, en cuyo caso esa autenticación no será considerada ARC.

La inclusión de clientes en los grupos a que se refieren los dos párrafos anteriores solo podrá realizarse luego de que el emisor haya ofrecido soluciones alternativas y el cliente no haya manifestado su aceptación, y será exclusivamente respecto de los clientes de la entidad a la fecha de entrada en vigencia de la norma. Adicionalmente, el emisor deberá informar de los riesgos que conlleva la mantención de los medios de autenticación que vienen utilizando.

Los emisores que opten por acogerse a esta excepción deberán informarlo a esta Comisión a más tardar el 1º de agosto de 2026, incluyendo el número de clientes incluido en los grupos y el total de clientes involucrados. Además, deberán enviar una actualización semestral."

⁴ Definición de la Ley 19.828 considerando adulto mayor a toda persona que haya cumplido 60 años.

VII. EVALUACIÓN DE IMPACTO

A partir de la publicación de la NCG N°538 con fecha 17 de junio de 2025 y su modificación dada por la NCG N°544 el 7 de agosto de 2025, la industria comenzó gradualmente a poner en marcha planes de eliminación de tarjetas de coordenadas para la implementación de la Norma. En ello, desde la publicación normativa, en agosto de 2025 el stock de tarjetas de coordenadas vigentes en la industria era de 10.462.850 las que se han reducido cerca de un 71% a marzo de 2026, alcanzando un total de 3.044.423 tarjetas vigentes⁵.

Respecto al uso de tarjetas de coordenadas como medio de autenticación, en los últimos 3 meses se observó una disminución en su uso en un poco menos del 46%, con un total de 2.327.050 tarjetas de coordenadas que fueron utilizadas a marzo de este año. De ellas, un total de 716.008 clientes utilizaron sus tarjetas como su único mecanismo de autenticación⁶, donde un poco más del 43% correspondieron a adultos mayores.

Con el cambio normativo propuesto, se espera que un subconjunto de estos clientes pueda seguir realizando sus transferencias electrónicas y no sean excluidas de este servicio financiero para realizar sus pagos.

Por otro lado, la propuesta normativa considera casos de excepción para la aplicación de autenticación reforzada para operaciones de bajo riesgo, pagos recurrentes y transferencias realizadas entre cuentas del mismo titular, con el mismo RUT y emisor, lo que conlleva aminorar parte de los costos de los emisores en la implementación de la normativa.

⁵ Según datos reportados por emisores a la CMF.

⁶ De acuerdo con cifras reportadas en el mes de abril de 2026.

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>



Regulador y Supervisor Financiero de Chile

www.cmfchile.cl

