

ANTE LOS FRAUDES FINANCIEROS, LOS BANCOS CONTINUAN OPERANDO BAJO MODELOS DE GESTION DEL RIESGO, QUE NO RESGUARDAN DEBIDAMENTE A LOS USUARIOS

En la sede de la Defensoría del Pueblo se llevó a cabo una **-Reunión de Trabajo-** con la presencia del Sr. Gerente General del Banco de Formosa, Lic. Daniel Padín y la Dra. María Beatriz Paz Saravia Responsable del Área de Canales y Asistencia al Usuario, quienes fueron recibidos por el Defensor del Pueblo, Dr. Leonardo Gialluca, Defensora Adjunta, Dra. Sylvina Portillo y Asesores Legales. Dicha convocatoria se realizó a requerimiento del Organismo de la Constitución atento a los reclamos recibidos por fraudes/estafas sufridas por los usuarios de la Billetera Virtual Onda de la citada entidad bancaria. **Los funcionarios bancarios indicaron que se trabaja permanentemente en los sistemas de seguridad, para mejorar y garantizar la no vulneración de los mismos, resaltando que todos los sistemas de seguridad, tanto de la Billetera Virtual Onda, como de la entidad bancaria, cumplen con los parámetros impuestos por el BCRA. Consultado el Licenciado respecto a los recientes problemas de la billetera Onda que generaron inconvenientes a los usuarios, los cuales dieron lugar a numerosas actuaciones desde este Organismo, explicó que los mismos fueron de carácter técnico y tuvieron origen fuera de la entidad, señalando que se encuentran trabajando en la resolución de estas situaciones, tomando contacto directo con cada uno de los clientes que fueron afectados, otorgándoseles a los usuarios damnificados soluciones definitivas.** Por otra parte, el Ombudsman Provincial, informó que, el aumento sostenido del fraude financiero está evidenciando que mientras las amenazas evolucionan con velocidad y sofisticación, muchas instituciones aún siguen operando bajo modelos de gestión del riesgo pensados para otra era. En este sentido, la **Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)** ha registrado en los últimos años más de 30 mil reportes por delitos informáticos, entre estafas por compra-venta por internet, la suplantación de identidad y accesos ilegítimos. Es una realidad que a medida que avanza la adopción de métodos de pago digitales, más se perfecciona el cibercrimen, pero a la hora de buscar cómo frenar este problema, suele mirarse hacia el lado equivocado. **No son los delincuentes más sagaces; quizás los bancos son parte del problema.** El crecimiento del fraude se debe más a una cultura institucional excesivamente conservadora que a un asunto técnico, porque los bancos vienen tratando el fraude como un riesgo tolerable y presupuestable en lugar de asumirlo como una prioridad de liderazgo. Esta es una mentalidad que hoy es insuficiente, teniendo en cuenta la velocidad del ecosistema bancario donde los pagos en tiempo real, las identidades sintéticas y el uso extensivo de Inteligencia Artificial por parte de redes criminales altamente coordinadas es una constante. **Por ello, el problema** se agrava cuando la prevención del fraude queda fragmentada entre áreas legales, de riesgo u operaciones, diseñadas para evitar exposición y retrasar decisiones. En estos esquemas, los equipos responsables carecen de autonomía, presupuesto y capacidad de innovación, lo que se traduce en respuestas lentas, modelos que tardan meses en actualizarse y arquitecturas tecnológicas que no acompañan la velocidad de los ataques actuales. Los sistemas basados en reglas rígidas generan altos niveles de falsos positivos y rechazos innecesarios. Con esto, se afecta la confianza del cliente y se elevan los costos operativos. Mientras tanto, los ciberdelincuentes operan con modelos ágiles, descentralizados y en tiempo real, muy similares a los de una startup tecnológica. **Las instituciones que no reaccionan a tiempo pierden dinero, credibilidad, depósitos y margen operativo.** Incluso, el incremento de litigios asociados a fallas en la protección contra el fraude comienza a generar impactos que trascienden el balance financiero, afectando costos de adquisición y reservas de capital. Esto implica pasar de estructuras orientadas a auditorías y documentación a modelos de gestión basados en **inteligencia en tiempo real, análisis de comportamiento y toma de decisiones integrada al negocio.** Algunas entidades ya están avanzando en esta dirección, transformando sus equipos antifraude en unidades ágiles, con enfoque de producto y responsabilidad directa sobre resultados. Estas capacidades permiten detectar fraudes con mayor precisión y habilitar nuevos casos de uso, como procesos de onboarding más fluidos, aprobaciones de crédito en tiempo real y experiencias personalizadas basadas en patrones de comportamiento. Para el sistema financiero argentino, la inacción puede convertirse en pérdidas, el fraude no puede seguir tratándose como un simple requisito de cumplimiento. Afrontar esta problemática es una verdadera prueba de liderazgo. La reputación está en juego y, si se pierde, con ella se va la confianza, que es lo más difícil de recuperar.