CIBERDELITOS

CTA- octubre 2025

Introducción

La acelerada digitalización de los servicios financieros en Uruguay ha facilitado el acceso a productos bancarios y de pagos electrónicos, pero también ha generado un entorno fértil para el crecimiento de los ciberdelitos. Estos delitos comprometen no solo la reputación de las instituciones financieras, sino también la confianza y seguridad de los usuarios, así como trae nuevos riesgos para éstos.

Es en este contexto que desde AEBU (Sindicato de trabajadores y trabajadoras del Sistema Financiero) consideramos pertinente y oportuno hacer algunos aportes para la Agenda Nacional de Seguridad Pública, enfocados principalmente en las principales problemáticas y desafíos vinculados a la protección de los usuarios y trabajadores del sector, así como en la protección de las instituciones ante ataques a sus sistemas, datos o infraestructuras tecnológicas.

Diagnóstico

Los ciberdelitos son conductas ilícitas que se valen de medios informáticos para cometer fraudes, accesos indebidos o vulneraciones a la integridad de datos y sistemas.

Particularmente, el sistema financiero es un campo muy sensible para estas prácticas, en vista de que es un sector intenso en tecnología, que en los últimos años ha presentado una digitalización acelerada, entendiendo esto como el desplazamiento de canales físicos a canales digitales para proveer servicios y siendo a su vez un sector neurálgico de la economía dónde se mueve dinero de manera constante entre agentes.

La digitalización en el sistema financiero si bien viene observándose hace tiempo, la pandemia de covid-19 implicó que muchas personas que anteriormente no utilizaban estos canales se vieran incentivadas o incluso obligadas a trasladarse a éstos. Particularmente en el sistema de pagos se observa en los últimos años una evolución con un marcado vuelco por canales digitales a la hora de realizar pagos (en 2024 el 77% de los pagos se hizo por vía electrónica)[1]. Este cambio acelerado dejó expuestos a muchos usuarios, quienes no tuvieron a tiempo acceso a conocimientos o advertencias adecuadas.

Por otra parte, asociado al incremento de incorporación tecnológica en el sistema financiero uruguayo, en línea con las tendencias globales, en los últimos años se han incrementado significativamente las tercerizaciones de servicios, principalmente

[1] Reporte Informativo del Sistema de Pagos Minorista – 2do. Semestre 2024 (Banco Central del Uruguay).

asociados a procesamiento de datos, desarrollo y mantenimiento de software, sistemas de seguridad informática y atención al cliente.

Si bien en un primer análisis esto conlleva a una reducción de costos para las instituciones, esta práctica traslada parte del riesgo operativo y cibernético a terceros. Esto genera nuevos puntos de vulnerabilidad, especialmente cuando las empresas contratadas no mantienen los mismos estándares de seguridad o cuando operan desde otras jurisdicciones, pudiendo generar vacíos legales.

Asimismo, la proliferación de proveedores desdibuja y complejiza el ámbito regulatorio y de control, lo que, unido a la concentración de actividades en pocos proveedores agrega nuevos riesgos al sistema.

Desde el lado de los usuarios, si bien a priori estos cambios implican una mejora en la experiencia de atención, la contracara es que existen nuevos riesgos que deben considerarse al analizar este fenómeno. Por este motivo, resulta relevante analizar de qué manera la tecnología ha afectado a los usuarios del sistema financiero y así pensar en posibles políticas que acompañen estas transformaciones mitigando los potenciales efectos negativos.

En relación con los nuevos riesgos asociados a la digitalización del sector, en 2024 Uruguay atendió 14.264 casos de ciberataques[2]. Asimismo, estos ataques están dejando de ser masivos, incrementando su sofisticación y personalización a través de nuevas tecnologías como la Inteligencia Artificial (IA).

Un claro ejemplo ocurrió en mayo de 2024, el Banco Santander comunicó un “acceso no autorizado” a un proveedor con información de clientes en España, Chile y Uruguay. Unas semanas después de esto, apareció una base de datos en BreachForums, foro de dark web utilizado por ciber atacantes.

La aparición de numerosos ciberataques en el sector trae aparejado que existan nuevos costos para las instituciones que invierten no solo en implementación de nuevos procesos si no en redes de ciberseguridad para poder paliar los crecientes ataques informáticos. A su vez, para las instituciones los hackeos de información son un riesgo para su reputación histórica y la potencial pérdida de confianza por parte de los usuarios.

Mientras que los nuevos riesgos para los usuarios se vieron materializados en un incremento en los reclamos por parte de los usuarios. El Informe estadístico del Servicio de Atención al Consumidor de 2024 elaborado por el Ministerio de Economía y Finanzas (MEF)[3] muestra cómo los servicios financieros tienen el tercer puesto en la cantidad de atenciones y que, a su vez, el sector mostró un importante crecimiento con respecto a los datos del año anterior.

[2] Datos de CERTUy (Centro Nacional de Respuesta a Incidentes de Seguridad Informática)
[3] Informe estadístico de las Atenciones en la Unidad Defensa del Consumidor – Ejercicio 2024 | Ministerio de Economía y Finanzas

Es importante considerar que los datos disponibles son de denuncias realizadas por las personas, por lo cual los datos implican un importante subregistro, ya que aproximadamente 9 de cada 10 no denuncian estas situaciones según declaraciones recientes del ministro del interior, por este motivo, se analizan tendencias y cantidad de atenciones.

Las denuncias recibidas por el BCU en 2024, detalladas en el reporte de atención al usuario financiero[4], se mantuvieron estables en comparación a 2023. Sin embargo, cuando se analizan las denuncias por tipo de problemática, la mayoría de estas denuncias y que a su vez muestran un sostenido crecimiento son las que se encuentran catalogadas "por desconocimiento de operaciones", que incluyen principalmente situaciones en las que las personas, bajo engaño, fraude o estafa revelan sus claves a terceros y se realizan operaciones no consentidas, así como casos en que se opera con una tarjeta hurtada.

Dichos riesgos, anteriormente eran asumidos por las propias instituciones financieras, y con estos nuevos procesos digitales, existe un traslado de responsabilidad hacia los usuarios. En este contexto, crece la probabilidad para los usuarios de exponerse a riesgos asociados a delitos cibernéticos, siendo fundamental que las medidas de ciberseguridad y regulaciones banco centralistas logren acompasarse a los cambios.

Como precedente, en 2025 la justicia falló por primera vez que una institución (BROU), en primera instancia, tuviera que reembolsar económicamente a clientes que fueron víctimas de fraude digital[5].

De todos modos, fue un caso puntual y no existe actualmente protocolo ni normativa clara sobre los procesos ante estas situaciones.

Marco regulatorio vigente

En este contexto, Uruguay aprobó en 2024 la Ley de Prevención y Represión de la Ciberdelincuencia[6]. La ley tipifica nuevos delitos penales, promueve medidas educativas y otorga a las instituciones de intermediación financiera (IIF) e instituciones emisoras de dinero electrónico (IEDE), la posibilidad de adoptar medidas preventivas.

La ley crea ocho nuevos delitos penales[7], y, aunque, por un lado, por varios actores se resalta la importancia de que estos se hayan tipificado, también hay críticas.

[4] https://usuariofinanciero.bcu.gub.uy/wp-content/uploads/2025/04/Usuario_Financiero_Reporte-2024.pdf

[5] https://www.montevideo.com.uy/Noticias/-Se-terminaron-anos-de-amargura--Justicia-fallo-a-favor-de-estafados-y-BROU-debera-pagar-uc934406

[6] https://www.impo.com.uy/bases/leyes-originales/20327-2024

[7] - *Acoso telemático*: Uso de medios digitales (internet, redes sociales, mensajes de texto, etc.) para perseguir, vigilar o intentar establecer contacto con otra persona de manera repetitiva, afectando gravemente su vida cotidiana.

Particularmente el Instituto de Derecho Penal de la Facultad de Derecho de la Universidad de la República, coincide en calificar los delitos creados como innecesarios y redundantes. Según los especialistas en la materia que han participado en el proceso de elaboración de esta ley, se definen conductas que ya estaban alcanzadas.

Se establece también en la ley la creación de un registro de ciberdelincuentes con el fin de identificar, gestionar y prevenir transacciones no consentidas, así como permite también a las instituciones inmovilizar fondos cuando se toma conocimiento de que en las cuentas ingresaron fondos de terceros en transacciones no autorizadas por el titular. Además, en esta ley se regula la promoción de medidas educativas a través de lo que denomina Campaña Nacional Educativa.

Por otra parte, en agosto 2025 el BCU hizo público un proyecto normativo que entraría en vigor a partir de abril 2026 que introduce cambios en la Recopilación de Normas de Regulación y Control del Sistema Financiero, estos cambios tienen el objetivo de proteger a los usuarios de eventuales fraudes modificando requerimientos de seguridad relativos al uso de instrumentos electrónicos.

Las modificaciones alcanzan a todos los emisores de instrumentos electrónicos, incluyendo: bancos, casas financieras, cooperativas de intermediación financiera, bancos de inversión, instituciones financieras externas, administradoras de grupos de ahorro previo, casas de cambio, empresas administradoras de crédito, entidades otorgantes de crédito, empresas de servicios financieros y empresas administradoras de plataformas para préstamos entre personas.

Se incorporan nuevas obligaciones y exigencias para implementar mecanismos de prevención y detección de irregularidades, como la necesidad de notificar al usuario cada vez que se intenten modificar datos, se delimitan los parámetros que permitan identificar transacciones inusuales o fuera de los patrones habituales de comportamiento de cada usuario, verificar la geolocalización desde donde se realizan

---

- *Fraude informático*: Ocurre cuando se emplean medios electrónicos para engañar a una persona y obtener un beneficio económico a su costa. Ejemplos comunes incluyen transferencias bancarias no autorizadas o el uso fraudulento de tarjetas de crédito.
- *Daño informático*: Se configura cuando alguien destruye, altera o inutiliza sistemas informáticos con la intención de causar daño, como el borrado de archivos, la introducción de virus o el bloqueo de accesos a sistemas críticos.
- *Acceso ilícito a datos*: Entrada no autorizada a sistemas informáticos ajenos para manipular o divulgar información confidencial sin consentimiento.
- *Interceptación ilícita*: Cuando se interceptan parcial o totalmente comunicaciones que están en tránsito en redes o sistemas informáticos, violando el derecho a la privacidad.
- *Vulneración de datos*: Se produce cuando una persona -empleando tecnología- accede, se apropia, usa o modifica información confidencial de terceros sin su autorización.
- *Suplantación de identidad*: cuando alguien asume falsamente la identidad de otra persona o entidad, usando redes sociales, correos electrónicos, cuentas bancarias u otras plataformas digitales para acceder a información personal y credenciales de acceso.
- *Abuso de dispositivos*: se configura cuando una persona crea, adquiere, importa, vende o proporciona a otros programas, credenciales o contraseñas diseñados para facilitar la comisión de un delito.

las transacciones, alertar sobre uso de dispositivos que no se utilizaron anteriormente, en esos casos reforzar la autenticación.

Se amplían las operaciones que requieren de autenticación reforzada, pasando a ser obligatoria además de para transferencias y pagos y solicitudes de préstamos, para el acceso a canales digitales de la institución, compras no presenciales con tarjetas y cualquier modificación de datos sensibles como credenciales, datos personales.

Otro punto incluido en este proyecto está relacionado con las sanciones aplicables a las instituciones por incumplir con las obligaciones, ampliando la gama de incumplimientos para que sean aplicables las multas.

Comentarios – aportes para la Agenda Nacional de Seguridad Pública

El ciberdelito es un fenómeno en expansión que afecta en gran dimensión al sistema financiero uruguayo. Si bien el país avanzó con la Ley N° 20.327, persisten desafíos significativos en la protección de los usuarios y apoyo a los trabajadores del sector, vinculados a la educación digital, la claridad normativa sobre responsabilidades en casos de fraude, entre otros.

La protección del consumidor financiero digital debe considerarse un componente central del Plan Nacional de Seguridad, con enfoque integral y preventivo.

Como primer punto, resulta necesaria una estrategia de educación financiera, abarcando además de conceptos financieros y económicos, educación en lo que respecta a conductas financieras saludables y formación en ciberseguridad. Dónde también se advierta y enseñe a los agentes acerca de los nuevos riesgos existentes y cómo proteger sus cuentas y datos, y de qué manera operar ante un posible delito informático. Podría pensarse en un programa coordinado entre las distintas instituciones que actualmente ya trabajan en educación financiera (BCU, ANEP, Udelar, agentes de la industria, AEBU, entre otros).

Estas iniciativas podrían ser acompañadas por campañas de bien público de concientización de los ciberataques.

Por otra parte, los trabajadores del sector son la primera línea de respuesta ante ciberataques, fraudes digitales o accesos indebidos. Por ello, las instituciones financieras deben priorizar políticas de formación continua y concientización en seguridad digital, así como las herramientas adecuadas para abordar estos casos. Resulta necesario disponer de roles o funciones especializadas en la atención de casos de ciberdelito, con el objetivo de que la atención sea inmediata y eficaz.

Los usuarios están expuestos a asumir enteramente la responsabilidad ante un ciberdelito o estafa en la mayoría de las veces, puesto que actualmente la responsabilidad es difusa, no está claro ni regulado quién asume las pérdidas, la normativa aún está en evolución, pero debería definir claramente estas

compensaciones y procesos garantizando protección a los usuarios. Dicha protección debe incluir criterios de riesgo que permitan el uso de los canales más expuestos a los ciberdelitos solo a aquellos clientes mejor preparados para enfrentar las amenazas.

Actualmente, cada institución cuenta con sus propios planes de respuesta a incidentes, lo cual suele generar demoras y tampoco está tan claro de qué manera proceder con quienes sufren un ciberdelito.

Por esto, es fundamental la protocolización y estandarización de acciones ante ataques cibernéticos, para un sistema financiero que tenga claro los pasos a dar, tanto desde las instituciones cómo desde los usuarios, resulta de vital importancia en este contexto. Donde se estipule qué operaciones tienen potencialidad de ser sometidas a ciberataques, se generen procedimientos claros tanto para los usuarios víctimas de estos ataques cómo para los trabajadores de las instituciones, asegurando transparencia y la mayor agilidad posible.

En esta línea, el intercambio de información con las autoridades debe ser fluido, considerando que será fuera de la institución financiera dónde se dictaminará el "fallo" del ciberataque, los posibles reintegros a las víctimas o multas para las instituciones.

Otro aspecto para considerar es que las instituciones financieras manejan un gran volumen de información de los usuarios, que debe ser protegida, cumpliendo con la Ley de Protección de Datos[8]. Debería establecerse, además, penas claras que responsabilicen a las instituciones en caso de incurrir en fallas que revelen datos indebidos de sus clientes, buscando un equilibrio entre protección de datos y mecanismos de prevención de fraude.

Asociado a esto, y considerando que el incremento en las tercerizaciones ocurrido en el último tiempo, lleva a que proveedores externos a las instituciones accedan a información de clientes e instituciones del sistema financiero, resulta necesario considerar que existe una ampliación de riesgos, referente a robos o uso indebido de datos personales y financieros. A su vez, si estos servicios se contratan en el exterior, pueden existir vacíos legales respecto al cumplimiento de normas de protección de datos y ciberseguridad.

Por ende, el incremento de las tercerizaciones en el sistema financiero exige también especial atención y que se consideren nuevas estrategias de supervisión, control y responsabilidad compartida, tanto de parte del regulador como de las instituciones. Es necesario que se promueva la adopción de estándares de ciberseguridad obligatorios para proveedores, así como también, mecanismos de auditoría y control, como forma de garantizar la protección de los datos y derechos de los usuarios.

[8] https://www.impo.com.uy/bases/leyes/18331-2008