# Grupo de trabajo sobre fraudes a cuentas mediante ataques cibernéticos

## INFORME FINAL

Noviembre 2022

BANCO CENTRAL DEL URUGUAY

BANCO CENTRAL
DEL URUGUAY

Trabajo realizado a través de la participación y colaboración de representantes de la Asociación de Bancos Privados del Uruguay, Banco de la República Oriental del Uruguay (BROU), MiDinero (Findarin S.A.), Oca Blue (OCA Dinero Electrónico S.A.), Prex (Econstar S.A.), URUTEC y representantes de la Asesoría Jurídica, de la Oficina de Innovación, de Sistema de Pagos y de la Superintendencia de Servicios Financieros del Banco Central del Uruguay bajo su coordinación.

BANCO CENTRAL
DEL URUGUAY

# ÍNDICE

BANCO CENTRAL
DEL URUGUAY

# CREACIÓN DEL GRUPO DE TRABAJO Y OBJETO

## CREACIÓN

A partir de los antecedentes de las diversas denuncias de usuarios financieros por desconocimiento de operaciones realizadas sobre sus cuentas sin su autorización y los diversos intercambios mantenidos entre el Banco Central del Uruguay (BCU) y las entidades financieras y del sistema de pagos, se verifica un incremento significativo de fraudes sobre cuentas, bajo distintas modalidades.

La Asociación de Bancos Privados del Uruguay realizó un planteo para atender la situación referida y la Comisión Especial de Innovación, Ciencia y Tecnología de la Cámara de Representantes del Poder Legislativo tuvo a estudio un Proyecto ley de Ciberdelincuencia, donde el Banco Central del Uruguay emitió opinión, el cual a la fecha de este informe se encontraría en vías de aprobación parlamentaria.

Sin perjuicio de los esfuerzos existentes tendientes a evitar o mitigar el impacto de los fraudes en el sistema financiero (en su sentido amplio) y en el perjuicio sufrido por los clientes, y en virtud de haberse detectado restricciones para atender estas nuevas formas delictivas, en acuerdo con el Presidente del Banco Central se valoró la necesidad considerar medidas, incluyendo propuestas de eventual análisis de modificaciones legales, en forma urgente para fortalecer las acciones para la prevención de los fraudes.

Con lo cual, con fecha 26 de agosto de 2022, el Superintendente de Servicios Financieros dispuso la formación de un Grupo de Trabajo sobre fraudes a cuentas mediante ataques cibernéticos, bajo la coordinación de la Jefa del Departamento Conductas de Mercado, Verónica Villete, integrándose al mismo los siguientes participantes:

En representación del BCU
Gervasio Dalchiele, (de la Asesoría Jurídica del Banco Central), Gabriel Lago y Antonio Zarrillo (del Área de Sistema de Pagos), y Nicolás Serrano, (representante de la Oficina de Innovación).

En representación de ABPU
Gabriel Cella (Banco Itaú Uruguay S.A.), María Elena Bandeira (HSBC Bank Uruguay S.A.), Martín Gómez (Scotiabank Uruguay S.A.) y Graciana Abelenda (Banco Santander S.A.).

En representación de BROU
Juan Llosa y Antonio Rodríguez.

En representación de las IEDEs
Clara Villalba (Prex) Pilar Pedrazzini y Gabriela Gómez (MiDinero), Gabriel Better (OCA Blue).

En representación de URUTEC
Carlos Ham y Enrique Serra.

BANCO CENTRAL
DEL URUGUAY

## OBJETO

El grupo de trabajo se conformó con el objeto de generar una propuesta de medidas que se puedan adoptar como guías (como ser propuesta de acuerdo entre las instituciones) y otras propuestas, como ser eventuales medidas legales a promover ante el Poder Legislativo.

La agenda fue la siguiente:

Se realizaron de 3 reuniones de trabajo, con un intervalo aproximado de 10 días entre cada una de ellas.

1. En la primera reunión se realizó un **diagnóstico** de la situación actual.
2. En la segunda reunión se realizó la **identificación y análisis de alternativas** para resolver las situaciones planteadas.
3. En la tercera reunión se definió el **camino a seguir y los compromisos** asumidos por las partes.

BANCO CENTRAL
DEL URUGUAY

# PROPUESTAS DE ACCIÓN

A partir del diagnóstico de la situación actual de fraudes en cuentas y del análisis de las alternativas disponibles para dar solución a los problemas y mitigar los riesgos identificados, el grupo de trabajo acordó los términos del presente documento, a poner en consideración del Directorio del Banco Central, con propuestas de acciones concretas a adoptar en el sistema (tanto por parte de las entidades intervinientes como del regulador).

La propuesta está dirigida a coordinar esfuerzos en la lucha contra el fraude cibernético y estafas financieras y a crear una mayor conciencia pública sobre el tema. La misma está orientada no solo a la prevención del fraude cibernético sino que también a brindar herramientas para permitir y facilitar una acción oportuna y efectiva por parte de las entidades y los organismos competentes para procurar, una vez consumado el delito, la recuperación de los fondos malversados.

A dichos efectos se plantean distintos compromisos a asumir por las partes, los cuales deberán de ser adoptados de manera consolidada, paralela, en tanto están dirigidos a distintos temas pero con el objetivo común, antes señalado.

Las acciones definidas son las siguientes:

1. Fortalecimiento de la Educación Financiera
2. Mejora continua en materia de detección y monitoreo de fraudes.
3. Establecer canales de comunicación e intercambio de información entre entidades – Red Colaborativa.
4. Desarrollo de un marco legal y/o fortalecimiento del marco normativo aplicable.

## 1. Fortalecimiento de la Educación Financiera

Se considera al cliente como parte del proceso de prevención de fraude, en tanto a mayor educación se logra una mayor prevención. Los usuarios de servicios financieros y del sistema de pagos juegan un papel importante al mantenerse informados de las amenazas emergentes a través de avisos y recomendaciones emitidas por las instituciones, el BCU y otras autoridades, y tomando precauciones para protegerse.

En ese sentido se realizan tres propuestas de acción a adoptar: a) desde las entidades del sistema, b) entre todos los agentes intervinientes en el sistema financiero y del sistema de pagos c) el regulador.

a) En relación al rol de las *entidades* se propone:

- Generar o incluir (para aquellas que ya dispongan) un plan de capacitación/educación financiera para el uso de instrumentos, alineado a la experiencia basada en incidentes:

- El Plan de educación contendrá aspectos como:

  - Usos del instrumento
  - Derechos y obligaciones
  - Regulación
  - Riesgos

- Tecnología

b) Trabajar de manera *colaborativa*, entre el BCU, la Unidad de Defensa del Consumidor del Ministerio de Economía y Finanzas (anterior Área de Defensa del Consumidor – ADC) y entidades supervisadas en:

- Acordar un Plan de Comunicación anual, con su cronograma previsto, de recomendaciones al público.

  Se establecerán en conjunto las temáticas a considerar y los canales de comunicación.

  - Contendrá alertas y aspectos de protección (por ej. Indicando al usuario cómo proteger su información personal y otras prácticas -como ser el evitar descargar archivos o aplicaciones en dispositivos móviles de fuentes no verificadas etc.-) actualizándolo según los incidentes observados. Dado que uno de los principales problemas actualmente se radica en que las personas comparten su OTP –factor de autenticación One Time Password-, hacer hincapié en ello. Por ejemplo, indicando al usuario que este sólo es usado para autorizar una transferencia o dar el alta de un nuevo producto, nunca para iniciar sesión, recuperar su cuenta, o similares.

  - Se procurará la asertividad en los mensajes, que sean correctos, sencillos (en una o dos oraciones), acotados, simples (por ejemplo que SI, y que NO hacer), populares y con el énfasis suficiente para que llegue al público objetivo. Para lo cual, corresponde evaluar adecuadamente los métodos y los canales que se utilizarán (medios masivos) en función del público al que va dirigido.
  - Se podrán comunicar obligaciones y responsabilidades del usuario, como las establecidas por la Autoridad Monetaria de Singapur en 2022 (Anexo I, numeral 2))

- Acordar trabajar en conjunto en campañas de comunicación para la emisión de alertas al público, cuando la situación así lo amerite.

  - Según la situación, podrá ser adecuado definir lenguaje común para las diferentes campañas. Así como la potestad de que cada institución pueda realizar mensajes customizados de acuerdo a lo que considere apropiado.

c) En relación al rol del *regulador*:

- Poner a disposición del cliente el acceso directo y ágil a la información sobre las últimas amenazas y medidas que pueden tomar para protegerse contra dichas amenazas en un sitio o medio de difusión común (por ej. El sitio del Portal del Usuario Financiero del BCU, Anexo VI).
- Campañas masivas en medios públicos para lograr mayor alcance.

## 2. Mejora continua en materia de detección y monitoreo de fraudes.

Dado el entorno dinámico, y en particular de los fraudes cibernéticos se propone continuar con la mejora continua en materia de detección y monitoreo de fraudes. El tema se aborda desde dos ópticas, la prevención y la acción.

*Medidas preventivas por parte de las entidades*

- Valorar e instrumentar las mejoras necesarias, a efectos de potenciar la seguridad transaccional de acuerdo con sus procedimientos de prevención de fraude y/o estafas.
  Esto incluye establecer mecanismos de monitoreo y revisiones continuas en materia de ciberseguridad y atender las observaciones emitidas por el supervisor (sin perjuicio de las exigencias reglamentarias) orientadas a mejorar los controles existentes y garantizar una protección adecuada al usuario contra las amenazas, mientras se mantienen servicios eficientes para los clientes.
  Se podrá hacer uso de modelos de prevención contando con mayor información de clientes (en base a alertas de cambios de comportamiento, de dispositivos, localización etc.).

  Posibles prácticas a considerar, a valorar por la entidad:

a) Medidas adoptadas en Singapur 2022 (Autoridad Monetaria de Singapur, Anexo I, numeral 1)):

- Eliminación del uso de enlaces -en los que se puede hacer clic- en correos electrónicos o SMS enviados a clientes minoristas.
- Retraso de al menos 12 horas antes de la activación de un nuevo soft token en un dispositivo móvil.
- Medidas de seguridad adicionales, como un período de espera (no inmediato) antes de la implementación de solicitudes de cambios clave en la cuenta, así como de los datos de contacto clave de un cliente.
- Etc. (Ver más medidas contenidas en el anexo señalado).

Para llevar adelante éstas prácticas se podrán establecer plazos de adecuación.

b) Medida contenida en la información de ASBA sobre Ciber Riesgo y Ciber resiliencia, de Julio 2022, para prevenir operaciones fraudulentas (compartida en el grupo de trabajo):

- Cuando un cliente realiza una operación que se sale de su patrón de conducta, recibirá una notificación.
- El cliente deberá iniciar sesión en la App / plataforma on line (como ser home banking) para autorizar la operación, utilizando su doble factor – no desde el correo, página o link de acceso recibido-.
- Si el cliente no reconoce la operación y no realiza ese paso la misma no se ejecuta.

c) Monitor de Fraude

Superados ciertos umbrales de riesgo, los sistemas de evaluación (SW) podrán impedir que la transacción se realice.

Cada institución indicará los niveles de riesgo que está dispuesta a tolerar y en qué casos se deberá valorar si corresponde rechazar la transacción.

Se podrán establecer diversos rangos de referencia (ejemplo porcentaje máximo de transacciones que generen alertas, porcentaje máximo de alertas erróneas -falsos positivos-).

d) Monitoreo de cuentas

El artículo 24 de la Ley N° 19.210 -ley de inclusión financiera- refiere a la no discriminación y gratuidad. No obstante, y dado que se ha observado en la práctica la apertura de cuentas básicas –sueldo- que luego son utilizadas como cuentas "mula" dejando de percibir los haberes, se podrá tener en consideración aquellos clientes que integran el Registro de Antecedentes cuya creación prevé el Proyecto de Ley de Ciberdelincuencia, para realizar un mayor monitoreo del uso de dichas cuentas y tomar las acciones que correspondan.

Sin perjuicio de la eventual utilidad de un Registro de este tipo, el funcionamiento, responsabilidades de los participantes y debida regulación, deberá ser debidamente analizado y ponderado por todos los involucrados, en forma previa a su instrumentación. Especialmente, debe considerarse que un registro como el señalado – sin base legal - puede afectar garantías y derechos de las personas en su relación con el sistema financiero.

A efectos del control de las cuentas corresponderá llevar a cabo un monitoreo proactivo, en vez de reactivo, desde el inicio de la relación contractual (a través de, por ejemplo, un adecuado conocimiento del cliente en particular en los casos de onboarding digital en lo que refiere a mecanismos más robustos para la validación de identidad).

e) Doble factor de autenticación

Si bien recientemente fue emitida una normativa referida al doble factor de autenticación para operaciones – transferencias y pagos- con instrumentos electrónicos dirigida a instituciones de intermediación financiera[1], una acción a tomar por la industria en general, y no solo a quienes les abarca dicha norma, es procurar utilizar múltiples factores de autenticación que combinen sus categorías – algo que se tiene, algo que se sabe, algo que se es- a efectos de evitar que métodos llamados como de segundo factor de autenticación, en realidad sean una autenticación en dos pasos usando el mismo tipo de factor, algo que se sabe por ejemplo.

- Otras prácticas de autenticación en función de lo observado internacionalmente
  Autorizar transacciones directamente a través del ingreso a una aplicación móvil de la institución (directamente desde allí), pero obligando que la autenticación del cliente en dicha aplicación para tal fin sea a través de, por ejemplo, un factor biométrico de modo de que el actor malicioso no pueda identificarse en la aplicación del propio dispositivo del usuario utilizando las credenciales ya robadas. Como alternativa, en dichas aplicaciones se podrá generar un OTP –One Time Password-, pero que el mismo cuente con la información necesaria para que el consumidor pueda entender el contexto en el

[1] Art.364 de la RNRCSF.

cual será usado dicho OTP. Es decir, que la aplicación indique que el OTP está siendo generado en este momento para ser usado para realizar una transferencia por determinado monto a determinado destinatario, o para acceder a un determinado préstamo por determinado monto, citando algunos ejemplos.

f) Otros mecanismos de prevención a considerar

- Ante inicios de sesión en un nuevo dispositivo.

Actualmente, el uso frecuente en la industria es de detección más que prevención.
Esto quiere decir que, si la institución detecta que su cliente se está conectando desde un dispositivo no usado previamente, advierta al usuario o lo prevenga, requiriendo que su cliente certifique/valide que es él quien está iniciando esa sesión, y no un actor malicioso en su propio dispositivo luego de haberle robado las credenciales. Para evitar que el actor malicioso logre hacer que el usuario autorice el inicio de sesión en el dispositivo malicioso, las medidas preventivas deberán alinearse a las medidas señaladas en el punto anterior.

- Notificaciones

Notificar al titular de la cuenta, ya sea a través de email o app, medio acordado de notificación, cada movimiento o alta de servicio relacionado a su cuenta o su relación con ellas. Es válido que el cliente pueda establecer ciertos umbrales, que lo pueda "customizar" según su interés o necesidades.

- Atender el adecuado balance entre la prevención de fraudes y la experiencia del cliente.

- Tender a homogeneizar la base de estándares de seguridad entre distintos sectores de la industria financiera y de sistema de pagos, debido a la interoperabilidad –para que las debilidades de una entidad no afecten a la operativa, riesgos o reputación de otra involucrada-.

Medidas reactivas por parte de las entidades

- Resolución de casos de clientes

Sin perjuicio que en todas las situaciones las entidades deben dar cumplimiento con las exigencias normativas referidas a la atención de reclamos de clientes que les aplique: Para los casos de reclamos por transacciones no autorizadas por su titular, todas las entidades garantizarán una comunicación adecuada con los clientes afectados. Brindaran la asistencia e información adecuadas a dichos clientes sobre la protección de sus cuentas, así como el estado de la situación del trámite.

Las vías de comunicación así como su alcance, serán definidos por la entidad de acuerdo a sus procesos y modelo de gestión y siempre en cumplimiento de la normativa que le sea aplicable.

A efectos de facilitar la adopción de las medidas inmediatas para ayudar a proteger las cuentas afectadas, se podrá implementar lo siguiente:

a) Indicar a los titulares de cuentas que desconozcan operaciones sospechosas –disponible también en la página web institucional- los pasos que deben cumplir inmediatamente.
A modo de ejemplo (lo indicado dependerá de la aprobación del proyecto de Ciberdelincuencia que permite el bloqueo de la operación) se le podrá indicar:

- Notificar a su entidad,

- Requerirle a los titulares que presenten la denuncia policial con relato de los hechos para facilitar la investigación. No obstante, si ello impidiera actuar prontamente, contándose con evidencia, corresponderá valorar actuar en cada situación concreta presentada prescindiendo de dicho requisito (cabe señalar que este punto ha sido parcialmente adoptado en el artículo 144 de la Ley 20.075, aprobada en el transcurso del funcionamiento de este grupo de trabajo),

- Asimismo, de corresponder, se le comunicará el contacto de la autoridad competente en el asunto.

b) Realizar las denuncias y gestiones de recupero pertinentes.

## 3. Establecer canales de comunicación, cooperación e intercambio de información entre entidades– red colaborativa.

A efectos de promover la colaboración y cooperación en términos de prevención de fraudes y estafas cibernéticas a nivel del ecosistema se plantean los siguientes compromisos a asumir, los que podrían documentarse en un acuerdo interinstitucional:

- Formalizar, a través de la redacción de un acuerdo marco de colaboración, los términos y condiciones del intercambio de información entre entidades del sistema (símil acuerdo de Argentina contenido en Anexo II) que contenga:

- Capacidad de contactar de manera oportuna con otras entidades,

- Capacidad de compartir experiencias de diferentes incidentes de seguridad.

- Prever la retroalimentación de: mejores prácticas, tecnologías emergentes, políticas de seguridad.

- Comunicación en tiempo real

- Valorar contar con una plataforma dinámica o sistema de intercambio de información entre entidades del sistema financiero que permita interactuar en tiempo real, tanto para informar por ejemplo sobre alertas, incidentes y vulnerabilidades ya confirmadas o predictivas, o fraudes consumados o intentos de fraudes.

Para ello, se deberá disponer de una infraestructura tecnológica segura y confidencial para compartir datos de la red de colaboración.

- Valorar contar con una plataforma del tipo Malware Information Sharing Platform (MISP) para entre otros aspectos compartir y almacenar datos e información de amenazas, de modo de ser utilizada como comunidad colaborativa sobre amenazas existentes, con el objetivo de ayudar a mejorar las medidas utilizadas contra los ataques dirigidos y establecer acciones preventivas y de detección.

- Valorar contar con bases unificadas de datos.

- Otras propuestas de colaboración:

- Crear un Comité de prevención de fraudes, estafas y ciberseguridad compuesto por representantes de la industria (ABPU, BROU, IEDEs, entre otros) y otros agentes como Urutec, Unidad de Defensa del Consumidor (anterior Área de Defensa del Consumidor), AGESIC y el BCU, para compartir problemática, valorar nuevas acciones a implementar o determinar eventuales necesidades normativas.
  Establecer periodicidad de reuniones anuales. Con posibilidad de ser convocado cuando así lo ameriten situaciones especiales.

- establecer equipos de trabajo interdisciplinarios y con los representantes antes referidos, dedicados a la prevención de actividades fraudulentas y estafas cibernéticas, para actuar cuando se lo requiera/convoque (ad hoc).

## 4. Desarrollo de un marco legal y/o fortalecimiento del marco normativo aplicable.

En los últimos años, y de la mano de un incremento del uso de los canales digitales, se ha visto incrementado el riesgo de fraude asociado a ese mayor uso. Asimismo, así como el mercado ha crecido con nuevos productos y servicios ofrecidos, han surgido también nuevas modalidades de fraude y estafa, que a pesar de los mecanismos de monitoreo de fraudes y alertas existentes en las entidades financieras, se requiere de nuevas herramientas y más efectivas que permitan una acción ágil y coordinada en el sistema financiero y del sistema de pagos.
A continuación se realizan propuestas para abordar dos temas que han sido valorados por el grupo como necesarios para brindar esa mayor agilidad en la respuesta así como para brindar garantías a las entidades para su uso. Estos dos temas refieren al análisis del bloqueo de cuentas y al relevamiento del secreto bancario en casos de fraude.

*Bloqueo de cuentas*

- En el artículo 144 de la Ley N° 20.075 de 20/20/2022 (Ley de Rendición de Cuentas), se introdujo una modificación al artículo 53 del Código del Proceso Penal, agregando un literal h con la siguiente redacción:

*"Artículo 53(Actuaciones de la autoridad administrativa sin orden previa).- Corresponderá a los funcionarios con funciones de policía realizar las siguientes actuaciones, sin necesidad de recibir previamente instrucciones particulares de los fiscales: (…)*

*h) Recibida la denuncia de presunta estafa, extorsión o receptación, con prueba fehaciente de depósito, giro, transferencia u otra forma de envío de dinero en cualquier moneda, mediante instituciones de intermediación financiera, la autoridad policial comunicará a la institución involucrada para que realice la inmovilización del dinero hasta la suma objeto de la presunta maniobra delictiva por un plazo de setenta y dos horas, tratándose de cuenta destinataria nacional o de noventa y seis horas, si la cuenta destinataria fuere extranjera.*

*Cuando el envío sea con destino a una persona física, la inmovilización será de setenta y dos horas a noventa y seis horas, tratándose de nacionales o extranjeros respectivamente. En el mismo momento, la medida se comunicará a la Fiscalía y al Banco Central del Uruguay a los efectos pertinentes. Vencido dicho plazo sin orden de Fiscalía para que la inmovilización sea definitiva hasta la resolución de la investigación, cesará la medida."*

La sola denuncia policial por presunta estafa, extorsión o receptación con prueba del envío del dinero habilitará a la autoridad policial a que comunique a las instituciones financieras que deben inmovilizar los montos de dinero involucrados en la presunta maniobra hasta por un plazo de 72 horas (o de 96 horas si la cuenta destinataria fuere extranjera).
Si bien no está claro a qué "efectos pertinentes" se le comunicaría la medida adoptada al BCU, se ha establecido con carácter de norma legal la inmovilización de fondos por hasta 72 y 96 horas según corresponda.

- Además, el tema referido a inmovilización de fondos se encuentra comprendido en el Proyecto de ley de Ciberdelincuencia (Anexo III, artículo 13 del proyecto). El articulo proyectado sobre el tema faculta a las entidades a la no ejecución de cualquier tipo de orden de retiro y/o transferencia de activos brindadas por personas físicas o jurídicas titulares o apoderados de cuentas, cuando hubieren tomado conocimiento, por cualquier medio de comunicación fehaciente, que en la o las cuentas referidas ingresaron fondos de terceros a través de transacciones que le fueran declaradas como desconocidas y no autorizadas por el titular de la o las cuentas de origen de los fondos transferidos

  El Banco Central del Uruguay comunicó en el grupo de trabajo estar de acuerdo con los fundamentos de base del Proyecto en tanto se percibe desde la Superintendencia de Servicios Financieros que las medidas de bloqueo de fondos han sido efectivas para su recupero. No obstante lo cual, se comunicaron las observaciones y comentarios que surgieron desde el Banco Central referidos a dicho Proyecto.

- Otras acciones a considerar en relación a los bloqueos de cuentas:

  El proyecto de Ciberdelincuencia, en lo que respecta al artículo de inmovilización de fondos prevé una medida reactiva, una vez consumado el hecho- por lo que se propone valorar realizar modificaciones al Proyecto referido para que contemple también los casos de *bloqueo temporario*, diferimiento de la operación o restricción de uso de un canal a ser utilizados de manera excepcional, y con carácter preventivo.

- *Bloqueo Temporario*, diferimiento de la operación o restricción de uso de un canal

Las instituciones podrán adoptar alguna de las siguientes medidas según su valoración de los hechos y las consecuencias para su cliente:

a) Restringir, con algún criterio objetivo, la realización de transferencias a través de sus canales digitales. El plazo máximo en la cual podrá hacerse uso de esta situación no podrá superar las X horas hábiles (a definir con Sistema de Pagos). En caso de detectarse un fraude por el ordenante de la transferencia, dentro del plazo de procesamiento por el sistema, podría impedirse la misma, al amparo de lo establecido en el artículo 6 literal A de la Ley N° 18.573, por no haber cumplido requisitos de validación del sistema. Esta herramienta puede resultar útil en casos de fraudes detectados oportunamente.

b) Cuando se encuentren ante una presencia masiva de estafas electrónicas, que buscan concretar transferencias de fondos no autorizadas de cuentas de sus clientes, podrán realizar un "bloqueo temporario" de todas o algunas de las transferencias en cuestión de manera preventiva, al amparo de lo establecido en el artículo 6 literal A de la Ley N° 18.573 referido.

Pautas para el bloqueo:

Dar aviso a su cliente que se va a utilizar el procedimiento de "bloqueo temporario".
En el caso de transferencias inmediatas, en virtud del mayor riesgo que representan, el bloqueo temporario podrá ser por hasta X horas hábiles (a definir con Sistema de Pagos).
Para el caso de transferencias compensadas, se podrá pedir el diferimiento de las transacciones. Esta modalidad implica que el banco emisor no desactiva las transferencias compensadas, pero le indica a la Cámara Compensadora –CCA- que postergue hasta X horas hábiles (a definir con Sistema de Pagos) el ingreso de determinadas transferencias al esquema de compensación.
Durante esas horas y siempre que sea en horario laboral de la CCA, la entidad emisora podrá indicar la liberación de dichas transferencias en cualquier momento por la vía de ratificar el ordenante su voluntad de realizar la transferencia, por ejemplo. La instrucción podrá ser para el total de transferencias que se encuentren retenidas o para un subgrupo de estas. Transcurridas las X horas, las transferencias se liberarán automáticamente, salvo aquellas que el banco emisor comunique a la CCA que deben ser anuladas.

*Secreto Bancario*

En la región se ha observado que ha surgido la necesidad de distintas jurisdicciones de promover cambios en la normativa de secreto bancario como ser en Argentina estableciendo una excepción para compartir información entre las instituciones –previa aprobación del BCRA-, sin necesidad de orden judicial (ver normativa Argentina, Anexo IV), así como también en Perú en donde se establecieron plazos cortos para la resolución judicial de su levantamiento (ver normativa Peruana, Anexo V), lo que le otorga mayor agilidad al sistema para actuar prontamente.

Habiendo analizado las opciones existentes, el grupo de trabajo propone estudiar una nueva eventual excepción al secreto bancario, a través de un agregado al artículo 1 de la Ley N° 17.948 de 8 de enero de 2006, para permitir el intercambio de información entre las entidades comprendidas en los artículos 1º y 2º de esta ley, con carácter excepcional, sin previa aprobación del BCU.

La propuesta apunta atender la problemática concreta de fraude en cuentas que convocó a reunión al grupo de trabajo. Sin perjuicio de lo cual, a futuro se podrá valorar la necesidad de realizar una revisión más profunda de la normativa referida a secreto bancario, que pueda abarcar también otras situaciones y mercados. Se advierte que en caso de realizarse, la misma deberá contener un análisis de la realidad y su eventual impacto ante cambios en la reglamentación referida (incluyendo mercado de valores), valoración de los potenciales beneficios e inconvenientes así como el análisis de normativa comparada.

Seguidamente se presenta una exposición de motivos así como la modificación legal proyectada.

## EXPOSICIÓN DE MOTIVOS

En los últimos años, y de la mano de un incremento del uso de los canales digitales, se ha visto incrementado el riesgo de fraude asociado a ese mayor uso. Asimismo, así como el mercado ha crecido con nuevos productos y servicios ofrecidos, han surgido también nuevas modalidades de fraude y estafa, que a pesar de los mecanismos de monitoreo y alertas existentes en las entidades del sistema financiero y de pagos, se requiere de nuevas herramientas y más efectivas que permitan una acción ágil y coordinada en el sistema financiero.

Ante este escenario han surgido distintos cambios o propuestas de cambios normativos como ser la obligatoriedad del doble factor de autenticación para transferencias bancarias o como ser la propuesta legal del Proyecto de Ciberdelincuencia. Asimismo, se ha trabajado en información y educación al usuario financiero sobre los riesgos, a través de la realización de intensas campañas de prevención de fraudes y de ciberseguridad en particular, llevadas adelante por los distintos agentes del sistema en forma individual y también de manera coordinada con otros organismos (como la AGESIC y el Banco Central del Uruguay).

Uno de los inconvenientes al que se ven enfrentadas las entidades actualmente es el impedimento legal para poder compartir información entre ellas, en el marco de investigaciones realizadas por denuncias de clientes que han perdido sus fondos al haber sido víctimas de fraude o estafa. También se ha observado el caso de delincuentes, que una vez que dejan de operar en una institución de plaza, logran introducirse como cliente en otra.

La propuesta de modificación legal, incorporando una aclaración sobre el alcance del secreto bancario para el intercambio de información entre las entidades comprendidas en el los artículo 1º y 2º de la Ley N° 17.948 de 8 de enero de 2006, con carácter excepcional y con el propósito determinado de la prevención de fraudes e impedir a tiempo sus efectos, pretende apoyar a las entidades financieras en el análisis y la prevención de las situaciones de fraude o estafa a clientes. La excepción proyectada únicamente podrá ser utilizada cuando fundadamente tenga el objeto referido.

Asimismo, permitirá logar una mayor efectividad en el recupero de los fondos, evitando que un mismo delincuente pueda actuar a través de distintos agentes del sistema financiero y de pagos sin ser advertido.
Adicionalmente, el proyecto de ley de Ciberdelincuencia que se encuentra actualmente para aprobación del Parlamento, entre otras cosas, prevé la creación de un Registro de antecedentes de personas que hayan cometido ciberdelitos y faculta a las entidades a la no ejecución de cualquier tipo de orden de retiro y/o transferencia de activos brindadas por personas físicas o jurídicas titulares o apoderados de cuentas, cuando hubieren tomado conocimiento, por cualquier medio de comunicación fehaciente, que en la o las cuentas referidas ingresaron fondos de terceros a través de transacciones que le fueran declaradas como desconocidas y no autorizadas por el titular de la o las cuentas de origen de los fondos transferidos.

A su vez, en el artículo 144 de la Ley N° 20.075 de 20/20/2022 (Ley de Rendición de Cuentas), se introdujo una modificación al artículo 53 del Código del Proceso Penal, agregando un literal h en el cual se establece que la sola denuncia policial por presunta estafa, extorsión o receptación con prueba del envío del dinero habilitará a la autoridad policial a que comunique a las instituciones financieras que deben inmovilizar los montos de dinero involucrados en la presunta maniobra hasta por un plazo de 72 horas (o de 96 horas si la cuenta destinataria fuere extranjera).

No obstante, lo anterior refiere a una medida reactiva, una vez ocurrida la estafa o el fraude al usuario del sistema financiero, mientras que la excepción al secreto bancario no solo permitirá actuar de manera ágil cuando el hecho fue consumado sino que también podrá ser utilizado de manera preventiva. A partir de las alertas de seguridad de los sistemas de gestión y monitoreo con que cuentan las entidades se podrá intercambiar información con el objeto de la prevención del delito.

En cuanto al artículo referido al Registro de Ciberdelincuentes, el mismo prevé facultar "a las Instituciones de Intermediación Financiera y a las Entidades Emisoras de Dinero Electrónico a crear Registros interinstitucionales **conteniendo datos** para identificar y prevenir transacciones no consentidas, operativas fraudulentas así como **los beneficiarios de estas.**" (resaltado no obra en original). A efectos de compartir la información referida, se requiere poder contar con respaldo legal que permita revelar dicha información.

En suma, esta propuesta de agregar un párrafo al artículo 1 de la Ley N° 17.948, apoya otros esfuerzos existentes tendientes a evitar o mitigar el impacto de los fraudes en el sistema y en el perjuicio sufrido por los clientes, y procura generar y fortalecer la confianza de los usuarios en el sistema financiero y en el sistema de pagos.

## PROYECTO DE MODIFICACIÓN LEGAL

Agregar un inciso segundo al Art. 1 de la Ley N° 17.948 de 8 de enero de 2006, con el siguiente texto:

***"No obstante, las entidades comprendidas en los artículos 1º y 2º del Decreto Ley N° 15.322 de 17 de setiembre de 1982 podrán intercambiar entre sí la información referida en el inciso precedente con carácter excepcional, con el objeto exclusivo de investigar y prevenir eventuales conductas delictivas cometidas a través de esas instituciones, siendo responsables por la divulgación de dicha información a terceros, en los términos del artículo 25 del citado Decreto-Ley."***

---

En tanto las Instituciones Emisoras de Dinero Electrónico no se encuentran alcanzadas por el secreto profesional bancario (art. 25 de la 15.322), sino que su responsabilidad es eventualmente penal en caso de violación al secreto profesional establecido en el art. 302 del Código Penal, no corresponde promover una excepción al secreto bancario para dichas figuras.

No obstante, cabe advertir que, al momento de promover este cambio legal se considere incorporar (en éste u otro artículo legal), la posibilidad del intercambio de información (con el objeto de investigar y prevenir eventuales conductas delictivas) entre las entidades comprendidas en los artículos 1º y 2º del Decreto Ley N° 15.322 de 17 de setiembre de 1982 y las Instituciones Emisoras de Dinero Electrónico (comprendidas en el artículo 4 de la Ley N° 19.210).

BANCO CENTRAL
DEL URUGUAY

# ANEXO I

- **Autoridad Monetaria de SINGAPUR, 2022**

"Framework for Equitable Sharing of Losses Arising from Scams" del MAS, Singapur.

https://www.mas.gov.sg/news/media-releases/2022/a-framework-for-equitable-sharing-of-losses-arising-from-scams

https://www.straitstimes.com/business/banking/draft-framework-for-fair-sharing-of-scam-losses-delayed-due-to-complexity-of-issues-involved-mas

Medidas adoptadas:

## 1- Entidades

Las instituciones financieras tienen la responsabilidad de proteger a sus clientes, por ejemplo, a través de controles sólidos para salvaguardar las cuentas de los clientes y medidas efectivas para detectar y responder a transacciones sospechosas.
Implementar medidas más estrictas que incluyan:

- Eliminación de enlaces en los que se puede hacer clic en correos electrónicos o SMS enviados a clientes
- El umbral para las notificaciones de transacciones de transferencia de fondos a los clientes se establecerá de manera predeterminada en $100 o menos
- Retraso de al menos 12 horas antes de la activación de un nuevo soft token en un dispositivo móvil.
- Notificación al número de móvil existente o al correo electrónico registrado en el banco siempre que haya una solicitud para cambiar el número de móvil o la dirección de correo electrónico de un cliente
- Medidas de seguridad adicionales, como un período de espera (no inmediato) antes de la implementación de solicitudes de cambios clave en la cuenta, así como en los datos de contacto clave de un cliente.
- Equipos de asistencia al cliente con dedicación y con buenos recursos para tratar con prioridad los comentarios sobre posibles casos de fraude
- Educación sobre estafas considerando alertas frecuentes

Estas medidas más estrictas prolongarán el tiempo necesario para ciertas transacciones bancarias en línea, pero proporcionarán una capa adicional de seguridad para proteger los fondos de los clientes.

## 2- Clientes

Los clientes tienen la responsabilidad de tomar las precauciones necesarias, especialmente al nunca revelar sus credenciales personales o bancarias a nadie, nunca hacer clic en los enlaces de los mensajes de texto o correos electrónicos que afirman haber sido enviados por un banco, y realizar transacciones solo a través del sitio web oficial o la aplicación móvil del banco.
La vigilancia del cliente sigue siendo de suma importancia. Los estafadores se adaptan rápidamente para dirigirse a los consumidores desprevenidos.

Se insta a los clientes a ejercer una mayor vigilancia y adherirse a las siguientes prácticas de seguridad digital:

- Nunca hacer clic en enlaces provistos en SMS o correos electrónicos supuestamente enviados por su entidad.
- Nunca divulgar o revelar sus credenciales o contraseñas de banca por Internet a nadie, incluidas las personas que dicen ser de bancos o agencias gubernamentales.
- Verifique la validez de los SMS o correos electrónicos recibidos llamando directamente a la entidad a través de la línea directa que figura en su sitio web oficial.
- Realizar transacciones solo en el sitio web oficial de la institución o a través de la aplicación móvil oficial del banco.
- Monitorear de cerca las notificaciones de transacciones recibidas del banco para que cualquier pago no autorizado se informe lo antes posible de modo de aumentar las posibilidades de recuperación.
- Mantenga sus dispositivos actualizados con los últimos parches de seguridad y software antivirus.

# ANEXO II

- **Argentina**

Acuerdo coordinación para establecer los términos y condiciones del intercambio de información y colaboración entre las entidades y/o empresas asociadas que adhieran al mismo


Acuerdo de Coordinacion.pdf

## ANEXO III

**Proyecto de Ley de Ciberdelincuencia, 2022**

VF Proyecto de Ley
CIBERDELINCUENCIA

## ANEXO IV

**Argentina, 2022**

Proyecto secreto
financiero y fiscal Art

Artículo 1 literal g) del proyecto.

Se exceptúan del deber de mantener secreto bancario a las entidades para casos especiales previa autorización del BCRA.

## ANEXO V

**Secreto Bancario Perú, 2022**

https://perulegal.larepublica.pe/temas-legales/constitucional/2022/07/04/contraloria-y-sbs-podran-solicitar-el-levantamiento-del-secreto-bancario-ley-31507-3224

*"Artículo 143.- LEVANTAMIENTO DEL SECRETO BANCARIO*

*El Secreto bancario no rige cuando la información sea requerida por:*

*1. Los jueces y tribunales en el ejercicio regular de sus funciones y con específica referencia a un proceso determinado, en el que sea parte el cliente de la empresa a quien se contrae la solicitud.*

*La Superintendencia Nacional de Aduanas y de Administración Tributaria - SUNAT, sin perjuicio de lo señalado en el numeral 10 del artículo 62 del Código Tributario, mediante escrito motivado puede solicitar al juez el levantamiento del secreto bancario en cumplimiento de lo acordado en tratados internacionales o en las Decisiones de la Comisión de la Comunidad Andina (CA) o en el ejercicio de sus funciones."*

*En estos casos, el Juez debe resolver dicha solicitud en el plazo de cuarentaiocho (48) horas contado desde la presentación de la solicitud."*

Con ésta modificación, al igual que el Fiscal de la Nación y las Comisiones investigadoras del Congreso, la Contraloría y la SBS ya no requieren de la participación de un juez para solicitar la información bancaria o tributaria de un funcionario o servidor público, o de un ciudadano en general, respectivamente.

BANCO CENTRAL
DEL URUGUAY

# ANEXO VI

**Portal del Usuario Financiero de la SSF**

Recomendaciones y advertencias

**https://usuariofinanciero.bcu.gub.uy/Paginas/Recomendaciones_advertencias.aspx**