

Ciberdelito en la era digital: los desafíos de seguridad que interpelan al sistema bancario

06/02/2026



Sergio Giménez, secretario general de la Asociación Bancaria Seccional Mendoza, analizó el complejo escenario del ciberdelito en la provincia. En un contexto donde los fraudes digitales crecen exponencialmente, el referente de los trabajadores bancarios advirtió sobre la falta de campañas educativas por parte de las entidades y la peligrosa pérdida de trazabilidad del dinero cuando las estafas derivan hacia billeteras virtuales no reguladas.

La vulnerabilidad pospandémica y el déficit en educación

El vuelco masivo de los usuarios a la virtualidad tras la crisis sanitaria no fue acompañado, según Giménez, por un fortalecimiento proporcional de la seguridad y, sobre todo, de

la formación del usuario. «Uno se anima a pensar que las empresas financieras invierten y van a la vanguardia en seguridad informática, pero en la práctica notamos con mucha nitidez que pospandemia hubo un aumento significativo en la bancarización. Lo que nos queda es un interrogante sobre las inversiones que el sistema financiero debería hacer para proteger a los clientes. En Argentina y Latinoamérica, los niveles de ciberdelito están en un orden de 14 veces más que en otras regiones del mundo», dijo a FM Vos 94.5.

«Si bien existe buena voluntad y se trabaja mucho al respecto, no vemos de parte de los empleadores una vocación por educar al cliente, advertir que no respondan llamadas no identificadas o correos sin identificación oficial. Es una situación transversal; antes creíamos que solo ocurría con adultos mayores, pero hoy las estafas golpean con fuerza a los clientes jóvenes», añadió.

El «agujero negro» de las billeteras virtuales

Uno de los puntos más críticos señalados por el titular de La Bancaria es la diferencia entre el sistema bancario tradicional, bajo la órbita del Banco Central (BCRA), y las plataformas digitales de pago. «El sistema financiero se hace cargo y la mayoría de los casos se resuelven cuando el dinero queda dentro del sistema. El problema surge con lo que llamamos cuentas con CVU de las billeteras virtuales. Mientras el dinero circula dentro de los bancos, vos podés seguir la trazabilidad. Cuando el fondo sale hacia las billeteras virtuales, esa trazabilidad se pierde», coincidió Giménez.

«Incluso ha habido casos resonantes donde fiscalías de delitos económicos han pedido información a estas plataformas y ni siquiera han respondido a la Justicia. Ahí el cliente queda en una situación de vulnerabilidad total», opinó.



La detección de un movimiento extraño en la cuenta bancaria suele ser el inicio de un periodo de profunda incertidumbre
El proceso de recuperación: ¿Qué pasa cuando el fraude se concreta?

La detección de un movimiento extraño en la cuenta bancaria suele ser el inicio de un periodo de profunda incertidumbre. Sin embargo, Sergio Giménez aclaró que, si bien el sistema no es instantáneo, existen mecanismos periciales dentro de los bancos para determinar la legitimidad de las operaciones y proceder a la devolución del capital cuando se comprueba el engaño. **«Hay que llevar tranquilidad en medio de la bronca que significa sentirse vulnerable. El sistema, en términos generales, es confiable. Cuando se analiza el área específica de cada entidad y se prueba que hubo un modus operandi de estafa, los bancos suelen encauzar la situación y revertir los movimientos. Lo que debemos entender es que no es automático; el usuario vive días de mucha zozobra creyendo que se hará cargo de una deuda imposible de pagar, pero la respuesta institucional termina llegando»**, aseveró el secretario general de la Asociación Bancaria Seccional Mendoza.

«La respuesta no es inmediata. No haces el reclamo y te

devuelven el dinero a las 24 horas. Lleva un proceso de investigación interna para verificar la trazabilidad, pero en la gran mayoría de los casos donde se prueba la ciberestafa, el banco produce la reversa de la operación», agregó.

Tarjetas de crédito versus débito

Existe una diferencia operativa fundamental en cómo se recupera el dinero. **«El trámite en tarjetas de crédito suele ser más dinámico porque se puede desconocer el consumo y simplemente no pagarlo mientras se investiga. En la caja de ahorro o cuenta corriente se complejiza un poco más, porque el banco debe realizar una devolución efectiva de dinero que ya salió de la cuenta»**, explicó Giménez.

«Hoy los bancos cuentan con espacios específicos donde trabajadores bancarios toman las denuncias y asesoran al cliente. Aunque el trámite pueda parecer lento, la mayoría de las situaciones terminan resolviéndose de forma favorable para el estafado», añadió.

El «famoso» Token: ¿Es reversible una operación autorizada?

El uso del token se ha convertido en la última frontera de seguridad, pero también en el principal objetivo de los delincuentes que utilizan ingeniería social para engañar a las víctimas. **«El sistema ha ido sumando capas: empezamos con un PIN, luego claves alfabéticas y ahora el token. Los delincuentes son profesionales y logran engañar al usuario para que les pase ese número. Cuando uno da el token, el análisis del banco es más pormenorizado porque hubo una autorización voluntaria»**, indicó Giménez.

«No obstante, los bancos tienen la tecnología para identificar si hubo un entramado de delincuencia detrás. Incluso habiendo autorizado con el token, si se concluye que fue una estafa, se procede a reversar la operación. El proceso es lento y genera semanas de zozobra, pero la respuesta institucional suele llegar», enfatizó al cierre de la charla.