PONTIFICIA UNIVERSIDAD
CATÓLICA DEL PERÚ

FACULTAD DE DERECHO

Programa de Segunda Especialidad en Protección al Consumidor

Medidas de Seguridad ante operaciones no reconocidas ¿Son efectivas?

Trabajo académico para optar el título de Segunda Especialidad en Protección al Consumidor

Autor:
Nicole Adriana Gamarra Aliaga

Asesor:
Carlos Rafael Velarde Aliaga

Lima, 2025

Informe de Similitud

Yo, VELARDE ALIAGA, CARLOS RAFAEL, docente de la Facultad de Derecho de la Pontificia Universidad Católica del Perú, asesor(a) del Trabajo Académico titulado "**Medidas de seguridad ante operaciones no reconocidas ¿Son efectivas?**", del autor(a) GAMARRA ALIAGA, NICOLE ADRIANA, dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 27%. Así lo consigna el reporte de similitud emitido por el software Turnitin el 07/12/2025.

- He revisado con detalle dicho reporte y el Trabajo Académico, y no se advierten indicios de plagio.

- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lima, 13 de diciembre del 2025

<table>
<tr><td colspan="2">VELARDE ALIAGA, CARLOS RAFAEL</td></tr>
<tr><td>DNI: 07633132</td><td rowspan="2">Firma:
  </td></tr>
<tr><td>ORCID:

https://orcid.org/0000-0003-0177-254X</td></tr>
</table>

RESUMEN

Las medidas de seguridad reguladas en nuestro ordenamiento jurídico no resultan eficientes ante los nuevos mecanismos de operaciones fraudulentas en la banca móvil, digital. Los distintos criterios que ha venido interpretando INDECOPI no resulta suficiente para generar seguridad jurídica tanto a los consumidores como a las entidades financieras para poder aplicarlos en sus sistemas de seguridad incluyendo el monitoreo de operaciones para poder identificar el patrón de consumo habitual de los usuarios.

En ese sentido, las medidas de seguridad han venido implementándose acorde a criterio de cada banco cumpliendo con lo establecido en la normativa peruana y además siguiendo los lineamientos de INDECOPI. Sin embargo, esto no parece ser suficiente para evitar el incremento de operaciones fraudulentas vía banca digitales y transacciones virtuales.

El presente artículo se enfoca en poder buscar un mecanismo para implementar a nuestro ordenamiento y en adoptar un criterio adicional que se ha venido implementando en otros países que puede resultar efectivo en nuestro país.

Palabras clave

Operaciones no reconocidas, operaciones fraudulentas, patrón de consumo habitual, banca digital, transacciones virtuales.

ABSTRACT

The security measures regulated under our legal system are not effective against the new mechanisms used to carry out fraudulent operations in mobile and digital banking. The various criteria developed by INDECOPI have not been sufficient to provide legal certainty for either consumers or financial institutions, particularly regarding their application within security systems, including transaction monitoring to identify users' usual consumption patterns.

In this context, security measures have been implemented according to each bank's own criteria, in compliance with Peruvian regulations and following INDECOPI's guidelines. However, this does not appear to be enough to prevent the rise of fraudulent operations conducted through digital banking and virtual transactions.

This article focuses on identifying a mechanism that could be incorporated into our legal system and on adopting an additional criterion that has been implemented in other countries, which may prove effective in Peru.

Keywords

Unrecognized transactions, fraudulent transactions, usual consumption pattern, Typical spending pattern, digital banking, virtual transactions.

ÍNDICE

INTRODUCCIÓN

Hoy en día se realizan transacciones mediante aplicativos móviles y operaciones vía internet con la finalidad de economizar tiempos y agilizar transacciones que realizamos día a día. No obstante, este recurso no ha traído solamente beneficios por el uso de estos aplicativos, sino que, también se ha prestado para que se efectúen operaciones fraudulentas, lo que afecta de manera significativa a todos los usuarios de las entidades financieras. Paralelamente, esto de igual manera afecta a las entidades financieras pues estas también se ven comprometidas en mejorar los mecanismos de seguridad que estos deben otorgar a sus usuarios.

En ese sentido, el presente artículo cuestiona si nuestra normativa sectorial conforme a las operaciones no reconocidas, son suficientes para otorgar mayor seguridad a sus usuarios y si la interpretación de INDECOPI es la adecuada a medida que la tecnología avanza, y junto con ella los mecanismos de fraude también.

Asimismo, es importante tener en cuenta qué medidas de seguridad adoptan otros países y si estas podrían verse aplicados en nuestro país, de manera que se realice un análisis en conjunto para generar mayor seguridad jurídica y este se vea reflejado en las resoluciones que vino emitiendo INDECOPI.

Por último, se detalla los resultados de una encuesta que demuestra que un número de personas han sido víctimas de fraude por diferentes tipos de operaciones con entidades financieras, con la misma que demuestra lo escasa que es la seguridad de las entidades financieras o la poca información que tienen los usuarios para poder evitar este tipo de operaciones.

ET LUX IN TENEBRIS LUCET
MCMXVII

1. Sistema financiero y sus operaciones

a. Consumidores en el sistema financiero

Primero, para hablar de consumidor, debemos tener presente el Código de Protección y Defensa del Consumidor, en la que define a uno como toda persona natural o jurídica que adquiere, utiliza o disfruta, como destinatario final, productos o servicios en el mercado[1]. No obstante, en el sector financiero, exige una caracterización más detallada por la complejidad del mismo servicio.

El consumidor financiero se enfrenta a productos de alta sofisticación, como créditos hipotecarios, tarjetas de crédito, operaciones electrónicas o instrumentos de inversión, los cuales incluyen riesgos no siempre comprendidos por el usuario promedio. Esto genera una situación de asimetría que se traduce en la necesidad de reforzar la transparencia y la responsabilidad de las entidades financieras.

Entonces, la característica particular del consumidor financiero es aquel es quien utiliza productos o servicios ofrecidos por entidades financieras con fines distintos a su actividad empresarial principal. Dicha definición se vincula directamente con el derecho a la protección frente a las asimetrías de información que caracterizan a las relaciones de consumo. Es evidente que el consumidor financiero tiene una desventaja de mayor amplitud a diferencia de otros tipos de consumidores, por la complejidad de sistema que se enfrenta los usuarios con los productos y servicios de estos.

Esto evidencia así, que hay cierta vulnerabilidad del consumidor financiero en que no solo hay falta de información, sino también es debido a la ausencia de un margen real de negociación en los contratos de adhesión. En este sentido, el deber del Estado y de las autoridades de supervisión es garantizar mecanismos que equilibren estas relaciones de consumo.

Por lo ya mencionado, podemos encontrar diferentes tipos de vulnerabilidad de los consumidores en el sistema financiero. Como ya nos pudimos anticipar, el consumidor se encontraría en una posición de desventaja informativa, pues estos no cuentan con los conocimientos técnicos suficientes para poder evaluar riesgos que se encuentra dentro del mismo sistema financiero, además de que los contratos que suscriben suelen tener términos muy complejos que no son de entendimiento sencillo por los consumidores, generando más vulnerabilidad. Asimismo, podemos encontrar una vulnerabilidad tecnológica, desde el momento que las entidades financieras implementaron este tipo de mecanismos para que los consumidores puedan realizar las operaciones correspondientes a sus productos o acceder a los servicios que estos se encuentran vinculados con las entidades. Es justamente dentro de este tipo de vulnerabilidad que pueden ocasionarse las operaciones fraudulentas mediante este tipo de mecanismos.

Para ello, considero pertinente mencionar que la jurisprudencia de INDECOPI ha reconocido esta situación de desventaja. Así, ha señalado que las entidades

[1] Ley N°29571, Código de Protección y Defensa del Consumidor.

financieras deben asumir un rol de diligencia reforzada en la prestación de sus servicios, dada la asimetría estructural existente. Este estándar se encuentra en línea con el principio pro-consumidor, que orienta la interpretación de las normas de protección en casos de ambigüedad.

Encontramos que INDECOPI se pronuncia sobre esta situación de desventaja informativa en diferentes resoluciones, tales como la Resolución N°1504-2025/CC1, la misma que dispone que "los proveedores tienen el deber de entregar los productos y prestar los servicios al consumidor en las condiciones ofertadas o previsibles, atendiendo a la naturaleza de estos, la regulación que sobre el particular se haya establecido y, en general, a la información brindada por el proveedor o puesta a disposición"[2]. Podemos interpretar de este extracto de la resolución alude básicamente que los servicios y productos ofertados por las entidades financieras deben tener condiciones y la información que los mismos debieron brindar a los usuarios o consumidores, siendo esto la obligación de informar a los clientes sobre las transacciones que realizará dentro de sus plataformas o establecimientos correspondientes.

Asimismo, en esta misma línea encontramos otra resolución de INDECOPI que habla sobre la idoneidad del servicio, la misma que en interpreta el artículo 20 del Código de Protección al Consumidor de la siguiente manera: "para determinar la idoneidad de un producto o servicio, se deberá comparar al mismo con las garantías que el proveedor haya brindado y a las que esté obligado, pudiendo estas ser explícitas (términos y condiciones expresamente ofrecidos), implícitas (fines y usos previsibles del producto/servicio según usos y costumbres del mercado) y legales (cumplimiento de los mandatos legales y las regulaciones vigentes)"[3]. Así, se puede entender que el cliente o usuario debe estar resguardado con las distintas garantías que establece tanto el proveedor en sus términos y condiciones, los fines para los que se está realizando el servicio y productos, y lo que establece la normativa sobre este tipo de transacciones que se llegue a realizar entre el consumidor y la entidad financiera.

Entonces, es claro que la postura de INDECOPI será siempre que los consumidores reciban todo tipo de información acerca del servicio o producto que estos estarán contratando con la entidad financiera, puestos que estos se encuentran en una posición de desventaja informativa frente a las operaciones que los proveedores financieros realizan por la misma naturaleza del core bancario.

b. Deber de información e idoneidad en el sistema financiero

Ahora bien, de acuerdo con esta vulnerabilidad entre los consumidores y las entidades financieras, debemos comprender que el deber de información constituye uno de los pilares del derecho del consumidor. En el ámbito financiero, cobra especial relevancia por la complejidad de los productos y la necesidad de

[2] Resolución N° 1504-2025/CC1-INDECOPI.
[3] Resolución Final N° 1477-2024/SPC-INDECOPI

transparencia para la toma de decisiones informadas, más aún cuando los productos involucran el dinero de los consumidores o usuarios.

Esto demuestra que no basta con entregar al consumidor documentos extensos y técnicos; es indispensable que la información sea comprensible, evitando omisiones que distorsionen la decisión del consumidor. No obstante, ese tipo de problemas lo podemos encontrar cotidianamente al aceptar los términos y condiciones del uso de los aplicativos de las entidades financieras, así como cualquier tipo de contratación que implique la revisión extensa de documentos, sin el apoyo de algún personal de la entidad financiera para un mejor entendimiento por parte del consumidor. Ese mismo tipo de problemas lo podemos encontrar con el uso de los aplicativos móviles para personas que no tienen acceso a dispositivos tecnológicos donde se encuentran estos; así también como las personas de tercera edad que no cuentan con el conocimiento suficiente sobre el uso de los mismos para poder acceder a sus productos que ofrece las entidades financieras.

La SBS y el INDECOPI han coincidido en señalar que la entrega de información estandarizada, mediante fichas resumen, constituye una buena práctica para reducir la asimetría. Asimismo, la información debe incluir los costos totales del producto, las tasas de interés efectivas y los riesgos asociados. Sin embargo, ante la presente problemática de operaciones fraudulentas, no resultarían suficientes para poder seguir evitando que estas malas prácticas sigan efectuándose. Tenemos el conocimiento de que este tipo de operaciones podrían llegar a ejecutarse inclusive cuando los consumidores han sido lo suficientemente diligentes para evitar este tipo de transacciones.

Con respecto a la idoneidad, este implica que el servicio debe prestarse conforme a lo que el consumidor espera legítimamente, atendiendo a las condiciones ofrecidas y a la naturaleza del producto. INDECOPI ha mencionado en la Resolución N.° 1234-2019/CC3-INDECOPI que, en los servicios financieros, la idoneidad no se reduce a la entrega material del producto, sino que se extiende a la seguridad, continuidad y confianza en las operaciones[4]. En ese sentido, los usuarios y consumidores esperan que las entidades financieras brinden la seguridad suficiente para el resguardo del dinero de las mismas que se encuentran dentro del resguardo de las entidades financieras.

Así, un servicio financiero es idóneo no solo cuando permite retirar efectivo o efectuar transferencias, sino cuando lo hace con garantías de seguridad, evitando fraudes y accesos no autorizados. La idoneidad se vincula también con la implementación de protocolos de monitoreo de operaciones, orientados a identificar transacciones inusuales. Este monitoreo se encuentra dentro del Reglamento de Tarjetas de Crédito y Débito, la misma que dentro de su artículo 17, se encuentra este tipo de medida de seguridad que tiene como objetivo detectar aquellas operaciones que no correspondan al comportamiento habitual de consumo del usuario[5]. Sin embargo, no es el único tipo de medida de

[4] Resolución N.° 1234-2019/CC3-INDECOPI.

[5] Resolución S.B.S. N°6523-2013 / Reglamento de Tarjetas de Crédito y Débito

seguridad que advierte este cuerpo legislativo, sino también, implementa la gestión de alertas por este tipo de monitoreo, identificación de patrones de fraude como análisis sistemático de la información histórica de las operaciones y establecer límites en diversos canales de atención para mitigar las pérdidas de fraude[6].

Encontramos, entonces, que el deber de información e idoneidad están establecidas en nuestra normativa de manera que las entidades financieras cumplan con brindar las medidas de seguridad necesarias para el resguardo de los productos y ejecución de servicios para los usuarios y consumidores; así como el deber de informar a los mismos con respecto a sus productos, las implicancias de estas y las consecuencias.

En la actualidad, esta regulación debería de ser aplicada en cada entidad financiera para que puedan cumplir con el monitoreo de operaciones conforme lo establece el Reglamento ya mencionado. Sobre estas medidas de seguridad, en la actualidad, podemos ver que diferentes entidades financieras han adoptado distintas formas de brindar confianza y resguardar la información y sus productos a los consumidores, no solamente de acuerdo con lo que establece la normativa, sino también un adicional para generar protección a los productos financieros. Entre estos podemos encontrar la adopción de aplicativos móviles con el fin de no usar las tarjetas en físico, lo cual, de una manera se busca evitar los riesgos que estos pueden sufrir como la clonación de tarjetas mediante el chip de las tarjetas, o también el skimming, el mismo que consiste cuando "un estafador utiliza un dispositivo, llamado skimmer, para robar información de una tarjeta de crédito o débito (…) captura los datos de la banda magnética de la tarjeta, que se pueden utilizar para crear tarjetas falsificadas o para realizar compras fraudulentas"[7].

Es claro que hoy en día se implementó en su mayoría de tarjetas de las entidades financieras las tarjetas NFC, cuyas siglas significa *Near Field Communication* "lo que traducido sería Comunicación de Campo Cercano (…) se trata de una tecnología que funciona por proximidad, cuando acercas un dispositivo a otro"[8]. De esta manera, no solamente las tarjetas físicas pueden evitar la clonación por el no uso del mismo chip para evitar fraudes como la clonación o el skimming, sino también por este tipo de sistemas se puede realizar el uso de dispositivos móviles para efectuar pagos con el teléfono móvil, al momento de que asocias estas tarjetas al celular.

Ahora bien, con respecto a las otras medidas de seguridad implementadas, encontramos que el mismo Reglamento de Ciberseguridad, en el artículo 2 literal j, establece cual es el mecanismo de uso factores de autenticación para poder verificar la identidad de un usuario, siendo las categorías: algo que solo el

[6] Ídem.

[7] Stripe. (22 de enero de 2025). Seis tipos de fraude en los pagos y como las empresas pueden prevenirlos.
https://stripe.com/mx/resources/more/six-types-of-payment-fraud

[8] Javier Penalva (21 de Marzo de 2025). NFC: qué es y para qué sirve en pleno 2025.
https://www.xataka.com/basics/nfc-que-es-y-para-que-sirve

usuario conoce, algo que solo el usuario posee y algo que el usuario es (características biométricas)[9].

Así también en su artículo 19, explica el mecanismo de autenticación reforzada para operaciones por canal digital (entiéndase canal digital los medios por el que se realizan transacciones por aplicativos móviles, plataformas digitales o inclusive con transacciones efectuadas desde el mismo celular), transacciones que demandan de una autenticación reforzada para aquellas operaciones que pueden llegar a ser fraudulentas siendo necesario la combinación de dos factores de autenticación, que correspondan a dos categorías distintas y que sean independientes uno del otro[10]. Podemos ver, que hay distintas medidas de seguridad que se han venido implementando por el mismo hecho que a medida que la tecnología avanza, esta también debería de ser regulada y junto con ella las medidas de seguridad que deberían de implementar como mínimo en este tipo de operaciones que realiza el uso de tecnología.

En ese sentido, considero que es importante informar a los usuarios sobre como funciona este mecanismo de seguridad ante operaciones digitales, no solamente para que comprendan los usuarios el uso de sus datos, contraseñas o sus datos biométricos de ser el caso, sino también para una comprensión sobre como este tipo de seguridad se puede ver vulnerada, o conocer el método de seguridad que las entidades financieras han venido implementando en sus plataformas digitales.

c. Patrón de consumo habitual en operaciones financieras

Ahora bien, entendiendo los deberes de información e idoneidad de los sistemas financieros y las medidas de seguridad que las entidades financieras están obligadas a tener, podemos encontrar que el patrón de consumo habitual está establecido en el mismo cuerpo normativo ya mencionado, dentro del artículo 2° numeral 5, se establece que el comportamiento habitual de consumo del usuario se enfoca en el tipo de operaciones que usualmente realiza cada uno con sus productos, considerando diversos factores, como por ejemplo el país de consumo, tipos de comercio, frecuencia, canal utilizado, entre otros, los cuales pueden ser determinados a partir de la información histórica de las operaciones de cada usuario[11]. Entonces, podemos acreditar que el patrón de consumo habitual es un conjunto de conductas transaccionales que caracterizan el uso que un consumidor hace de los servicios financieros los cuales incluyen distintas variables como el monto, la frecuencia, los horarios, los canales utilizados y la geolocalización de las operaciones.

Inicialmente, INDECOPI adoptó un criterio restrictivo: la responsabilidad por operaciones fraudulentas recaía, en gran medida, en el consumidor, bajo la premisa de que debía custodiar adecuadamente sus claves y credenciales.

[9] Resolución S.B.S. N°504-2021 / Reglamento para la Seguridad de la Información y la Ciberseguridad
[10] Ídem.
[11] Resolución S.B.S. N°6523-2013 / Reglamento de Tarjetas de Crédito y Débito

No obstante, a partir de resoluciones como la N°432-2021/SPC-INDECOPI, se consolidó un cambio de enfoque. Se estableció que corresponde a las entidades financieras demostrar que implementaron mecanismos efectivos de seguridad, incluyendo sistemas de monitoreo que alerten sobre operaciones que se aparten del patrón de consumo habitual del cliente[12].

Este pensamiento crítico por parte de INDECOPI refleja un rígido pensamiento del estándar de diligencia exigido a las entidades financieras. Se reconoce que los consumidores y usuarios carecen de los medios técnicos para identificar fraudes sofisticados, siendo las entidades las que disponen de recursos tecnológicos para prevenirlos, teniendo en cuenta los conceptos que las normativas sectoriales sobre el tema establecen para reforzar este tipo de seguridad en los sistemas de las entidades financieras.

2. Operaciones no reconocidas en la realidad

a. Habitualidad de operaciones no reconocidas

Vfgt Como se ha podido señalar en el capítulo anterior, INDECOPI ha venido desarrollando una doctrina basada en comparación entre la operación u operaciones presuntamente fraudulenta con el patrón histórico de conducta del usuario. Con respecto a este tema, encontramos que INDECOPI ha venido sancionando los últimos a distintas entidades financieras con respecto a la no adopción de medidas de seguridad por autentificación reforzada. Es así como Andina nos anuncia que “el sistema financiero concentra el 90% de las sanciones por operaciones no reconocidas, reveló hoy el INDECOPI”[13], es un porcentaje alto, teniendo en cuenta todos los procedimientos que INDECOPI tiene en su custodia. Dentro de los procedimientos específicamente de servicios financieros, se encuentra que “del 2021 a marzo de 2025, impuso 2,891 sanciones a 271 proveedores por operaciones no reconocidas”[14]. Es decir, dentro del universo de los procedimientos de los servicios financieros, el cual es amplio, se encuentran más de 2800 sanciones por el tema de operaciones no reconocidas.

Las cifras son alarmantes, pues es un indicador que refleja que las medidas de seguridad implementadas por las entidades financieras no resultan lo suficientemente eficientes. Estas sanciones se encuentran “relacionadas a tarjetas de crédito (54.8%), seguidas por cuentas de ahorros (29.8%), las mismas que se impusieron luego de evaluar la responsabilidad de bancos y entidades financieras en operaciones, consumos o transferencias que no fueron reconocidas por los titulares”[15].

Si bien las cifras mencionadas son inquietantes, se debe tener en cuenta que Asbanc ha determinado que, luego de la pandemia, al haberse incrementado

[12] Resolución N.° 432-2021/SPC-INDECOPI.
[13] Andina. (11 de marzo de 2025). Sistema financiero concentra 90% de sanciones por operaciones no reconocidas. https://andina.pe/agencia/noticia-indecopi-sistema-financiero-concentra-90-sanciones-operaciones-no-reconocidas-1026373.aspx
[14] Ídem.
[15] Ídem.

este tipo de transacciones por plataformas digitales, ha traído como consecuencia a la vez las estafas en tarjetas de crédito y débito en operaciones en línea. Fortinet menciona que “el aumento de virus cibernético ha crecido significativamente: en marzo del 2020 incrementó en un 131% en comparación al 2019.

De igual manera nuestro país ha sufrido más de 613 millones de intentos de ciberestafas hasta junio del último año (2021)”[16]. Estas estadísticas demuestran que las operaciones fraudulentas mediante plataformas digitales se han visto incrementadas a raíz de la pandemia hasta la fecha, estas cifras han venido en aumento, según el artículo, los delitos más comunes de estafa electrónica son: phishing, smishing, pharming y vishing[17]. Esto lo sustenta ASBANC misma, mencionan que “el monto promedio que pierde una persona por fraude tras el robo de su celular es de aproximadamente 2450 soles”[18], el cual es una cifra que es mucho mayor al sueldo mínimo legal de miles de personas.

En ese sentido, ASBANC recomienda una serie de consejos para poder cuidar nuestro dinero que se encuentran en nuestras cuentas o en los créditos que se asignan a los productos que tenemos con las entidades financieras. Entre ellas se encuentran la claves personales que no deban ser compartidas y estar bajo nuestro control, evitar ingresar a enlaces sospechosos que solo buscan robar información nuestra, el acceso a la plataforma de los bancos directamente del banco, evitar usar wifi públicas para realizar operaciones bancarias, entre otros[19]. De acuerdo a esta información, es claro que hay diferentes maneras de ser víctimas de fraudes mediante este tipo de operaciones digitales, las mismas que se han visto incrementadas a lo largo de estos años.

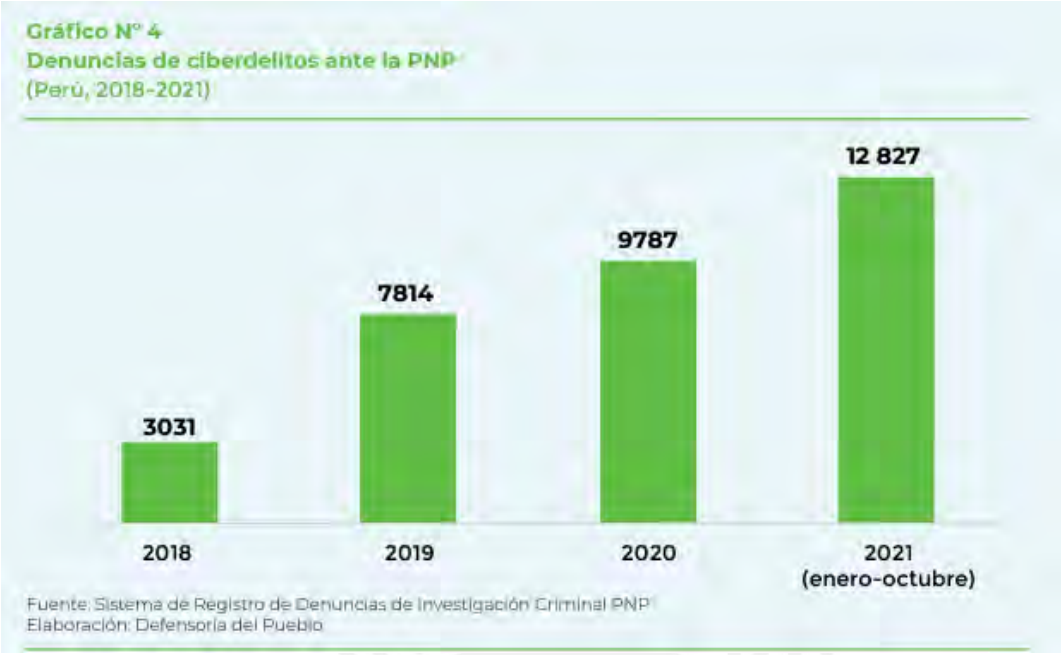
Esto va de la mano con las denuncias que se han venido presentando frente a la PNP durante los últimos años por estos ciberdelitos, de acuerdo al siguiente cuadro que se encuentra a continuación:

[16] La República. (24 de marzo de 2021). Asbanc: 38% de estafas en tarjetas de crédito y débito fueron por internet. https://larepublica.pe/economia/2021/03/24/asbanc-38-de-estafas-en-tarjetas-de-credito-y-debito-fueron-por-internet

[17] Ídem.

[18] Asbanc. (15 de julio de 2025). Cuida tu gratificación: Evita fraudes con estos consejos de ciberseguridad y actúa rápido ante un robo. https://asbanc.com.pe/noticia/cuida-tu-gratificacion-evita-fraudes-ciberseguridad

[19] Ídem.



Fuente: Defensoría del Pueblo (2016) La Ciberdelincuencia en el Perú: Estrategias y Retos del Estado (Informe Defensorial N° 001-2023-DP/ADHPD)

Lo que demuestra la imagen expuesta anterior, es que "las denuncias se cuadriplicaron entre los años 2018 y 2021, pasando de 3031 a 12,827"[20]. Este cuadro demuestra que estamos presentando una grave situación de inseguridad digital para poder realizar las transacciones operacionales en línea, en plataformas digitales y con el uso de nuestros datos personales que se pueda prestar para cometer delitos informáticos.

b. Operaciones no reconocidas en otros países

Para entender mejor estos mecanismos de las operaciones digitales en otros países, es ideal como regulan estas operaciones en otros países y si estas cuentan con una regulación especial. En ese sentido, detallaré por cada país sus operaciones técnicas y la regulación al respecto.

Comenzamos con España, la misma que encontramos dentro de su Real Decreto-ley 12/2018, brinda como objetivo el garantizar un nivel de seguridad tanto en redes como en sistemas de información en la Unión Europea, esta misma impone a las entidades financieras la obligación de gestionar riesgos, notificar incidentes significativos y cooperar con la autoridad competente, designada en España como el Instituto Nacional de Ciberseguridad (INCIBE). Este organismo funge como equipo de respuesta ante incidentes de seguridad informática y coordina con las autoridades financieras y de seguridad del Estado

[20] Defensoría del Pueblo (2016) La Ciberdelincuencia en el Perú: Estrategias y Retos del Estado (Informe Defensorial N° 001-2023-DP/ADHPD)
https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

para prevenir y mitigar ciberataques en el sistema financiero[21]. Es claro que tienen una regulación más específica para la sección de seguridad con respectos a los incidentes u operaciones que sean posiblemente fraudulentas, a diferencia de nuestra regulación que solo contamos con la SBS.

Del mismo modo, en los servicios de banca móvil, si el sistema detecta múltiples accesos desde dispositivos distintos o geolocalizaciones atípicas, el proveedor tiene la obligación de bloquear temporalmente el acceso, evaluar el riesgo y, si corresponde, notificar el incidente al Banco de España y al INCIBE, conforme a lo dispuesto en el Real Decreto-ley 12/2018 y las Circulares del Banco de España sobre servicios de pago[22]. Como se puede ver en este caso, hay una comunicación directa entre las entidades financieras con el Banco de España y el INCIBE, los cuales coordinan para evaluar el riesgo y de ser el caso decidan realizar el bloqueo respectivo temporal de las operaciones.

Como podemos ver, España es un país que tiene una regulación más específica e involucra distintas entidades que pueden intervenir para mitigar estas operaciones. A diferencia de Perú que solo contamos con dos entidades que realiza una investigación al respecto siendo INDECOPI y SBS respectivamente según las facultades que tienen cada una de ellas.

Con respecto a otro país con que comparar, encontramos a Chile, el cual dentro de su Ley N°21459, regula el marco legal frente a la realidad tecnológica contemporánea, incorporando delitos informáticos modernos, mejorando los procedimientos de investigación y ampliando la responsabilidad penal, inclusive para personas jurídicas[23]. Asimismo, vemos que la ley establece distintos delitos como: ataque a la integridad de un sistema informático, acceso ilícito (sin autorización o excediendo la autorización), interceptación ilícita de información transmitida, falsificación informática, receptación de datos informáticos obtenidos ilícitamente, entre otros[24]. Asimismo, un elemento adicional es que añade a las personas jurídicas como responsables penales, es decir, una empresa podría ser penalmente responsable si se comprueba la comisión del delito fue en provecho de esta empresa o por personas bajo su supervisión[25].

Además, Chile cuenta con entidades que regulan este tipo de operaciones y estos han regulado estándares mínimos para reforzar la ciberseguridad en el sistema que se maneja en el país. Por ejemplo, encontramos a la Comisión para el Mercado Financiero, el mismo que ha emitido circulares y normativas de riesgo operacional, control interno y gestión de continuidad para bancos, aseguradoras, intermediarios de valores y administradoras de fondos. Por ejemplo, las Circulares N° 1939 y N° 2020 establecen exigencias de ciberresiliencia para

[21] Boletín Oficial del Estado (BOE). (2018). Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (NIS). BOE-A-2018-12192. https://www.boe.es/eli/es/rdl/2018/09/07/12/con

[22] Banco de España. (2019). *Proyecto de Circular sobre servicios de pago*. Madrid: Banco de España.

[23] Ley 21.459, Ley de Delitos Informáticos. Diario Oficial de la República de Chile, 20 de junio de 2022. https://www.bcn.cl/leychile/navegar?idNorma=1177743

[24] Ídem.

[25] Ídem.

bancos, así como estándares para infraestructura tecnológica segura[26]. Como podemos ver, también este país cuenta con otras entidades que se refuerzan entre sí para mejorar la ciberseguridad de los usuarios de las entidades financieras y de las operaciones que estos pueden realizar en el día a día.

Entre otros países, podemos ver a Colombia, siendo la normativa Circular Externa N°052 2007, en el punto 4.9, establece las obligaciones adicionales por parte de las entidades financieras a través de internet, mencionando seis puntos que se encuentran obligados a realizar cuando son operaciones efectuadas por internet, siendo las siguientes: "i) Implementar los algoritmos y protocolos necesarios para brindar una comunicación segura; ii) Realizar como mínimo dos veces al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de transacciones por este canal. Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del canal, deberá realizarse una prueba adicional; iii) Promover y poner a disposición de sus clientes mecanismos que reduzcan la posibilidad de que la información de sus transacciones pueda ser capturada por terceros no autorizados durante cada sesión; iv) Establecer el tiempo máximo de inactividad, después del cual se deberá dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones; v) Informar al cliente, al inicio de cada sesión, la fecha y hora de último ingreso a este canal; e, vi) implementar mecanismos que permitan a la entidad financiera verificar constantemente que no sean modificados los enlaces (links) de su sitio Web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS."[27].

En la normativa de Colombia, ante operaciones realizadas por internet, se puede encontrar seis obligaciones que tienen las entidades financieras con sus usuarios para que estos puedan realizar sus operaciones de manera segura, brindando medidas de seguridad que refuercen este tipo de transferencias. Entre ellas podemos encontrar que la responsabilidad recae en las entidades financieras plenamente, toda vez que estas se encuentran en mejor posición para poder realizar este tipo de mecanismos de seguridad.

Si bien en esta normativa no encontramos los factores de autenticación como lo tenemos en nuestra normativa nacional, eso no quita el hecho que Colombia ha implementado distintas figuras que sería bueno tenerlo en cuenta dentro de nuestro país, como la implementación de algoritmos y protocolos para brindar una comunicación segura, o como también la realización de dos veces al año una prueba de vulnerabilidad y penetración a sus equipos, o sistemas que utiliza

[26] Banco Central de Chile. (s.f.). *Construyendo ciber resiliencia en la industria financiera*. Santiago: Banco Central.
https://www.bcentral.cl/contenido/-/detalle/construyendo-ciber-resiliencia-en-la-industria-financiera

[27] Circular 052 de 2007 [Superintendencia Financiera de Colombia]. Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios. 15 de octubre de 2007.
https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=6141

las entidades financieras. Este tipo de pruebas no lo encontramos regulado en nuestra normativa nacional, la cual podría ser de mucha utilidad, pues ya tuvimos un caso en el que la ineficiente seguridad de una entidad financiera ha sido vulnerado, de manera que se ha filtrado datos personales y sensibles de sus usuarios a terceros no autorizados.

c. Posible solución adoptado en Estados Unidos

En materia de protección del consumidor financiero, uno de los principales déficits observados en el sistema peruano radica en la ausencia de procedimientos ágiles y uniformes de devolución frente a operaciones fraudulentas no reconocidas. La práctica bancaria actual suele someter estos reclamos a evaluaciones internas extensas (usualmente se tardan hasta 30 días hábiles por procedimientos internos de cada entidad financiera), lo que genera frustración, pérdida de confianza y, en casos graves, perjuicio económico inmediato para los usuarios.

En contraste, diversas normativas de otros países han incorporado el modelo de "reembolso rápido" o "fast track refund", que impone al proveedor financiero la obligación de acreditar la legitimidad de la operación dentro de un plazo breve y, en caso de no lograrlo, reintegrar provisionalmente los fondos al cliente. Este sistema traslada la carga probatoria hacia la entidad financiera, dado que estos se encuentran en mejor posición para poder demostrar la validez de estas operaciones, por su superioridad técnica y control sobre los medios digitales que ellos administran directamente.

El referente más consolidado se encuentra en la Regulation E de la Federal Reserve Board y la Consumer Financial Protection Bureau (CFPB) de los Estados Unidos, que regula las transferencias electrónicas de fondos bajo la Electronic Fund Transfer Act (EFTA). Dicha normativa dispone que, cuando un consumidor reclama una operación no autorizada, el banco debe investigar dentro de un plazo máximo de diez días hábiles; si la investigación excede dicho plazo, la entidad está obligada a reembolsar provisionalmente los fondos mientras concluye el proceso de verificación[28]. Este mecanismo garantiza la protección inmediata de la liquidez del consumidor y fomenta la diligencia de las instituciones financieras en el control de riesgos operativos.

Este tipo de medidas se han adoptado en la Unión Europea mediante la Directiva (UE) 2015/2366, conocida como PSD2 (Payment Services Directive 2), el mismo que desarrolla que el proveedor del servicio de pago debe devolver inmediatamente al usuario el importe de una operación no autorizada, salvo prueba en contrario de que la transacción fue autenticada, registrada y ejecutada correctamente[29]. El fundamento de este régimen es la asimetría de la

[28] Consumer Financial Protection Bureau (CFPB). (s. f.). § 1005.11 Procedures for resolving errors. *12 CFR Part 1005 (Regulation E).*
https://www.consumerfinance.gov/rules-policy/regulations/1005/11/

[29] Parlamento Europeo & Consejo de la Unión Europea. (2015). *Directiva (UE) 2015/2366 sobre los servicios de pago en el mercado interior (PSD2).* Diario Oficial de la Unión Europea, L 337/35.
https://eur-lex.europa.eu/eli/dir/2015/2366/oj

información que existe entre el usuario y el proveedor, el consumidor no tiene acceso a los sistemas internos ni la capacidad para demostrar fallas técnicas o brechas de seguridad de las que están a cargo únicamente las entidades financieras.

i. Posible implementación dentro de Perú

Dentro del marco normativo peruano, este enfoque podría verse implementado mediante una modificación reglamentaria o resolución de la SBS, que establezca un tipo de procedimiento de devolución inmediata de fondos por operaciones fraudulentas, en los siguientes términos:

1. **Plazo de investigación:** podría proponerse un máximo de diez (10) días hábiles contados desde la notificación del reclamo por parte del usuario o cliente.
2. **Reembolso provisional obligatorio:** si al término del plazo no se acredita de manera fehaciente la autorización de la operación, el banco debería reintegrar provisionalmente los fondos al usuario afectado por este tipo de operación/es no reconocida/s.
3. **Revisión posterior y reversión:** si la entidad demuestra posteriormente que el cliente participó de manera dolosa o facilitó el fraude por negligencia grave, podrá revertir el abono, previa comunicación motivada y sujeta a revisión administrativa.
4. **Supervisión administrativa:** la SBS debería supervisar los tiempos de respuesta y publicar indicadores trimestrales de cumplimiento como parte de las funciones a cargo de esta entidad administrativa, generando transparencia y en aras conforme al Código de Protección al Consumidor.

Este mecanismo tendría un efecto reparador, disuasorio y preventivo, pues, de esta manera alienta a las entidades financieras a invertir en mejoras tecnológicas, autenticación robusta y monitoreo en tiempo real, con el fin de evitar incurrir en costos de reembolso por fallas de seguridad o las multas que traen como consecuencia este tipo de operaciones luego de un procedimiento ante INDECOPI. Asimismo, otorga al consumidor financiero una vía pronta de restitución que no sustituye la investigación penal o administrativa, pero restablece su situación patrimonial de forma inmediata.

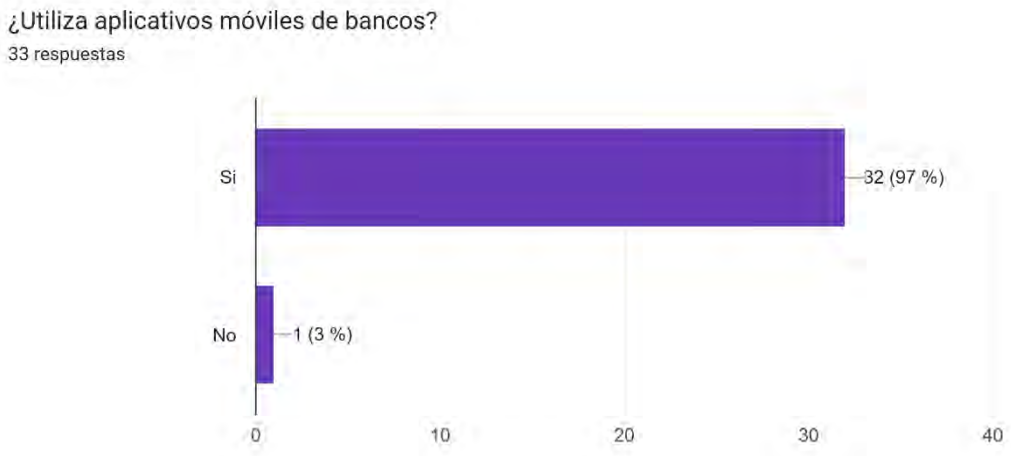
En ese sentido, la implementación de un sistema “fast track” de devolución rápida constituiría una solución de impacto inmediato y bajo costo regulatorio, alineada con prácticas internacionales que se han aplicado en Estados Unidos y Unión Europea, generando una mayor protección a los usuarios o consumidores financieros, los principios de equidad, transparencia y trato justo que rigen la protección del consumidor financiero. Su adopción fortalecería la confianza en la banca digital, reduciría los procedimientos que se denuncian ante INDECOPI y contribuiría al desarrollo sostenible del sistema financiero peruano.

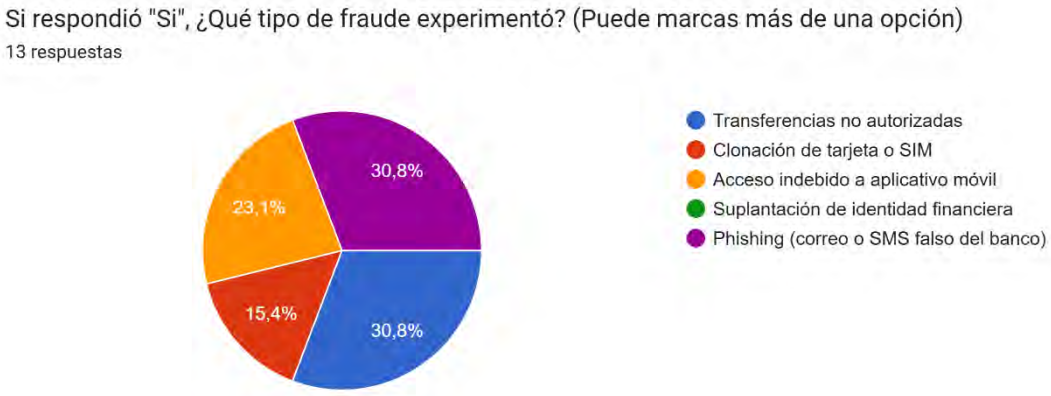
3. Situación actual en Perú sobre operaciones fraudulentas

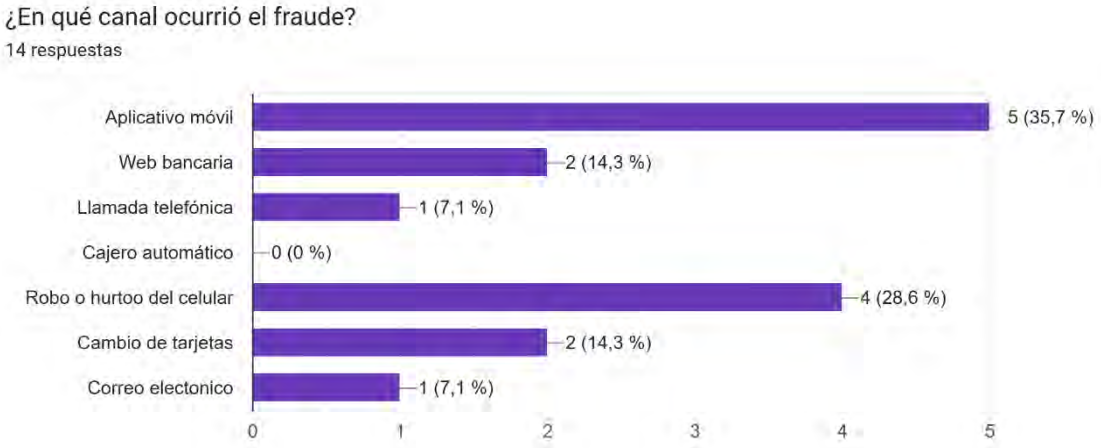
Para el presente artículo se efectuó una pequeña encuesta para poder mostrar la situación sobre este tipo de operaciones. La encuesta tiene como nombre “Víctimas de operaciones fraudulentas en el Perú”, el mismo que tuvo como objetivo identificar las características básicas de las personas que pudieron haber sido afectadas por fraudes financieros y analizar los mecanismos mediante los cuales se produjeron los incidentes. Se analizaron 33 respuestas válidas, anonimizadas y procesadas de forma agregada. Los resultados permiten extraer una aproximación a los patrones de vulnerabilidad y a los canales más expuestos a riesgos cibernéticos.

Comenzamos con que los resultados de género evidencian una distribución equilibrada: 15 mujeres y 15 hombres, con un caso adicional de persona que prefirió no declarar su identidad de género. Este equilibrio sugiere que la exposición al riesgo de fraude financiero no distingue significativamente por sexo, sino más bien por el nivel de alfabetización digital y la frecuencia de uso de canales electrónicos.

En cuanto a la modalidad del fraude, se observa que 11 participantes reportaron haber sido víctimas de algún tipo de operación fraudulenta, mientras que 18 manifestaron no haberlo sido. Respecto a los canales utilizados, el 17% de las víctimas no declaró el medio del fraude, lo cual revela la necesidad de más información sobre las denuncias de los incidentes. Las personas que sí declararon el canal, los casos más frecuentes se produjeron a través de aplicativos móviles (4 casos) y robo o hurto de celulares (4 casos). En menor proporción, se identificaron incidentes vinculados al cambio de tarjetas (2 casos), llamadas telefónicas (1 caso), correo electrónico (1 caso) y plataformas web bancarias (1 caso). Estos resultados concuerdan con la tendencia creciente del uso de la banca móvil de las entidades financieras en el país y pone de relieve la vulnerabilidad asociada a la pérdida o manipulación de dispositivos inteligentes, tal como se observa en los siguientes cuadros:

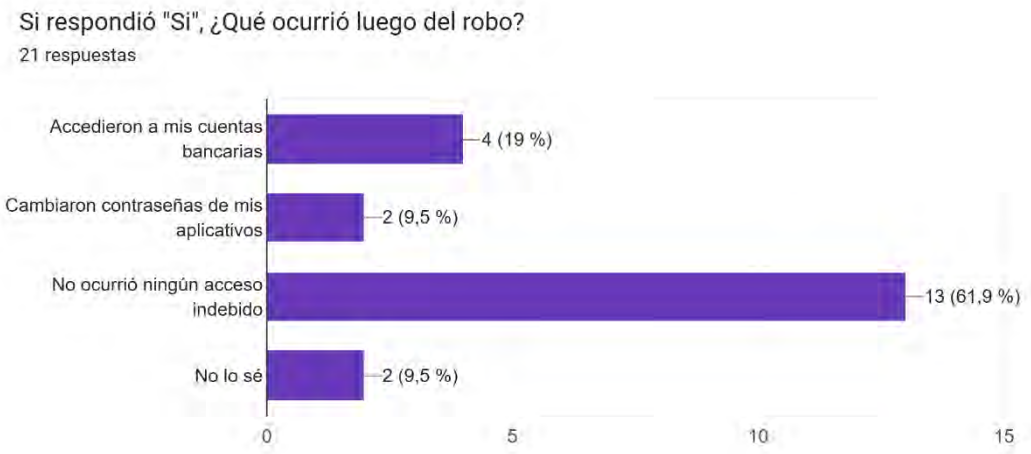






Con respecto a los montos afectados, las opciones propuestas oscilaban entre un monto menor a S/1,000.00 soles, otro monto entre S/1,000.00 y S/5,000.00, y la tercera opción es mayor a S/5,000.00, cuyo resultado se detalla en el cuadro a continuación:

Las consecuencias de los robos o hurtos que se efectuaron a las víctimas se manifiestan de distintas maneras, de las cuales, 4 personas afirman que accedieron a sus cuentas bancarias, 2 cambiaron contraseñas de sus aplicativos móviles, 13 aseguran que no ocurrió ningún acceso indebido al aplicativo, por último, 2 personas no saben que pudo haber sucedido luego del robo, el siguiente cuadro demuestra las respuestas:



Los resultados de la encuesta revelan que el fraude digital es una problemática transversal, que exige fortalecer la seguridad cibernética, la regulación financiera y los mecanismos de respuesta inmediata al consumidor. Solo mediante una acción coordinada entre los sectores público y privado se podrá garantizar la confianza en el sistema financiero peruano y reducir el impacto de los delitos informáticos sobre la población, siendo este un problema que afecta a la mayoría de personas que utilizan estos recursos para transferencias más efectivas y rápidas; sin embargo, con un alto riesgo de fraude.

CONCLUSIONES Y/O RECOMENDACIONES

El consumidor financiero se encuentra en una posición de vulnerabilidad estructural que encuentra un apoyo en el marco normativo y jurisprudencial reforzado. Encontramos que el marco normativo fue implementándose a medida que las operaciones digitales han venido realizándose con mayor frecuencia en el día a día. El deber de información y la idoneidad del servicio constituyen estándares básicos que deben cumplirse para garantizar relaciones de consumo justas.

La noción de patrón de consumo habitual ha evolucionado en la jurisprudencia de INDECOPI, pasando de ser un argumento defensivo para convertirse en un parámetro esencial para evaluar la diligencia de las entidades financieras.

Asimismo, la ciberseguridad se posiciona como un eje transversal de la protección al consumidor financiero, no solamente en el Perú, sino también, como se ha podido ver, en otros países, de manera que se encuentran distintas entidades entrelazadas para reforzar este tema que es un problema en distintas partes del mundo. Las experiencias comparadas demuestran que la regulación debe combinar estrategias de prevención, supervisión y educación digital. En este sentido, el fortalecimiento de los mecanismos de ciberresiliencia resulta indispensable para garantizar la confianza y seguridad del sistema financiero.

La implementación del mecanismo de devolución rápida podría ser un avance muy determinante en la protección del consumidor financiero frente a operaciones no reconocidas. Su finalidad es de garantizar una restitución inmediata de los fondos sustraídos, de manera que evita que el consumidor financiero asuma los efectos económicos de una falla de seguridad o de un fraude digital. Este enfoque reconoce la asimetría de información que existe entre las entidades financieras y los usuarios de estos, y traslada de manera razonable la carga probatoria hacia las mismas entidades, dado que son ellas las que controlan los sistemas tecnológicos, los protocolos de autenticación y los registros de cada transacción.

La viabilidad de esta medida en nuestro país podría ser óptima, ya que podría implementarse mediante una resolución de la Superintendencia de Banca, Seguros y AFP – SBS sin requerir una reforma legislativa. El procedimiento podría contemplar un plazo de aproximadamente diez días hábiles para la investigación, de manera que el siguiente paso sea la obligación de reembolsar provisionalmente el monto reclamado, hasta que se encuentre una prueba fehaciente de participación dolosa o negligente del consumidor financiero. Con ello, el Perú se alinearía a los estándares idóneos de otros países de protección financiera y fortalecería la confianza de los consumidores en el sistema bancario digital.

BIBLIOGRAFÍA

- Andina. (11 de marzo de 2025). Sistema financiero concentra 90% de sanciones por operaciones no reconocidas. https://andina.pe/agencia/noticia-indecopi-sistema-financiero-concentra-90-sanciones-operaciones-no-reconocidas-1026373.aspx
- Asbanc. (15 de julio de 2025). Cuida tu gratificación: Evita fraudes con estos consejos de ciberseguridad y actúa rápido ante un robo. https://asbanc.com.pe/noticia/cuida-tu-gratificacion-evita-fraudes-ciberseguridad
- Banco de España. (2019). Proyecto de Circular sobre servicios de pago. Madrid: Banco de España.
- Banco Central de Chile. (s.f.). *Construyendo ciber resiliencia en la industria financiera*. Santiago: Banco Central. https://www.bcentral.cl/contenido/-/detalle/construyendo-ciber-resiliencia-en-la-industria-financiera
- Boletín Oficial del Estado (BOE). (2018). Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (NIS). BOE-A-2018-12192. https://www.boe.es/eli/es/rdl/2018/09/07/12/con
- Circular 052 de 2007 [Superintendencia Financiera de Colombia]. Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios. 15 de octubre de 2007. https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=6141
- Consumer Financial Protection Bureau (CFPB). (s. f.). § 1005.11 Procedures for resolving errors. 12 CFR Part 1005 (Regulation E). https://www.consumerfinance.gov/rules-policy/regulations/1005/11/
- Defensoría del Pueblo (2016) La Ciberdelincuencia en el Perú: Estrategias y Retos del Estado (Informe Defensorial N° 001-2023-DP/ADHPD) https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf
- La República. (24 de marzo de 2021). Asbanc: 38% de estafas en tarjetas de crédito y débito fueron por internet. https://larepublica.pe/economia/2021/03/24/asbanc-38-de-estafas-en-tarjetas-de-credito-y-debito-fueron-por-internet
- Ley N°29571, Código de Protección y Defensa del Consumidor.
- Ley 21.459, Ley de Delitos Informáticos. Diario Oficial de la República de Chile, 20 de junio de 2022. https://www.bcn.cl/leychile/navegar?idNorma=1177743
- Parlamento Europeo & Consejo de la Unión Europea. (2015). Directiva (UE) 2015/2366 sobre los servicios de pago en el mercado interior (PSD2). Diario Oficial de la Unión Europea, L 337/35.

https://eur-lex.europa.eu/eli/dir/2015/2366/oj
- Resolución N° 1234-2019/CC3-INDECOPI.
- Resolución N° 432-2021/SPC-INDECOPI.
- Resolución S.B.S. N°6523-2013 / Reglamento de Tarjetas de Crédito y Débito
- Resolución S.B.S. N°504-2021 / Reglamento para la Seguridad de la Información y la Ciberseguridad
- Stripe. (22 de enero de 2025). Seis tipos de fraude en los pagos y como las empresas pueden prevenirlos. https://stripe.com/mx/resources/more/six-types-of-payment-fraud
- Javier Penalva (21 de Marzo de 2025). NFC: qué es y para qué sirve en pleno 2025. https://www.xataka.com/basics/nfc-que-es-y-para-que-sirve