

Agosto 2025

- MARCO NORMATIVO VIGENTE Y PROYECTO EN CONSULTA PUBLICA

Seguridad de los Instrumentos Electrónicos

Introducción

El objetivo del proyecto normativo puesto a consulta pública es fortalecer la protección de los usuarios de los eventuales fraudes contemplando los riesgos de los distintos instrumentos electrónicos.

En este sentido, reforzar la seguridad de los mismos es fundamental a la hora de alcanzar dicho objetivo.



Marco Normativo - 01

definiciones

Agosto 2025

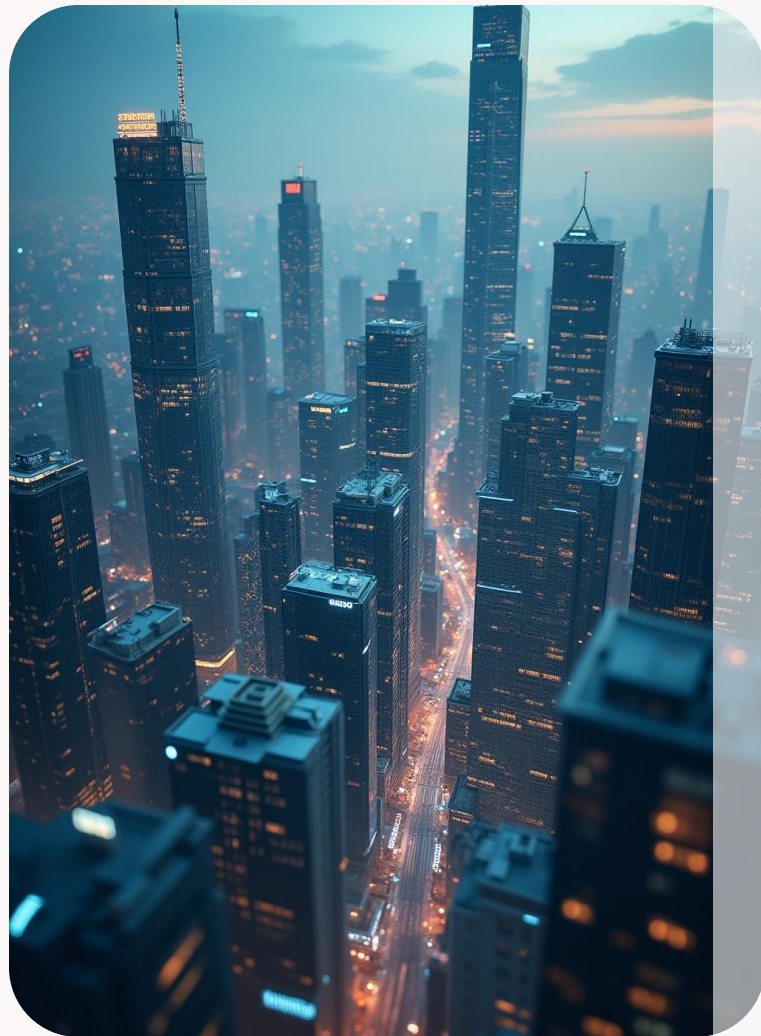
Ámbito de aplicación de la normativa y definición

A quien aplica?

Empresas de intermediación financiera, casas de cambio, empresas de servicios financieros, empresas administradoras de crédito, empresas otorgantes de crédito y empresas administradoras de plataformas de préstamos entre personas.

Que se entiende por **instrumento electrónico**?

Aquellos que permiten realizar operaciones por medios electrónicos. Entre otros, quedan comprendidos los que permiten realizar operaciones con los cajeros automáticos, por Internet o por vía telefónica, las transferencias electrónicas de fondos o información, y las tarjetas de crédito y débito





Medidas actuales de 02 Seguridad y Autenticación

CIRCULAR 2472 DEL 27/12/24

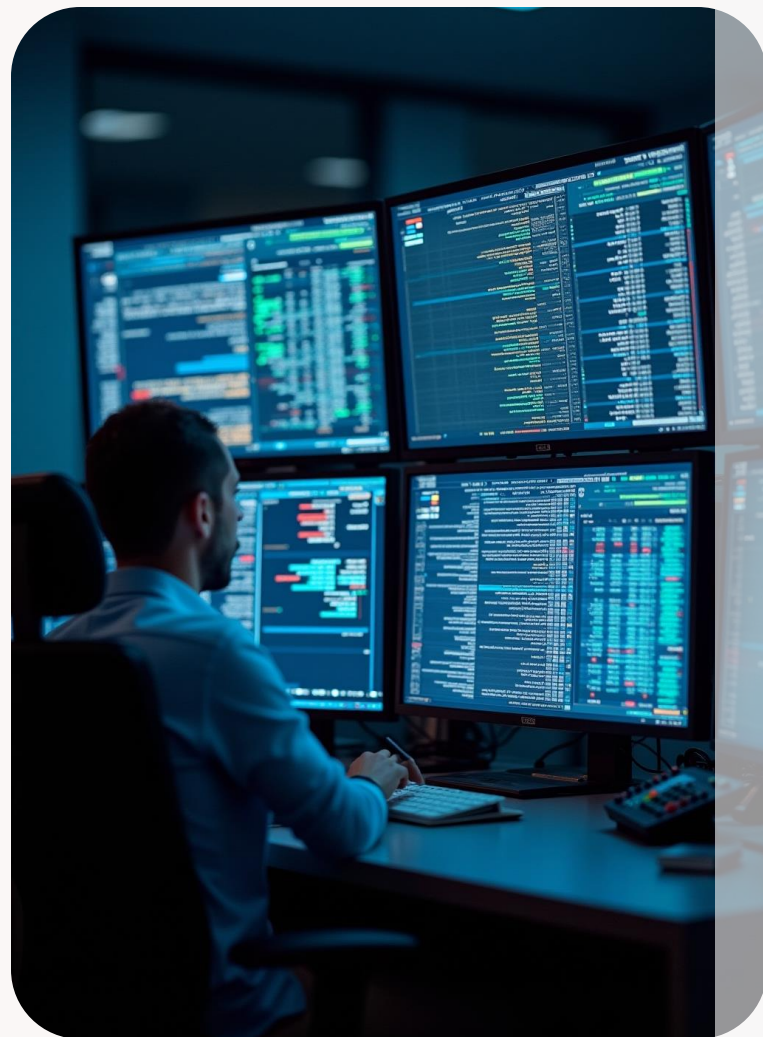
Obligaciones actuales del emisor

Los emisores deben garantizar la seguridad del sistema en que operan los instrumentos electrónicos, implementando metodologías de autenticación ajustadas al riesgo de las transacciones.

Se exige un doble factor de autenticación para transferencias o pagos a terceros desde una cuenta bancaria así como en solicitudes de préstamos no presenciales.

Deben tener medidas de control que permitan monitorear y controlar hechos irregulares vinculados al uso del instrumento o sistema en que operan.

Además se debe ofrecer al usuario la posibilidad de recibir notificaciones vía medio electrónico cada vez que se procesa una transacción con uno de estos instrumentos (debiendo ser alguno de estos medios sin costo)



Medidas previstas de Seguridad y Autenticación

03

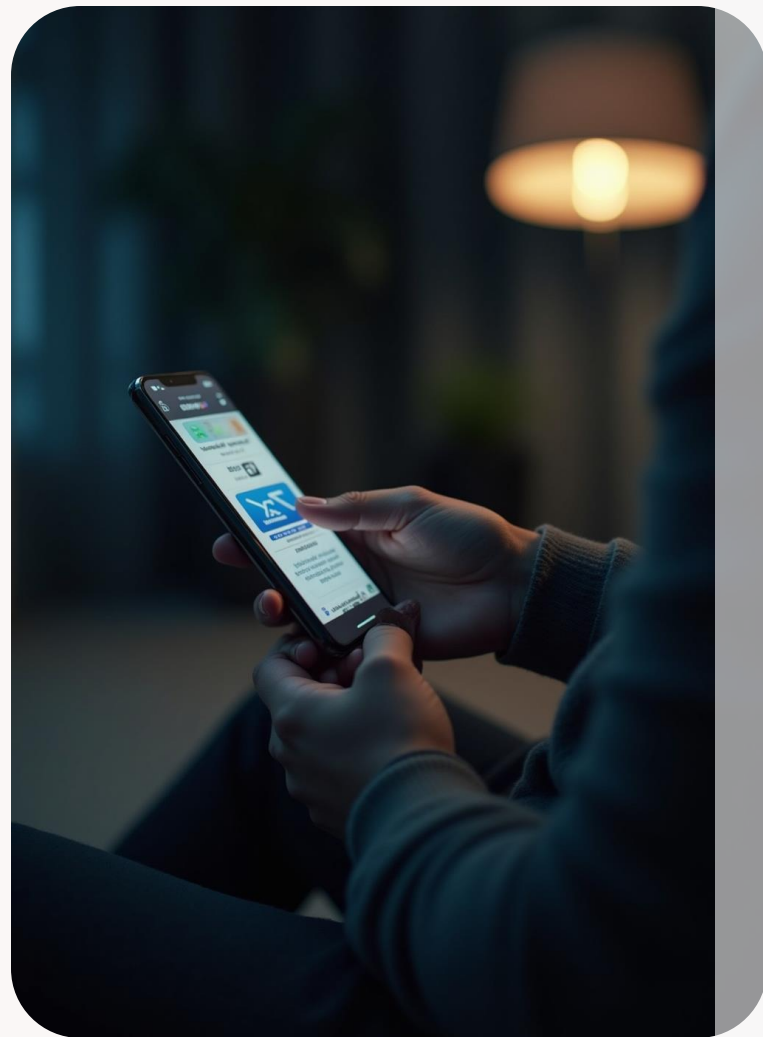
PROYECTO EN CONSULTA PÚBLICA

2025

Autenticación reforzada- Extensión

Se extiende la autenticación reforzada a las siguientes operaciones:

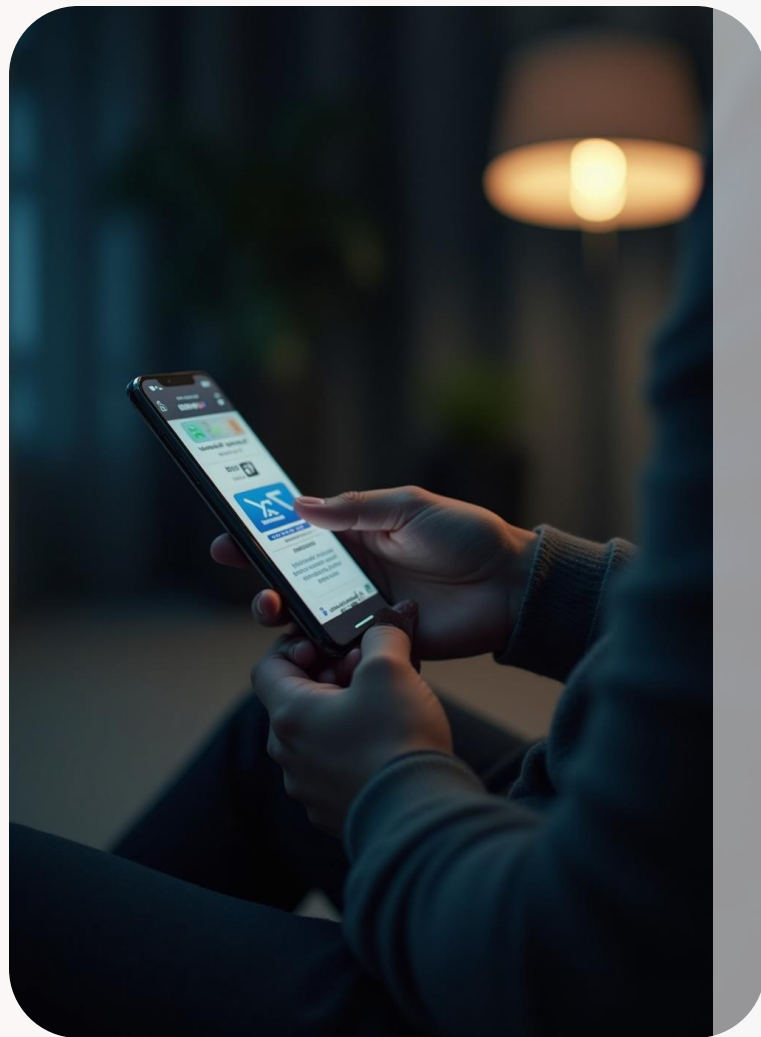
- Acceso de los clientes a los canales digitales de la institución.
- Compras con tarjetas de crédito y débito realizadas en forma no presencial.
- Acceso, modificación o actualización de datos sensibles, incluidos credenciales, información personal, parámetros de seguridad o medios de contacto.



Autenticación reforzada- Excepciones

Se puede no aplicar la autenticación reforzada en:

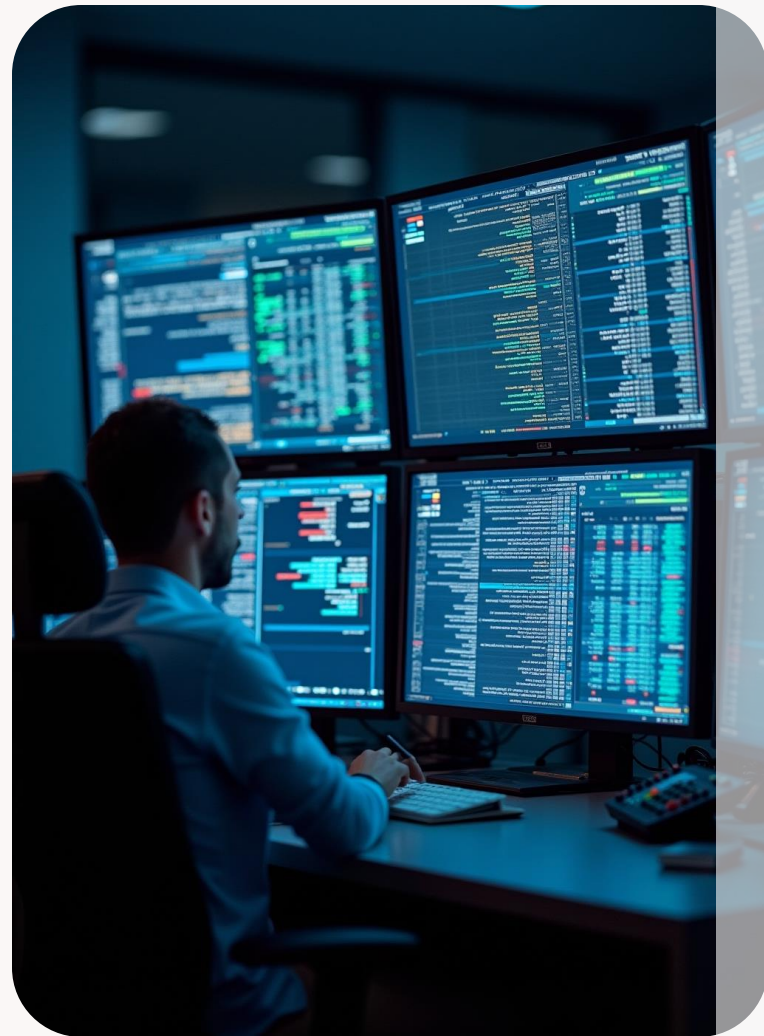
- Transferencias o pagos a terceros asignados a una lista de beneficiarios de confianza. (La creación y actualización de la referida lista requiere la aplicación del doble factor de autenticación).
- Transferencias en las que el ordenante y el beneficiario sean la misma persona y ambas cuentas sean mantenidas en la misma institución.
- Pagos de peajes y en el transporte público.
- 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.



Sistema de monitoreo- nuevos requisitos

Se incorporan requisitos que deberán cumplir los sistemas de monitoreo y control a efectos de detectar hechos irregulares vinculados con el uso del instrumento o el entorno en el que opera:

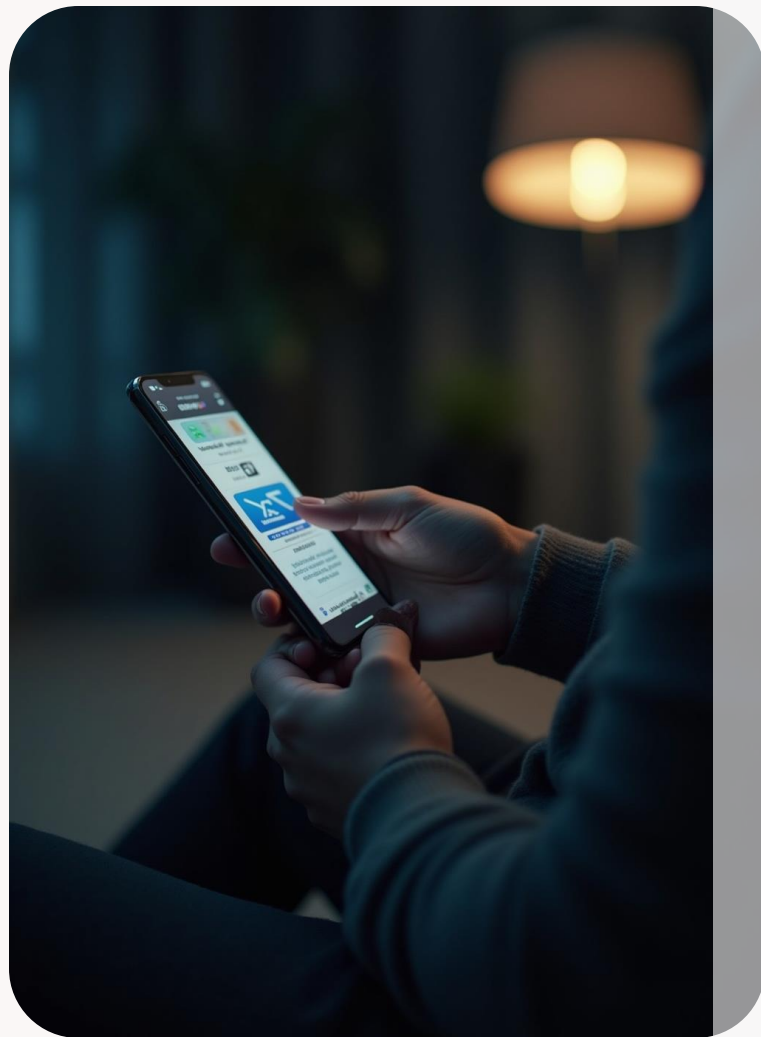
- la identificación de transacciones inusuales o fuera de patrones habituales de comportamiento del cliente (ej: montos significativamente mayores a los habituales; cantidad y frecuencia de transacciones superior al patrón de uso normal).
- verificación de geolocalización de dichas transacciones (ej: ausencia de declaración de viaje; compras hechas desde distintos países en un corto lapso de tiempo).
- alertas sobre el uso de dispositivos desconocidos.
- identificación de patrones sospechosos en transacciones rechazadas por cantidad o motivos.



Notificaciones usuarios- Incorporación

Se agrega la obligación de 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,
- cualquier tipo de parámetro operativo y/o de seguridad.



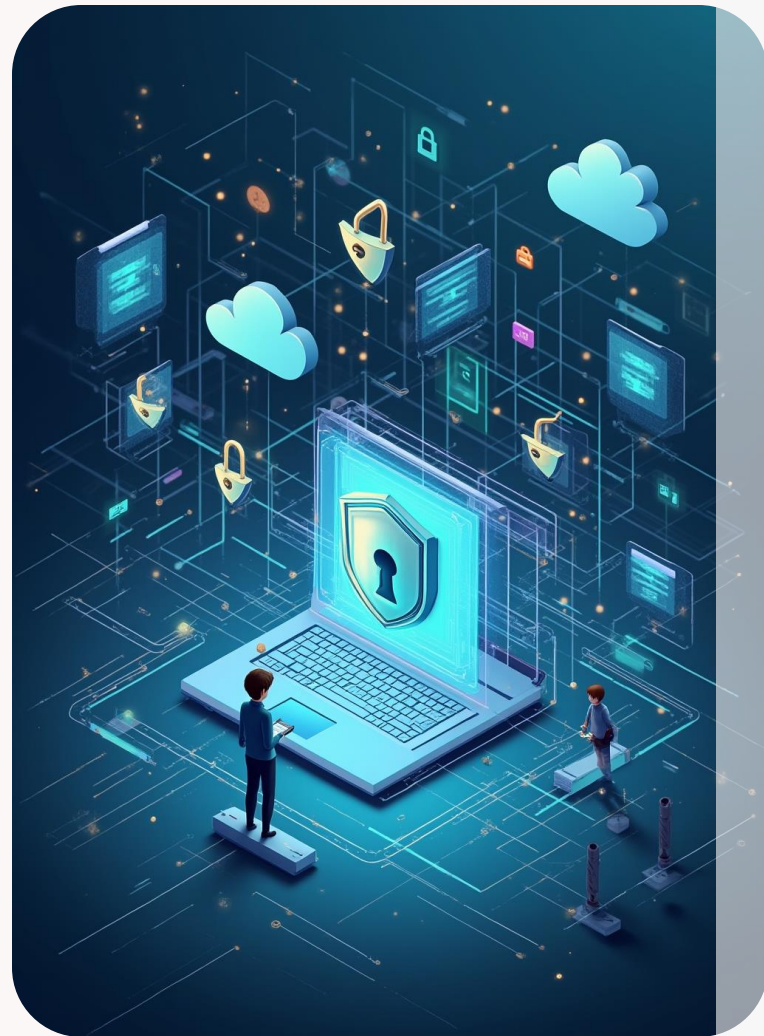
Conclusiones

La regulación contribuye a fortalecer el marco en material de seguridad de los instrumentos electrónicos.

Impulsa sistemas de monitoreo efectivos y autenticación reforzada para mitigar riesgos de fraude.

La protección y notificación al usuario son esenciales para mantener la confianza en transacciones digitales.

Estas medidas contribuyen a un entorno financiero más seguro y confiable.



MUCHAS GRACIAS