PROYECTO NORMATIVO

RECOPILACIÓN DE NORMAS DE REGULACIÓN Y CONTROL DEL SISTEMA FINANCIERO

LIBRO IV – PROTECCIÓN AL USUARIO DE SERVICIOS FINANCIEROS

TÍTULO II – INSTRUMENTOS ELECTRÓNICOS

ARTÍCULO 364 (OBLIGACIONES DEL EMISOR). El emisor del instrumento electrónico deberá:

a. Informar por escrito al usuario del instrumento electrónico, previo a la celebración del contrato, de sus obligaciones y responsabilidades en el uso del sistema, indicando como mínimo las que sean aplicables entre las enumeradas en los artículos 366 y 367. Dicha comunicación deberá realizarse en un documento distinto al contrato suscrito por las partes, sin perjuicio de ser incluidas también en él.

b. Revelar el número de identificación personal u otra clave únicamente al usuario.

c. Entregar solamente aquellos instrumentos electrónicos solicitados expresamente por el cliente, salvo cuando se trate de la renovación de un instrumento electrónico que ya poseía.

d. Proporcionar al cliente elementos que le permitan comprobar las operaciones realizadas, de los cuales al menos uno deberá ser sin costo para los clientes.

e. Proporcionar al cliente elementos que le permitan identificar claramente el motivo de una operación no aceptada, salvo en los casos en que se deban respetar requisitos de confidencialidad establecidos legal o reglamentariamente.

f. Informar al cliente sobre los principales riesgos a que está expuesto al utilizar el instrumento electrónico para realizar transacciones financieras, y proporcionarle recomendaciones sobre cómo debe protegerse adecuadamente para mitigar dichos riesgos.

g. Informar el procedimiento que deberá seguir el cliente para efectuar la notificación de sustracción, hurto, rapiña o extravío del instrumento electrónico o de alguna de las circunstancias previstas en el literal h) del artículo 366, garantizar la existencia de medios adecuados para realizarla y acreditar que dicha notificación ha sido efectuada. A estos efectos, el emisor (o la institución por él indicada) proporcionará al usuario un número que identifique su denuncia y señalará la fecha y hora de la misma. Los medios para efectuar la

notificación deberán operar todos los días del año, durante las veinticuatro horas.

h. Demostrar, en caso de un reclamo del usuario en relación con alguna transacción efectuada, y sin perjuicio de cualquier prueba en contrario que el usuario pueda producir, que la transacción:

- ha sido efectuada de acuerdo con los procedimientos acordados con el cliente;
- ha sido registrada y contabilizada correctamente;
- no se ha visto afectada por un fallo técnico o por cualquier otra anomalía; y
- ha sido correctamente autenticada de acuerdo con la metodología establecida para la misma, debiendo además poner a su disposición - independientemente si el instrumento fue utilizado en el país o en el exterior - la información resguardada señalada en el literal i) y cualquier otro elemento que permita demostrar que dicha transacción fue realizada por el cliente o por terceros con conocimiento del cliente.

En caso de no poder demostrarlo, el emisor será responsable de la transacción reclamada, siempre que no sea atribuible a incumplimientos de las obligaciones del usuario. A efectos de cumplir con esta obligación no serán oponibles las condiciones de los contratos que el emisor hubiese firmado con terceros.

~~i.~~ Establecer medidas que permitan garantizar razonablemente la seguridad del ~~sistema~~ **entorno** en que opera el instrumento, que incluyan metodologías de autenticación asociadas a los riesgos de los distintos tipos de transacciones y niveles de acceso para asegurar que las operaciones realizadas en el mismo sean las efectuadas por las personas autorizadas, **considerando cuando corresponda, lo dispuesto en el artículo 364.1**. ~~Sin perjuicio de ello, las transferencias o pagos a terceros realizados desde una cuenta bancaria y las solicitudes de préstamos que fueran realizadas en forma no presencial requerirán como mínimo un doble factor de autenticación. Asimismo, deberán establecer medidas de monitoreo y control que permitan detectar hechos irregulares vinculados con el uso del instrumento o el sistema en el que opera, incluyendo los cambios e intentos de cambios de clave, número de identificación personal, dirección, teléfono y correo electrónico de contacto, medios establecidos para recibir comunicaciones, entre otros.~~

~~Dicho sistema~~ **Se** deberá resguardar, como mínimo:

- fechas y horas de las operaciones;
- contenidos de los mensajes;
- identificación de operadores, emisores y receptores;
- cuentas y montos involucrados;
- mecanismo de autenticación del usuario utilizado en la operación;
- identificación de la terminal desde la cual se operó; y
- si la operación fue realizada en forma presencial o remota.

j. Establecer un sistema de monitoreo y control que permita detectar hechos irregulares vinculados con el uso del instrumento o el entorno

en el que opera, incluyendo los cambios e intentos de cambios de clave, número de identificación personal, dirección, teléfono y correo electrónico de contacto, así como otros medios establecidos para recibir comunicaciones, entre otros.

Dicho sistema deberá cumplir con los siguientes requisitos mínimos:

- **permitir identificar transacciones inusuales o fuera de los patrones habituales de comportamiento del cliente (por ejemplo: montos significativamente mayores a los habituales; cantidad y frecuencia de transacciones superior al patrón de uso normal).**
- **verificar la geolocalización desde donde se realizan las transacciones (ausencia de declaración de viaje; compras hechas desde distintos países en un corto lapso de tiempo, entre otros).**
- **alertar sobre el uso de dispositivos desconocidos y, en ese caso, reforzar la autenticación.**
- **identificar patrones sospechosos en la cantidad de transacciones rechazadas o sus motivos.**

k. Velar por el correcto funcionamiento del sistema, y la prestación continua del servicio, en circunstancias normales.

l. Anular del sistema a los instrumentos electrónicos el día en que pierdan validez (por vencimiento o por decisión de las partes conforme a los términos del contrato).

m. Determinar los medios y formas por los cuales la institución se podrá comunicar con el cliente. Deberá indicarle, de ser el caso, que nunca le solicitará que revele sus claves de identificación personal bajo ninguna circunstancia ni por ningún medio.

   El usuario declarará – como mínimo – dos direcciones de contacto (dirección, teléfono, correo electrónico, entre otras) a los efectos de recibir comunicaciones, notificaciones o avisos en relación con el instrumento electrónico, debiendo el emisor establecer medidas que garanticen razonablemente la veracidad de la información proporcionada. Estas medidas deberán establecerse al momento de celebración del contrato y toda vez que se solicite la modificación de dichos datos. En el caso de clientes que dispongan de una sola dirección de contacto, cuando se solicite su modificación la institución deberá obtener otra dirección a efectos de cumplir con lo dispuesto en el literal m).

n. Comunicar al usuario la comisión de cualquier ilícito o hecho irregular vinculado al instrumento electrónico de su titularidad al detectarlo o tomar conocimiento del mismo. Asimismo, deberá comunicarle todo intento o solicitud de modificación de los datos referidos en el literal i), indicando la solicitud de modificación recibida. Cuando se trate de la información de contacto del cliente, la comunicación deberá dirigirse, como mínimo, a dos de las direcciones de contacto válidas previamente y deberá indicar el

procedimiento a seguir para validar o rechazar el cambio solicitado. Una vez realizada la modificación, se deberá comunicar tal extremo al usuario.

o. Ofrecer al usuario la posibilidad de recibir notificaciones vía medios electrónicos (correo electrónico, mensajería instantánea, SMS, notificación en su propia aplicación, entre otros) cada vez que se procesa una transacción vinculada al instrumento electrónico de su titularidad, la que deberá indicar los medios disponibles para realizar consultas o reclamos vinculados con la transacción. Al menos uno de dichos medios electrónicos deberá ser sin costo.

   El usuario podrá modificar los parámetros de estas notificaciones o decidir no recibirlas. En este último caso, el emisor deberá guardar la constancia de la decisión informada del cliente de no recibir dichas notificaciones por medios que permitan su verificación, conforme a lo dispuesto por el artículo 496.

   Asimismo, las instituciones deberán notificar al usuario vía medios electrónicos cada vez que se intenten modificar datos tales como claves, número de identificación personal, dirección, teléfono, correo electrónico de contacto, medios y parámetros establecidos para recibir comunicaciones y notificaciones o cualquier tipo de parámetro operativo y/o de seguridad.

VIGENCIA: Las modificaciones dispuestas precedentemente regirán a partir del 1 de abril de 2026.

ARTÍCULO 364.1 (AUTENTICACIÓN REFORZADA DE CLIENTES).

Las medidas de seguridad a que refiere el literal i) del artículo 364 deberán incluir la aplicación de mecanismos de autenticación reforzada de clientes, como mínimo, para las siguientes operaciones:

a) **Acceso de los clientes a los canales digitales de la institución.**
b) **Compras con tarjetas de crédito y débito realizadas en forma no presencial.**
c) **Transferencias o pagos realizados desde cuentas bancarias.**
d) **Solicitudes de préstamos realizadas por medios no presenciales.**
e) **Acceso, modificación o actualización de datos sensibles, incluyendo credenciales, información personal, parámetros de seguridad o medios de contacto.**

La autenticación reforzada de clientes exige la utilización de al menos dos factores de autenticación de distintas categorías (conocimiento, posesión e inherencia).

Asimismo, se admitirá como mecanismo de autenticación reforzada de clientes para las solicitudes de préstamos que fueran realizadas en forma no presencial, la firma electrónica avanzada brindada por prestadores en el marco de la Ley N°

18.600 de 21 de setiembre de 2009 y sus modificativas y disposiciones reglamentarias.

Se aceptará la firma electrónica avanzada basada en certificados emitidos por prestadores acreditados ante la Unidad de Certificación Electrónica o que sean reconocidos como equivalentes cuando hayan sido emitidos por entidades no establecidas en el territorio nacional.

Las instituciones podrán optar por no aplicar un doble factor de autenticación en los siguientes casos:

1. **Transferencias o pagos a terceros asignados a una lista de beneficiarios de confianza.**

   La creación y actualización de la referida lista requiere la aplicación del doble factor de autenticación.

2. **Transferencias en las que el ordenante y el beneficiario sean la misma persona y ambas cuentas sean mantenidas en la misma institución.**

3. **Pagos de peajes y en el transporte público.**

4. **Pagos realizados por clientes que sean personas jurídicas mediante el uso de procesos y/o protocolos que garanticen mecanismos robustos de autenticación, autorización y seguridad, a criterio de la Superintendencia de Servicios Financieros.**

   Estos mecanismos deben considerar al menos los siguientes aspectos, según resulten aplicables a la modalidad operativa implementada:

   - **Gestión centralizada de usuarios, en la cual cada usuario que accede a la plataforma utilizada haya sido creado y gestionado a través de, al menos, dos Administradores de Seguridad formalmente autorizados a tales efectos por el cliente.**

   - **Autenticación reforzada mediante múltiples factores al acceder a la plataforma.**

   - **Flujo de aprobación de transacciones de acuerdo a niveles de riesgos y considerando el principio de separación de deberes.**

   - **Control de sesión con desconexión automática por inactividad y por sesiones múltiples.**

   - **Monitorización activa de patrones de comportamiento y prevención de fraudes que prevea notificaciones a los**

Administradores de Seguridad designados en el caso de comportamientos no habituales o sospechosos.

- **En el caso del uso de sistemas de conectividad "host to host", deberán establecerse mecanismos de conectividad seguros para la trasmisión de datos íntegros entre la institución y sus clientes corporativos.**

  Dichos mecanismos deberán incluir, como mínimo, cifrado de datos de extremo a extremo; métodos de autenticación mutua robustos; registro centralizado de actividades; sistemas de detección de intrusos y de seguridad de red diseñado para monitorear, filtrar y controlar el tráfico de red entrante y saliente basado en reglas de seguridad predeterminadas; validación de datos de entrada y salida de las solicitudes entre cada host; adecuada gestión de vulnerabilidades; y documentación actualizada y versionada de las interfaces que intervienen en las conexiones.

VIGENCIA: Las modificaciones dispuestas precedentemente regirán a partir del 1 de abril de 2026, salvo las excepciones dispuestas en los numerales 1. a 4. que podrán aplicarse a partir de la fecha de publicación de la correspondiente Resolución en el Diario Oficial.

LIBRO VII – RÉGIMEN SANCIONATORIO Y PROCESAL

PARTE I – SANCIONES PARA INSTITUCIONES DE INTERMEDIACIÓN FINANCIERA

TÍTULO VI – OTRAS SANCIONES

ARTÍCULO 690.5 (MULTA POR INCUMPLIMIENTO DE LAS OBLIGACIONES DE LOS EMISORES DE INSTRUMENTOS ELECTRÓNICOS).

Las instituciones de intermediación financiera que no cumplieren con las obligaciones a que refieren los artículos 364 **y 364.1** serán sancionadas con una multa no inferior al 1/10.000 (uno por diez mil) ni superior al 2/1.000 (dos por mil) de la responsabilidad patrimonial básica para bancos.

VIGENCIA: Las modificaciones dispuestas precedentemente regirán a partir del 1 de abril de 2026.