CÁMARA URUGUAY FINTECH

Revisión de la normativa sobre seguridad de instrumentos electrónicos

La Circular N.º 2497, emitida por la Superintendencia de Servicios Financieros del Banco Central del Uruguay y aprobada el 29 de diciembre de 2025, introduce una revisión integral de la normativa aplicable a la seguridad de los instrumentos electrónicos, con el objetivo explícito de **proteger a los usuarios frente a fraudes y usos indebidos en entornos digitales.**

La norma alcanza a un amplio conjunto de entidades, incluyendo instituciones de intermediación financiera, empresas administradoras de crédito, entidades otorgantes de crédito, empresas de servicios financieros, casas de cambio, empresas de transferencia de fondos y plataformas de préstamos entre personas, consolidando un enfoque transversal de gestión de riesgo en medios de pago electrónicos.

Entre los principales cambios, se refuerzan las **obligaciones de los emisores de instrumentos electrónicos**, estableciendo la responsabilidad de implementar medidas razonables de seguridad sobre el entorno operativo del instrumento.

Esto incluye la correcta autenticación de las operaciones, la conservación de evidencias técnicas suficientes y la capacidad de demostrar, ante reclamos del usuario, que una transacción fue correctamente autenticada, registrada y no afectada por fallas técnicas. En caso contrario, la responsabilidad recae sobre el emisor, salvo incumplimiento probado del usuario.

La normativa incorpora requisitos explícitos en materia de **monitoreo y control**, exigiendo que las instituciones cuenten con sistemas capaces de detectar hechos irregulares o potencialmente fraudulentos. Estos sistemas deben permitir identificar transacciones inusuales respecto al comportamiento habitual del cliente, verificar la geolocalización de las operaciones, alertar sobre el uso de dispositivos desconocidos y detectar patrones sospechosos en transacciones rechazadas. Asimismo, se establece la obligación de evaluar periódicamente la eficacia del sistema de monitoreo y adoptar medidas correctivas cuando se detecten desvíos.

Un aspecto central de la Circular es el fortalecimiento de las **obligaciones de notificación al usuario**. Las instituciones deben informar por medios electrónicos no solo cada transacción realizada, sino también todo intento o solicitud de modificación de datos sensibles, tales como credenciales, información personal, medios de contacto o parámetros de seguridad.

Estas notificaciones deben realizarse de forma oportuna y utilizando, como mínimo, dos medios de contacto válidos cuando se trate de cambios críticos.

En materia de **autenticación reforzada**, se amplía la exigencia de aplicar mecanismos de doble factor de autenticación para operaciones de alto riesgo, incluyendo el acceso a canales digitales, transferencias o pagos desde cuentas bancarias, solicitudes de préstamos no presenciales y la modificación de datos sensibles. La norma define la autenticación reforzada como el uso de al menos dos factores de distintas categorías (conocimiento, posesión e inherencia), admite el uso de dispositivos de confianza como factor de posesión y reconoce explícitamente la validez de tecnologías como passkeys y firma electrónica avanzada, bajo ciertas condiciones.

La Circular también prevé **excepciones acotadas** a la aplicación del doble factor de autenticación, como transferencias a beneficiarios de confianza, operaciones entre cuentas del mismo titular dentro de la misma institución, pagos de transporte público y determinados esquemas corporativos que cuenten con controles robustos de seguridad, sujetos a la evaluación de la Superintendencia.responsabilidad patrimonial básica de cada institución.

Finalmente, se refuerza el **régimen sancionatorio**, extendiendo las multas por incumplimiento de estas obligaciones a todas las entidades alcanzadas por la norma, con sanciones económicas proporcionales a la responsabilidad patrimonial básica de cada institución. La entrada en vigencia general de las modificaciones se fija para el **1.º de octubre de 2026**, con algunas disposiciones que pueden aplicarse desde la publicación de la resolución.

En conjunto, esta normativa consolida una expectativa regulatoria clara: las instituciones que operan instrumentos electrónicos deben adoptar un enfoque preventivo, basado en riesgo, con controles técnicos, monitoreo continuo, autenticación robusta y comunicación activa con el usuario como pilares centrales de la gestión de fraude y seguridad digital.