El postergado adiós a las tarjetas de coordenadas

Un salto real en la seguridad bancaria

Hay decisiones que parecen técnicas, pero en realidad son de sentido común. El retiro de la tarjeta de coordenadas es una de ellas. Durante años, los bancos en Chile protegieron operaciones sensibles con un cartón plastificado que, si bien fue útil en su momento, hoy equivale a dejar la llave pegada en la puerta: cómodo, pero altamente vulnerable.

Hasta hace unos días, la norma de la Comisión para el Mercado Financiero (CMF) establecía que la tarjeta de coordenadas desaparecería el 1 de agosto de 2025, dando paso obligatorio a la Autenticación Reforzada de Clientes (ARC) en operaciones críticas. Sin embargo, la institución acaba de anunciar que la medida se posterga un año: será exigida recién a partir del 1 de agosto de 2026 para dar más tiempo a los bancos para ajustar sistemas, capacitar personal y asegurar soluciones inclusivas para todos los usuarios.

¿Nos pone esto a la vanguardia global? No. Pero sí nos alinea —aunque más tarde— con estándares internacionales como la Strong Customer Authentication (SCA) del reglamento PSD2 europeo, que exige múltiples factores independientes y, como elemento clave, el vínculo dinámico: un mecanismo que ata la autenticación al monto y al destinatario de la operación, invalidándola automáticamente si algo cambia.

Este modelo, bien aplicado, reduce drásticamente el fraude en pagos remotos y mejora la trazabilidad del sistema. La evidencia es clara: Microsoft calcula que activar múltiples factores de autenticación disminuye en un 99 % el riesgo de cuentas comprometidas. Google, por su parte, reportó cero incidentes de phishing tras adoptar llaves de seguridad con estándares FIDO, que operan con códigos temporales generados desde hardware y con verificación criptográfica real.

En Chile, el debate público ha girado en torno a la inclusión: ¿qué pasa con los adultos mayores que no usan smartphones? La respuesta existe y ya está en marcha: tokens físicos equivalentes, enrolamiento asistido en sucursales y soporte accesible. La seguridad no tiene por qué ser excluyente si se diseña bien.

Con un año extra sobre la mesa, el riesgo es que el impulso se diluya. Que la prórroga sea excusa para demorar inversiones o postergar mejoras. La autenticación reforzada no debe convertirse en una promesa eterna; tiene que ser una experiencia simple, medible y accesible. El enrolamiento debe tomar minutos, no semanas. Los tokens deben estar disponibles en sucursal sin burocracia. El soporte debe funcionar a la primera. Y deben existir métricas públicas que demuestren avances concretos: usuarios activos, reducción de fraudes, éxito en la activación de biometría.

La CMF ya reguló y entrego nuevos plazos. La banca tiene ahora tiempo extra para perfeccionar la implementación. Y los usuarios, la oportunidad de prepararnos: activar biometría, familiarizarnos con nuevos métodos y no aprobar nunca lo que no iniciamos. Si cada actor aprovecha este año adicional, el resultado seguirá siendo tangible: menos fraude, más confianza y un sistema donde la seguridad deje de depender de un papel impreso para integrarse, de verdad, en cada transacción.

Fernando Abrego.