PONTIFICIA UNIVERSIDAD
CATÓLICA DEL PERÚ

FACULTAD DE DERECHO

Programa de Segunda Especialidad en Derecho de Protección al Consumidor

“El deber de idoneidad en los servicios financieros frente a operaciones no reconocidas: análisis crítico del criterio del patrón del consumo en la jurisprudencia de Indecopi”

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

Autor:
Brenda Valeria Torres Castañeda

Asesor:
Julio Baltazar Durand Carrión

Lima, 2025

Informe de Similitud

Yo, DURAND CARRION, JULIO BALTAZAR, docente de la Facultad de Derecho de la Pontificia Universidad Católica del Perú, asesor(a) del Trabajo Académico titulado "**El deber de idoneidad en los servicios financieros frente a operaciones no reconocidas: Análisis crítico del criterio del patrón del consumo en la jurisprudencia de Indecopi**", del autor(a) TORRES CASTAÑEDA, BRENDA VALERIA, dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 17%. 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">DURAND CARRION, JULIO BALTAZAR</td></tr>
<tr><td>DNI: 06726360</td><td rowspan="2">Firma:
  </td></tr>
<tr><td>ORCID:

https://orcid.org/0000-0002-2926-1912</td></tr>
</table>

RESUMEN

El presente trabajo pretende analizar si el criterio del patrón de consumo, utilizado por Indecopi para evaluar operaciones no reconocidas, proporciona una protección adecuada al consumidor frente al fraude electrónico. Para ello, el estudio se divide en cuatro secciones que permiten revisar el marco normativo vigente, su aplicación en la práctica, la relación que tiene con estándares internacionales y una propuesta de fortalecimiento normativo y técnico.

En la primera sección se estudia el marco normativo del deber de idoneidad y las obligaciones de seguridad que recaen sobre las entidades financieras. Si bien la normativa peruana busca proteger al consumidor- al exigir medidas mínimas y trasladar la carga de la prueba al proveedor-, su efectividad real depende en gran parte de que las entidades financieras cuenten con sistemas tecnológicos capaces de prevenir y detectar operaciones irregulares, lo que en la práctica no siempre ocurre.

La segunda sección identifica cómo Indecopi aplica el patrón de consumo en sus decisiones. La falta de uniformidad en su interpretación y la ausencia de parámetros técnicos claros terminan generando dudas tanto para los consumidores como para las entidades, lo que vuelve menos predecible las decisiones que se emiten.

La tercera sección compara la normativa peruana con estándares internacionales. En esta sección, se advierte que el sistema es aun reactivo y que existe desigual implementación de herramientas como la autenticación reforzada.

Finalmente, la cuarta sección propone un fortalecimiento normativo y técnico. Se formulan propuestas de mejoras orientadas a reforzar la protección del consumidor financiero a partir del análisis desarrollado en la sección 3.

Palabras clave

Deber de idoneidad, servicios financieros, patrón habitual de consumo, fraude electrónico.

ABSTRACT

This study seeks to analyze whether the “consumption pattern” criterion used by Indecopi to assess unrecognized transactions provides adequate consumer protection against electronic fraud. To that end, the research is divided into four sections that examine the current regulatory framework, its practical application, its relationship with international standards, and a proposal for normative and technical strengthening.

The first section reviews the regulatory framework governing the duty of suitability and the security obligations imposed on financial institutions. Although Peruvian regulations aim to protect consumers—by requiring minimum security measures and shifting the burden of proof to the provider—their actual effectiveness largely depends on whether financial institutions have technological systems capable of preventing and detecting irregular transactions, which in practice does not always occur.

The second section examines how Indecopi applies the consumption-pattern criterion in its decisions. The lack of uniformity in its interpretation and the absence of clear technical parameters generate uncertainty for both consumers and financial institutions, ultimately reducing the predictability of the decisions issued.

The third section compares Peruvian regulations with international standards. It finds that the system remains predominantly reactive and that the implementation of tools such as strong customer authentication is uneven.

Finally, the fourth section proposes normative and technical enhancements. It presents recommendations aimed at strengthening the protection of financial consumers based on the analysis developed in Section 3.

Keywords

Duty of suitability, financial services, consumer spending pattern, scams.

ÍNDICE

INTRODUCCIÓN

El incremento de servicios financieros digitales y el uso extendido de tarjetas de crédito y débito, han permitido realizar transacciones con mayor facilidad. Sin embargo, también han incrementado los fraudes electrónicos y con ello reclamos por operaciones no reconocidas.

Ante esta situación, Indecopi ha adoptado el criterio del patrón de consumo como una herramienta central para evaluar la idoneidad del servicio financiero brindado. No obstante, su aplicación no ha sido uniforme, generando debate respecto a su eficacia.

El presente trabajo pretende analizar si dicho criterio de patrón de consumo realmente brinda una protección adecuada a los consumidores financieros y si su uso es compatible con los estándares de seguridad que demandan los sistemas modernos de pago.

Para ello, el presente trabajo ha sido dividido en cuatro secciones: el marco normativo del deber de idoneidad, su aplicación práctica del patrón de consumo en la jurisprudencia de Indecopi, las comparaciones con ciertos modelos internacionales y, finalmente, una propuesta de mejora normativa y técnica.

SECCIÓN 1: EL DEBER DE IDONEIDAD EN LOS SERVICIOS FINANCIEROS

Este trabajo desarrolla en su primera parte del tema “El deber de idoneidad en los servicios financieros en el Perú”. El objetivo específico que se tiene en esta sección es estudiar el marco normativo del deber de idoneidad en el Código de Protección y Defensa del Consumidor, así como también de su Reglamento de Tarjetas de Crédito y Débito de la SBS. Para llegar a este objetivo, se plantea como problema específico la siguiente cuestión: ¿Cuál es el alcance del deber de idoneidad en los servicios financieros respecto a las operaciones no reconocidas?

La hipótesis que aquí se plantea es que en el Perú el deber de idoneidad en los servicios financieros frente a operaciones no reconocidas implica una especial protección al consumidor. Pero, en la práctica las entidades financieras estarían cumpliendo este deber de forma muy limitada, centrándose en el aspecto contractual y no asegurando sistemas eficaces de prevención, autenticación y monitoreo de las transacciones.

La falta de aplicación efectiva de las normas hace que los usuarios sean cada vez más vulnerables a fraudes, phishing y otros tipos de riesgos digitales. Esto demuestra que la protección al consumidor no debe apoyarse solo en la regulación, sino también en que las entidades financieras cuenten con tecnología y medios necesarios.

Esta sección sienta las bases normativas y doctrinales para comprender por qué el “patrón de consumo” no es suficiente.

1.1. Marco normativo del deber de idoneidad

El presente Código de Protección y Defensa del Consumidor o también denominado Ley N° 29571, establece en sus artículos 18 y 19 el deber de idoneidad, los cuales se encuentran ubicados en el Capítulo III del Título I.

Este deber de idoneidad garantiza que los productos o servicios que son ofrecidos en el mercado respondan a estándares o condiciones mínimas de calidad, seguridad y de conformidad con lo que el consumidor espera recibir. Cabe resaltar que no solo se limitan a reconocer a la idoneidad como uno de los

principios básicos de las relaciones de consumo, sino que además señalan cómo los proveedores tienen responsabilidad ante eventuales incumplimientos.

En base a la lectura del artículo 18 del Código, este menciona que debe haber coherencia entre lo que el consumidor espera obtener y lo que efectivamente recibe. En ese sentido, este articulo garantiza la sintonía que debe haber entre la promesa del proveedor y la experiencia del servicio o producto consumido. Además, implica que este bien o servicio cuente con las características y la calidad adecuada para satisfacer la necesidad que motivó su adquisición.

En el caso del artículo 19, este menciona que quien es responsable de garantizar la idoneidad de los productos o servicios es el proveedor. Ante un reclamo por incumplimiento de esta obligación, le corresponde a este mismo demostrar que ese incumplimiento no es a consecuencia de una conducta suya. Es así que este articulo 19 reafirma la responsabilidad del proveedor sobre los productos o servicios que ofrece.

En ese sentido, el marco de deber de idoneidad señalados en el artículo 18 y 19 del Código, es especialmente importante en los servicios financieros, donde el uso de tarjeta de crédito y débito implican ciertas condiciones y medidas de seguridad para prevenir operaciones sospechosas.

En tales supuestos, el deber de idoneidad señalado en el artículo 18 del Código de Protección y Defensa del Consumidor exige constatar que el servicio efectivamente satisface lo que un consumidor razonable espera recibir. Tal constatación no solo debe considerar los compromisos expresamente asumidos por la entidad bancaria, sino también las obligaciones legales que le resultan exigibles, conforme al artículo 20 del mismo Código (Silvestre Bermúdez, 2021, p. 28).

A nivel sectorial, el Reglamento de Tarjetas de Crédito y Débito aprobado por la Superintendencia de Banca, Seguros y AFP (SBS) (en adelante el “Reglamento”), profundiza en la concreción del deber de idoneidad, pues les impone a las entidades emisoras la obligación de incorporar mecanismos de seguridad que se encuentran orientadas a disminuir la posibilidad de operaciones irregulares o no reconocidas. Lejos de formular simples

declaraciones generales, el Reglamento introduce exigencias técnicas muy puntuales, como es la implementación de sistemas de supervisión permanente, herramientas de detección y bloqueo de transacciones sospechosas y protocolos de verificación de identidad que respalden la legitimidad de las operaciones efectuadas mediante tarjetas.

Ahora bien, el Reglamento ha experimentado diversas modificaciones a lo largo de los años, en razón al avance de la innovación tecnológica y a los nuevos riesgos que esta conlleva para la seguridad de los usuarios. En ese sentido, el 28 de junio del 2024 se aprobaron cambios sustanciales mediante la Resolución SBS N° 2286-2024. Dicha Resolución introduce exigencias técnicas que concretan el deber de idoneidad en los servicios financieros. Así, por ejemplo, el artículo 16, numeral 7, establece que las entidades emisoras deben aplicar procesos de autenticación reforzada con al menos dos factores, de acuerdo con el Reglamento de Ciberseguridad.

Esta obligación alcanza tanto a las operaciones con tarjeta presente, mediante chip y PIN u otro factor que determine la SBS; como a las operaciones con tarjeta no presente, mediante códigos dinámicos u otros factores verificables bajo el estándar EMV 3DS; y también a las billeteras móviles basadas en tokenización, que requieren mecanismos adicionales de validación. Complementariamente, el artículo 23, numeral 10, prevé que las pérdidas ocasionadas por operaciones no reconocidas recaen en la entidad financiera cuando estas se ejecutan sin el cumplimiento del requisito de doble autenticación.

En ese sentido, desde el 1 de julio del 2025, entró en vigencia lo dispuesto en el artículo 23 del Reglamento, referido a la responsabilidad de las entidades proveedoras frente a las operaciones no reconocidas. Con ello, se produce un cambio trascendental, pues la responsabilidad se traslada expresamente a los proveedores y se invierte la carga de la prueba, pues ya no es el consumidor quien debe acreditar su falta de intervención, sino que corresponde a la entidad probar la responsabilidad del cliente; de lo contrario, asumirá íntegramente las pérdidas ocasionadas. Este esquema no solo fortalece la tutela del usuario, sino que también contribuye a reducir los riesgos de fraude y de operaciones ejecutadas por terceros no autorizados (Velazco Velazco, 2024, pp. 14 – 15). De

este modo, la regulación sectorial no se presenta aislada, sino que complementa lo establecido por el Código de Protección y Defensa del Consumidor, trasladando al campo financiero obligaciones dirigidas a consolidar la confianza en las transacciones electrónicas.

Este marco normativo, debe interpretarse y articularse con otros principios rectores del derecho de consumo: (a) deber de información, (b) deber de seguridad y (c) confianza legítima.

a) Deber de información

El deber de información implica que el proveedor debe poner en conocimiento del consumidor las características, condiciones y efectos esenciales vinculados al contrato y al bien o servicio objeto de la transacción. La intensidad de este deber no es uniforme, pues varía en función de la naturaleza del producto o servicio: aquellos de mayor complejidad o valor económico requieren una explicación más detallada que otros de uso cotidiano o más simples (Durand & Flores, 2024, pp. 111-112).

Cuando se trata del caso de las tarjetas y las operaciones electrónicas, esto significa que el usuario debe recibir información clara antes de usar el servicio, por ejemplo, sobre cómo funcionan los mecanismos de seguridad, en qué casos no se aplican y a qué canales acudir si es que ocurriera una operación no reconocida. Además del tiempo disponible para presentar el reclamo.

También, conservar evidencias electrónicas que acrediten el consentimiento del consumidor (como la aceptación de términos y condiciones, comprobantes de validación o mensajes de confirmación).

b) Deber de seguridad

Es necesario distinguir entre el deber de idoneidad y el de seguridad en el ámbito financiero. Y es que, aunque el deber de seguridad se podría entender como lo implícito en las expectativas razonables del consumidor, nuestro ordenamiento lo recoge de otra manera, siendo más orientado a proteger a los usuarios frente a los riesgos que puedan poner en peligro su integridad y su patrimonio (LEX, 2021).

Es así que el deber de seguridad en servicios financieros, y en particular el uso de tarjetas de pago, se refiere a la puesta en marcha de medidas y controles preventivos para identificar riesgos, la prevención de fraudes y asegurar que las transacciones se realicen dentro de los parámetros de usos correctos.

En ese sentido, las entidades financieras están obligadas a implantar ciertas medidas técnicas como la autenticación multifactor, tokens, los estándares EMV, cifrado de datos o gestión de claves.

En aquellos casos vinculados a monitoreo, las entidades financieras deben disponer de un sistema anti-fraude en tiempo real, o de scoring de transacciones y plataformas de inteligencia de seguridad, así como disponer de políticas de ciberseguridad. Cabe mencionar que al ser dinámico el deber de seguridad, se pide una actualización constante.

c) Confianza legítima

El principio de confianza legítima se encuentra regulado en el artículo cuarto del título preliminar del TUO de la LPAG o también denominada Ley N° 27444 e indica que cuando una autoridad actúa de cierta manera, genera en los consumidores seguridad de que seguirá haciéndolo así. Por eso, la administración no debe cambiar sus decisiones o actuaciones de forma repentina, sin una justificación válida (Huaroto Gutiérrez, 2023).

La confianza legítima se refleja a través de la expectativa que tiene el consumidor de que todo se llevará a cabo en razón a los estándares aplicables. Esta expectativa se construye a partir de la regulación vigente, la comunicación comercial, entendida como la información ofrecida por el proveedor o como ha actuado la entidad antes y cuales han sido las practicas comunes en el sector.

En síntesis, estas normas demuestran que el deber de idoneidad en los servicios financieros no se limita con solo cumplir con el contrato, sino que también exige con brindar seguridad y protección al usuario, más aún ante el aumento de operaciones no autorizadas en el entorno digital. Con ello se busca un sistema más protector y efectivo.

1.2. Alcance del deber de idoneidad en operaciones no reconocidas y limitaciones en la práctica peruana

Se debe precisar que contamos con una interpretación amplia del deber de idoneidad ya que la carga de la prueba la tiene el proveedor financiero y con ello surgen ciertos retos. Pues, conlleva a que las entidades financieras se actualicen en sus sistemas tecnológicos y que estas permitan prevenir y también detectar operaciones fraudulentas o no reconocidas.

Entre los principales retos se encuentra el de mantener actualizado los sistemas de seguridad y verificación. Esto incluye usar métodos como la autenticación en varios pasos, la tokenización, los estándares EMV3DS, el cifrado de datos y gestión de contraseñas o claves. Los cuales requieren ser probados periódicamente y revisados para asegurar que realmente funcionen, sobre todo porque las formas de fraude van cambiando y se vuelven más sofisticadas con el tiempo.

En la práctica, a pesar que en la norma se mencione que las entidades financieras deben asumir las pérdidas de las operaciones no reconocidas, es difícil asegurar que funcione realmente la autenticación, principalmente cuando hay muchas operaciones al mismo tiempo o que combinan los múltiples canales de pago.

Por ejemplo, en el caso de los token digitales, si bien se presentan como una herramienta clave para fortalecer la protección del consumidor en operaciones no reconocidas. Pues, al generar códigos únicos de seis dígitos de manera aleatoria y renovarlas generalmente cada minuto, permite añadir una capa adicional de seguridad sobre las contraseñas tradicionales, lo que reduce significativamente la posibilidad de accesos no autorizados (García Salirrosas & Bendezú Delgadillo, 2024, p. 28). No obstante, aquello puede generar también una dependencia tecnológica, ya que obliga a los usuarios a contar con dispositivos compatibles y de acceso continuo a la infraestructura que genera los tokens.

Asimismo, si bien los tokens son técnicamente seguros, existe el riesgo de sufrir un ciberataque o phishing, mediante el cual se engaña al usuario para que revele

información confidencial como puede ser la clave del token. Esto al día de hoy sigue representando un problema real. Pues, en el Perú el phishing no cuenta con una regulación propia; su tratamiento se realiza dentro del marco general de los delitos informáticos, específicamente bajo los artículos 8 y 9 de la Ley N° 30096.

Bajo premisa de esta normativa, se considera phishing cualquier acto de fraude que implique el acceso indebido a sistemas o manipulación de datos con fines ilícitos. Esta regulación contrasta con legislaciones más completas como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, que impone reglas claras para las empresas en cuanto a la protección de información personal, regulando incluso la transferencia internacional de datos y ampliando los derechos de las personas sobre el control de su información (Ccoyllo Sánchez, 2025).

En ese sentido, pese a la claridad normativa y a la transferencia de la carga de prueba al proveedor, enfrenta diversas dificultades en la práctica.

Ejemplo de ello, es lo ocurrido en octubre del 2024 cuando los datos personales de tres millones de usuarios del banco Interbank fueron expuestos en el foro de la dark web (Redacción EC, 2024). Aquella filtración de datos demostró que no existían auditorias de seguridad idóneas para detectar aquellos accesos no autorizados. Además, la demora por parte de Interbank demostró la deficiencia que se tiene con respecto a los protocolos de seguridad en relación a incidentes.

Lo sucedido en el caso de Interbank alerta a la importancia de fortalecer la supervisión y de contar con ciertas prácticas de ciberseguridad estandarizadas para todo el sistema financiero en Perú.

SECCIÓN 2: JURISPRUDENCIA DE INDECOPI Y EL CRITERIO DEL "PATRÓN DE CONSUMO"

En esta presente segunda sección del trabajo denominada *"Jurisprudencia de Indecopi y el criterio del patrón de consumo"*, se tiene por objetivo identificar de qué manera ha sido aplicado el criterio del "patrón de consumo" en las resoluciones recientes de Indecopi. Con el fin de alcanzar el objetivo, nos planteamos la siguiente pregunta: ¿Cómo emplea Indecopi el criterio del patrón de consumo en la resolución de casos de operaciones no reconocidas?

La hipótesis plantea que la forma en la que actualmente se aplica el criterio de patrón de consumo no es clara ni predecible, lo que genera decisiones diferentes entre los casos y afecta la seguridad jurídica tanto de los consumidores como de los proveedores.

La sección 2 se estructura en tres apartados. En el subcapítulo 2.1. se desarrolla el concepto de patrón de consumo, por lo cual se aborda su definición jurisprudencial, así como su vinculación con el deber de idoneidad y la buena fe contractual.

En el subcapítulo 2.2.se analiza la aplicación práctica de este criterio a través de ciertos casos resueltos por Indecopi. Para ello, abordaremos los relacionados con las entidades financieras Interbank y BBVA, contrastando las decisiones en las cuales se reconoció o se excluyó la responsabilidad del proveedor financiero.

En el subcapítulo 2.3 se examina aquellos problemas detectados en la aplicación del patrón de consumo, en ella se observa la ausencia de parámetros técnicos objetivos, la falta de uniformidad, entre otras.

De esta manera, la sección 2 busca evidenciar cómo la actual interpretación del patrón de consumo por parte de Indecopi, pese a su utilidad teórica, presenta vacíos metodológicos y prácticos que limitan su eficacia en la protección del consumidor financiero frente a operaciones no reconocidas.

2.1. Conceptualización del “patrón de consumo”

El patrón de consumo o también denominado comportamiento habitual de consumo se encuentra establecido en el Reglamento de Tarjetas de crédito y débito en su artículo 2 numeral 5. Este comportamiento habitual hace alusión al conjunto de operaciones que se realiza de manera regular con las tarjetas de crédito o débito. Para su identificación, se toman en cuenta distintos elementos como el país donde se suelen efectuar sus compras, los tipos de establecimientos que frecuenta, la periodicidad de sus transacciones, el canal empleado (presencial, virtual, cajero, etc.) entre otros. En ese sentido, dichos patrones pueden establecerse a partir del historial de operaciones registradas por la propia entidad financiera.

Asimismo, el artículo 17 del Reglamento de tarjetas de crédito y débito también impone a las entidades financieras un deber activo de vigilancia basado en el análisis de comportamiento habitual de consumo del cliente. En ese sentido, a través de mecanismos tecnológicos de supervisión continua deben detectar cuando el comportamiento regular del cliente presenta cambios que no corresponden con su historial y que por ende debe generar algún tipo de alerta para reducir riesgos de fraude.

De acuerdo con Pareja (2022), el patrón de consumo habitual del usuario puede definirse dentro de un contexto especifico o utilizando todos los datos históricos que las instituciones financieras tienen sobre el comportamiento de gasto de cada cliente (p. 3). En ese contexto, corresponde a cada entidad financiera determinar la forma en cómo llevará a cabo la supervisión de transacciones, aplicando los criterios internos que haya definido y actuando conforme a las disposiciones emitidas por el ente regulador. Por lo que, cada entidad financiera tiene libertad para establecer sus propios criterios sobre qué considera un comportamiento normal de consumo.

El patrón de consumo o comportamiento habitual del cliente se encuentra ligado directamente con el deber de idoneidad y el principio de buena fe contractual. En cuanto se trata de un mecanismo que permite a las entidades financieras a garantizar un servicio confiable y protegido frente a riesgos.

En ese sentido, el deber de idoneidad regulados en los artículos 18 y 19 del Código, se materializa al asegurar que el servicio de pago con tarjetas funcione bajo estándares que protege los intereses de los consumidores. Mientras que la buena fe contractual se encuentra ligada en cuanto exige que tanto el cliente como la entidad financiera actúen de manera diligente, transparente y leal o de buena fe durante toda la relación contractual. Por lo que la buena fe orienta el comportamiento ético y diligente de las partes; mientras que el patrón de consumo es un instrumento que permite materializar dicha obligación.

2.2. Aplicación práctica en la Jurisprudencia de Indecopi: Casos BBVA, Caja Trujillo e Interbank

En el desarrollo jurisprudencial de Indecopi, el concepto de patrón de consumo ha sido objeto de una evolución interpretativa significativa en los últimos años. A través de diversas resoluciones, la autoridad administrativa ha ido delimitando los parámetros para identificar cuando una operación debe ser considerada inusual y por tanto correspondería atribuir responsabilidad a las entidades financieras por infracción al deber de idoneidad.

a) Caso Carlos Calle vs BBVA (Resolución 077-2023/SPC-INDECOPI)

En el caso del señor Carlos Calle vs. BBVA, la Sala Especializada en Protección al consumidor adoptó un criterio técnico y restrictivo, en el cual se priorizaba la existencia de un historial previo para determinar el comportamiento habitual del cliente.

En dicho pronunciamiento, se consideró que no era exigible al banco activar alertas ante la primera operación cuestionada, en cuanto aún no se contaba con información suficiente que permitiera definir el patrón de consumo del usuario. La Sala sostuvo que el deber de monitoreo solo se activa una vez que el proveedor cuenta con un conjunto de operaciones que permitan establecer parámetros objetivos de comparación. Por lo que, este criterio implicó que la responsabilidad del banco se limitara a las operaciones posteriores, es decir, a aquellas que ya podían contrastarse con un comportamiento histórico.

En ese sentido, el enfoque que se brindó a través de esta resolución es que se otorgó amplia discrecionalidad a las entidades financieras para determinar conforme a su sistema interno de gestión de riesgos, cuando una transacción debía ser considerada atípica.

b) Caso MHAC Construction S.A.C. vs Caja Trujillo (Resolución 1641-2023/SPC-INDECOPI)

Posteriormente, en el caso MHAC Construction S.A.C. vs Caja Trujillo, la Sala reafirmó esta línea interpretativa, consolidando el enfoque técnico iniciado en el caso BBVA. En dicho pronunciamiento, se determinó que la operación impugnada- por un monto de S/30,116.50 soles – no resultaba inusual, ya que se encontraba dentro de los valores de consumo previamente registrados por el cliente (siendo la operación mayor anterior de S/ 50,000.00 soles). Asimismo, la entidad había implementado correctamente las medidas de autenticación, mediante el uso de HomeBanking y token de seguridad, lo que evidenciaba el cumplimiento del artículo 17 del Reglamento de Tarjetas de crédito y débito.

En el caso en cuestión, Indecopi precisó que el uso de un canal distinto o una nueva plataforma digital no basta por si solo para calificar una operación como irregular, siempre que el monto se mantenga dentro del rango de consumo histórico. Por lo que, no correspondía sancionar a la Caja Trujillo, al haberse verificado que las transacciones se encontraban dentro de un patrón económico razonable.

De esta manera, este segundo caso confirma la tendencia hacia un modelo de evaluación objetivo y cuantitativo del patrón de consumo, en donde el monto individual constituye el principal parámetro de análisis, mientras que la frecuencia, canal y lugar de ejecución se valoran de manera complementaria.

c) Caso Medina vs Interbank (Resolución 2293-2024/SPC-INDECOPI)

No obstante, en el caso Medina Vs. Interbank, la autoridad corrige parcialmente el enfoque anterior, adoptando una posición más estricta y acorde con la finalidad protectora del artículo 18 del Código de protección y defensa del consumidor. Es así que, en esta resolución, la Sala observó que la primera operación

controvertida por el monto de S/ 4,994.50 soles superaba ampliamente la mayor transacción previa registrada (S/ 35.90 soles). En consecuencia, dicha operación debió ser identificada como inusual desde el primer momento, activando los mecanismos de seguridad y monitoreo previstos en el artículo 17 del Reglamento de Tarjetas de crédito y débito.

La omisión de parte del banco en actuar ante esa primera operación generó responsabilidad administrativa, pues permitió que se realizaran posteriormente seis operaciones adicionales fraudulentas. A diferencia del criterio sostenido en el caso BBVA, Indecopi consideró que la obligación de detección no depende exclusivamente de la existencia de un patrón consolidado, sino que surge desde el inicio de la relación contractual en la medida que el proveedor ya cuenta con información mínima sobre el comportamiento del cliente.

Ahora bien, el contraste entre estas resoluciones permite identificar tres criterios recurrentes de valoración utilizados por Indecopi al aplicar el concepto de patrón de consumo:

(i) Frecuencia y monto de las operaciones que determinan sin existe una variación relevante frente al comportamiento previo del consumidor.
(ii) Lugar y medio de ejecución, considerando si las transacciones se realizaron en canales o ubicaciones inusuales (cajeros, POS o plataformas digitales).
(iii) Historial de consumo del cliente, entendiéndose como el conjunto de operaciones que reflejan su conducta económica habitual.

Sin embargo, la ponderación de estos elementos ha variado. Pues, mientras que en casos como el de BBVA y Caja Trujillo se privilegia el monto individual como parámetro principal, en el caso de Interbank se recupera una visión más integral que atiende tanto al valor económico como al entorno y la frecuencia de las operaciones.

2.3. Problemas detectados en la aplicación del criterio

De la revisión de la jurisprudencia reciente de INDECOPI, se constata que el patrón de consumo se ha consolidado como un criterio útil para determinar la

idoneidad en los servicios financieros. No obstante, en la práctica presenta una serie de inconsistencias que generan falta de predictibilidad en las decisiones y la efectividad de la tutela del consumidor.

En ese sentido, dentro de los principales problemas detectados se encuentran la falta de uniformidad con respecto a los criterios de valoración, la falta de parámetros técnicos verificables y las dificultades probatorias que enfrentan los consumidores derivados de interpretaciones dispares.

Sobre la falta de uniformidad con respecto a los criterios de valoración:

Como se puede apreciar de lo señalado en el numeral 2.2 uno de los principales problemas identificados es la falta de uniformidad en los criterios de evaluación de patrón de consumo en las diferentes resoluciones emitidas por la Sala de Protección al Consumidor.

Como se ha explicado, por ejemplo, en la Resolución N° 077-2023/SPC-INDECOPI, en este caso la autoridad consideró que el deber de monitoreo solo se activaba cuando existía un registro previo suficiente para definir el comportamiento del cliente. No obstante, en casos como la Resolución 2293-2024/SPC-INDECOPI, se determinó que la responsabilidad del proveedor podía configurarse incluso ante la primera operación irregular, si esta era claramente inusual frente al historial conocido. Estas variaciones evidencian que no existe un estándar jurisprudencial uniforme respecto del momento en que se activa el deber de detección de operaciones inusuales. Pues, como se puede apreciar en algunas oportunidades se tiene un enfoque técnico-gradual y en otras un enfoque protector y preventivo.

Sobre la ausencia de parámetros técnicos o indicadores cuantificables:

Otro de los principales problemas detectados en la aplicación del criterio es la ausencia de parámetros técnicos o normativa que permita establecer de manera objetiva cuando una operación debe ser considerada fuera del patrón habitual de un usuario financiero.

En ese sentido, ni el Código ni el Reglamento de Tarjetas de crédito y débito contemplan indicadores uniformes que puedan delimitar la variabilidad entre los consumos regulares y las operaciones atípicas. Pues, como ha señalado Pareja

“el citado estándar se elabora a partir de la configuración particular de cada empresa” (2022, p.2). En ese sentido, el concepto de comportamiento habitual de un usuario queda formulado de manera general, teniendo cada entidad financiera una interpretación y capacidad tecnológica particular.

Como consecuencia de esta falta de estandarización normativa es que se genera una heterogeneidad en los sistemas de monitoreo por parte de las instituciones financieras. Por lo que cada proveedor financiero crea sus propios algoritmos o modelos predictivos basados en el monto, la frecuencia, el canal, etc. Sin embargo, no hay un modelo o lineamiento que permita evaluar su eficacia o compararlos entre entidades.

Este vacío en la regulación financiera peruana genera una desprotección para los consumidores que nos obliga a reflexionar en qué medidas se podrían adoptar que contengan parámetros técnicos reforzados para armonizar la gestión del riesgo operativo en todo el sistema.

SECCIÓN 3: COMPARACIÓN DE LA NORMATIVA PERUANA CON LOS ESTÁNDARES INTERNACIONALES EN MATERIA DE SEGURIDAD FINANCIERA

La tercera sección de este trabajo, titulada “Comparación de la normativa peruana con los estándares internacionales en materia de seguridad financiera”, tiene como objetivo específico comparar el marco el marco regulatorio peruano sobre operaciones no reconocidas con los estándares internacionales en seguridad financiera, a fin de identificar las buenas practicas que podrían complementar y fortalecer la regulación nacional.

Para alcanzar dicho objetivo, se plantea como problema específico la siguiente interrogante: ¿Qué estándares internacionales podrían complementar la regulación peruana en esta materia?

Como hipótesis de esta sección planteamos que las normas internacionales sobre seguridad financiera, como las de Chile, Colombia y España, tienen reglas más claras, una mejor supervisión y una distribución más equilibrada con respecto a las responsabilidades. Esto hace que en esos países la protección al consumidor sobre operaciones no reconocidas sea más efectiva.

En ese sentido, la sección se estructura en tres subcapítulos. El subcapítulo 3.1 analiza a Perú y a Chile, en donde el modelo chileno limita la responsabilidad del usuario y, al mismo tiempo, obliga a que las entidades financieras cuenten con sistemas que detecten y controlen operaciones inusuales.

El subcapítulo 3.2. analiza a Perú y a Colombia, en donde se evidencia la importancia de una institucionalidad sólida. Mientras que en el subcapítulo 3.3 se examina a Perú y a España, en donde la autenticación reforzada y la corresponsabilidad del proveedor son pilares en la seguridad financiera.

Con la sección 3 se pretende demostrar que el Perú si bien ha avanzado con medidas para fortalecer la seguridad financiera, aún existen brechas sobre coordinación institucional, educación del consumidor, así como la estandarización técnica.

3.1. Perú y Chile: responsabilidad y prevención tecnológica

En Chile se cuenta con la Ley N° 21.234 (2020), la cual muestra un avance significativo sobre protección en operaciones no reconocidas en Latinoamérica. Además, esta norma reformó la Ley N° 20.009 la cual limita la responsabilidad del usuario de tarjetas o de medios denominados electrónicos en caso de hurto o robo o fraude, siempre y cuando se notifique oportunamente al banco.

De acuerdo con Cordero y Contardo (2020), la ley consolidó la doctrina judicial previa en Chile, que ya atribuía el riesgo del fraude al emisor o prestador del servicio financiero, pues atribuía el riesgo del fraude al emisor o prestador del servicio financiero, sobre la base de que el control operativo del riesgo recae en dichas entidades y no en el consumidor.

Así en el nuevo marco se profundizó la distribución del riesgo a favor del usuario y se estableció que las operaciones fraudulentas por montos iguales o inferiores a 35 UF deben ser asumidas íntegramente por el proveedor, sin posibilidad de oposición inmediata. En ese sentido, esta nueva regulación introdujo umbrales claros de responsabilidad y plazos definidos, pues el emisor debe cancelar los cargos o restituir los fondos en un plazo máximo de cinco días hábiles tras el

reclamo o siete en caso el monto supere las 35 UIF. Además, que en tales casos la entidad solo puede imputar responsabilidad al cliente si acredita que actuó con dolo o culpa grave, lo que implica una inversión de la carga probatoria y una obligación reforzada de demostrar diligencia por parte del proveedor financiero.

No obstante, los autores advierten que el nuevo marco deja abiertas interrogantes de técnica legislativa y de aplicación práctica, entre ellas, la definición de "culpa grave" del usuario, la compatibilidad de los plazos con la ley del consumidor y el impacto en la instantaneidad de las transferencias electrónicas. Además, la Ley N° 21.234 prohíbe a los bancos ofrecer seguros para cubrir riesgos que la propia ley impone al emisor, en ese sentido, se evita una sobreprotección contractual.

Comparativamente, el Perú ha avanzado en una línea similar con la reciente modificación del Reglamento de Tarjetas de Crédito y Débito de la SBS, vigente desde julio de 2025, que traslada la carga de la prueba a las entidades financieras y las obliga a asumir la perdida en caso de operaciones no reconocidas si es que no demuestran la responsabilidad del cliente. No obstante, a diferencia de Chile, la regulación peruana aún carece de umbrales cuantificables de riesgo, limites objetivos de responsabilidad y plazos procesales claros para la restitución de fondos, aspectos que otorgan a Chile una mayor certeza operativa.

Por ejemplo, en Chile con la nueva Ley se prohíbe a los emisores ofrecer seguros contra riesgos que la ley ya les obliga a asumir (como extravío, robo o fraude), evitando que pague por una cobertura ficticia. En cambio, en Perú no existe una disposición equivalente. Las entidades financieras sí pueden ofrecer seguros contra fraude electrónico, incluso por operaciones que, bajo la nueva regulación, deberían estar cubiertas por la responsabilidad del proveedor. Esto puede generar una carga económica innecesaria y adicional para los consumidores.

Por otro lado, a diferencia del modelo chileno que exige a las entidades financieras adoptar sistemas que permitan monitoreo y gestión de alertas conforme a "*las mejores prácticas de la industria"* y bajo la supervisión del órgano fiscalizaros, el marco peruano, si bien lo recoge en el artículo 17 del Reglamento

de Tarjetas de Crédito y Débito, con obligaciones análogas de detección de operaciones inusuales, gestión de alertas e identificación de patrones de fraude, aún mantiene un esquema de aplicación más flexible y autorregulado. Pues, en la norma peruana no se hace referencia expresa a estándares técnicos uniformes ni a metodologías validadas por las autoridades, limitándose a requerir el análisis histórico de operaciones. En ese sentido, se tiene como resultado que cada entidad financiera conserva autonomía para definir sus algoritmos y umbrales de riesgo, sin que exista un mecanismo de auditoria externa.

En consecuencia, mientras el modelo chileno persigue uniformidad y un control técnico, en el marco peruano se privilegia la autonomía tecnológica, que genera niveles variables de diligencia y a la vez dificulta la supervisión integral por parte de la SBS e Indecopi.

3.2. Perú y Colombia: institucionalidad y educación financiera

En materia de protección al consumidor financiero, el modelo colombiano tiene la Ley N° 1328 de 2009 que creó el Sistema de Atención al Consumidor Financiero (SAC), que establece mecanismos para la prevención, atención y resolución de controversias entre usuarios y entidades financieras. Asimismo, dentro del marco, se institucionalizó la figura de la Defensoría del Consumidor Financiero (DCF), el cual es un órgano independiente designado por cada entidad vigilada, encargado de tramitar los reclamos y formular recomendaciones ante la Superintendencia Financiera de Colombia.

En ese sentido, el sistema colombiano combina tres dimensiones: (i) la atención directa de reclamos mediante el DCF, (ii) la supervisión estatal por la Superintencia Financiera, y (iii) la educación financiera como prevención.

Ahora bien, aunque las decisiones del Defensor no son jurídicamente vinculantes, su existencia es obligatoria para todas las entidades supervisadas. Este diseño otorga al DCF legitimidad institucional y coherencia dentro de un sistema legal integrado (Superintendencia Financiera de Colombia, 2023).

No obstante, en Perú se carece de un marco similar, pues la SBS y el Indecopi cumplen funciones de protección y supervisión. Además, la reciente Defensoría

del Cliente Financiero, relanzada por iniciativa del propio sistema financiero, representa un esfuerzo positivo hacia la especialización, pero carece de reconocimiento legal formal eso limita su capacidad de supervisión y seguimiento.

Según la Defensoría del Cliente Financiero (2022), este servicio especializado actúa como una instancia gratuita y de segunda instancia para los usuarios que no han logrado resolver sus reclamos. No obstante, su naturaleza es opcional y autorregulada, lo que impide consolidarla como política uniforme a diferencia del esquema colombiano que articula prevención y supervisión bajo un marco jurídico único.

3.3. Perú y España: autenticación reforzada y corresponsabilidad:

Tanto España como Perú han avanzado en la implementación de mecanismos de autenticación reforzada en los servicios financieros, aunque con distintos niveles de madurez regulatoria, supervisión y uniformidad técnica. Si bien en ambos casos el objetivo es fortalecer la seguridad de las operaciones electrónicas, reducir los fraudes y consolidar la confianza de los usuarios financieros.

En España, el Real Decreto-Ley N° 19/2018, que transpone la Directiva (UE) 2015/2366 (PSD2), introdujo la autenticación reforzada del cliente (Strong Customer Authentication) como requisito obligatorio para toda operación que implique acceso a cuentas, pagos electrónicos o acciones con algún tipo de riesgo de fraude. Este sistema exige el uso de al menos dos factores de autenticación de distinta naturaleza: (i) conocimiento (algo que el usuario sabe, como un PIN o contraseña), (ii) posesión (algo que el usuario tiene, como un token o dispositivo) y (iii) inherencia (algo que el usuario es, como la biometría)[1].

Su supervisión está centralizada en el Banco de España y la European Banking Authority (EBA), que mediante el Reglamento Delegado (UE) 2018/389 establecen estándares técnicos homogéneos y auditorias periódicas para verificar la eficacia de los mecanismos aplicados. En ese sentido, en el caso de

[1] **España.** (2018, 23 de noviembre). *Real Decreto-ley 19/2018, de servicios de pago y otras medidas urgentes en materia financiera*. *Boletín Oficial del Estado*, núm. 284, 24 de noviembre de 2018.

operaciones no reconocidas, solo puede eximirse el proveedor si es que demuestra que aplicó correctamente la autenticación reforzada, aquello configura un régimen de corresponsabilidad técnica y jurídica.

Ahora bien, en Perú se cuenta con la Superintendencia de Banca, Seguros y AFP (SBS), la cual ha venido reforzando su marco regulatorio a través del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad (Resolución SBS N° 504-2021) y más recientemente, la Resolución SBS N° 2286-2024, vigente desde el 1 de julio de 2025. Esta norma precisa los factores válidos de autenticación reforzada y alinea la regulación peruana con las prácticas internacionales, incorporando estándares como el EMV 3D Secure (verificación robusta de identidad en línea) y la EMV Tokenization, la cual reemplaza el número real de la tarjeta por un identificador único o token en operaciones de comercio electrónico.

Por lo que, el esquema peruano exige: (i) para transacciones con tarjeta presente, el uso del chip o su representación digital y un PIN como segundo factor, (ii) para operaciones sin tarjeta presente (en línea), los datos de la tarjeta y un código de verificación dinámico o factor verificable en línea, (iii) para billeteras móviles (como Apple pay o Google pay), la autenticación inicial se realiza con los factores anteriores y las operaciones posteriores mediante tokenización y un segundo factor adicional.

Cabe resaltar que la Resolución SBS N° 02220-2025 extendió el plazo hasta el 1 de abril de 2026 para que todas las entidades financieras cumplan con terminar de implementar estos mecanismos. Luego de dicha fecha, las entidades asumirán responsabilidad por la falta de aplicación del segundo factor, salvo prueba de dolo o negligencia del usuario[2].

En ese sentido, a diferencia del modelo español, el marco peruano aún carece de una autoridad técnica supranacional que supervise la interoperabilidad o emita parámetros uniformes de auditoria. Si bien la SBS ha alineado la normativa a estándares internacionales, su fiscalización sigue siendo interna y progresiva,

[2] **Superintendencia de Banca, Seguros y AFP (SBS).** (2025, julio). *SBS Informa N.º 24 – Autenticación reforzada: medidas de seguridad para proteger las operaciones financieras*. Superintendencia de Banca, Seguros y AFP del Perú.

lo que deja margen para la autorregulación tecnológica de las entidades. Lo que evidencia la necesidad de que el marco peruano evolucione hacia un modelo de corresponsabilidad integral, donde la autenticación reforzada se vincule directamente con el deber de idoneidad y la trazabilidad de la responsabilidad en el entorno financiero digital.

SECCIÓN 4: PROPUESTA DE FORTALECIMIENTO NORMATIVO Y TÉCNICO EN EL PERÚ FRENTE A OPERACIONES NO RECONOCIDAS

La cuarta sección titulada “Propuesta de fortalecimiento normativo y técnico en el Perú frente a operaciones no reconocidas”, tiene como objetivo formular propuestas de mejora orientadas a reforzar la protección del consumidor financiero a partir del análisis comparado desarrollado en la sección anterior.

El problema central que guía este apartado busca responder a la siguiente pregunta: ¿Cómo puede el marco normativo peruano incorporar estándares internacionales de seguridad financiera y responsabilidad compartida, garantizando la eficacia de la autenticación reforzada y la gestión preventiva del fraude?

La hipótesis planteada sostiene que la adopción de un modelo mixto, que combine la responsabilidad proactiva del proveedor (como en Chile), la institucionalidad especializada (como en Colombia) y la autenticación reforzada bajo supervisión técnica (como en España), lograrían mejorar la respuesta del sistema financiero peruano frente a operaciones no reconocidas y fortalecer la confianza del usuario financiero.

Esta sección se estructura en dos subcapítulos. El subcapítulo 4.1 presenta la justificación de la propuesta, identificando las principales brechas normativas y operativas del marco peruano actual. Mientras que el subcapítulo 4.2 presenta las propuestas concretas derivadas del análisis comparado.

De esta manera, la sección 4 busca cerrar el análisis con una propuesta integral y viable, que le permita al ordenamiento peruano avanzar hacia un modelo de protección financiera más efectiva en concordancia con los estándares

internacionales y el deber de idoneidad previsto en nuestro Código de Protección y Defensa del Consumidor.

4.1. Justificación de la reforma: limitaciones del modelo peruano actual

Acorde a lo desarrollado a lo largo del trabajo se puede constatar que el modelo peruano de protección frente a operaciones no reconocidas aun presenta vacíos en el plano normativo como en lo técnico.

En primer lugar, hay una carencia de uniformidad y objetividad con respecto a la aplicación del criterio del patrón de consumo. Si bien es un instrumento valioso para detectar operaciones inusuales, la falta de parámetros técnicos como son los márgenes de variación o niveles de riesgo, deja su evaluación a la discrecionalidad de cada entidad financiera. Esta situación puede conllevar a producir resultados dispares y dificultad a la hora de ser supervisados por la SBS e Indecopi.

En segundo lugar, si bien el Reglamento para la gestión de la seguridad de la información y la ciberseguridad (Resolución SBS N° 504-2021), ha introducido la autenticación reforzada, en la práctica aún se encuentra en una etapa inicial. Pues, la falta de una autoridad técnica que evalué la eficacia de los mecanismos de autenticación o que establezca estándares comunes limita el impacto real de esta herramienta.

Asimismo, la actual arquitectura institucional peruana es fragmentada. La SBS, el Indecopi y la Defensoría del Cliente Financiero actúan de manera complementaria, pero sin una coordinación estructural. A diferencia del modelo colombiano, donde el DCF se integra dentro del marco de la Superintendencia Financiera con facultades vinculantes; en cambio, en Perú opera como un mecanismo de resolución alterna sin capacidad sancionadora ni supervisora.

Por último, se observa que el enfoque actual sigue siendo principalmente reactivo, es decir, se actúa después de que ocurre el fraude, en lugar de enfocarse en prevenirlo o educar al usuario para evitarlo. Esto limita el verdadero alcance del deber de idoneidad, que no solo debería implicar corregir errores o

responder ante reclamos, sino también anticiparse a los riesgos mediante sistemas tecnológicos seguros y programas de educación financiera.

En conjunto, estos aspectos muestran la necesidad de avanzar hacia un modelo más coordinado y uniforme donde las entidades financieras, la SBS y el Indecopi trabajen bajo reglas claras, controles más eficaces y responsabilidades compartidas, que permita una protección real y preventiva al consumidor financiero.

4.2. Propuesta de reforma

La propuesta que se plantea busca que el deber de idoneidad en los servicios financieros vaya más allá de la simple obligación de ofrecer un servicio sin fallas. Se trata de que las entidades financieras asuman un compromiso activo de prevención del riesgo, especialmente frente a fraudes y fallas tecnológicas. Para lograrlo, se proponen tres líneas principales de reforma:

a) Fortalecimiento normativo y regulatorio

En primer lugar, se propone definir de manera uniforme lo que debe entenderse por “operación fuera del patrón de consumo”, incorporando en el Reglamento de Tarjetas de Crédito y Débito una descripción técnica que considere factores como la frecuencia, monto, ubicación y canal de uso de las transacciones. Actualmente, aunque la SBS y las resoluciones de Indecopi ya reconocen estos criterios como en los casos expuestos en el presente informe, no existe una definición estandarizada ni parámetros cuantitativos mínimos que orienten a las entidades. Lo cual genera diferencias en la forma en que cada banco detecta comportamientos inusuales.

Asimismo, sería recomendable que la SBS establezca auditorías externas obligatorias sobre los sistemas de monitoreo de fraude y autenticación, siguiendo modelos como el español, donde las entidades deben reportar sus controles de ciberseguridad ante la autoridad supervisora.

b) Innovación tecnológica y responsabilidad compartida

Se plantea que el uso de autenticación reforzada sea obligatorio en todas las operaciones que puedan presentar algún riesgo, aplicándose en todo el sistema financiero. Esto aseguraría que toda transacción requiera al menos dos factores de autenticación, reduciendo la posibilidad de fraude.

Además, podría implementarse una plataforma nacional de monitoreo de fraudes, administrada conjuntamente por la SBS e Indecopi, que concentre las alertas y facilite la detección temprana de patrones sospechosos a nivel de sistema.

También, se podrían adoptar estándares internacionales de monitoreo, similares a las “prácticas de la industria” aplicadas en Chile, para garantizar un nivel técnico mínimo y homogéneo en todo el sector.

c) Educación financiera y prevención del fraude

Finalmente, se propone que la SBS y la DCF lideren un Plan Nacional de Educación Financiera y Ciberseguridad, orientada a capacitar a los usuarios sobre el uso seguro de canales digitales y los riesgos de fraude electrónico. Asimismo, se podrían crear incentivos regulatorios para las entidades que desarrollen campañas de educación o que incorporen tecnologías avanzadas de verificación, como la biometría o sistemas de detección de patrones en tiempo real.

CONCLUSIONES Y/O RECOMENDACIONES

- Si bien la normativa peruana busca proteger a los consumidores, al trasladar la carga de la prueba a los proveedores y al establecer requisitos de seguridad sobre operaciones con tarjetas o las denominadas billeteras digitales. En la práctica, su eficacia depende de que las entidades financieras cuenten con sistemas tecnológicos avanzados, que les permita actualizar los procesos de autenticación y puedan realizar un constante monitoreo en caso de fraudes u operaciones no reconocidas. Además, lo sucedido en el caso Interbank refuerza nuestra teoría de que aún no contamos con solidas auditorias de ciberseguridad.
- El análisis de la jurisprudencia de Indecopi demuestra que, si bien el criterio del patrón de consumo constituye una herramienta valiosa para evaluar la idoneidad del servicio financiero frente a operaciones no reconocidas, en la práctica se evidencian notorias inconsistencias. Las resoluciones analizadas (BBVA, Caja Trujillo e Interbank) reflejan la coexistencia de enfoques distintos: uno técnico y restrictivo, que supedita la detección de operaciones inusuales a la existencia de un historial consolidado, y otro más protector, que activa el deber de vigilancia desde la primera transacción irregular. En ese sentido, la falta de uniformidad en la interpretación, sumada a la ausencia de parámetros técnicos objetivos y verificables, genera inseguridad jurídica tanto para los consumidores.
- El análisis comparativo muestra que, aunque el Perú ha dado pasos importantes para fortalecer la seguridad financiera, su regulación todavía presenta vacíos frente a modelos internacionales más avanzados. En Chile, la ley distribuye de forma clara la responsabilidad frente al fraude y obliga a los bancos a contar con sistemas de monitoreo que detecten operaciones fuera del comportamiento habitual. Esto permite una respuesta más rápida ante posibles fraudes. En Colombia, la protección al consumidor financiero es más completa porque existe una coordinación institucional clara entre la Superintendencia Financiera y la DCF. Este sistema no solo resuelve reclamos, sino que promueve la educación financiera. Finalmente, en el caso de España se evidencia un modelo consolidado, en el que la autenticación reforzada del cliente es obligatoria y supervisada por una autoridad técnica. En el Perú, aunque se han

implementado normas para implementar este sistema, su aplicación aun es gradual y no tiene una supervisión tan estricta.

- En síntesis, el sistema peruano aún enfrenta limitaciones importantes en la protección frente a operaciones no reconocidas, principalmente por su enfoque reactivo y la falta de uniformidad técnica entre las entidades financieras. Si bien la normativa ha incorporado avances como la autenticación reforzada y el uso del patrón de consumo, su aplicación sigue siendo desigual y carece de una supervisión centralizada. Por ello, resulta necesario fortalecer el marco normativo mediante estándares claros y verificables. De igual forma, la educación financiera y la corresponsabilidad del usuario deben consolidarse como componentes esenciales del deber de idoneidad.
- En conjunto, las conclusiones parciales expuestas demuestran que el criterio del patrón del consumo de Indecopi, tal como es aplicado actualmente, no garantiza plenamente la protección al consumidor financiero frente al fraude electrónico. Si bien es útil, su eficacia depende de que existan estándares tecnológicos homogéneos, una regulación clara y preventiva, así como una supervisión técnica y sólida.

BIBLIOGRAFÍA

Ccoyllo Sánchez, Alonso Sebastián. "La regulación del phishing en el sistema financiero peruano." *Boletín Jurídico Sociedades*, 3 de enero de 2025, https://boletinsociedades.com/2025/01/03/la-regulacion-del-phishing-en-el-sistema-financiero-peruano/

Cordero, L., & Contardo, J. I. (2020, 26 de agosto). *Regulación de los riesgos del fraude bancario: algunas interrogantes que deja la nueva Ley Nº 21.234*. El Mercurio. Recuperado de https://www.elmercurio.com/legal/movil/detalle.aspx?Id=908882&Path=/0D/DE/

Defensoría del Cliente Financiero. (2022, 22 de agosto). *Defensoría del cliente financiero: un servicio gratuito para atender reclamos con entidades financieras*. Banca para Todos. Recuperado de https://www.asbanc.com.pe/noticia/defensoria-del-cliente-financiero-un-servicio-gratuito-para-atender-reclamos-con-entidades-financieras

Durand, J. B., & Flores Flores, P. (2024). *Derecho del consumidor*. Lima: Editorial LP S.A.C.

García Salirrosas, R., & Bendezú Delgadillo, K. J. (2024). *Tokens digitales: herramienta de autenticación y seguridad en entornos virtuales* [Trabajo de suficiencia profesional, Universidad Peruana de Ciencias Aplicadas]. Lima, Perú. Recuperado de: https://upc.aws.openrepository.com/bitstream/handle/10757/674105/Garc%c3%ada_SR.pdf?sequence=15&isAllowed=y

Huaroto Gutierrez, K. (2023). *La inaplicación del Principio de Confianza Legítima del Indecopi en las resoluciones de productos alimentarios envasados* (Trabajo académico de segunda especialidad). Pontificia Universidad Católica del Perú, Lima, Perú. Recuperado de: https://tesis.pucp.edu.pe/server/api/core/bitstreams/f6df492b-5f6e-444f-8a24-b1e3fbd6c6fb/content

LEX. (2021, 29 de noviembre). ¿Las medidas de seguridad forman parte del deber de idoneidad en la prestación de servicios financieros? Pasión por el

Derecho. https://lpderecho.pe/medidas-seguridad-deber-idoneidad-prestacionservicios-financieros/

Pareja Palomino, J. (2022). *Algunas críticas a las medidas de seguridad en materia de patrón de consumo en el empleo de tarjetas de pago.* (Trabajo académico de segunda especialidad). Pontificia Universidad Católica del Perú, Lima, Perú. Recuperado de: https://tesis.pucp.edu.pe/server/api/core/bitstreams/d0b1865e-0168-4f86-93c1-59ccd2f3f40c/content

Redacción EC. (2024, 31 de diciembre). *El caso Interbank y otros 6 incidentes de ciberseguridad que marcaron el 2024 en Latinoamérica*. *El Comercio*. https://elcomercio.pe/tecnologia/actualidad/el-caso-interbank-y-otros-6-incidentes-de-ciberseguridad-que-marcaron-el-2024-en-latinoamerica-noticia/

Silvestre Bermúdez, J. K. (2021). *La aplicación de medidas de seguridad para casos de operaciones inusuales en tarjetas de crédito y débito en materia de protección al consumidor* (Trabajo académico de segunda especialidad). Pontificia Universidad Católica del Perú, Lima, Perú. Recuperado de: https://tesis.pucp.edu.pe/server/api/core/bitstreams/7c15d711-4a63-44b5-8274-0d6683307a3d/content

Superintendencia de Banca, Seguros y AFP (30 de octubre de 2013). Resolución SBS N° 6523-2013. Reglamento de Tarjetas de Crédito y Débito. Recuperado de: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1089323

Superintendencia de Banca, Seguros y AFP. (28 de junio de 2024). Resolución SBS N.° 02286-2024. Modifican el Reglamento de Tarjetas de Crédito y Débito, el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, el Reglamento de Gestión de Conducta de Mercado del Sistema Financiero y el Reglamento de Reclamos y Requerimientos. Recuperado de: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1379642

Superintendencia Financiera de Colombia. (2013). *Apuntes sobre Derecho del Consumidor Financiero*. Bogotá, Colombia: SFC.

Superintendencia Financiera de Colombia (2023). *Guía del Defensor del Consumidor Financiero y del Sistema de Atención al Consumidor Financiero (SAC)*. Bogotá: SFC.

Velazco Velazco, N. C. (2024). *¿Me devolverán mi dinero?: Análisis del marco normativo en protección al consumidor del comercio electrónico en el Perú* (Trabajo académico de segunda especialidad). Pontificia Universidad Católica del Perú, Lima, Perú. Recuperado de: https://tesis.pucp.edu.pe/server/api/core/bitstreams/2b2e8748-14ba-4db4-8beb-0ca7fe86d45d/content