H · D
LEGAL

HDGROUP.CL

Alerta Legal

Fintech

Abril 2025

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

+56 2 2405 3200
AV. VITACURA 2939 – 8TH FLOOR
LAS CONDES. SANTIAGO. CHILE

Con fecha 14 de abril de 2025, la Comisión para el Mercado Financiero (**CMF**) publicó una propuesta normativa (**Propuesta Normativa**) concerniente a las medidas de seguridad y autenticación de operaciones sometidas a la 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 este contexto, en conformidad a lo estipulado en el inciso noveno del artículo 4 de la Ley N°20.009, la CMF, por medio de 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 CMF determinará los supuestos de uso y transacciones en que resulte obligatorio por parte del emisor el uso de autenticación reforzada*".

En virtud de lo anterior, esta Propuesta Normativa busca establecer de forma concreta:

1. Estándares mínimos sobre seguridad, registro y autenticación de transacciones.
2. Supuestos de uso y transacciones en los que resulte obligatorio el uso de autenticación reforzada de clientes (**ARC**) por parte del respectivo emisor.

En este sentido, con respecto a los **estándares mínimos sobre seguridad y registro** se establecen requisitos generales para los emisores, quienes deberán 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 pertinentes, entre las que se incluyen las siguientes:

- Mecanismos de cifrado y protección de datos sensibles.
- Registros auditables y trazables de todas las transacciones y eventos de autenticación.
- Medidas de independencia y diferenciación de los factores de autenticación utilizados.
- Monitoreo continuo de patrones de transacciones para detectar posibles fraudes.

- Medidas de protección para el almacenamiento y transmisión de los respectivos códigos de autenticación.

Adicionalmente, se instituyen los criterios de independencia, robustez y diferenciación de factores. En virtud de estos criterios 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.
- Los dispositivos utilizados para la autenticación reforzada posean mecanismos de detección de manipulación o clonación.
- Las medidas de autenticación no sean reutilizables ni predecibles, evitando el uso de mecanismos estáticos.
- Los dispositivos confiables han sido registrados bajo procedimientos rigurosos que garantizan la acreditación de titularidad y posesión.
- 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 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.
- 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.

Por otro lado, con respecto a los **supuestos de uso de ARC**, la Propuesta Normativa regula los casos de aplicación obligatoria de ARC, los cuales son los siguientes:

- 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.

No obstante, también exceptúa la obligación de ARC 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.
- Pagos recurrentes a beneficiarios particulares por montos y periodicidad predefinidos por el usuario, siempre que hayan sido validados previamente, al momento de originarse la recurrencia o suscribirse el respectivo plan de pagos, mediante ARC.
- 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.

Asimismo, la Propuesta Normativa concretiza la responsabilidad que le cabe a los emisores por los perjuicios ocasionados a los usuarios por el incumplimiento de los estándares de seguridad, autenticación y registro establecidos en la normativa en consulta. Todo lo anterior será fiscalizado por la CMF, la cual podrá imponer sanciones a quienes infrinjan los deberes indicados.

Por último, las instituciones tendrán que ajustar sus procedimientos y medidas de seguridad y autenticación asociadas a medios de pago y transacciones electrónicas dentro del plazo de 1 año contado desde la dictación de la normativa definitiva, debiendo informar a la CMF 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 plazos, hitos y elementos físicos y lógicos involucrados o impactados.

La Propuesta Normativa puede ser consultada en el siguiente enlace: https://www.cmfchile.cl/institucional/legislacion_normativa/normativa_tramite_ver_archivo.php?id=2025041422&seq=1

Para más información, contactar a:

Matías Langevin
Socio Fintech
mlangevin@hdgroup.cl

Fernanda Aillach
Asociada Fintech
faillach@hdgroup.cl