COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

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 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 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 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.

Solange Michelle Berstein Jauregui

Firmado digitalmente por Solange Michelle Berstein Jauregui
Fecha: 2025.06.17 14:32:10 -04'00'

SOLANGE MICHELLE BERSTEIN JÁUREGUI

PRESIDENTA

COMISIÓN PARA EL MERCADO FINANCIERO