CMF emite nueva normativa de seguridad para medios de pago y expertos advierten "puntos sensibles"

El fin de la regulación es establecer lineamientos comunes respecto a los mecanismos mediante los cuales se realizan las transacciones.

19 de Junio de 2025 | 15:41 | Por Pablo San Martín, Emol

Emol

La Comisión para el Mercado Financiero (CMF) publicó una nueva normativa que fija estándares mínimos de seguridad, registro y autenticación aplicables al proceso de pagos y transacciones electrónicas.

La medida, que da cumplimiento al mandato del artículo 4 de la Ley N° 20.009, apunta a fortalecer la protección de los usuarios frente al fraude electrónico y estandarizar los protocolos utilizados por emisores de tarjetas de pago y otros prestadores financieros.

Y los expertos ya anticipan lo que podría devirar de su aplicación. Si bien la consideran positiva, también advierten sobre posibles efectos indeseados.

NOTICIAS RELACIONADAS

Se consolidan: Uso de billeteras digitales para pagos sin contacto anota inédito crecimiento de 1.000% en 2023

12

CMF publica normativa que aumenta el pago mínimo en tarjetas de crédito: ¿Qué es?

28

El objetivo de la norma

El objetivo de esta regulación es establecer lineamientos comunes respecto a los mecanismos mediante los cuales se realizan las transacciones electrónicas.

Esto, a través de la fijación de criterios claros de robustez e independencia para los sistemas de autenticación y registro.

Entre sus principales disposiciones se encuentra la exigencia del uso de Autenticación Reforzada de Clientes (ARC) en transferencias de fondos y en procesos de incorporación de clientes a plataformas digitales. Aunque la entrada en vigor general de la normativa está fijada para el 1 de agosto de 2025, las obligaciones asociadas a la ARC comenzarán a regir desde julio de 2026.

La CMF indica que si bien la Ley de Fraudes ya contemplaba ciertos requerimientos para emisores de medios de pago, esta nueva normativa avanza en la definición de estándares obligatorios, mientras se estudia también la posibilidad de extender exigencias a otros actores del sistema de pagos minoristas.

La opinión de los expertos

Fernanda González, abogada asociada de ARH Abogados, valoró positivamente la iniciativa. "La normativa representa un avance significativo en materia de protección de los usuarios del sistema financiero frente al fraude electrónico, al establecer estándares generales y obligatorios para todos los actores del mercado", sostuvo.

A su juicio, la regulación mejora el escenario anterior, en el que las medidas de seguridad eran definidas por cada entidad de forma individual, generando brechas y una cobertura dispareja.

No obstante, González también advirtió posibles dificultades durante la implementación. **"La exigencia de utilizar múltiples factores de autenticación podría dificultar el acceso a ciertos servicios financieros por parte de adultos mayores o de otros grupos con menor familiaridad tecnológica"**, indicó.

Sostuvo, asimismo, que "una de las categorías de autenticación reforzada —el factor de posesión — contempla el uso de dispositivos como smartphones o la recepción de mensajes OTP (One Time Password) por SMS. Esto involucra necesariamente a otros actores del mercado, como las compañías telefónicas, cuyas plataformas también pueden ser vulnerables a ataques, como ha quedado demostrado en casos recientes de duplicación de tarjetas SIM".

"En este sentido, la norma debió abordar de manera más integral la participación de estos terceros, estableciendo estándares o protocolos mínimos en coordinación con otros reguladores sectoriales. De lo contrario, se corre el riesgo de mantener una regulación excesivamente fragmentada, que no considere adecuadamente todos los eslabones del proceso de autenticación", aseguró.

En tanto, Álvaro Moraga, socio de Moraga CIA, aseguró que **"uno de los puntos más sensibles, advertido incluso durante la fase de consulta, es la aplicación de la presunción de dolo o culpa grave establecida en la Ley N° 20.009 cuando se utiliza voluntariamente la Autenticación Reforzada de Clientes (ARC) en operaciones no obligatorias".**

"Esta regla -argumentó- aunque legalmente vigente, puede generar efectos contraproducentes, desincentivando la innovación y la adopción proactiva de mecanismos avanzados de seguridad por parte de emisores más pequeños".

"Otro aspecto relevante es el plazo de implementación de la ARC en los casos de uso obligatorios, fijado para julio de 2026. Si bien este plazo debe respetarse y en ningún caso posponerse, sería deseable que la CMF habilite mecanismos de consulta o flexibilización temporal para Fintech de menor tamaño o capacidad operativa. No es razonable exigir la misma velocidad de adopción a una startup que a una entidad bancaria consolidada, sin reconocer las diferencias en escala, recursos y experiencia", finalizó.