UNIVERSIDAD NACIONAL DEL ALTIPLANO

ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO

TESIS

LA FALTA DE PREDICTIBILIDAD DE LOS PRONUNCIAMIENTOS DEL INDECOPI EN MATERIA DE OPERACIONES FRAUDULENTAS EFECTUADAS POR INTERNET

PRESENTADA POR:

RAISA VEROSCA LIMACHE FRISANCHO

PARA OPTAR EL GRADO ACADÉMICO DE:

MAESTRO EN DERECHO
CON MENCIÓN EN: DERECHO ADMINISTRATIVO Y GERENCIA PÚBLICA

PUNO, PERÚ

2024

RAISA VEROSCA LIMACHE FRISANCHO

LA FALTA DE PREDICTIBILIDAD DE LOS PRONUNCIAMIENTOS DEL INDECOPI EN MATERIA DE OPER...

My Files
My Files
Universidad Nacional del Altiplano

Detalles del documento

Identificador de la entrega
trn:oid:::8254:417194842

Fecha de entrega
18 dic 2024, 9:36 a.m. GMT-5

Fecha de descarga
18 dic 2024, 9:52 a.m. GMT-5

Nombre de archivo
LA FALTA DE PREDICTIBILIDAD DE LOS PRONUNCIAMIENTOS DEL INDECOPI EN MATERIA DE OP....docx

Tamaño de archivo
862.0 KB

171 Páginas

47,453 Palabras

266,299 Caracteres

UNIVERSIDAD NACIONAL DEL ALTIPLANO
ESCUELA DE POST GRADO
Dr.Sc. Wilder Ignacio Velazco
DOCENTE

8% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 12 palabras)

Fuentes principales

6%	Fuentes de Internet
1%	Publicaciones
6%	Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.° de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

UNIVERSIDAD NACIONAL DEL ALTIPLANO
ESCUELA DE POST GRADO
Dr.Sc. Wilder Ignacio Velazco
DOCENTE

UNIVERSIDAD NACIONAL DEL ALTIPLANO
ESCUELA DE POSGRADO
COORDINACIÓN DE INVESTIGACIÓN
PUNO-PERÚ
Ruben Jared Luque Coyla
ING. ESTADÍSTICO E INFORMÁTICO
CIP. 116625

turnitin Página 2 of 180 - Descripción general de integridad Identificador de la entrega trn:oid:::8254:417194842

UNIVERSIDAD NACIONAL DEL ALTIPLANO

ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO

TESIS

LA FALTA DE PREDICTIBILIDAD DE LOS PRONUNCIAMIENTOS DEL INDECOPI EN MATERIA DE OPERACIONES FRAUDULENTAS EFECTUADAS POR INTERNET

PRESENTADA POR:

RAISA VEROSCA LIMACHE FRISANCHO

PARA OPTAR EL GRADO ACADÉMICO DE:

MAESTRO EN DERECHO

CON MENCIÓN EN: DERECHO ADMINISTRATIVO Y GERENCIA PÚBLICA

APROBADA POR EL JURADO SIGUIENTE:

PRESIDENTE

.....
D.Sc. JOSE ASDRUBAL COYA PONCE

PRIMER MIEMBRO

.....
D.Sc. WALDYR WILFREDO ALARCON PORTUGAL

SEGUNDO MIEMBRO

.....
M.Sc. LIGIANCARLO JHONATAN MEDINA ALVAREZ

ASESOR DE TESIS

.....
D.Sc. WILDER IGNACIO VELAZCO

Puno, 17 de mayo de 2024.

ÁREA: Ciencias sociales.
TEMA: Estado, Empresa y Sociedad Civil.
LÍNEA: Derecho.

DEDICATORIA

A mi familia y amigos, por su cariño incondicional y apoyo constante.

Raisa Limache

AGRADECIMIENTOS

Mi agradecimiento profundo a los docentes de la Escuela de Posgrado de la Universidad Nacional del Altiplano, en especial a mi asesor, el doctor Wilder Ignacio Velasco, por los conocimientos impartidos y apoyo constante en la ejecución y redacción de la presente investigación.

Al Indecopi, por haber proporcionado con prontitud la información solicitada sobre los procedimientos que son materia de la presente investigación.

A mis colegas de la Oficina Regional del Indecopi de Tacna, por su apoyo en la búsqueda de bibliografía, por su comprensión e invaluable amistad.

A mis padres y hermano, por todo su amor, apoyo y confianza.

A mi tía, Carmen Frisancho, por su invaluable ayuda y apoyo en este proceso.

A D.M., por su apoyo incondicional y valiosas apreciaciones.

A Toulouse, por su entrañable compañía en las largas noches de desvelo.

Raisa Limache

ÍNDICE GENERAL

Pág.

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE ANEXOS

ACRÓNIMOS

CC1	:	Comisión de Protección al Consumidor n.° 1
CPC	:	Comisión de Protección al Consumidor
ORPS 2	:	Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor n.° 2
ORPS	:	Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor
SBS	:	Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones
SERNAC	:	Servicio Nacional del Consumidor
SFC	:	Superintendencia Financiera de Colombia
SPC	:	Sala Especializada en Protección al Consumidor del Tribunal del Indecopi
TUO	:	Texto Único Ordenado

RESUMEN

El auge del uso de internet para realizar operaciones bancarias ha traído consigo un aumento en la utilización de métodos fraudulentos que buscan obtener los fondos de los usuarios de servicios financieros. En este contexto, la presente investigación tuvo como objetivo analizar la problemática jurídica subyacente en la predictibilidad de los pronunciamientos del Indecopi emitidos a nivel nacional en materia de operaciones fraudulentas efectuadas por internet durante 2022 y 2023. Para ello, se determinó si los pronunciamientos del Indecopi son predictivos, y luego se comparó la legislación y la jurisprudencia peruana con las de España, Colombia y Chile, y consideró lecciones que podrían implementarse para mejorar la predictibilidad de los pronunciamientos. El enfoque de investigación es cualitativo, de tipo descriptivo, comparativo y aplicado, y las técnicas la observación documental y análisis de contenido. Los resultados demostraron que los pronunciamientos del Indecopi no son predictivos, al observarse criterios diferentes al evaluar la responsabilidad de la entidad financiera, dictar medidas correctivas e imponer sanciones. Se evidencia también que los pronunciamientos de otros países difieren a los del Indecopi, principalmente porque son resueltos en la vía judicial y las entidades financieras solo son exoneradas de responsabilidad si logran acreditar dolo, negligencia o fraude del consumidor. Se concluye que es necesario unificar criterios para mejorar la predictibilidad de las decisiones del Indecopi y se sugiere la adopción de un nuevo enfoque que se adapte al constante avance tecnológico y la creciente vulnerabilidad del usuario frente a situaciones de fraude.

Palabras clave: Fraude informático, medidas de seguridad y monitoreo, operaciones no reconocidas, órganos resolutivos del Indecopi, principio de predictibilidad, servicios bancarios y financieros

ABSTRACT

The rise in the use of the Internet to carry out banking transactions has brought with it an increase in the use of fraudulent methods that seek to obtain funds from users of financial services. In this context, the present investigation aimed to analyze the legal problem underlying the predictability of Indecopi's pronouncements issued nationwide regarding fraudulent operations carried out over the Internet during 2022 and 2023. To do so, it was determined whether Indecopi's pronouncements are predictive, and then Peruvian legislation and jurisprudence were compared with those of Spain, Colombia and Chile, and lessons that could be implemented to improve the predictability of the pronouncements were considered. The research approach is qualitative, descriptive, comparative and applied, and the techniques are documentary observation and content analysis. The results showed that Indecopi's pronouncements are not predictive, as different criteria are observed when evaluating the responsibility of the financial entity, dictating corrective measures and imposing sanctions. It is also evident that the pronouncements of other countries differ from those of Indecopi, mainly because they are resolved through judicial channels and financial institutions are only exonerated from liability if they manage to prove fraud, negligence or consumer fraud. It is concluded that it is necessary to unify criteria to improve the predictability of Indecopi's decisions and it is suggested that a new approach be adopted that adapts to the constant technological advance and the increasing vulnerability of the user in the face of fraud situations.

Keywords: Banking and financial services, computer fraud, Indecopi's resolution instances, predictability principle, security and monitoring measures, unrecognized transactions.

INTRODUCCIÓN

La presente investigación aborda la problemática de las operaciones bancarias no reconocidas efectuadas mediante internet, con un enfoque específico en la problemática subyacente de la predictibilidad de los pronunciamientos del Indecopi a nivel nacional durante los años 2022 y 2023. La elección del tema obedece al crecimiento exponencial del uso de internet para llevar a cabo operaciones bancarias y financieras, lo que ha generado la necesidad de comprender la posición del Indecopi frente a este fenómeno, al ser la entidad encargada de dirimir las controversias en fuero administrativo que se susciten en dicha materia. Dada la relevancia de este tema en el contexto actual, la investigación busca contribuir al conocimiento y protección de los derechos e intereses económicos de los consumidores y proveedores de servicios financieros, ya que la falta de predictibilidad en los pronunciamientos del Indecopi genera incertidumbre en los administrados sobre el resultado que obtendrán, afectando la confianza en el sistema y la seguridad jurídica. El área en la que se ubica esta investigación es la de las ciencias sociales, específicamente en el derecho administrativo. El propósito de la investigación es analizar la problemática jurídica subyacente en la predictibilidad de los pronunciamientos del Indecopi emitidos a nivel nacional en materia de operaciones fraudulentas realizadas a través de internet. Al respecto, se plantean objetivos específicos que incluyen determinar si los pronunciamientos emitidos por el Indecopi en primera y segunda instancia administrativa durante los años 2022 y 2023 son predictivos, para luego identificar las similitudes y diferencias que estos guardan con los pronunciamientos emitidos por instituciones de países como España, Colombia y Chile, a fin de extraer recomendaciones o lecciones que puedan implementarse para mejorar la predictibilidad de los criterios emitidos por el Indecopi. El enfoque de investigación elegido es el cualitativo y se enmarca en el tipo de investigación descriptiva, comparativa y aplicada. Se utiliza el método descriptivo para abordar la predictibilidad en los pronunciamientos del Indecopi y comparar los mismos con los de instituciones de España, Colombia y Chile. El método de recolección de datos es la observación directa, y se utilizan fichas de observación y de análisis de contenido como instrumentos para recopilar la información.

La investigación inicia con un análisis teórico sobre los tipos de fraude informático y el sistema financiero, destacando conceptos clave como los tipos de

operaciones, los instrumentos de pago y las medidas de seguridad que deben adoptar las entidades financieras. Posteriormente, se examina la legislación peruana vigente en relación con la responsabilidad de las entidades financieras y los derechos de los consumidores en casos de operaciones fraudulentas, para luego realizar una revisión sobre los procedimientos administrativos sancionadores tramitados por el Indecopi y definir el principio de predictibilidad. Seguidamente, se presentan los antecedentes de la investigación, tanto a nivel nacional como internacional, se plantean el problema y los objetivos, así como los métodos de investigación utilizados. Luego, se efectúa el análisis de resultados y la discusión, el cual se divide en tres partes: la primera, aborda el análisis de la jurisprudencia sobre operaciones bancarias no reconocidas emitida por el Indecopi, examinándose casos específicos y evaluando la predictibilidad de las resoluciones; la segunda parte, se centra en la comparación de la legislación y jurisprudencia emitida por instituciones de Chile, Colombia y España con los pronunciamientos del Indecopi y la legislación peruana; y la tercera parte, establece las lecciones o recomendaciones que pueden implementarse para mejorar la predictibilidad de los criterios emitidos por el Indecopi. Finalmente, exponemos las conclusiones y recomendaciones obtenidas con base en el contenido del marco teórico, el análisis de los resultados y la discusión.

CAPÍTULO I

REVISIÓN DE LITERATURA

1.1 Contexto y marco teórico

1.1.1 Modalidades de fraude informático

Según Mayer (2018) el fraude informático consiste en la manipulación o alteración de datos o programas informáticos o la obtención de información personal o secreta de los clientes de los bancos o de sus cuentas o tarjetas, con la finalidad de causar un perjuicio económico a su víctima. Las modalidades de fraude informático más conocidas son las siguientes:

A. Phishing

El *phishing*, como término, tiene su origen etimológico en la palabra en inglés *fishing* (pesca) y busca evocar la idea de pesca de información o de mordedura del anzuelo, pues a través de él se pretende que las potenciales víctimas proporcionen de manera consciente o inconsciente la información necesaria para que el hechor pueda cometer el fraude (Mayer y Oliver, 2020).

Se trata de una estafa realizada con la intención de engañar a la potencial víctima, para que revele datos relevantes y personalísimos vinculados a sus cuentas bancarias (números de tarjeta, códigos de identificación personal o contraseñas) u otra información privada (Semana, 2014).

Según Divito (2021) esta pesca de usuarios se hace progresivamente mediante señuelos cada vez más sofisticados. En una primera etapa, se realiza mediante la denominada ingeniería social, un método no técnico que requiere necesariamente de la interacción humana y que busca la manipulación de la víctima potencial para que entregue voluntariamente su información (Krombholz y otros, como se citó en Mayer y Oliver, 2020). El instrumento utilizado es el correo electrónico o mensaje de texto, mediante el cual el estafador usa el nombre de una empresa de confianza del sistema financiero para enviar mensajes a la

posible víctima y obtener su número de tarjeta y clave secreta (Balcazar, 2017). O podrá hacerlo de forma masiva (*Deceptive phishing*), enviando mensajes genéricos a un grupo indeterminado de personas para que informen sus datos por la misma vía o redirigirlos a sitios web clonados para que ingresen su información en la creencia de que están ejecutando dicha acción en una página web confiable (Divito, 2021). En una segunda fase, se popularizó el uso de un software malicioso (*malware*) que se introduce en el ordenador de la posible víctima para enviar desde allí la información personal y atacar directamente sus operaciones (Mayer y Oliver, 2020).

B. Pharming

El *pharming* es un método fraudulento estrechamente vinculado con el phishing, por lo que resulta normal que sean considerados en conjunto o que este se clasifique tan solo como una variante (Mayer y Oliver, 2020).

En esencia, para Oxman (2013) supone la elaboración y puesta en funcionamiento de un sitio web falso por parte del estafador, con similitudes evidentes con la página oficial de una entidad bancaria, lo que implica el diseño de una interfaz y la modificación de protocolos DNS; de tal manera que la víctima potencial, al ingresar a la página web, no se percate de que está ingresando en un sitio web falso y entregue su información confidencial. En algunas ocasiones, el estafador instala un *malware* en la página falsa, que le permite extraer la información necesaria con la sola visita de la víctima, no requiriendo la introducción o digitación de ningún dato. Incluso, puede predeterminar la posición del enlace en la recomendación de búsqueda para incrementar las posibilidades de acceso (Abad y Reyes, 2022).

C. Smishing

El *smishing* es una modalidad de *phishing*, por la que se envía mensajes de texto a las víctimas potenciales utilizando el nombre de empresas bancarias de confianza, para obtener sus datos personales

(Abad y Reyes, 2022). El término *smishing* está compuesto por la contracción de las siglas en inglés SMS que significan "mensaje corto de texto" (Ventura, 2021). El mensaje puede dirigir a los usuarios a sitios web falsos o conducirlos a efectuar llamadas telefónicas en las que se les solicita su información (Duran, 2020).

Es una forma de fraude informático que consiste en obtener datos personales o financieros de los usuarios mediante el envío de mensajes de texto que contienen enlaces a sitios web falsos o números de teléfono fraudulentos (Ventura, 2021). Es decir, no es más que una forma de hacer *phishing*, pero utilizando, como medio para el engaño, un mensaje de texto al dispositivo de telefonía móvil (Semana, 2014).

D. Vishing

Otra modalidad de estafa es el *vishing*, término que deriva de la comunión de dos palabras en inglés: *Voice* y *phishing*. En estos casos, el estafador recrea una voz automatizada para hacerse pasar como personal de cualquiera de las entidades bancarias de confianza y así poder obtener la información personal necesaria que le permita acceder a las cuentas de las víctimas potenciales (López, 2015).

En el *vishing*, el hechor usa llamadas telefónicas con tecnología *VoIP (Voice over internet protocol)* para hacerse pasar por otra persona o entidad (Duran, 2020). Puede realizarse con llamadas telefónicas que usan voces automáticas, robóticas o mensajes de voz que fingen ser un familiar (López, citado por Ventura, 2021) o el trabajador de una entidad bancaria para cometer el delito. Se puede usar el *phishing* o *smishing* para brindarle a la víctima un número telefónico al que puede llamar (Abad y Reyes, 2022).

E. Spyware

Se trata de usar una aplicación (troyano) que los estafadores han introducido en el ordenador de la víctima luego de que esta accediera a alguna página web infestada de virus, para que una vez dentro comience a enviar, desde el equipo informático, los datos necesarios para realizar el

ilícito (claves de acceso, etc.) hacia el ordenador del delincuente (Abad y Reyes, 2022). Es un método más técnico, que no requiere de la participación voluntaria de la víctima potencial. Esta modalidad, según Javato (como se citó en Silvestre, 2021), "puede capturar hábitos de navegación, mensajes de correo, contraseñas y datos bancarios para transmitirlos a otro destino en Internet".

F. Skimming

El *skimming* hace referencia a la duplicación fraudulenta y sin consentimiento de los datos personales contenidos en la tarjeta de crédito o débito (Abad y Reyes, 2022). Específicamente, busca copiar los datos que se encuentran en la banda magnética que posee la tarjeta a través de dispositivos que se colocan en cajeros automáticos o comercios (Balcazar, 2017). Este dispositivo (conocido como *skimmer*) tiene por finalidad leer la banda magnética de la tarjeta para clonar o copiar su información para su posterior uso fraudulento (Castillo, 2018). Los datos se almacenan y se transfieren a una nueva tarjeta falsa con una identidad diferente, que se usa para hacer compras o retiros fraudulentos (Ponce, 2022).

G. SIM Swapping

De acuerdo con De Romaña (2022) consiste en utilizar la información de la víctima potencial, específicamente su número telefónico, para notificar a la empresa operadora de un supuesto robo o pérdida de su equipo celular y solicitar la reposición del servicio en un nuevo chip móvil. De esta manera, el estafador se apodera del número telefónico de la víctima y accede a la información personal vinculada al celular o a la *SIM Card* (como las cuentas de correo o membresías, datos de aplicaciones o cuentas bancarias), para realizar operaciones bancarias no reconocidas, ya sean transferencias o solicitudes de créditos. Este método es de difícil detección e imposibilita la reacción rápida de la víctima potencial, ya que suele ocurrir durante la madrugada, aprovechando que esta se encuentra dormida; además que, mientras se ejecuta el fraude, el usuario tendrá la línea cortada en su equipo celular.

1.1.2 Servicios Financieros

De acuerdo con Stucchi et al. (2021) los servicios bancarios tienen un rol muy importante en el desarrollo económico de un país. Tomando en cuenta la perspectiva del consumidor y sus necesidades, los servicios bancarios pueden tener dos dimensiones: la del ahorrista del banco que obtiene a cambio un pago (tasa de interés pasiva) por los depósitos que realiza; o, la del prestatario, que contrata un crédito específico o una línea de crédito, para viabilizar necesidades que, de lo contrario, no se solucionarían. Así, dos necesidades complementarias se conectan: la de ahorrar y la de obtener recursos.

1.1.3 Operaciones bancarias

Según Broseta (1994) las operaciones bancarias (o contratos bancarios) se clasifican de forma tradicional, atendiendo a la función económica que verifican, en operaciones activas, pasivas o neutras:

A. Tipos de operaciones bancarias

A.1 Operaciones activas

Son aquellas en las cuales los bancos realizan colocaciones (financiamiento e inversiones) y se convierten en acreedores de sus clientes, recibiendo a cambio una retribución que adopta la forma de intereses (Betancourt, como se citó en Balcázar, 2017). En este tipo de operaciones, los bancos proporcionan sumas de dinero a sus clientes utilizando los capitales recibidos de estos o de sus propios recursos financieros, adquiriendo el derecho a su devolución en los términos de forma, plazo y condiciones acordados (Broseta, 1994). En esencia, los bancos funcionan como mediadores en el mercado de capitales, usando fondos captados a través de depósitos y aportes de capital propio para brindar apoyo financiero a los clientes (Puémape, 2013).

A.2 Tipos de contratos de crédito

Según Stucchi et al. (2021) los contratos de crédito implican una transferencia efectiva o potencial de dinero desde la entidad bancaria o financiera hacia el consumidor, por lo que pueden clasificarse en:

contratos de préstamo o mutuo dinerario, en estos casos existirá la obligación del proveedor de entregar al consumidor una cantidad de dinero y del consumidor de restituir el capital más los intereses pactados, comisiones y gastos aplicables; y, contrato sobre línea de crédito, en el que la obligación del proveedor consistirá en entregar una línea de crédito en favor del usuario, dentro de los límites y condiciones contratados, y el consumidor tendrá la obligación de pagar las sumas de dinero utilizadas y la retribución por los intereses, comisiones y gastos aplicables. Un ejemplo clásico es el contrato de Tarjeta de Crédito.

A.3 Operaciones pasivas

Son aquellas en las que los bancos admiten o aceptan capitales ajenos que depositan los clientes y los aprovechan en la colocación de préstamos a otros usuarios, pagándoles a cambio un interés que se incrementa con el tiempo. Con este tipo de operaciones se busca obtener capitales ociosos o que tengan pequeños rendimientos para generar ganancias a través de la inversión y obtener mayores beneficios de los que tendrían si estuviesen inactivos (Balcázar, 2017). Son aquellas en las que los bancos reciben recursos monetarios y financieros de sus clientes o de otras instituciones crediticias, convirtiéndose en deudora al recibir sumas de dinero y otorgar a la parte depositante el derecho de exigir su devolución en condiciones previamente acordadas, abarcando forma, plazo y términos establecidos en el acuerdo (Broseta, 1994). En este contexto, el dinero depositado, siendo de origen externo, se gestiona, invierte y duplica, canalizándolo hacia aquellos que necesitan capital o liquidez (Puémape, 2013). La operación pasiva más distintiva es el depósito bancario.

A.4 El depósito bancario

Según Broseta (como se citó en Blossiers, 2016) es un contrato por el cual los clientes depositan sumas de dinero a un banco, que adquiere la propiedad de dichos montos con el compromiso de restituirlos en las condiciones pactadas (tiempo, moneda y monto), pagando además un interés fijado por ley o de forma privada. A través

del depósito, el cliente obtiene la custodia de los montos entregados con un servicio de caja a su disponibilidad y una rentabilidad creciente por las sumas que son inmovilizadas, mientras que el proveedor tiene la obligación de conservar el dinero hasta que el consumidor lo requiera, pagando intereses, comisiones o gastos pactados (Stucchi et al., 2021). Según Blossiers (2016) existen tres tipos de depósitos: a) depósitos simples: que comprenden depósitos a la vista, a plazo y con previo aviso; b) depósitos en cuenta corriente; y, c) depósitos de ahorro.

A.5 Operaciones neutras

Son aquellas que implican la realización de un servicio (Blossiers, 2016). Son operaciones de mediación (transferencias, giros, efectos tomados al cobro) y de custodia (alquiler de cajas de seguridad, etc.), por las que el banco cobra determinadas comisiones que no significan un volumen importante de sus ingresos (Balcazar, 2017).

1.1.4 Instrumentos de pago

A. Tarjeta de crédito

Según Blossiers (2016) la tarjeta de crédito es un instrumento que utiliza el titular para acceder a una línea de crédito por un plazo determinado y realizar con ella distintas operaciones como la adquisición de bienes o servicios en establecimientos afiliados o disposición de dinero en efectivo en cajeros autorizados. Por las operaciones realizadas, el cliente se obliga a pagar a la empresa emisora de la tarjeta, el importe por las cantidades utilizadas y los demás cargos atribuidos e informados previamente.

Siguiendo esa línea, para Ghersi (como se citó en San Miguel, 2019) el contrato de tarjeta de crédito implica el acuerdo entre una empresa especializada y un cliente para abrir un crédito a favor de este último, el cual le permite adquirir bienes o servicios en establecimientos específicos con los cuales la empresa tiene acordada una comisión correspondiente.

Por su parte, para Camacho (2019) la tarjeta de crédito implica una forma de financiamiento en la que se adquiere la responsabilidad de reembolsar el monto utilizado, así como de abonar los intereses, comisiones bancarias y cargos acordados según los términos del contrato, lo cual es detallado en el estado de cuenta que se envía mensualmente. En ese marco, Puémape (2013) señala que la tarjeta funciona como documento de legitimación personal e intransferible para identificar al usuario en la prestación de servicios, basándose en un contrato entre la entidad financiera y el cliente.

Para los autores, Avelino et. al (como se citó en Silvestre, 2021) la tarjeta de crédito es un pequeño crédito del que se dispone solo a través de la emisión del plástico y que sirve como medio de pago. Si bien la línea de crédito atada a la tarjeta plastificada tiene un límite que va disminuyendo con cada uso, este se restaura en tanto se hace el pago del consumo.

Siguiendo la línea de lo anterior, el Reglamento de Tarjetas de Crédito y Débito (2013) define a la tarjeta de crédito como un medio de pago que puede ser físico o digital y que se encuentra vinculado a una línea de crédito otorgada por la empresa emisora de la tarjeta. A través de este instrumento el titular o usuario puede pagar por bienes, servicios, obligaciones u otros servicios adicionales.

En resumen, el contrato de tarjeta de crédito es complejo y crea una relación triangular entre el comprador, el vendedor y la entidad financiera, a través de la cual se facilita al comprador la adquisición de bienes y servicios del vendedor, comprometiéndose a pagar el precio en un plazo establecido a la entidad emisora de la tarjeta; así, esta última asume la deuda al pagar de inmediato al vendedor, deduciendo las comisiones acordadas (Patrón, 2011).

A.1 Partes intervinientes

Siguiendo lo anterior, de acuerdo con Betancourt (como se citó en Balcázar, 2017) las partes involucradas en la contratación de una tarjeta

de crédito son: el emisor, que será una empresa bancaria o financiera que emite el plástico a nombre de un titular; el establecimiento afiliado, que es el comercio que acepta el crédito concedido al usuario a través de una relación previa con la entidad emisora, buscando mejorar sus ventas al formar parte de la lista de comercios afiliados (Puémape, 2013); y, el titular, que es la persona natural o jurídica autorizada a emplear la tarjeta por la entidad emisora tras una evaluación crediticia de capacidad de endeudamiento (Puémape, 2013).

Para Figueroa (2010) el contrato de tarjeta de crédito reúne las siguientes relaciones jurídicas:

Contrato entre la entidad emisora y el usuario: Implica la apertura de crédito por parte del emisor en favor del titular de la tarjeta. Se concede al usuario un límite máximo de crédito para realizar compras o utilizar servicios. El usuario se compromete a pagar periódicamente los resúmenes de cuenta y el incumplimiento de plazos conlleva el pago de intereses moratorios.

Contrato entre la entidad emisora y los proveedores adheridos: Denominado “contrato de afiliación”, este acuerdo obliga al afiliado a aceptar compras o servicios mediante la presentación de la tarjeta de crédito. El banco emisor se compromete a pagar las boletas presentadas por el afiliado, deduciendo la comisión acordada.

Relaciones entre el usuario y el proveedor: La compra o utilización de servicios por parte del usuario en el comercio afiliado se liquida al contado por el emisor, presentando las boletas firmadas por el usuario.

A.2 Tipos de contratos de tarjeta de crédito

Según San Miguel (2019) se identifican dos tipos de contrato de tarjeta de crédito: bilateral y trilateral, según la cantidad de partes involucradas. En el contrato bilateral, actúan dos partes: por un lado, el emisor y el proveedor considerados como un solo sujeto y, por otro lado, el usuario. Un ejemplo de esta situación es el caso de aquellas tarjetas de

crédito emitidas por empresas que suministran bienes o servicios directamente al usuario, permitiéndole postergar el pago y realizarlo en cuotas periódicas. Por otro lado, el contrato trilateral involucra a tres partes: el emisor, el consumidor y el proveedor. En este caso, el emisor actúa como intermediario en los pagos, pagando al proveedor y recibiendo periódicamente el importe debido del consumidor.

Por otra parte, según el Reglamento de Tarjetas de Crédito y Débito (2013) el tipo de línea de crédito puede ser: revolvente, cuando el deudor tiene la flexibilidad de utilizar y pagar repetidamente el crédito disponible, es decir, una vez que el deudor realiza pagos y reduce el saldo pendiente, ese monto pagado vuelve a estar disponible para su uso; y, no revolvente, en los que una vez que el prestatario utiliza el crédito y realiza pagos para saldarlo, esos montos pagados no vuelven a estar disponibles o no puede reutilizarlos.

A.3 Instrumentalización

Para Figueroa (2010) la ejecución de este contrato implica la utilización de diversos instrumentos para su implementación adecuada, entre los cuales se encuentra, en primer lugar, la solicitud, que es redactada en un formulario por el emisor y contiene las cláusulas contractuales aplicables entre emisor y usuario. Se trata de un contrato tipo o por adhesión y, en el caso de tarjetas otorgadas por bancos, se configura como un contrato de apertura de crédito; además, en algunos casos exige la apertura de una cuenta corriente como parte del proceso.

Otro elemento esencial es la tarjeta de crédito o plástico, que es un documento emitido por el emisor y entregado al usuario. Este instrumento es fundamental, ya que el usuario debe presentarlo al realizar sus compras en los comercios afiliados al sistema.

Además, se deben considerar los comprobantes de venta o uso del crédito, los cuales son firmados por el usuario en cada transacción comercial llevada a cabo en los comercios adheridos al sistema. Finalmente, el resumen mensual de cuenta o estado de cuenta constituye

otro componente esencial, que proporcionado por el emisor al usuario y detalla las compras realizadas con la tarjeta durante el período mensual.

B. Tarjeta de débito

Según Silvestre (2021) es un instrumento que le permite a su titular realizar operaciones con cargo a fondos depositados previamente, de acuerdo con lo contratado con la empresa emisora. Con esta tarjeta, el titular puede adquirir bienes o servicios en establecimientos de proveedores que se encuentren afiliados, pagar sus obligaciones, efectuar retiros de cualquiera de los canales que la empresa ponga a su disposición o utilizar otros servicios asociados que se encuentren dentro de los límites o características pactadas previamente, que impliquen el débito de los montos de sus depósitos previos. En esa misma línea, para Camacho (2019), la tarjeta de débito es un medio de pago que permite efectuar múltiples transacciones, que se realizan con cargo a una cuenta asociada y solo son posibles si hay fondos suficientes en dicha cuenta.

Siguiendo lo anterior, de acuerdo con el Reglamento de Tarjetas de Crédito y Débito (2013) es un instrumento de pago que puede tener soporte físico o digital y que permite efectuar operaciones mediante el uso de fondos depositados previamente ante la entidad emisora. Mediante este medio el titular o usuario puede pagar por bienes, servicios, obligaciones u otros servicios asociados, de acuerdo con las condiciones previamente acordadas.

B.1 Partes intervinientes

Las partes intervinientes son el emisor, que puede ser una empresa bancaria o financiera encargada de emitir el plástico a nombre de un titular, dándole la opción de que pueda disponer del dinero que depositó con anterioridad en su cuenta. Segundo, el titular, que es una persona natural o jurídica, a la que, previa contratación, la empresa le entrega la tarjeta (Betancourt, como se citó en Balcázar, 2017).

1.1.5 El deber de idoneidad en servicios bancarios

Según Stucchi et al. (2021) para las operaciones financieras en concreto, el derecho a la idoneidad implica la correspondencia entre los servicios financieros que espera recibir el consumidor y los que realmente recibe de parte de la entidad. Dicho concepto, conforme señala el Código de Protección y Defensa del Consumidor (2010) se encuentra fuertemente vinculado a la libre elección del consumidor, quien tiene derecho a elegir libremente la alternativa dentro del mercado financiero o bancario, que se adecúe a sus necesidades. En esa línea, el deber de idoneidad (establecido en los artículos 19 y 20 del Código) exige a los proveedores que se cumpla con:

- Las garantías legales, derivadas de exigencias normativas contenidas en instrumentos como el Código, la Ley General del Sistema Financiero o las resoluciones o circulares emitidas por la SBS, que prevalecen sobre la autonomía de la voluntad de las partes.
- Las garantías explicitas, provenientes de una fuente netamente contractual y que surgen como expresión de la voluntad de las partes, por lo que se encuentran determinadas por aquello que le fue ofrecido al consumidor (de forma directa o a través de la publicidad) y materializadas en las condiciones y términos estipulados en contratos bancarios de consumo. Hay que recordar que determinadas cláusulas generales de contratación (como en el caso de créditos hipotecarios o de consumo; depósitos de ahorro, a plazos, por compensación de tiempo de servicio o en cuenta corriente; o servicios financieros de dinero electrónico) requieren de la aprobación administrativa previa por parte de la SBS, como un mecanismo de protección al derecho de los consumidores.
- Las garantías implícitas, derivadas de lo que resulte o deba resultar evidente en relación con las características o términos exigibles al servicio; por lo que tienen un carácter residual.

Ahora, si bien las garantías legales son mayores a las implícitas, son las explícitas las que se relacionan de una forma más directa con el consumidor, pues son las que se le informa previamente o al momento de realizar la contratación del servicio (Stucchi et al., 2021).

En esa misma línea, la SPC señala que, de acuerdo con la garantía legal contemplada en el artículo 17° del Reglamento de Tarjetas de Crédito y Débito (2013), el parámetro de idoneidad en la prestación de este tipo de servicios se encuentra comprendido por las medidas de seguridad atribuidas a las entidades financieras por la normativa sectorial, encontrándose, entre ellas, ineludiblemente, el deber de monitoreo y detección de consumos inusuales o sospechosos. Por tanto, un consumidor que contrata un producto financiero tendrá la expectativa razonable de que la entidad financiera desplegará, sin excepción, las medidas de seguridad a las que legalmente está obligada, por lo que la omisión o adopción inadecuada de dichas medidas implicará que la prestación del servicio financiero no sea idónea. Por tanto, corresponde a la entidad administrativa evaluar el cumplimiento de dicha garantía legal, incluso aunque el consumidor no hubiera cuestionado su observancia de forma completa o explícita (*Resolución 2609-2022/SPC-INDECOPI*, 2022).

Para Patrón (2011) la seguridad es una condición inherente a los servicios financieros en el mercado y complementaria a su idoneidad, aunque no constituya la principal prestación que las entidades financieras realizan. Por tanto, la idoneidad debe evaluarse considerando todas las condiciones del servicio, exigiendo un nivel de seguridad adecuado que los proveedores deben garantizar para que los consumidores puedan disfrutar de las prestaciones sin inconvenientes.

En ese sentido, en la prestación de servicios y productos financieros en los que se verifique la afectación de cuentas o líneas de crédito de los consumidores por operaciones no reconocidas o fraudulentas, en el marco del parámetro de idoneidad, se deberá analizar, primero, el cumplimiento de la garantía legal, que involucra a la normativa emitida por la SBS bajo el principio de especialidad; y, segundo, de la garantía explícita, que implica la entrega del servicio en las condiciones en que fueron pactadas (Silvestre, 2021).

1.1.6 Las relaciones de consumo en las actividades bancarias

De acuerdo con Stucchi et al. (2021) para el caso de las relaciones de consumo en actividades bancarias, existirán dos partes intervinientes. Por un lado, el consumidor, que, siguiendo la definición del Código, puede ser cualquier

persona natural o jurídica que utiliza como destinatario final un producto o servicio para sí mismo, su familia o grupo social y siempre en un ámbito alejado de su actividad empresarial. También pueden ser consumidores los microempresarios que evidencien asimetría informativa en productos o servicios que no forman parte de su giro del negocio o en servicios transversales (como es el caso del servicio financiero). Y, por otro lado, el proveedor que, puede ser toda persona natural o jurídica que, habitualmente, comercializa bienes y/o presta servicios a los consumidores. En este caso, serían todas aquellas empresas bancarias o financieras autorizadas por la SBS que brindan servicios de intermediación financiera en operaciones pasivas o activas. Entre estas entidades se incluyen empresas bancarias y financieras, cajas rurales y municipales de ahorro y crédito.

1.1.7 Los servicios *Fintech* y las relaciones de consumo en el ámbito bancario y digital

En la actualidad, es normal que la mayoría de las entidades bancarias (y sobre todo las de mayor alcance o presencia en el mercado) busquen actualizar sus servicios, utilizando plataformas digitales que se renuevan y mejoran constantemente. A esto, se unen las iniciativas de desarrollo de aplicaciones tecnológicas que agilizan la prestación de los servicios bancarios a los consumidores, que reciben el nombre de *Fintech* (Stucchi et al., 2021).

El término *Fintech* surge de la fusión de dos conceptos (*financial* y *technology*) y se asocia al uso que le dan las empresas financieras a la tecnología para prestar sus servicios. Este método implica el ahorro de tiempo y recursos al utilizar como instrumentos equipos electrónicos dinámicos y generalizados (el celular o computadoras), que permiten democratizar el acceso a servicios financieros y realizar operaciones como transferencias de dinero, otorgamientos de crédito, compras, pagos, cobros y gestión de información financiera (Stucchi et al., 2021).

En nuestros días, es usual que las entidades financieras brinden sus servicios a través de su Banca por Internet (utilizando sus páginas web o plataformas digitales), su Banca Móvil (usando aplicativos instalados en equipos celulares) o que se utilicen POS o aplicativos móviles para sistemas de pagos

(billeteras digitales como Yape o Plin). Aun así, el proceso de modernización no termina, ya que recientemente se ha sustituido el uso de números telefónicos para realizar los pagos (al ser información sensible) por la implementación de códigos QR que son asignados a cada usuario para ser escaneados por quien decida realizar la transferencia (Stucchi et al., 2021).

1.1.8 Tipos de operaciones según su habitualidad

A. Operaciones usuales y no usuales

De acuerdo con Silvestre (2021) operaciones usuales son aquellas que coinciden con la actividad regular del titular; es decir, las operaciones recurrentes y estándar del titular de la tarjeta. Por ejemplo, si un usuario acostumbra a retirar mil soles cada mes, de forma repetitiva y constante, se entenderá que dicha operación es usual, ya que existe un patrón habitual en sus transacciones.

De acuerdo con el Reglamento de Tarjetas de Crédito y Débito (2013) inciso 2 del artículo 5, se puede inferir que la habitualidad de los consumos se encuentra estrechamente vinculada con el ámbito territorial, la frecuencia de las operaciones, el canal utilizado, el tipo de comercio, entre otros aspectos que convergen en un historial durante un tiempo o periodo determinado. De tal manera que serán operaciones usuales, todas aquellas que se ajusten el patrón de consumo del usuario y, por un ejercicio lógico de oposición, serán operaciones no usuales aquellas que no corresponden a la habitualidad de los consumos del usuario y se encuentran fuera de su patrón de comportamiento.

En complemento con lo anterior, según Lozano (2008) se clasifican como operaciones inusuales aquellas que, por su cuantía o atributos, no se vinculan con la actividad económica típica del cliente o que, debido a su cantidad, montos o características particulares, se apartan de los estándares de normalidad establecidos en el segmento de mercado correspondiente.

B. Operaciones no reconocidas o fraudulentas

Para Silvestre (2021) son todas aquellas generadas por parte de un tercero no legitimado, que suplanta la identidad del titular para realizar diversos consumos que este no reconoce. En general, estos casos se presentan porque el titular no tiene los cuidados debidos en el uso del plástico o se generan brechas en los mecanismos de seguridad de las entidades que emiten las tarjetas.

Siguiendo esa línea, según Aldana (como se citó en Balcázar, 2017) las operaciones no reconocidas son las transacciones fraudulentas que el titular de la tarjeta no reconoce en su totalidad, entendiéndose como aquellas en las que existe una sustitución indebida del titular de la tarjeta para que un tercero que usurpa la identidad del consumidor realice con ella una operación que ocasiona un perjuicio económico a los titulares, proveedores y/o establecimientos afiliados. En resumen, en estas operaciones, el titular de la tarjeta indica no haber realizado ni aprobado las operaciones, a pesar de que las mismas se realizaron con la tarjeta o con información de esta (Quispe, 2021).

1.1.9 Medidas de seguridad en instrumentos de pago

De acuerdo con Meza (2012) si bien la prestación principal en los contratos de tarjeta de crédito o débito es otorgarle al titular la posibilidad de realizar transacciones económicas en cualquiera de las modalidades previstas en el contrato, con cargo al pago de las obligaciones derivadas, hay un riesgo creciente y casi connatural al uso del plástico que obliga a las entidades financieras a implementar medidas de seguridad que disminuyan la posibilidad de la ocurrencia de un fraude o uso indebido del mismo. Así, la seguridad no es una prestación principal como tal, sino más bien una obligación para garantizar la idoneidad de las transacciones.

A decir de Silvestre (2021) en los servicios financieros, cuando el proveedor ofrece como servicio la contratación de una tarjeta, implícitamente ofrece proteger al consumidor de operaciones inusuales por medio de determinadas medidas de seguridad. Ello, a fin de que los titulares dispongan de

su dinero de forma natural, libre e intuitiva, mientras las entidades bancarias se encargan de generar las condiciones necesarias para mantenerlos a salvo de estafadores (Aware, 2019).

Siguiendo esta idea, Patrón (2011) indica que las empresas financieras que operan tarjetas de crédito o débito tienen la responsabilidad de garantizar la seguridad del instrumento utilizado en las transacciones (plástico) y de asegurar el respeto de las líneas de crédito; además, deben implementar sistemas de seguridad y mecanismos para que los usuarios informen rápidamente la pérdida o robo de sus tarjetas.

En esa misma línea, la SPC señala que la seguridad es una condición implícita en los servicios prestados en el mercado, por lo que se encuentra integrada al deber de idoneidad. De esta manera, las medidas de seguridad se convierten en una presencia necesaria para que las transacciones realizadas con las tarjetas se realicen correctamente y generen confianza y tranquilidad en los usuarios (Resolución 0004-2010/SC2-INDECOPI, 2010).

No obstante, según Misra et al. (2020) a la par que las entidades financieras hacen esfuerzos para mejorar sus condiciones de seguridad, las personas que pretenden realizar un fraude optimizan también sus recursos para conseguir sus propósitos. Por consiguiente, la implementación de mecanismos de seguridad lleva implícita una serie de desafíos asociados, como son la naturaleza dinámica del perfil del comportamiento fraudulento, que las transacciones tienden a parecer legítimas para evitar ser detectadas, entre otros.

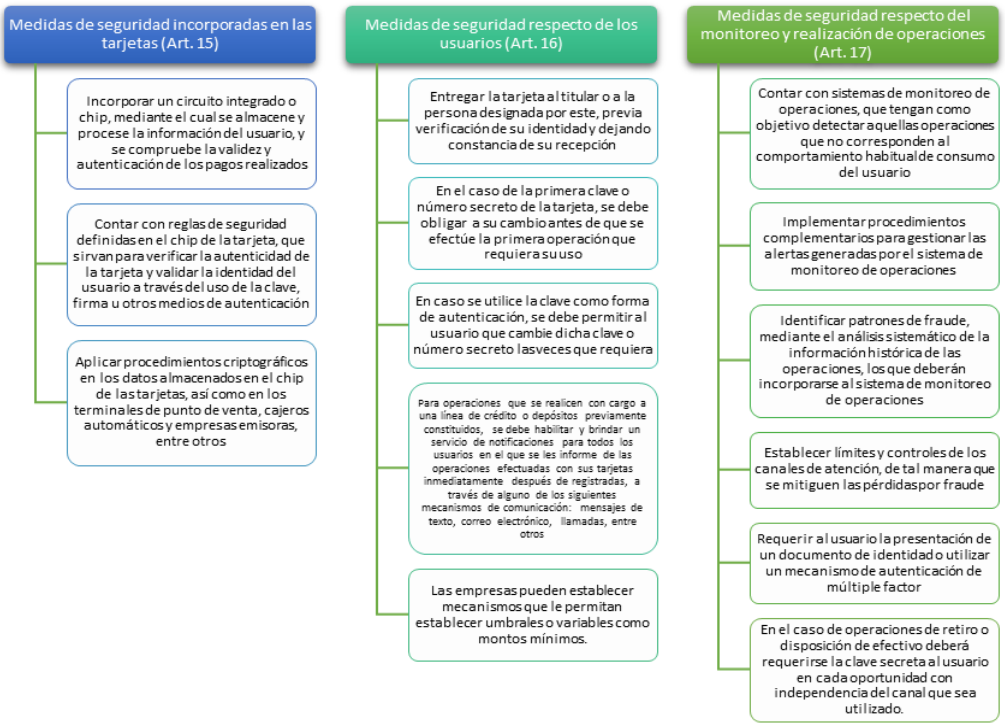
En nuestro país, a lo largo de los años, la SBS ha emitido diversas normas que establecen las medidas de seguridad que deben adoptar las entidades bancarias durante la ejecución de operaciones con tarjetas. No obstante, es necesario que las entidades bancarias, además de dar cumplimiento a estas normas, mejoren y adapten su sistema de seguridad y monitoreo al avance continuo de la tecnología, con el objetivo de garantizar transacciones más seguras y confiables.

Uno de los instrumentos legales emitidos por la SBS es el Reglamento de Tarjetas de Crédito y Débito (2013) que establece las diversas medidas de

seguridad que deben implementar las entidades bancarias para el uso de tarjetas de crédito y débito, encontrándose, entre estas, las siguientes:

Figura 1

Medidas de seguridad en el uso de tarjetas de crédito y débito



Nota: Información extraída del Reglamento de Tarjetas de Crédito y Débito.

A. Seguimiento de operaciones que correspondan a patrones de fraude

Según Meza (2012) las empresas que emiten tarjetas deben contar con un sistema de seguimiento de operaciones que permita detectar de forma razonable aquellas transacciones que, por sus características particulares, puedan corresponder a un fraude. En tal sentido, deben adoptar las siguientes medidas: (i) mecanismos para el aviso inmediato al usuario sobre las posibles operaciones fraudulentas; y, (ii) mecanismos que permitan tomar acciones para el bloqueo temporal o la cancelación definitiva de la tarjeta, en caso sea necesario (Artículo 22 del Reglamento de Tarjetas de Crédito y Débito).

B. Mecanismos de comunicación

Las empresas que emitan las tarjetas se encuentran en la obligación de poseer una infraestructura que garantice que puede contar con un sistema de atención (sea propio o de terceros) que permita a los usuarios comunicar el extravío o sustracción de sus tarjetas o información, o las operaciones no reconocidas que se hubieran podido realizar. Este sistema deberá estar disponible por 24 horas al día, todos los días del año y otorgar la posibilidad de acreditar la fecha, hora y contenido de cada comunicación (sea esta realizada a través de medios físicos o electrónicos), a la que además se le asignará un código de registro a manera de constancia (Reglamento de Tarjetas de Crédito y Débito, 2013, artículo 21).

1.1.10 La Banca electrónica

La Banca Electrónica, definida como la prestación de servicios financieros a través de equipos informáticos en tiempo real (Banco Central de Reserva del Perú, como se citó en Begazo y Vela, 2022), abarca todos los aspectos de la automatización bancaria, incluyendo procesos internos del banco y sus relaciones con otras entidades, constituyendo así una banca plenamente informatizada. Entre los servicios electrónicos de automatización bancaria tenemos los siguientes (Begazo y Vela, 2022):

- Cajeros automáticos o ATM (Automated Banking Machine): son equipos informáticos que permiten a los clientes de una entidad bancaria realizar operaciones bancarias como el retiro de efectivo, transferencias bancarias o la gestión de control sobre sus cuentas, sin la presencia de un empleado de la entidad financiera.
- POS (*Point-of-Sale Systems*): son dispositivos electrónicos que se colocan en establecimientos comerciales con la finalidad de que los clientes puedan efectuar el pago automatizado por la compra de los bienes o servicios que ofrecen.
- Banca virtual (*Virtual Banking*) o banca por internet: La banca virtual permite realizar diversas operaciones a través de internet, como abrir cuentas, transferencias, pagos a distancia y envíos de dinero, requiriéndose

solo un dispositivo con acceso a internet, como un teléfono móvil, tableta u ordenador, para hacer uso de estos servicios (Santander, 2020).

- Banca telefónica: Permite a los clientes de una entidad a efectuar operaciones mediante llamadas o mensajes de texto desde sus dispositivos móviles o teléfonos fijos.
- Banca móvil: Permite realizar las mismas actividades que la banca por internet, con la diferencia de que estas se realizan a través de un dispositivo móvil que tiene instalado un software o aplicación (APP) (Wells Fargo, como se citó en Begazo y Vela, 2022).
- Billeteras digitales: Es un aplicativo móvil que sirve como un monedero electrónico, ya que permite cargar dinero de forma virtual, transferirlo a otras billeteras, bancos o entidades financieras, pagar servicios y compras (Perú Retail, 2023). En el Perú, existen diversos tipos de billeteras digitales y algunas se encuentran respaldadas por un banco o empresa que emite el dinero electrónico. Entre las más usadas están Yape, Plin, IzipayYa, Agora y Bim (Gobierno del Perú, 2024).

1.1.11 Medidas de seguridad en operaciones realizadas a través de internet

El artículo 14 del Reglamento de Tarjetas de Crédito y Débito (2013) establece que las entidades financieras solo pueden cargar a las cuentas las operaciones que se encuentren sustentadas en órdenes de pago correctamente suscritas y autorizadas por los consumidores; además, dichas órdenes podrán ser reemplazadas por autorizaciones efectuadas a través de medios electrónicos y/o firmas electrónicas.

Así también, es importante traer a colación lo establecido en los artículos 7 y 23 de dicho reglamento, que precisan que la opción para realizar operaciones por medio de internet, desde páginas web, aplicaciones de dispositivos móviles, entre otros -que no sean ofrecidos por la empresa- requiere ser solicitada o

habilitada por el titular al ser un servicio adicional asociado a la tarjeta de crédito.

De manera específica, en 2009, la SBS emitió la Circular G-140-2009, Gestión de la seguridad de la información (2009) cuyo artículo 6 establece que, para la transferencia de fondos a terceros a través de canales electrónicos, las entidades financieras deben implementar un esquema de autenticación de clientes con dos (2) factores como mínimo, siendo que uno de ellos debe ser de generado o asignado dinámicamente, o tener un nivel de seguridad igual o superior.

Actualmente, el Reglamento de Gestión de la Seguridad de la Información y la Ciberseguridad (2021) define la autenticación como el proceso para verificar la identidad de una entidad mediante credenciales asignadas, utilizando uno o más factores de autenticación independientes para asegurar que el uso no autorizado de un factor no comprometa la fiabilidad de los otros (artículo 2). Así, es responsabilidad de la entidad implementar procesos de autenticación para controlar el acceso a los servicios digitales, considerando los factores de autenticación requeridos, los estándares criptográficos vigentes, los plazos y condiciones en las que se requerirá al usuario volver a autenticarse, y los controles de seguridad necesarios para prevenir amenazas. Los procesos de autenticación deben ser reevaluados si la tecnología utilizada deja de contar con soporte del fabricante o si se descubren nuevas vulnerabilidades. Además, la entidad debe mantener y proteger los registros detallados de cada enrolamiento de usuario, intento de autenticación, y operación que requiera autenticación previa, así como implementar herramientas y procedimientos para monitorear transacciones y reducir la posibilidad de fraudes, incorporando escenarios de fraude conocidos y el compromiso de los elementos utilizados para la autenticación (artículo 17).

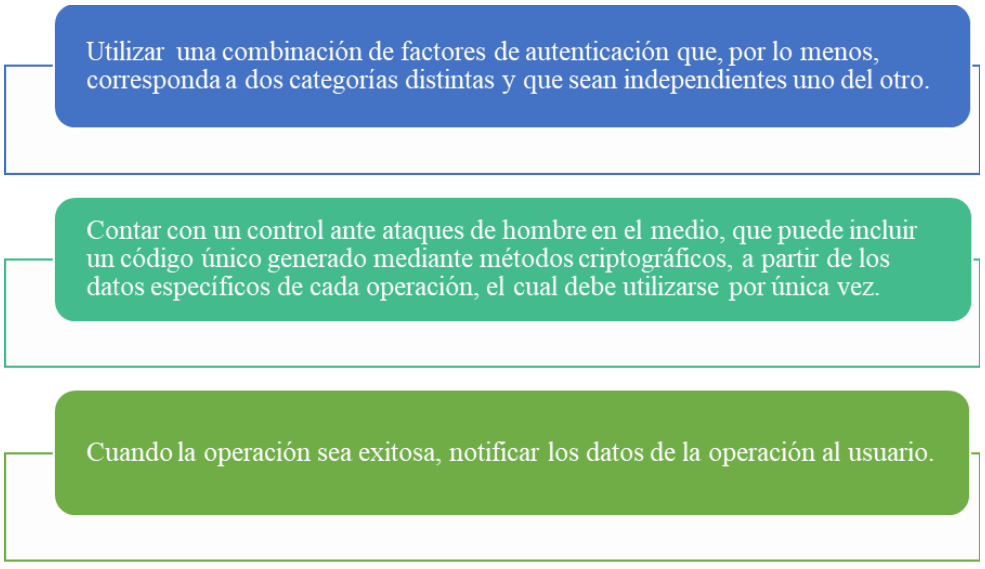
Adicionalmente, en su artículo 2 literal j), se señala que los factores de autenticación que permiten verificar la identidad del usuario se dividen en las siguientes “categorías”: (i) algo que solo el usuario conoce; (ii) algo que solo el usuario posee, y; (iii) algo que el usuario es.

El artículo 18 establece que el enrolamiento de usuarios en canales digitales requiere la verificación de identidad, utilizando al menos dos factores biométricos o dos factores independientes, excepto para productos de seguros bajo el régimen simplificado, donde se permite un único factor biométrico. Además, se deben generar y asignar credenciales al usuario, con procedimientos para gestionar su ciclo de vida, incluyendo activación, suspensión, reemplazo, renovación, revocación, y asegurando su confidencialidad e integridad cuando sea necesario.

En el caso de operaciones realizadas en canales digitales (por ejemplo, Banca por Internet o Banca Móvil) que impliquen: (i) pagos o transferencias de fondos a terceros, (ii) registro de un beneficiario de confianza, (iii) la contratación de un producto o servicio, (iv) la modificación en los productos contratados; y, (v) la modificación de límites y condiciones, el proveedor deberá implementar la autenticación reforzada, que consiste en lo siguiente (artículo 19):

Figura 2

Autenticación reforzada para operaciones por canal digital



Nota: Reglamento de Gestión de la Seguridad de la Información y la Ciberseguridad.

A. Sistema biométrico

La biometría nace de la contemplación de la naturaleza y la idea de que somos seres únicos e irrepetibles. Por eso, la palabra tiene su

origen fonético en los términos griegos *bios* (vida) y *metrón* (medida). Se trata de una tecnología que se caracteriza por permitir el reconocimiento de algún rasgo único e identificable de cada persona, mediante un proceso determinado que se aplica comúnmente para la seguridad y el control de acceso (Castagnola, como se citó en Balcázar, 2017).

La biometría combina aspectos técnicos y científicos que permitan una autenticación confiable sobre la base de la biología con la finalidad principal de darle mayor seguridad a determinada información. En palabras simples, significa medir datos biológicos, por lo que existe una biometría física, que utiliza como instrumento de medición o lectura de las huellas dactilares, el ADN, la geometría de la mano, escaneos de retina, y reconocimiento facial, y de biometría del comportamiento, como los patrones de habla, las pulsaciones de teclas, firmas o formas de andar (Banga y Pillai, 2021; Coello, 2019).

En la mayoría de los casos, cualquiera de las modalidades biométricas que se utilice empleará algoritmos de detección de vida que faciliten la distinción entre una muestra real y una versión digital, impresa o recreada de otra manera, así se evitará que las imágenes o vídeos extraídos de redes sociales se puedan utilizar para, por ejemplo, desbloquear un escaneo de reconocimiento facial. En la actualidad, la biometría es el método más utilizado para autenticar la identidad de los clientes bancarios en cualquiera de sus canales, donde se incluyen la web, los dispositivos móviles, cajeros automáticos, teléfono, asistentes digitales u otros (Aware, 2019).

B. Patrón de consumo

El numeral 5 del artículo 2 del Reglamento de Tarjetas de Crédito y Débito (2013) señala que el comportamiento habitual de consumo del usuario:

> [S]e refiere al tipo de operaciones que usualmente realiza cada usuario con sus tarjetas, 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 que registra la empresa.

El patrón de consumo es el producto de una serie de factores o características determinadas por la entidad, con base en la información histórica de las actividades del usuario con su tarjeta. Dicha información, según la SPC, tendrá en cuenta el monto, el tipo de operación, el análisis sobre la habitualidad de la operación (*Resolución 0023-2020/SPC-INDECOPI*, 2020), así como la frecuencia entre operación y operación (*Resolución 0022-2020/SPC-INDECOPI*, 2020).

1.1.12 Procedimiento administrativo sancionador en protección al consumidor

El artículo 106 del Código establece que el Indecopi es responsable de tramitar el procedimiento sancionador por infracción a las normas de protección al consumidor. De acuerdo con Tirado (2015) este procedimiento tiene por propósito disuadir la comisión de infracciones que transgredan los derechos de los consumidores mediante la imposición de sanciones monetarias (como medida represiva) y el dictado de medidas correctivas en favor del consumidor (como medida reparadora).

Respecto a la naturaleza del procedimiento de protección al consumidor tramitado en Indecopi, la posición mayoritaria en la doctrina considera que es un procedimiento sancionador con rasgos de trilateral, pues abarca dos relaciones jurídicas: una bilateral sancionadora en la que prevalece el interés público y otra trilateral que comprende los intereses privados de las partes del procedimiento (Peláez-Ypanaqué, 2014); en ese sentido, les son aplicables tanto las normas del régimen sancionador como del trilateral (Morón, 2018).

De acuerdo con Stucchi et al. (2021) existen dos tipos de procedimientos administrativos tramitados por el Indecopi para resolver disputas entre consumidores y proveedores: **el procedimiento sumarísimo y el procedimiento ordinarios** Ambos tienen un carácter sancionador, ya que, en caso de violaciones a los derechos del consumidor, se imponen las sanciones

correspondientes. Además, estos procedimientos pueden ordenar medidas correctivas para resarcir al consumidor por las consecuencias directas e inmediatas de la infracción, revertir sus efectos o prevenir su recurrencia.

- **Procedimiento Sumarísimo:** El procedimiento sumarísimo en Indecopi se caracteriza por su celeridad y agilidad, con un plazo máximo de treinta (30) días hábiles por instancia para su tramitación y resolución. Se tramitan por esta vía las denuncias cuyo valor del producto o servicio materia de controversia no sea superior a tres unidades impositivas tributarias (UIT); así como aquellas que traten únicamente sobre incumplimientos de acuerdos conciliatorios, de medidas correctivas, de medidas cautelares, liquidación de costas y costos, falta de atención a reclamos y requerimientos de información, métodos abusivos de cobranza, demora y falta de entrega del producto, al margen de su cuantía (artículo 125 del Código). Los Órganos Resolutivos de Procedimientos Sumarísimos actúan como la primera instancia administrativa, mientras que la Comisión de Protección al Consumidor o las Comisiones con facultades desconcentradas asumen la segunda instancia administrativa.
- **Procedimiento Ordinario:** Contrastando con el procedimiento sumarísimo, el procedimiento ordinario se aplica a casos de mayor complejidad o impacto económico, requiriendo un análisis más detallado y actuación probatoria más amplia. Estos procedimientos deben ser tramitados y resueltos en un máximo de ciento veinte (120) días hábiles por instancia. En esta vía se tramitan denuncias relacionadas con productos o servicios de valor superior a tres (3) Unidades Impositivas Tributarias (UIT) o de valor inapreciable, así como casos que involucran reclamos por productos peligrosos, discriminación, servicios médicos, actos que afectan intereses colectivos o difusos, entre otros. La Comisión de Protección al Consumidor o la Comisión con facultades desconcentradas toman la primera instancia administrativa, y la SPC asume la segunda instancia administrativa. Este procedimiento también puede iniciarse de oficio por la autoridad.

1.1.13 El principio de predictibilidad en los procedimientos administrativos

El artículo IV del T.U.O. de la Ley 27444, Ley del Procedimiento Administrativo General (2019) establece, en su numeral 1.15, que el principio de predictibilidad o de confianza legítima consiste en que la autoridad administrativa proporciona a los ciudadanos o sus representantes información precisa, exhaustiva y fiable sobre cada procedimiento a su cargo, asegurando que en todo momento comprendan claramente los requisitos, procesos, plazos estimados y los resultados potenciales. Además, las acciones de la autoridad administrativa se alinean con las expectativas legítimas de los ciudadanos, basadas en la práctica y los precedentes administrativos, a menos que, por razones debidamente justificadas, decida apartarse de ellas.

Al respecto, Cairampoma (2014) señala que este principio implica que la Administración tiene la obligación de generar en el administrado el conocimiento suficiente sobre el íter del procedimiento, el tiempo que tomará, los resultados que debe esperar y las medidas o remedios que está habilitado a solicitar o debe adoptar. Adicionalmente, esta obligación implica que, en los procedimientos homólogos, en los que las partes pueden ser distintas, pero la materia es similar y les son aplicables normas iguales, la Administración no podrá resolver de manera diferente en cada caso.

Siguiendo esa línea, Huamán (2017) indica que este principio reclama que la administración se vincule a sus actos propios, por lo que si desea apartarse de los lineamientos o fundamentos que ha construido debe fundamentar debidamente la nueva posición que asumirá.

Por su parte, Cabrera y Quintana (2013) discrepan de la posición anterior y consideran que la predictibilidad es una exigencia en la actuación de cada órgano de la entidad administrativa; en ese sentido, es aceptable que existan enfoques discordantes o formas distintas de aplicar la ley en las instancias de cada entidad o incluso entre sus diversos órganos de línea.

Para Guzmán (2013) el principio de predictibilidad requiere que la Administración obtenga resultados predecibles o consistentes entre sí, por lo que

los ciudadanos, al momento de iniciar un trámite, deberían tener una expectativa certera del resultado final que alcanzarán.

Por su lado, según Morón (2018) la seguridad jurídica administrativa podría definirse como el respeto a resolver siguiendo los antecedentes de criterios institucionales o los precedentes de interpretaciones en casos similares, por lo que si la autoridad toma una decisión que se aparte de dichos criterios, ello deberá ser de carácter excepcional y encontrarse debidamente justificado.

Rey (como se citó en Morón, 2018) sostiene que, en relación con el principio de predictibilidad, el Estado no puede desconocer las prácticas administrativas ni los criterios jurisprudenciales sin una justificación adecuada, sino que solo puede hacerlo en circunstancias específicas, respetando las expectativas razonables generadas en los ciudadanos en cuanto a la preservación de las normas, y a los actos o comportamientos que reflejen una posición clara y definida.

En conclusión, la predictibilidad en la administración pública es importante para fomentar una relación de confianza entre la autoridad y los administrados, ya que fortalece la transparencia en la administración pública, promueve la toma de decisiones informadas por parte de los ciudadanos y contribuye a establecer expectativas claras en los administrados, de tal forma que, desde el principio, estos conozcan con certeza el resultado o producto final que obtendrán al concluir el trámite del procedimiento. La mayoría de los autores coinciden en que la predictibilidad implica que la administración se vincule a sus propios actos. Por tanto, cualquier desviación de los lineamientos o criterios establecidos debe ser fundamentada de manera adecuada, garantizando la coherencia y la motivación de las decisiones administrativas.

1.2 Antecedentes

1.2.1 Internacionales

Calvo (2022) concluyó que la normativa española de servicios de pago y los criterios jurisprudenciales recientes establecen una responsabilidad cuasi objetiva para las entidades bancarias, invirtiendo la carga probatoria en favor del consumidor; en ese sentido, se presume automáticamente la falta de autorización

si el cliente niega haber realizado las operaciones, siendo la entidad la encargada de demostrar la actuación fraudulenta o negligencia grave del cliente.

Castillo (2018) se planteó como objetivo general conocer el contexto del delito informático y los sujetos del delito. La investigación concluyó que el progreso en las tecnologías de la información y la comunicación ha transformado la sociedad, facilitando un acceso amplio a la información y la comunicación global; sin embargo, también introdujo riesgos significativos para quienes no están familiarizados con las tácticas o modalidades de estafa o hurto de los delincuentes cibernéticos.

Divito (2021) se planteó como objetivo analizar las maniobras de obtención ilegítima de información de tarjetas bancarias, identificadas como *skimming* y *phishing*. Se concluyó que el rápido avance tecnológico ha planteado desafíos legales en la persecución de delitos vinculados a nuevas formas de defraudación, como el *skimming* y *phishing*. Si bien el análisis jurisprudencial revela que estas acciones se consideran actos preparatorios y no delitos ejecutivos, la falta de tipificación directa de estos genera lagunas legales, por lo que se sugiere la necesidad de incorporar un nuevo tipo penal para abordar específicamente estas conductas en el Código Penal.

Duran (2020) se planteó como objetivo describir las principales características, modos de perpetración y vulneración de la seguridad informática a través de la modalidad delictiva *Carding*. La investigación concluye que el *Carding*, considerado un delito emergente, tiene raíces antiguas, ampliando su alcance con internet. Las nuevas formas digitales de defraudación, como el *phishing* y *skimming*, presentan desafíos constantes, por lo que es esencial denunciar estas conductas para su investigación y judicialización, ya que la actualización de conceptos es crucial ante estas amenazas en evolución.

Escárate (2015) concluyó que el uso de tarjetas de crédito y el delito de uso fraudulento de estas son conductas que están en constante movimiento y dinamismo, pues el número de tarjetas aumenta a diario, y los avances tecnológicos permiten nuevas formas de comisión del delito; por tanto, es necesario generar nuevas interpretaciones que resguarden los derechos de las

personas afectadas y revisar constantemente la legislación existente, a fin de no dejar desamparados tanto a los usuarios de las tarjetas.

Hernández (2020) concluyó que, en ausencia de normas específicas sobre fraudes en operaciones bancarias electrónicas, se aplica un régimen de responsabilidad objetiva basado en el riesgo, similar al que se usa para el pago de cheques falsos o adulterados, pese a que el juez valora aspectos como la diligencia y el cuidado de las entidades financieras, como si se tratase de un juicio basado en responsabilidad con culpa. En ese sentido, el autor propone aplicar el régimen subjetivo de responsabilidad, que fomente la reciprocidad de esfuerzos entre banco y cliente para prevenir daños en operaciones electrónicas. En consecuencia, la asignación de pérdidas debe basarse en incumplimientos y culpa proporcional, evitando responsabilidades extracontractuales inapropiadas.

Manjarrés (2023) concluye que, ante el aumento de canales electrónicos para la disposición de fondos, las entidades bancarias tienen la responsabilidad de implementar rigurosas medidas de seguridad para proteger a los consumidores y sus depósitos, a fin de prevenir operaciones fraudulentas en el ámbito digital. Por otro lado, el deber de autoprotección por parte de los consumidores financieros constituye una obligación central, siendo esencial su colaboración en la adopción de prácticas seguras y en la comprensión de las recomendaciones proporcionadas por los bancos. En cuanto a la responsabilidad contractual de las instituciones bancarias ante operaciones ilícitas, se enfatiza la necesidad de un examen exhaustivo de la culpa del consumidor en caso revele información confidencial, aplicando la teoría de la concurrencia de culpas para graduar la responsabilidad entre ambas partes. Finalmente, se resalta que el control eficiente de los hábitos transaccionales no solo minimiza el riesgo de fraude, sino que fortalece las relaciones comerciales entre banco y cliente.

Morales y Prieto (2021) realizan un estudio sobre la responsabilidad del consumidor, la entidad de crédito y el establecimiento de comercio en caso de fraude con tarjetas de crédito en Colombia. Utilizando el Análisis Económico del Derecho para evaluar la racionalidad y la eficiencia de la norma que protege al consumidor frente al fraude, concluyen que esta no resulta eficiente para los tres intervinientes, pues afecta de manera desigual sus costos y beneficios.

Oxman (2013) concluyó que la legislación chilena requiere una adaptación urgente para abordar adecuadamente el *phishing* y *pharming*, ya que la actual normativa penal no tipifica de manera efectiva los fraudes bancarios más comunes realizados a través de plataformas en línea. La falta de figuras legales específicas para abordar estas conductas genera una situación atípica e inadecuada en la legislación actual, lo que resulta en sentencias contradictorias y socava la seguridad jurídica en transacciones comerciales en línea. Así, se subraya la necesidad de una revisión y actualización de la legislación para abordar de manera efectiva los fraudes bancarios en la era digital.

1.2.2 Nacionales

Abad y Reyes (2022) se plantean como objetivo determinar la forma en que las operaciones fraudulentas y delitos informáticos afectan el derecho patrimonial de los consumidores. El método de investigación que utilizaron fue el mixto. La conclusión de la investigación fue que las transacciones fraudulentas y los delitos informáticos afectan principalmente el derecho de propiedad y el derecho a contratar de los consumidores.

Balcázar (2017) se planteó como objetivo determinar las medidas de seguridad que deben agregarse a la Resolución SBS 6523-2013 a fin de evitar operaciones fraudulentas en las tarjetas y resguardar los intereses del consumidor financiero. La investigación es aplicada, descriptiva y documental, y emplea los métodos inductivo, deductivo, analítico y sintético, así como el método jurídico exegético. Las conclusiones fueron las siguientes: (i) existe la necesidad de implementar el sistema biométrico en el Reglamento a fin de prevenir operaciones no reconocidas, ya que ello generará mayor seguridad para los consumidores, especialmente en personas de la tercera edad o con discapacidades; y, (ii) existe la necesidad de que las áreas de monitoreo de las entidades financieras refuercen su seguridad con límites de consumo, claves de bloqueo y controles más rigurosos para detectar fraudes oportunamente.

Begazo y Vela (2022) analizaron la aplicación de criterios tuitivos en la responsabilidad administrativa de entidades financieras por infracción al deber de idoneidad por casos de fraude informático. La investigación es explicativa, pura, transversal y cualitativa, con un diseño no experimental. Las conclusiones

de la investigación fueron las siguientes: (i) la Autoridad de consumo de Arequipa aplica adecuadamente criterios protectores de los derechos del consumidor al imponer medidas correctivas y sanciones a proveedores de servicios financieros cuando incurren en una infracción, por lo que, en casos de incumplimiento, los consumidores pueden recurrir ante el Indecopi para lograr la satisfacción de sus pretensiones; (ii) la casuística evidencia una consistencia en la línea analítica de la autoridad, demostrando el cumplimiento del principio de predictibilidad y garantizando la seguridad jurídica; y, (iii) aunque las resoluciones suelen favorecer a los denunciantes, la ejecución de los actos finales a menudo excede el plazo normativo

Linares (2020) se plantea como objetivo corroborar si en la región La Libertad, entre 2017 y 2019, las entidades bancarias observan regularmente el deber de idoneidad en aquellos casos en que existan operaciones supuestamente fraudulentas realizadas con tarjetas de crédito y débito. La metodología utilizada fue cualitativa, con un diseño no experimental de tipo transversal. La conclusión fue que dichas entidades bancarias no cumplen con el deber de idoneidad, ya que para las operaciones fraudulentas realizadas con tarjetas, no despliegan mecanismos de seguridad básicos como: (i) el asegurarse de que el usuario haya habilitado previamente la opción de permitir operaciones por internet, (ii) contar con un sistema que permita monitorear y analizar el comportamiento habitual del usuario e identificar patrones de fraude, y, (iii) alertar al usuario sobre las operaciones fraudulentas para que se bloquee la tarjeta temporalmente.

Mora (2020), como objetivo principal, se planteó analizar los criterios a ser implementados por las entidades financieras para una correcta operatividad de sus sistemas de monitoreo, y por el Indecopi al ordenar el extorno de operaciones fraudulentas realizadas con tarjeta. La conclusión de la investigación fue que existe una sostenida divergencia de criterios por parte de la SPC, por lo que se hace necesario establecer un criterio general de identificación de patrones de fraude; sin embargo, adoptar esta idea podría facilitar que se realicen transacciones que no superen el valor máximo de las operaciones establecido a partir el historial de comportamiento financiero del usuario, dificultando su detección por el Banco.

Pareja (2022) se planteó como objetivo analizar cada una de las modificaciones realizadas e incorporadas por la SBS en la normativa propia de las tarjetas de crédito, pero que además se vinculen con la contratación de servicios adicionales y la aplicación de un sistema de notificaciones. La conclusión de la investigación fue que, a través de las modificaciones, se estableció la obligación de cambiar la forma en que se eligen los servicios adicionales y se autorizó la puesta en ejecución de un servicio que notifique las transacciones efectuadas a través de tarjetas de crédito.

Quispe (2021) se planteó como objetivo general identificar las principales dificultades en el proceso de atención de reclamaciones por operaciones no reconocidas a través del análisis de los reportes de resultados de tiempos de atención y cantidad de reclamos atendidos. La investigación es no experimental, cualitativa, descriptiva y transversal. Las conclusiones de la investigación fueron que: (i) se identificaron y separaron las acciones operativas en áreas específicas para optimizar el tiempo de los analistas al atender reclamos por operaciones no reconocidas; (ii) la automatización mediante macros y la consolidación de bases aumentaron la productividad diaria; y, (iii) la pronta resolución de reclamos contribuye a la satisfacción y fidelización del cliente.

San Miguel (2019) se planteó como objetivo general establecer la importancia de utilizar de manera adecuada la tarjeta de crédito que es otorgada por una entidad financiera. El método de investigación utilizado fue el inductivo y el alcance de la investigación descriptivo. Las conclusiones de la investigación fueron que el contrato de tarjeta de crédito es complejo y trilateral, involucrando al consumidor, la entidad crediticia y al proveedor. De otra parte, el uso responsable de un instrumento de pago influye en el acceso futuro al crédito y beneficios, por lo que la educación financiera es crucial.

Sifuentes (2022) se planteó como objetivo analizar la falta de predictibilidad para determinar el comportamiento habitual de un consumidor en el uso de transacciones con tarjeta o cuenta de ahorros, en el análisis de denuncias por operaciones fraudulentas. La investigación concluyó que no existe, dentro de la normativa sectorial, una regulación que brinde seguridad jurídica en referencia al patrón de consumo, por lo que es necesario que tal

indeterminación se solucione, estableciéndose como periodo de examinación un plazo de 6 meses previos a la fecha en que se realizaron las operaciones.

Silvestre (2021) se planteó determinar y analizar las medidas de seguridad instauradas para el uso de tarjetas de crédito y débito y su forma de aplicación, para resguardar los intereses económicos del consumidor en los casos de operaciones inusuales. La investigación concluyó que las medidas de seguridad implementadas por las entidades financieras para detectar y determinar qué operaciones son consideradas como no reconocidas no son aplicadas eficientemente lo que resulta en una protección inadecuada para el consumidor; ello se debe a la falta de una regulación que uniformice los criterios de aplicación, permitiendo así una protección preventiva y eficaz

Ventura (2021) se planteó como objetivo justificar la necesidad de incorporar los delitos de *phishing, smishing y vishing* en el sistema penal peruano. La investigación, de tipo exploratorio y enfoque cualitativo, concluyó que estas modalidades carecen de regulación en la legislación actual, por lo que existe la necesidad de tipificarlas. El autor señala también que existen deficiencias legislativas y logísticas en el sistema de justicia para abordar eficazmente los delitos informáticos.

CAPÍTULO II

PLANTEAMIENTO DEL PROBLEMA

2.1 Identificación del problema

Las operaciones bancarias no reconocidas son aquellas realizadas sin el consentimiento del titular de una cuenta o tarjeta, ya sea por fraude, error o negligencia. Estas operaciones pueden causar perjuicios económicos y morales a los usuarios, quienes tienen derecho a reclamar y obtener una solución satisfactoria por parte de las entidades bancarias. Sin embargo, en muchos casos, los reclamos no son atendidos adecuadamente, lo que obliga a los usuarios a recurrir a otras instancias para defender sus derechos.

En Perú, el Indecopi es el organismo administrativo encargado de resolver controversias entre usuarios financieros y entidades bancarias, según el Código de Protección y Defensa del Consumidor – Ley 29571. Esta institución cuenta con un procedimiento sancionador que busca restablecer el equilibrio entre las partes, analizar la responsabilidad de los proveedores, sancionar conductas infractoras y dictar medidas correctivas a favor de los consumidores. Dicho procedimiento es tramitado en primera instancia por los ORPS y las Comisiones de Protección al Consumidor, y en segunda instancia por las Comisiones de Protección al Consumidor y la SPC, respectivamente.

No obstante, los órganos resolutivos del Indecopi no cuentan con un criterio uniforme a nivel nacional al resolver estos casos, ya que, de la revisión de las resoluciones emitidas, se observan criterios disímiles al evaluar la idoneidad y pertinencia de las medidas de seguridad y monitoreo implementadas por las entidades bancarias, al dictar medidas correctivas en favor de los consumidores afectados e imponer sanciones, lo que podría generar incertidumbre tanto en los consumidores como en las empresas respecto del resultado que podrían obtener una vez concluido el procedimiento, afectando las expectativas legítimas que podrían haberse generado en los administrados y la eficacia del sistema de resolución conflictos en materia de consumo. Por estas consideraciones, se plantean las siguientes preguntas de investigación:

2.2 Definición del problema

2.2.1 Problema general

¿Cuál es la problemática jurídica subyacente en la predictibilidad de los pronunciamientos del Indecopi emitidos a nivel nacional en materia de operaciones fraudulentas efectuadas por internet durante los años 2022 a 2023?

2.2.2 Problemas específicos

- ¿Son predictivos los pronunciamientos del Indecopi emitidos a nivel nacional en materia de operaciones fraudulentas tanto en primera como segunda instancia administrativa durante los años 2022 a 2023?
- ¿Cuáles son las similitudes y diferencias entre los pronunciamientos emitidos en otros países, como España, Colombia y Chile, en casos de operaciones fraudulentas efectuadas por internet y los pronunciamientos emitidos por el Indecopi?
- ¿Cuáles son las recomendaciones o lecciones que pueden implementarse para mejorar la predictibilidad de los pronunciamientos del Indecopi en casos de operaciones fraudulentas efectuadas por internet?

2.3 Intención de la investigación

El propósito de la investigación es analizar la problemática jurídica subyacente en la predictibilidad de los pronunciamientos del Indecopi emitidos a nivel nacional en materia de operaciones fraudulentas efectuadas por internet durante los años 2022 a 2023. Para ello, en principio, determinaremos si los pronunciamientos del Indecopi emitidos a nivel nacional en dicha materia son predictivos. Los resultados de este estudio se comparan con los pronunciamientos emitidos por instituciones de otros países y se proponen recomendaciones o lecciones para mejorar la predictibilidad y, por ende, fortalecer la confianza de los administrados en los procedimientos administrativos sancionadores tramitados por el Indecopi.

En este contexto, la investigación se propone contribuir a que las decisiones emitidas por el Indecopi se fundamenten en criterios objetivos, razonables, previsibles y actuales, con el fin de salvaguardar los derechos e intereses económicos tanto de los consumidores como de los proveedores de servicios financieros, promoviendo así un

entorno legal que fomente una mayor confianza en los servicios ofrecidos por el Indecopi.

2.4 Justificación

La presente investigación se centra en el análisis de los pronunciamientos recientes emitidos por el Indecopi y por instituciones de países como Chile, Colombia y España en materia de operaciones fraudulentas efectuadas por internet. Este tema es relevante debido a que el uso masivo de tarjetas de crédito y débito, así como de los servicios de banca móvil, banca por internet, billeteras electrónicas o compras en páginas web, se está extendiendo a gran velocidad entre la población. Si bien la implementación de estos servicios amplía el acceso de la población al sector financiero y bancario y permite la realización de transacciones desde cualquier ubicación geográfica, también ha generado mayores riesgos para la ocurrencia de actos de fraude informático, que se hacen cada vez más complejos y sofisticados, conforme avanza la tecnología (Escárate, 2015).

Las operaciones no reconocidas, efectuadas como consecuencia de fraude informático, vulneran los derechos e intereses económicos de los consumidores y proveedores de servicios financieros, generando así una cuestión contenciosa que requiere ser resuelta a través de un procedimiento administrativo que cumpla con las expectativas legítimamente generadas en los consumidores. Sin embargo, en la actualidad, existe una notoria falta de predictibilidad en los pronunciamientos del Indecopi emitidos a nivel nacional en los casos de operaciones fraudulentas efectuadas por internet, ya que los órganos resolutivos emiten fallos que difieren ampliamente en todo el país, lo que podría generar incertidumbre tanto en los consumidores como en las empresas, respecto al resultado que obtendrán al final del procedimiento administrativo. Esta falta de predictibilidad puede incluso dar lugar a una percepción de arbitrariedad por parte de la autoridad administrativa, ya que si los consumidores no pueden anticipar cómo se resolverán sus casos, es menos probable que confíen en dicho sistema de resolución de controversias, lo que podría incluso desincentivar la presentación denuncias administrativas.

En tal sentido, esta investigación consiste en un estudio exploratorio y seguirá un enfoque cualitativo a fin de determinar si los pronunciamientos del Indecopi emitidos durante los años 2022 a 2023 en los casos de operaciones fraudulentas

efectuadas por internet son predictivos. Seguidamente, efectuaremos una comparación de los pronunciamientos del Indecopi con los de instituciones de otros países (España, Colombia y Chile) lo que será de gran importancia para identificar recomendaciones o lecciones que pueden implementarse, a fin de mejorar la predictibilidad de los pronunciamientos emitidos por dicho ente administrativo.

La importancia de esta investigación radica en su contribución al conocimiento y a la protección de los derechos e intereses económicos de los consumidores y proveedores de servicios financieros en el contexto de las operaciones fraudulentas realizadas por internet. Asimismo, sus resultados proporcionarán información actualizada y relevante que servirá como base para la elaboración de lineamientos, que recojan y unifiquen los criterios de los órganos resolutivos del Indecopi a nivel nacional.

2.5 Objetivos

2.5.1 Objetivo general

- Analizar la problemática jurídica subyacente en la predictibilidad de los pronunciamientos del Indecopi emitidos a nivel nacional en materia de operaciones fraudulentas efectuadas por internet durante los años 2022 a 2023.

2.5.2 Objetivos específicos

- Determinar si los pronunciamientos del Indecopi emitidos a nivel nacional en materia de operaciones fraudulentas tanto en primera como segunda instancia administrativa durante los años 2022 a 2023 son predictivos.
- Comparar los pronunciamientos emitidos en otros países como España, Colombia y Chile para resolver controversias en materia de operaciones bancarias fraudulentas con los pronunciamientos emitidos por el Indecopi.
- Establecer recomendaciones o lecciones que puedan implementarse para mejorar la predictibilidad de los pronunciamientos del Indecopi en casos de operaciones fraudulentas efectuadas por internet.

CAPÍTULO III

METODOLOGÍA

3.1 Acceso al campo

La investigación se llevó a cabo desde la ciudad de Puno, pero la jurisprudencia, doctrina y normas analizadas tienen alcance nacional. La investigación se enfocó en analizar los criterios o pronunciamientos emitidos por los órganos resolutivos del Indecopi en casos de operaciones fraudulentas efectuadas por internet durante los años 2022 a 2023, tanto en primera (ORPS y CPC) como segunda instancia (CPC y SPC). Debe tenerse en cuenta que, las provincias en las que el Indecopi cuenta con órganos resolutivos son: Lima, Ancash - Sede Chimbote, Arequipa, Cajamarca, Cusco, Ica, Junín, La Libertad, Lambayeque, Loreto, Piura, Puno, San Martín y Tacna.

Para ello, se presentaron solicitudes de acceso a la información pública ante el Indecopi, en las que se requirió un listado de los procedimientos administrativos que cumplan con los parámetros del objeto de estudio. Sin embargo, aunque el Indecopi proporcionó el listado en el plazo legal, surgieron dificultades al buscar las resoluciones digitalizadas en el “Buscador de Resoluciones del Indecopi”, ya que no se encontraron las resoluciones emitidas por algunas oficinas regionales, por lo que se tuvo que presentar nuevas solicitudes de acceso para obtener la información restante, lo que retrasó durante algunos días la ejecución de la presente investigación.

Por otra parte, se analizaron los fallos emitidos por la Superintendencia Financiera de Colombia, los Juzgados de Policía Locales de Chile y las Audiencias Provinciales de España en materia de operaciones fraudulentas durante 2022 y 2023. Para ello, se realizó la búsqueda de los fallos emitidos por dichos órganos resolutivos en la materia estudiada. Estos fueron encontrados en los sistemas de búsqueda o portales de transparencia del Poder Judicial de dichos países, utilizando frases clave como "*phishing*", "fraude bancario" y "operaciones fraudulentas". La investigación se llevó a cabo a lo largo del año 2023 y principios del 2024.

3.2 Selección de informantes y situaciones observadas

Según Hernández et al. (2014) en los estudios cualitativos es prescindible el tamaño de la muestra desde un enfoque probabilístico, pues el interés del investigador

es la profundidad y no la generalización de los resultados a una población más amplia. Tratándose de una investigación cualitativa, tal como señala Pineda (2008), la revisión de las resoluciones busca comprender la practicidad con la que se desarrolla el tema objeto de estudio, y por tanto no se basa en esquemas rigurosos y formales. En ese sentido, el presente estudio prescindirá de una población y muestra desde un punto de vista probabilístico.

En lo que respecta a los informantes, predominan las fuentes documentales, ya que la información clave para la presente investigación se encuentra principalmente en las resoluciones o sentencias emitidas sobre operaciones bancarias fraudulentas efectuadas a través de internet. La selección de resoluciones del Indecopi y de las sentencias de otros países se realizó mediante un muestreo no probabilístico de casos tipo (R. Hernández et al., 2014), tomando en cuenta que la muestra está constituida por los criterios adoptados por cada uno de los órganos resolutivos del Indecopi a nivel nacional, así como los fallos emitidos por la Superintendencia Financiera de Colombia, los Juzgados de Policía Locales de Chile y las Audiencias Provinciales de España en dicha materia. En ese sentido, para analizar las resoluciones de Indecopi, se seleccionaron de manera aleatoria al menos dos resoluciones por órgano resolutivo emitidas durante los años 2022 y 2023. En el caso de las sentencias de otros países, se seleccionaron también de forma aleatoria aquellas relacionadas con el tema de estudio, que se encontrasen dentro de los parámetros establecidos.

El enfoque elegido es el cualitativo (Ruiz et al., 2013) se realizó un análisis a profundidad de la predictibilidad de los pronunciamientos del Indecopi a nivel nacional, así como, de los fallos emitidos por la Superintendencia Financiera de Colombia, los Juzgados de Policía Locales de Chile y las Audiencias Provinciales de España en casos de operaciones fraudulentas efectuadas por Internet en los años 2022 y 2023. El tipo de investigación es descriptiva, ya que analizamos la predictibilidad de los pronunciamientos del Indecopi, comparativa, porque contrastamos dichos fallos y la legislación peruana con los de España, Colombia y Chile; y aplicada, porque proponemos soluciones prácticas para mejorar la predictibilidad en el contexto de operaciones fraudulentas efectuadas por internet (Hernández et al., 2014).

Los métodos de investigación científicos son: el método descriptivo, a través del cual se realizó un estudio de la predictibilidad de los pronunciamientos del Indecopi en

materia de operaciones no reconocidas efectuadas por Internet en los años 2022 y 2023, así como de las sentencias emitidas en Chile, Colombia y España sobre la materia; el método de observación directa, que sirvió para observar los criterios resolutivos del Indecopi a nivel nacional y los fallos emitidos en otros países; finalmente, el método de análisis de contenido permitió analizar la predictibilidad de los pronunciamientos del Indecopi a nivel nacional y desarrollar si, en la experiencia comparada, existen criterios o razonamientos que desarrollen con mayor amplitud la responsabilidad de las entidades bancarias en los casos de operaciones no reconocidas, de tal forma que, de dicha experiencia, se puedan extraer lecciones o recomendaciones que permitan mejorar la predictibilidad de los pronunciamientos emitidos por el Indecopi.

De otro lado, se emplearon técnicas de investigación tomando en cuenta cada objetivo específico. Así, para evaluar la predictibilidad de los pronunciamientos de Indecopi a nivel nacional, se utilizaron las técnicas de observación y análisis de contenido. La observación facilitó la recopilación de información sobre la legislación nacional y las resoluciones de Indecopi en la materia de estudio. Por otro lado, el análisis de contenido permitió evaluar la información recopilada, a fin de determinar la predictibilidad en el análisis de la responsabilidad de la entidad bancaria, las medidas correctivas y las sanciones impuestas. Respecto del segundo y tercer objetivo específico, a fin de comparar los pronunciamientos de Indecopi con los emitidos en otros países (España, Colombia y Chile), se aplicaron también las técnicas de observación y análisis de contenido. La observación se centró en recabar información sobre la legislación vigente y las sentencias emitidas; y, el análisis de contenido facilitó la evaluación de la información recopilada y permitió comparar estos resultados con los pronunciamientos del Indecopi a fin de extraer criterios o razonamientos que desarrollen con mayor amplitud la responsabilidad de las entidades bancarias en los casos de operaciones no reconocidas, a fin de extraer lecciones que permitan mejorar la predictibilidad de los pronunciamientos emitidos por el órgano administrativo. En ambos casos, se utilizaron como instrumentos las fichas de observación y las fichas de análisis de contenido.

3.3 Estrategias de recogida y registro de datos

Como se señaló en el punto anterior, se utilizaron como instrumentos de recolección de datos las fichas de observación y las fichas de análisis de contenido.

Respecto del análisis de los criterios o pronunciamientos emitidos por los órganos resolutivos del Indecopi en casos de operaciones fraudulentas efectuadas por internet durante los años 2022 y 2023, se recabó, a través de las fichas de observación, información de las resoluciones tanto de primera (ORPS y CPC) como segunda instancia (CPC y SPC) a nivel nacional. El número total de resoluciones analizadas es de setenta y cuatro (74), las cuales fueron emitidas por los órganos resolutivos de Lima, Ancash - Sede Chimbote, Arequipa, Cajamarca, Cusco, Ica, Junín, La Libertad, Lambayeque, Loreto, Piura, Puno, San Martín y Tacna durante los años 2022 y 2023. Luego, se registraron, a través de las fichas de análisis, los criterios aplicables para la determinación de responsabilidad de las entidades financieras, que abarca el examen de los parámetros de seguridad y monitoreo implementados por el proveedor, la gestión de alertas y los mecanismos de bloqueo de los instrumentos de pago, las medidas correctivas ordenadas y las sanciones impuestas, ello, a fin de determinar la predictibilidad de dichos pronunciamientos a nivel nacional.

Por otro lado, respecto del análisis de los criterios o sentencias emitidos por instituciones de otros países, se recopiló la siguiente información a través de las fichas de observación: en el caso de Chile se analizaron cuatro sentencias emitidas por los Juzgados de Policía Locales, una sentencia emitida en un proceso de protección y una resolución emitida como resultado de un procedimiento voluntario colectivo entre el SERNAC y una entidad financiera; en el caso de Colombia se analizó un caso emitido en última instancia por la Corte Suprema de Justicia; y, en el caso de España, se analizaron seis sentencias emitidas por las Audiencias Provinciales.

Cabe indicar, que también se efectuó la recopilación de las disposiciones normativas establecidas en cada país respecto de la materia objeto de estudio, así, en el caso peruano, se registró, a través de las fichas de observación, las disposiciones contenidas en el Código de Protección y Defensa del Consumidor, en el Reglamento de Tarjetas de Crédito y Débito y en el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad. En el caso de Chile, se analizó la Ley 20.009 que establece el régimen de limitación de responsabilidad para titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude; por el lado colombiano, la Circular Básica Jurídica (C.E. 029/14) que contiene las normas relacionadas a la seguridad y calidad del servicio que prestan las entidades bancarias; y, finalmente, en el caso de España, el Real Decreto Ley 19/2018 del 23 de

noviembre de 2018, de servicios de pago y otras medidas urgentes en materia financiera. Debe precisarse que, durante la recolección de datos, nos centramos en aquellas disposiciones que desarrollan las medidas que deben adoptar las entidades financieras ante casos de operaciones no reconocidas efectuadas por internet.

3.4 Análisis de datos y categorías

La información recabada fue analizada utilizando la técnica del análisis de contenido. La legislación nacional, así como la jurisprudencia relacionada con el tratamiento de las operaciones bancarias fraudulentas fue analizada descomponiendo los pronunciamientos o criterios emitidos por los órganos resolutivos, con base en las siguientes categorías:

- La responsabilidad del usuario o consumidor titular de los instrumentos de pago.
- La carga de la prueba en los procedimientos por operaciones no reconocidas.
- Las medidas de seguridad implementadas por las entidades financieras.
- Validación de operaciones en canales virtuales: aspectos clave de autenticación.
- Valoración del patrón de consumo.
- Gestión de alertas generadas por el sistema de monitoreo de operaciones.
- Medidas correctivas.
- Sanción.

Dicho análisis, permitió identificar los criterios similares o disímiles por categoría de los pronunciamientos emitidos por los órganos resolutivos del Indecopi a nivel nacional, a fin de determinar si los mismos son predictivos. De otro lado, se analizó la legislación y jurisprudencia de Chile, Colombia y Brasil, identificando los criterios adoptados para el análisis de responsabilidad de la entidad bancaria, así como las sanciones y medidas adoptadas para proteger a los consumidores, a fin de extraer lecciones o recomendaciones para mejorar la predictibilidad de los pronunciamientos emitidos por el Indecopi.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1 Resultados

4.1.1 Objetivo Específico N.° 1

A. Sobre la responsabilidad del usuario o consumidor titular de los instrumentos de pago

El ORPS de Loreto[1] señala que, el hecho de que un consumidor no sea diligente en el uso de su tarjeta al haber proporcionado información confidencial sobre la misma no enerva la obligación de la entidad financiera de cumplir con las garantías legales que regulan su servicio, como son las medidas de seguridad frente a las operaciones efectuadas por los consumidores. Este razonamiento es respaldado por el ORPS de Huaraz[2], que indica que, en los casos de rechazo de una transacción por el consumidor, la responsabilidad de demostrar la autenticación y registro de las operaciones corresponde a la entidad financiera sin admitir excepciones.

Por su parte, la SPC[3] en un pronunciamiento ha señalado que, más allá de la conducta negligente de los consumidores, la autoridad administrativa debe verificar si la entidad financiera cumple con su deber de monitorear las operaciones de sus clientes, pues dicha obligación debe garantizarse al tratarse de una exigencia legalmente impuesta por la normativa sectorial. En la resolución citada, el consumidor brindó información a un tercero sobre su tarjeta de crédito, lo que ocasionó que se efectúen transacciones por comercio electrónico, por lo que hubo un actuar negligente del consumidor. No obstante, la autoridad administrativa, más allá de evaluar si el consumidor compartió información sensible sobre su tarjeta, debe analizar si el proveedor aplicó sus sistemas de monitoreo en la realización de las operaciones

1 Resolución Final 009-2023/PSO-INDECOPI-LOR
2 Resolución 1-2021/PSO-INDECOPI-HRZ
3 Resolución 12-2021/SPC-INDECOPI

supuestamente efectuadas por el consumidor. Por tanto, en los casos en los que se advierta que el consumidor obró de manera negligente y entregó información confidencial a un tercero sobre el producto financiero del que es titular, ello podría ser analizado como un supuesto de ruptura del nexo causal solo cuando se verifique la validación de los mecanismos de seguridad existentes.

De lo anterior se verifica que existe un criterio uniforme entre los órganos resolutivos del Indecopi de no considerar la conducta negligente del consumidor en el uso de la tarjeta como un factor determinante para exonerar de responsabilidad a la entidad bancaria; ya que, la autoridad debe verificar si el proveedor cumplió con adoptar las medidas de seguridad legal y contractualmente establecidas durante la ejecución de las operaciones bancarias cuestionadas. Este criterio, a nuestro parecer, enfatiza la responsabilidad de las entidades financieras en garantizar la seguridad en las transacciones bancarias y constituye un criterio tuitivo en favor de los consumidores.

B. Sobre la carga de la prueba en los procedimientos por operaciones no reconocidas

En materia de protección al consumidor, los órganos resolutivos del Indecopi adoptaron el criterio de la Sala de Defensa de la Competencia n.° 2, actualmente SPC[4], que establece que la carga de la prueba, en los casos de operaciones bancarias no reconocidas, recae en el proveedor (entidad financiera). Esto se debe a que es el proveedor quien posee más información y medios para demostrar el procesamiento válido de las operaciones y la adopción de medidas de seguridad.

Partiendo de esta premisa, el ORPS de La Libertad[5] indica que, en mérito del principio proconsumidor, corresponde al consumidor acreditar la existencia y cuantía de las operaciones, y al proveedor demostrar su correcta ejecución, autenticación y que las operaciones forman parte del patrón de comportamiento del consumidor, para

[4] Resolución 270- 2008/TDC-INDECOPI
[5] Resolución 4-2023/PSO-INDECOPI-LAL

desvirtuar la existencia de patrones de fraude. En la misma línea, el ORPS de Tacna[6] respalda la teoría de las cargas dinámicas o *favor probationis* y propone trasladar la carga probatoria a la parte en mejores condiciones para producir la prueba. En el contexto de operaciones bancarias no reconocidas, el proveedor está en una posición más ventajosa para generar pruebas, lo que justifica la necesidad de flexibilizar la carga de la prueba[7].

Estos criterios encuentran respaldo en el artículo 23 del Reglamento de Tarjetas de Crédito y Débito (2013) que establece la responsabilidad del proveedor de demostrar la correcta autenticación y registro de la transacción frente al rechazo o reclamo del consumidor.

En conclusión, el criterio general de los órganos resolutivos a nivel nacional consiste en que la carga de probar el correcto y válido procesamiento de las operaciones y la adopción de medidas de seguridad recae en el proveedor, al estar en una mejor posición y contar con más información que el usuario.

C. Evaluación de las medidas de seguridad implementadas por las entidades financieras

Del análisis de las resoluciones materia de evaluación, se verifica que los órganos resolutivos del Indecopi presentan discrepancias en su enfoque al abordar si las medidas de seguridad implementadas por las entidades financieras fueron idóneas. Algunos órganos, como el ORPS de Huaraz, el ORPS de Junín, el ORPS de Puno, el ORPS de Tacna, el ORPS de Loreto, el ORPS de Piura, el ORPS de San Martín, el ORPS de Lima Norte, la CPC de Junín, la CPC de La Libertad, la CPC de Lambayeque, la CPC de Tacna, la CC1 y el ORPS de La Libertad optan por analizar en primer lugar la validez de las operaciones, que consiste en verificar si se llevó a cabo la validación de la identidad del usuario mediante el ingreso de datos confidenciales, como el uso de claves o firmas, u otros métodos de autenticación; una vez superada esta fase,

6 Resolución 144-2023/PSO-INDECOPI-TAC
7 Resoluciones 0590-2022/PSO-INDECOPI-AQP, 0339-2023/CPC-INDECOPI-JUN, 0349-2023/CPC-INDECOPI-JUN, 0037-2023/CPC-INDECOPI-LAL, 0828-2022/CPC-INDECOPI-LAL y 0058-2023/CPC-INDECOPI-TAC

proceden a examinar si las operaciones se ajustan al patrón de consumo histórico del usuario.

Siguiendo esa línea, la CPC del Indecopi Lima Norte[8] establece un proceso de evaluación que abarca dos aspectos: (i) verificar si las transacciones en cuestión se llevaron a cabo cumpliendo los requisitos de validez, lo cual implica validar la identidad del usuario a través de métodos de autenticación, así como el correcto registro de la tarjeta de débito o crédito; y, (ii) determinar si las operaciones cuestionadas y autorizadas por la entidad financiera se ajustan al historial de transacciones previas del denunciante, es decir, si están en línea con el patrón de consumo habitual del usuario. De manera similar, la CPC de Ica[9] considera la acreditación de la validez de las operaciones como un filtro inicial; luego del cual, se procede a evaluar el cumplimiento del deber de monitoreo y detección de operaciones inusuales.

En el caso específico del ORPS de Huaraz, el análisis se centra en evaluar la documentación presentada por la entidad financiera para acreditar la validez de las operaciones. Si esta documentación no se proporciona, la denuncia puede ser declarada fundada[10] sin abordar el cumplimiento de las medidas adicionales de monitoreo o seguridad, como la identificación de patrones de fraude o comportamientos no habituales en el usuario. Siguiendo esa línea, otros órganos, como el ORPS de Tacna y ORPS 2, declaran fundada la denuncia directamente si las operaciones no cumplen con los requisitos de autenticación o validez.

En contraposición con el enfoque anterior, la SPC[11] establece que, para que la autoridad administrativa concluya que una operación fue realizada en forma válida, y se exima de responsabilidad a la entidad financiera, se debe verificar, en primer lugar, si las operaciones eran inusuales según el análisis sistemático de la información histórica de las transacciones del cliente. Posteriormente, se debe efectuar un análisis enfocado en la verificación de la concurrencia de los requisitos de

8 Resoluciones 488-2023 y 298-2023/CPC-ILN
9 Resolución 85-2023/CPC-INDECOPI-ICA
10 Resolución 23-2022/PSO-INDECOPI-HRZ
11 Resolución 2063-2018/SPC-INDECOPI y 2144-2023/SPC-INDECOPI

validación de identidad del usuario u otros mecanismos de autenticación, como la activación de la tarjeta, el uso de canales autorizados y la correcta introducción de la clave secreta. En caso se demuestre que las operaciones poseen características sospechosas, su realización debe generar una alerta oportuna en su sistema y se deberán adoptar las medidas oportunas y conducentes a impedir la ocurrencia de cargos adicionales.

En ese marco, el ORPS de Puno[12] sigue el criterio de la SPC al analizar, en primer lugar, el patrón de consumo habitual del titular de la tarjeta, a fin de determinar si la entidad financiera debió tomar medidas de seguridad adicionales para alertar y evitar la realización de transacciones que no se ajustan al comportamiento habitual de consumo del cliente.

Por su lado, los ORPS de Cusco, ORPS de Ica, ORPS de Ancash Sede Chimbote, CPC de Ancash Sede Chimbote, CPC de Cajamarca, CPC de Cusco, ORPS de Cajamarca y CPC de Puno adoptan un enfoque similar, ya que, en primer lugar, verifican si la entidad financiera llevó a cabo el monitoreo y la detección de operaciones inusuales, ello incluye evaluar los mecanismos de comunicación inmediata al usuario sobre posibles operaciones fraudulentas, considerando la generación de alertas de consumo inusual o sospechoso; y, posteriormente, analizan si las operaciones fueron realizadas de manera válida, es decir, cumpliendo con los requisitos de autenticación establecidos por cada entidad financiera.

Es relevante destacar el pronunciamiento específico del ORPS de Cusco que, en un caso particular[13], realizó la evaluación de la adopción de medidas de seguridad y determinó que la operación cuestionada no superó las medidas de detección de patrones de fraude, lo que resultó en que la denuncia sea declarada fundada sin la necesidad de evaluar el segundo filtro. Este mismo criterio es compartido en algunos pronunciamientos por el ORPS de Cajamarca[14], que privilegia el análisis

12 Resolución 72-2023-PSO-INDECOPI-PUN
13 Resolución 432-2023/PSO-INDECOPI-CUS
14 Resolución 7-2022/PSO- INDECOPI-CAJ

del patrón de consumo del usuario; por lo que, si la operación es inusual o no concuerda con el patrón histórico del consumidor, considera innecesario verificar la correcta autenticación de la operación.

En resumen, los órganos resolutivos muestran diferentes enfoques al evaluar la idoneidad de las medidas de seguridad en casos de operaciones bancarias no reconocidas. Algunos priorizan el análisis de validez de las operaciones, declarando fundada la denuncia si no se cumplen los requisitos de autenticación. Otros, utilizan este criterio como un primer filtro, para luego examinar el historial de transacciones en busca de patrones de fraude. En contraste, ciertos órganos priorizan el análisis del comportamiento habitual del consumidor a fin de detectar patrones de fraude, procediendo a evaluar la validez de las operaciones solo si se supera este primer filtro.

Esta variabilidad de criterios puede impactar significativamente en el resultado final de los casos, ya que el orden en la aplicación de estos filtros, en algunos casos, influye en la determinación de la responsabilidad del proveedor. En ese sentido, se sugiere que los órganos resolutivos adopten un enfoque más integral que considere tanto el análisis de la validez de las operaciones como la adopción de medidas de monitoreo y detección de operaciones inusuales implementadas por las entidades financieras.

En este contexto, consideramos que el enfoque más adecuado es realizar un análisis inicial de la autenticación válida de las operaciones, seguido por la evaluación del patrón de consumo del usuario. Esto se debe a que la evaluación del comportamiento habitual del consumidor en la ejecución de las operaciones constituye un análisis ex post de la operación, es decir, se lleva a cabo después de la ejecución de la primera operación que se considera no habitual o fraudulenta. Sin embargo, para que este análisis sea efectivo, las operaciones deben haber superado correctamente el proceso de validación, que incluye el correcto enrolamiento y autenticación en la ejecución de las operaciones.

Es importante destacar que, si las operaciones no fueron válidamente procesadas o autenticadas, esto podría indicar un defecto o falla en los sistemas de la entidad. En tal caso, la responsabilidad recaería únicamente en el banco, ya que, al tener el deber de custodia de los fondos de sus usuarios, es fundamental que asegure el óptimo funcionamiento de sus sistemas para evitar la ejecución de operaciones no autorizadas por el usuario.

D. Validación de operaciones en canales virtuales: aspectos clave de autenticación

Al examinar este aspecto, se observa que el ORPS 2, el ORPS de Ica, el ORPS de Tacna y la CC1 establecen inicialmente que el titular de una tarjeta tiene la libertad de utilizarla en diversos canales de atención, como cajeros automáticos, Banca por Internet, Banca Móvil y comercios afiliados, siempre que posea una línea de crédito o fondos suficientes[15]. En ese marco, las operaciones realizadas a través de estos canales pueden clasificarse en "con tarjeta presente" o "con tarjeta no presente", y corresponde a las entidades financieras implementar medidas de seguridad específicas[16] para asegurar la validez de estas operaciones.

En las operaciones "con tarjeta presente", la tarjeta debe estar físicamente presente y pasar por un terminal de venta o lector de banda magnética o chip, requiriéndose la firma electrónica o la suscripción de la orden de pago para autorizar la transacción y/o el ingreso de datos confidenciales u otros mecanismos de autenticación. En contraste, las operaciones "con tarjeta no presente" no requieren la presencia física de la tarjeta, ya que la autorización se efectúa por medios digitales; en estos casos, se necesita el ingreso de datos impresos en el plástico, como el número de tarjeta, fecha de vencimiento, código CVV *(Card Verification Value o CVV)* o claves digitales.

Por tanto, para que las entidades financieras carguen válidamente el importe de las operaciones en las cuentas vinculadas a las tarjetas,

[15] Resolución 1725-2022 (ORPS n.° 2)
[16] Resoluciones 121-2023/PSO-INDECOPI-ICA, 146-2023/PSO-INDECOPI-TAC, 1954-2023 (CPC n.° 1) y 1775-2023 (CPC n.° 1)

deben acreditar, en el caso de las operaciones "con tarjeta no presente", que estas fueron autorizadas a través de medios electrónicos y/o firmas electrónicas. En cuanto a las operaciones "con tarjeta presente", deben demostrar la firma del cliente en las órdenes de pago o el ingreso de la clave secreta y/o información confidencial.

En concordancia con lo anterior, el ORPS de Tacna[17] propone efectuar el siguiente análisis al momento de verificar si la entidad financiera cumplió con las medidas de autenticación correspondientes: (i) verificar la habilitación de la tarjeta para operaciones por el canal de internet, (ii) verificar si el monto de la operación se encontraba dentro del límite autorizado; y, (iii) analizar si hubo autorización del usuario para efectuar las operaciones cuestionadas.

La Sala[18] resalta la importancia de verificar en el contrato la habilitación del producto para operaciones en línea y la concurrencia de requisitos para su validación, como la activación de la tarjeta y el ingreso de la clave secreta o dinámica predeterminada. En este contexto, el ORPS de Piura[19] subraya que las operaciones por internet requieren del consentimiento previo del titular y que, una vez superado este filtro, se deben analizar los medios probatorios que sustenten la validez de las operaciones, como los reportes de los sistemas presentados por las entidades financieras.

En relación con el análisis de los reportes de sistemas presentados por las entidades financieras, la SPC[20] considera importante que dichos reportes detallen información clave, como el número de cuenta, fecha y hora de la operación, monto, nombre del comercio, código de respuesta y modo de ingreso. La CPC de Lambayeque[21] resalta la importancia de la inclusión de la fecha y hora del inicio de sesión (la cronología de las operaciones), la confirmación de la operación, el producto implicado, el número de transacciones y los códigos correspondientes. En ese sentido,

17 Resolución 146-2023/PSO-INDECOPI-TAC
18 Resolución 1648-2017/SPC-INDECOPI
19 Resolución 501-2023/PSO-INDECOPI-PIU
20 Resolución 2144-2023/SPC
21 Resolución 447-2022/CPC-INDECOPI-LAM

la falta de presentación de los reportes que demuestren la correcta realización de las operaciones permite colegir que estas no fueron efectuadas válidamente[22].

Es importante destacar el grado de fiabilidad que los órganos resolutivos del Indecopi otorgan a los reportes generados por los sistemas de la entidad financiera, pues no se cuestiona su posible alteración o si los códigos mencionados en estos acreditan de forma inequívoca el correcto procesamiento de las operaciones cuestionadas.

De la revisión de las resoluciones, también se debe mencionar que muchos de los órganos resolutivos no evalúan el cumplimiento de las disposiciones establecidas en el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, pese a que las disposiciones relativas a los requisitos de autenticación contenidos en dicha norma entraron en vigor desde el 2 de julio de 2022. Así, se observa que, en lugar de aplicar la normativa vigente, continúan aplicando normativas derogadas[23] u optan por no evaluar el cumplimiento de los mecanismos de seguridad contemplados en la citada normativa[24], analizando únicamente el cumplimiento de las obligaciones contenidas en el Reglamento de Tarjetas de Crédito y Débito.

En conclusión, la validez de las operaciones en canales virtuales implica la correcta implementación de medidas de seguridad durante el enrolamiento y la autenticación para ejecutar operaciones, las cuales varían de acuerdo con el tipo de canal utilizado. Para demostrar la validez de las operaciones, las entidades financieras deben presentar documentación diversa, como reportes detallados o capturas de pantalla de sus sistemas, en los que se verifique la afiliación al canal a través del cual se realizan las operaciones, el correcto enrolamiento del usuario al

22 Resolución 23-2022/PSO-INDECOPI-HRZ
23 Resoluciones 24-2023/PSO-INDECOPI-ICA y 50-2023/PSO-INDECOPI-JUN.
24 Resoluciones 3-2023-PSO-INDECOPI-CHT, 10-2023-PSO-INDECOPI-CHT, 77-2023-CPC-INDECOPI-PUN, 85-2023-INDECOPI-ICA, 102-2023-PSO-INDECOPI-PUN, 121-2023-PSO-INDECOPI-ICA, 136-2023-PSO-INDECOPI-TAC, 144-2023-PSO-INDECOPI-TAC, 146-2023-PSO-INDECOPI-ICA, 172-2023-PSO-INDECOPI-ICA, 179-2023-INDECOPI-CUS, 195-2023-INDECOPI-CUS, 246-2023-ILN-PSO, 274-2023-PSO-INDECOPI-SAM, 302-2023-PSO-INDECOPI-CUS, 303-2023-PSO-INDECOPI-CUS, 323-2023-PSO-INDECOPI-LAM, 339-2023-INDECOPI-JUN, 349-2023-INDECOPI-JUN, 363-2023-INDECOPI-CUS, 412-2023-PSO-INDECOPI-CUS, 419-2023-PSO-INDECOPI-CUS, 432-2023-PSO-INDECOPI-CUS, 501-2023-PSO-INDECOPI-PIU, 575-2022-PSO-INDECOPI-JUN, 620-2022-PSO-INDECOPI-JUN, 1754-2022 (ORPS n.° 2), 1773-2023 (CPC n.° 1) y 1775-2023 (CPC n.° 1).

canal digital, la activación de métodos de autenticación reforzada, y la correcta ejecución de dichos métodos de autenticación para validar las operaciones, como puede ser la biometría, u otro factor de autenticación. La responsabilidad de la entidad bancaria en este punto se determina en función de su capacidad para demostrar el correcto cumplimiento de sus obligaciones, por lo que, si el proveedor no presenta la información que acredite que las operaciones fueron válidamente efectuadas, la consecuencia lógica es que se declare fundada la denuncia.

Sobre este punto, existe la necesidad de que se establezca un criterio unificado que señale los aspectos que se deben verificar a fin de determinar si las operaciones se efectuaron o no de forma válida. Siguiendo los criterios anteriormente expuestos, consideramos importante que los órganos resolutivos evalúen los siguientes aspectos al analizar la validez de las operaciones efectuadas por Banca Móvil o Banca por Internet: (i) la condición activa de la tarjeta al momento de las operaciones; (ii) la afiliación o habilitación del canal a través del cual se realizaron las operaciones, y la activación de las claves digitales o biometría para validar las operaciones; (iii) el correcto enrolamiento del usuario a la Banca por Internet o Banca Móvil, que consiste en la verificación de la identidad del usuario, la implementación de las medidas necesarias para reducir la posibilidad de suplantación, así como la generación de credenciales y su asignación al usuario.

Además, según el Reglamento de Gestión de la Seguridad de la Información y la Ciberseguridad (2021) se debe verificar la implementación de la autenticación reforzada para operaciones efectuadas por canal digital, para tal efecto, se debe analizar: (iv) la utilización de, por lo menos, 2 factores de autenticación que correspondan a categorías distintas y sean independientes uno del otro; dichos factores puede consistir en la generación, remisión e ingreso de claves dinámicas o token (las cuales pueden ser enviadas a través de mensajes de texto (SMS) al celular o al correo electrónico afiliado

previamente por el consumidor[25]), o el reconocimiento biométrico[26] para confirmar y concretar las operaciones. En casos de validación biométrica, se deberá acreditar la afiliación del consumidor al sistema biométrico[27]; salvo que se trate de una operación exenta de utilizar la autenticación reforzada (artículo 20 del Reglamento); (v) la implementación de un control ante ataques de hombre en el medio, que puede incluir un código generado mediante métodos criptográficos, cuyo uso debe ser por única vez; y, (vi) la notificación al usuario de los datos de la operación exitosa.

En el caso de las operaciones realizadas en comercios electrónicos (*e-commerce*), la lectura del Reglamento de Gestión de la Seguridad de la Información y Ciberseguridad sugiere que estas operaciones no están exentas de implementar la autenticación reforzada para su validez. Sin embargo, la falta de precisión en el reglamento podría llevar a criterios distintos por parte de los órganos resolutivos. En este sentido, es necesario que Indecopi adopte un criterio uniforme para determinar si las operaciones efectuadas a través de comercios electrónicos deben aplicar la autenticación reforzada. Sin perjuicio de ello, consideramos que, en estos casos, será esencial verificar si en el contrato se estipuló la posibilidad de realizar operaciones en comercios electrónicos o la efectiva habilitación del producto (tarjeta) para efectuar compras a través de comercios electrónicos desde páginas web y/o aplicaciones de dispositivos móviles distintos a los provistos por la entidad financiera[28].

E. Análisis y valoración del patrón de consumo

E.1 Antigüedad de los estados de cuenta para determinar patrones de fraude

Con el objetivo de examinar el patrón de consumo del usuario, es común que los órganos resolutivos soliciten los estados de cuenta del

[25] Resolución 146-2023/PSO-INDECOPI-ICA
[26] Resolución 10-2023/PSO-INDECOPI-CHT y 171-2023/PSO-INDECOPI-ICA
[27] Resolución 1954-2023 (CPC n.° 1)
[28] Resolución 58-2023/CPC-INDECOPI-TAC

consumidor denunciante. Sin embargo, al analizar las resoluciones materia de investigación, se evidencia que los órganos resolutivos del Indecopi adoptan diversos enfoques al solicitar y evaluar esta información.

Un criterio predominante consiste en requerir los estados de cuenta del consumidor denunciante con al menos 6 meses de antelación a la operación no reconocida[29]. No obstante, de la revisión de los pronunciamientos, se verifica que no existe un estándar o criterio uniforme al momento de requerir esta información, ya que algunos órganos resolutivos solicitan y analizan los estados de cuenta emitidos con una anticipación de 3 meses[30], 4 meses[31], 5 meses[32], 7 meses[33], 12 meses[34], 1 año y 2 meses[35], 1 año y 5 meses[36] e incluso 3 años[37].

En ese contexto, al evidenciarse una discrepancia de criterios entre los órganos resolutivos al requerir los estados de cuenta para analizar patrones de fraude, resulta imperativo llegar a un consenso general para establecer un periodo razonable. Dado que el patrón de consumo tiene una naturaleza subjetiva y está sujeto a las características económicas del usuario, es susceptible de cambiar a lo largo de su vida; por consiguiente, no resultaría óptimo evaluar información demasiado antigua; de otro lado, considerar los estados de cuenta de solo uno o dos meses resultaría insuficiente, ya que en un periodo tan corto no podría formarse un auténtico patrón de consumo.

En este sentido, y en línea con el criterio mayoritario de los órganos resolutivos, consideramos que la información solicitada debe abarcar un periodo de al menos seis meses y como máximo un año de antelación a la ejecución de la operación no reconocida, ya que este periodo de tiempo es suficiente para observar la formación del patrón de

29 Resolución 63-2023-INDECOPI-ICA
30 Resolución 1754 2022 (ORPS n.° 2)
31 Resolución 0590-2022/PSO-INDECOPI-AQP
32 Resolución 0073-2023/PSO-ILN
33 Resolución 274-2023/PSO-INDECOPI-SAM
34 Resoluciones 146 2023/PSO-INDECOPI-ICA, 528 2022/PSO-INDECOPI-JUN, 9-2023/PSO-INDECOPI-LOR, 26-2023/CPC-INDECOPI-TAC, 37-2023/CPC-INDECOPI-LAL y 136 2023/PSO-INDECOPI-TAC
35 Resolución 0105-2023/CPC-INDECOPI-TAC
36 Resolución 598-2022/PSO-INDECOPI-JUN
37 Resolución 065-2022/CPC-INDECOPI-PUN

consumo del usuario, al mismo tiempo que toma en consideración que este no debe ser muy antiguo.

E.2 Criterios para identificar operaciones que no corresponden al comportamiento habitual del consumidor

En las resoluciones bajo análisis, se aborda la compleja tarea de analizar la detección de operaciones inusuales realizadas con tarjetas de crédito y débito. Este análisis implica evaluar, en principio, si las operaciones materia de cuestionamiento se encuentran dentro de los patrones típicos de comportamiento de los consumidores.

A fin de evaluar si las operaciones se encuentran dentro del comportamiento habitual de consumo del usuario se consideran diversos factores. Al realizar un examen integral de las resoluciones objeto de investigación, encontramos que la selección de los parámetros o factores para determinar la habitualidad de una operación varía dependiendo del criterio de cada órgano resolutivo. Por consiguiente, los diversos parámetros o factores considerados por los órganos resolutivos, de manera resumida, son los siguientes:

Canal, según el Reglamento de Tarjetas de Crédito y Débito el canal es cualquier medio físico o virtual al que acceden los usuarios para efectuar operaciones monetarias (banca por internet o banca móvil, cajeros automáticos, terminales de punto de venta o POS, agentes, agencias, entre otros). Así, se podría considerar atípica una operación si el consumidor la realiza a través de un canal no utilizado anteriormente[38].

Frecuencia o continuidad, se examina la frecuencia y el número de operaciones realizadas en periodos cortos de tiempo. La continuidad

[38] Los órganos resolutivos que utilizan dicho criterio son: el ORPS de Tacna, ORPS de Huaraz, ORPS de Cajamarca, ORPS de Ica, ORPS de Cusco, ORPS de Puno, ORPS de Arequipa, ORPS de Indecopi Lima Norte, ORPS de Ancash Sede Chimbote, CPC de Cusco, CPC La Libertad, CPC Tacna, CPC Cajamarca.

de las transacciones, especialmente cuando se efectúan en sucesión, puede indicar un comportamiento inusual[39].

Tipo de moneda, se analiza si la operación se realizó en dólares o soles, considerando este aspecto como un factor relevante para la detección de operaciones sospechosas[40].

Lugar o establecimiento, en operaciones con tarjeta presente, se verifica si las transacciones se realizaron en distintas agencias o ventanillas del mismo banco o en diversas ciudades de manera simultánea, lo cual podría ser una señal de fraude. En el caso de operaciones con tarjeta no presente, se verifica si el consumidor efectuó consumos con anterioridad en los comercios electrónicos a través de los cuales se ejecutaron las operaciones cuestionadas[41].

Límite operacional, se considera el importe máximo permitido por día para operaciones en canales digitales, cajeros automáticos, entre otros, para detectar cualquier exceso que pueda ser indicativo de fraude[42].

Horario, el horario en que se realizan las operaciones también se toma en cuenta, considerando las operaciones realizadas en horarios inusuales (de noche o madrugada) como un factor de sospecha[43].

Tipo de operación, se examina la naturaleza de la operación, que puede ser un giro, una transferencia (diferida o inmediata), un depósito, un retiro, el pago de servicios, o el uso de billeteras electrónicas como Yape o Plin, entre otras. Dado que cada tipo de operación puede exigir distintas validaciones y comportamientos, se podría clasificar la

39 Los órganos resolutivos que utilizan dicho criterio son: ORPS de Junín, ORPS de Cajamarca, ORPS de Ica, ORPS de Puno, ORPS de Arequipa, ORPS Indecopi Lima Norte, ORPS La Libertad, ORPS Ancash Sede Chimbote, CPC de Cusco, CPC de Ica, CPC de Junín, CPC de La Libertad, CPC de Tacna y CPC de Cajamarca.

40 Los órganos resolutivos que utilizan dicho criterio son: ORPS de Cajamarca y CPC de Cusco.

41 Los órganos resolutivos que utilizan dicho criterio son: ORPS Junín, ORPS de Tacna, ORPS de Ica, ORPS de Puno, ORPS de Indecopi Lima Norte, ORPS de La Libertad, CPC de Tacna y CPC de Cajamarca.

42 Los órganos resolutivos que utilizan dicho criterio son: ORPS de Junín.

43 Los órganos resolutivos que utilizan dicho criterio son: ORPS de Junín.

operación como atípica si el consumidor realiza transacciones que no concuerdan con las efectuadas previamente[44].

Importe, la cuantía de las operaciones desempeña un papel fundamental en la identificación de transacciones fraudulentas. Su análisis requiere una revisión minuciosa de los montos involucrados en las transacciones del consumidor, evaluando su coherencia con el historial de consumo previo. Este análisis puede realizarse de la siguiente manera:

Por importe individual, el órgano resolutivo puede realizar un análisis individual de cada operación cuestionada y compararla con las operaciones de mayor valor efectuadas a lo largo del historial de consumos anteriores del denunciante, ya que, si las operaciones denunciadas superan los montos habituales o máximos registrados en el historial del consumidor, podríamos encontrarnos ante patrones de fraude[45].

En algunos casos, se realiza una sumatoria de las operaciones fraudulentas para determinar si el monto total se encuentra dentro del rango de gasto esperado o si es significativamente superior[46]. También, se puede analizar el importe o monto máximo consumido por día en periodos anteriores y compararlo con la sumatoria de las operaciones materia de cuestionamiento[47].

También se puede considerar el importe global de operaciones por mes o periodo, que implica contrastar el monto de las operaciones con el promedio mensual de consumo del denunciante. Si los montos

44 Los órganos resolutivos que utilizan dicho criterio son: ORPS de Junín, ORPS de Huaraz, ORPS de Cajamarca, ORPS de Puno, CPC de La Libertad y CPC de Tacna.

45 Los órganos resolutivos que utilizan dicho criterio son: ORPS Junín, ORPS de Tacna, ORPS de Cajamarca, ORPS de Ica, ORPS de Cusco, ORPS de Puno, ORPS de Arequipa, ORPS de Indecopi Lima Norte, ORPS de La Libertad, ORPS de Ancash Sede Chimbote, CPC de Cusco, CPC de Ica, CPC de Junín, CPC de La Libertad, CPC de Tacna y CPC de Cajamarca.

46 Los órganos resolutivos que utilizan dicho criterio son: ORPS de Junín, ORPS de La Libertad, ORPS de Indecopi Lima Norte y CPC n.° 1.

47 Los órganos resolutivos que utilizan dicho criterio son: ORPS de Cajamarca, ORPS de Arequipa, ORPS de Indecopi Lima Norte, ORPS de La Libertad y ORPS 2.

superan límites establecidos o no concuerdan con el comportamiento histórico, se interpreta como un indicador de transacción atípica[48].

En este punto, es importante mencionar que el ORPS de Huaraz y la CC1[49] señalan que, a efectos de verificar la habitualidad de una operación, la entidad financiera debe efectuar un análisis sistemático de la información histórica del cliente, contrastando integralmente las operaciones cuestionadas con el total de transacciones realizadas anteriormente por el denunciante. Este análisis no puede basarse en un factor o criterio aislado, sino que debe considerar factores como el importe de las operaciones, los canales utilizados, la frecuencia de las transacciones, país de consumo, tipos de comercio, entre otros.

Complementando la idea anterior, el ORPS de Tacna, la CPC de Junín y el ORPS de Cajamarca[50] destacan que la revisión del historial de consumo del cliente debe considerar la libertad que tienen los consumidores para realizar transacciones en diversos canales y por montos variables. Por tanto, imponer restricciones indebidas a esta libertad no solo podría restringir la autonomía de los consumidores, sino también generar complicaciones y costos adicionales para las entidades financieras. En consecuencia, la evaluación de operaciones inusuales debe realizarse mediante un análisis completo y objetivo, evitando la aplicación de criterios restrictivos que puedan limitar las transacciones financieras legítimas de los clientes. Por lo tanto, el patrón de consumo asociado al producto financiero se determinará mediante la comparación integral entre las operaciones cuestionadas y las transacciones realizadas previamente por los denunciantes, considerando diversos factores o criterios de evaluación, siendo insuficiente concluir que una operación es inusual basándose en un solo factor o criterio aislado.

Sin perjuicio de lo anterior, el ORPS de Tacna y la SPC[51] [52] argumentan que la clasificación de una operación como sospechosa debe

48 Los órganos resolutivos que utilizan dicho criterio son: ORPS de Cajamarca, ORPS de Cusco, ORPS de Arequipa, ORPS del Indecopi Lima Norte, CPC de Cusco, CPC de La Libertad y CPC de Junín.
49 Resoluciones 044-2023/PSO-INDECOPI-HRZ y 1775-2023 (CPC n.° 1)
50 Resolución 6-2022/PSO-INDECOPI-CAJ, 146-2023/PSO-INDECOPI-TAC, 339-2023/CPC-INDECOPI-JUN y 349-2023/CPC-INDECOPI-JUN
51 Resoluciones 2144-2023 y 2006-2023/SPC

regirse por un criterio objetivo, como el registro de los consumos máximos totales realizados por cada cliente en meses anteriores. Además, para determinar si es necesario generar una alerta por consumo inusual, se deberá analizar la totalidad de los consumos efectuados por el titular de la tarjeta durante el período en cuestión, teniendo en cuenta tanto las operaciones denunciadas como las demás transacciones realizadas con cargo a las cuentas del cliente.

Al respecto, la CPC de Puno y la CPC de Cusco[53] subrayan que la formación del patrón de consumo está influenciada por aspectos individuales de cada cliente, por lo que no se puede concluir que el procesamiento de una operación con características específicas sea atípico para todos los consumidores. En ese sentido, consideran que un criterio objetivo para determinar el comportamiento habitual de consumo de un usuario deberá tener en cuenta el monto de las operaciones que el consumidor solía transferir usualmente con el producto objeto de la denuncia.

Por otra parte, es importante mencionar en este punto el criterio de algunos órganos resolutivos al analizar casos en los que la operación cuestionada se llevó a cabo a través de un canal que no había sido utilizado previamente por el consumidor. Por ejemplo, el ORPS 2 argumenta que la falta de uso de un canal específico o la realización de operaciones por montos diferentes a los previamente efectuados no debe considerarse automáticamente como indicativo de comportamiento inusual o sospechoso por parte del consumidor, salvo que existan restricciones específicas[54]. En concordancia con esta perspectiva, el ORPS de Lambayeque sostiene que es posible utilizar cualquier medio de pago para realizar una primera operación en el día, en un canal o por un monto no registrado anteriormente, sin que esto sea considerado como inusual[55].

52 Resolución 136-2023/PSO-INDECOPI-TAC
53 Resolución 076-2023/CPC-INDECOPI-PUN y 549-2022/CPC-INDECOPI-CUS
54 Resolución 1725 2022 (ORPS n.° 2)
55 Resolución 562 2022/PSO-INDECOPI-LAM

De manera similar, el ORPS de Junín, la SPC, la CPC de Puno y la CPC de Cusco[56] [57] coinciden en que la falta de utilización de un canal específico, la ejecución de operaciones por montos diferentes, entre otras características, no deben ser interpretadas automáticamente como señales de comportamiento inusual por parte del consumidor, sino que tales factores deben ser evaluados de manera conjunta con la información recopilada del historial de consumos del cliente, específicamente en lo que respecta al importe de las operaciones que solía realizar.

De lo expuesto, se colige que existen enfoques diversos por parte de los órganos resolutivos al momento de abordar los factores que definen el comportamiento habitual del consumidor, ya que, algunos órganos resolutivos llevan a cabo un análisis integral y conjunto de los factores que influyen en el comportamiento habitual, mientras que otros sostienen que solo el factor del importe constituiría un criterio objetivo al momento de examinar el patrón de consumo.

Desde nuestra perspectiva, el criterio más adecuado y acorde con lo dispuesto en el numeral 5 artículo 2 del Reglamento de Tarjetas de Crédito y Débito (2013) (el cual señala que, para definir el comportamiento habitual del consumidor, se deben considerar diversos factores tales como el canal, la frecuencia, el tipo de comercio, entre otros), es el que considera efectuar un análisis integral y sistemático de los factores de comportamiento habitual, ya que de esta forma se garantiza una evaluación más completa y objetiva del comportamiento del consumidor; por consiguiente, se evitará la imposición de restricciones indebidas que podrían afectar la autonomía y fluidez de las transacciones financieras legítimas de los clientes. Este análisis debe partir de un examen completo del historial de consumo de los usuarios, que considere diversas circunstancias y criterios para la detección de operaciones sospechosas, como son el canal, la frecuencia o continuidad, el tipo de moneda, el lugar o establecimiento, el límite operacional, el

[56] Resoluciones 339-2023, 349-2023/CPC-INDECOPI-JUN y 195-2023/CPC-INDECOPI-PUN
[57] Resoluciones 2144-2023, 2006-2023/SPC y 076-2023/CPC-INDECOPI-PUN

horario y el tipo de operación e importe, y no limitarse al análisis de solo uno o algunos de estos factores.

Por otra parte, sobre la falta de utilización de un canal específico para realizar las operaciones, coincidimos con el criterio mayoritario que señala que, por sí solo, no debería interpretarse como señal de un comportamiento inusual; no obstante, podría constituir un indicio, que debe ser evaluado de forma conjunta o integral con otros factores de comportamiento habitual.

F. Gestión de alertas generadas por el sistema de monitoreo de operaciones

F.1 Sobre la generación de alertas

Sobre este punto, la CPC de Lambayeque[58] subraya que la presencia de uno de los criterios o circunstancias de *inusualidad* no es suficiente para inferir que una operación es fraudulenta, sino que, se necesitan circunstancias suficientes que, al concurrir, activen una alerta en el sistema de monitoreo. Esta activación, según esta Comisión, requerirá que primero se ejecute al menos una primera operación.

En una línea similar, el ORPS de Huaraz[59] establece que la activación de una alerta en el sistema de monitoreo de una entidad financiera frente a presuntas operaciones inusuales requiere de la materialización de más de una operación en un periodo específico, ya que ello permite la identificación de un patrón de operaciones anómalo que puede desencadenar en acciones preventivas por parte del banco, con el fin de evitar operaciones adicionales.

De manera similar, el ORPS de Ica[60] [61] advierte que las entidades financieras no tienen la capacidad de generar alertas previas en el sistema de monitoreo; por tanto, la alerta se generará después de la realización de la primera operación inusual.

58 Resolución 310-2022/CPC-INDECOPI-LAM
59 Resolución 44-2023/PSO-INDECOPI-HRZ
60 Resolución 121-2023/PSO-INDECOPI-ICA
61 Resolución 171 2023/PSO-INDECOPI-ICA

En la misma perspectiva, el ORPS de Cusco[62] menciona que la primera operación inusual debe ser el desencadenante de la alerta, teniendo en cuenta que su generación está vinculada al patrón de consumo previamente establecido por el consumidor. De igual manera, el ORPS de Ancash Sede Chimbote[63] indica que, en el caso de la primera operación objeto de cuestionamiento, es lógico que la entidad financiera no emita alertas si no la considera sospechosa o fraudulenta.

De la misma forma, los ORPS de Lambayeque, Tacna, Loreto y la CC1[64] concuerdan en que, para que el sistema de monitoreo emita una alerta, es necesario que ocurran previamente operaciones inusuales, ya que no es factible que el sistema se active antes de la realización de transacciones que exhiban características atípicas o fraudulentas.

Según el ORPS 2[65] las entidades financieras tienen la obligación de informar a sus usuarios acerca de las operaciones que se efectúen con sus tarjetas; de tal manera que, si toma conocimiento de operaciones que él no reconoce, pueda solicitar el bloqueo de su tarjeta y evitar que se realicen operaciones posteriores. Es importante señalar que, la falta de notificación de las operaciones al consumidor, especialmente de la primera operación inusual, implica que la entidad financiera deba asumir la responsabilidad por las operaciones no reconocidas posteriores.

Por su lado, la CPC de Ancash Sede Chimbote, la CPC de Cusco y la SPC[66] subrayan que, para activar la alerta de seguridad, la operación debe ser procesada por la entidad financiera, ya que el sistema de monitoreo no tiene una naturaleza predictiva, sino que se construye con cada operación realizada por el consumidor y se activa después de ejecutarse una operación inusual o sospechosa.

El criterio de la SPC[67] establece que, en caso de que se realice una operación considerada inusual o presuntamente fraudulenta, la

62 Resolución 412 2023/PSO-INDECOPI-CUS
63 Resolución 3-2023/PSO-INDECOPI-CHT
64 Resoluciones 562 2022-PSO-INDECOPI-LAM, 146-3023-PSO-INDECOPI-TAC, 1775-2023 (CPC n.° 1) y 9-2023/PSO-INDECOPI-LOR
65 Resolución 1912-2022 (ORPS n.° 2)
66 Resoluciones 243-2022/CPC-INDECOPI-CHT y 363-2023/CPC-INDECOPI-CUS
67 Resoluciones 2144-2023 y 2086-2023/SPC

entidad financiera debe tomar acciones inmediatas para mitigar sus posibles consecuencias negativas. Estas medidas no requieren que la operación cuestionada sea analizada previamente para su procesamiento en el sistema, sino que permiten a las entidades financieras tomar acciones luego de su ejecución.

De igual forma, el ORPS de Arequipa[68] sostiene que la generación de la alerta requiere que la operación que la desencadena sea procesada, ya que la entidad financiera no tiene la capacidad de prever el uso fraudulento de los productos financieros que gestiona. En este contexto, no sería factible exigir al proveedor que anticipe la evaluación de una operación, dado que implicaría asumir la naturaleza fraudulenta de todas las operaciones con la tarjeta y requeriría una validación especial con el titular.

Siguiendo el mismo criterio, la CPC de Cajamarca y la CPC de Tacna[69] consideran que, si se demuestra que las operaciones no son habituales, la entidad financiera está obligada a generar una alerta desde la primera operación y ponerse en contacto con el consumidor para verificar si reconoce dicha transacción. Del mismo modo, el ORPS de San Martín[70] indica que la entidad financiera, ante la realización de una operación inusual, debe generar una alerta para corroborar que fue realizada por su titular; en caso contrario, debe impedir que la transacción se concrete.

Respecto a este punto, la mayoría de los órganos resolutivos comparten el criterio de que la generación de alertas en el sistema de monitoreo exige la materialización de más de una operación inusual en un periodo específico; además, coinciden en que la activación de alertas ocurre después de la realización de la primera operación inusual, pues el sistema de monitoreo no tiene una naturaleza preventiva. Este criterio busca encontrar un equilibrio entre la detección de operaciones fraudulentas y la protección de los intereses del titular de la tarjeta, ya

68 Resolución 590-2022/PSO-INDECOPI-AQP
69 Resolución 363-2023/CPC-INDECOPI-CAJ
70 Resolución 274-2023/PSO-INDECOPI-SAM

que antes de tomar medidas preventivas, se requerirá la confirmación de patrones de comportamiento anómalo, a fin de evitar bloqueos o trabas innecesarias que puedan vulnerar la libertad del usuario para realizar operaciones o que puedan afectar su experiencia en el uso de sus productos financieros.

F.2 Sobre la adopción de medidas preventivas

De lo anteriormente expuesto, se evidencia una tendencia en los órganos resolutivos en considerar que es la primera operación inusual ejecutada la que activa la alerta. A partir de este punto, se entiende que la entidad financiera está obligada a tomar medidas inmediatas para prevenir la ejecución de operaciones posteriores. Una de estas medidas es el bloqueo preventivo; el cual, de acuerdo con la CC1[71], tiene el propósito de evitar que se lleven a cabo transacciones adicionales que puedan afectar los intereses del titular de la tarjeta.

Según la CPC de Cusco, CPC de Junín, ORPS de Cajamarca y CPC de Ica[72] es responsabilidad del banco emitir una alerta ante la realización de operaciones inusuales y comunicarse con el consumidor para que confirme la transacción o, en su defecto, proceder al bloqueo de la tarjeta para evitar consumos adicionales de naturaleza inusual. En la misma línea, el ORPS de Cusco, la CPC de Ancash Sede Chimbote, el ORPS de Junín y el ORPS de Ancash sede Chimbote[73] sostienen que es deber del banco generar una alerta ante operaciones sospechosas, comunicarse con el consumidor para que valide la operación, y en caso de no lograr contacto o de comprobar que no se trata del titular, aplicar el bloqueo preventivo de la tarjeta para evitar transacciones adicionales.

Continuando con la idea anterior, según el ORPS de Huaraz[74] el banco tiene la responsabilidad de alertar al usuario para que realice el bloqueo preventivo de la tarjeta y evite la continuación de operaciones

71 Resolución 1775-2023 (CPC n.° 1)
72 Resolución 195-2023/CPC-INDECOPI-CUS, 146 2023/PSO-INDECOPI-ICA, 121-2023/PSO-INDECOPI-ICA, 339-2023/CPC-INDECOPI-JUN, 7-2022/PSO-INDECOPI-CAJ
73 Resoluciones 412 2023/PSO-INDECOPI-CUS, 243-2022/CPC-INDECOPI-CHT, 528 2022/PSO-INDECOPI-JUN y 182-2022/PSOINDECOPI-CHT
74 Resolución 40 2023/PSO-INDECOPI-HRZ

posteriores inusuales. Según este órgano, la entidad financiera debe notificar al consumidor mediante una llamada o mensaje sobre los consumos no reconocidos, con el objetivo de prevenir la realización de transacciones adicionales.

Es importante señalar que, de acuerdo con la Sala[75] las acciones preventivas destinadas a evitar la continuación de operaciones inusuales o fraudulentas deben ser activadas de manera inmediata y oportuna. En ese orden de ideas, el ORPS 2[76] indica que las entidades financieras deben proporcionar un servicio de notificaciones para todos sus usuarios, con el objetivo de informarles sobre las operaciones realizadas con sus tarjetas.

En conclusión, se observa una práctica generalizada entre los órganos resolutivos respecto de considerar que la primera medida preventiva que la entidad financiera debe adoptar es la comunicación con el consumidor para confirmar la validez de la transacción; y, en caso de no lograr establecer comunicación con el usuario, debe proceder con el bloqueo preventivo de la tarjeta para evitar transacciones posteriores.

La comunicación activa con el consumidor constituye un aspecto importante a fin de verificar la autenticidad de la operación y obtener su confirmación. En situaciones donde no es posible establecer contacto con el titular, el bloqueo preventivo de la tarjeta es considerado una medida fundamental para evitar transacciones adicionales de naturaleza inusual. No obstante, pese a la importancia del sistema de gestión de alertas para evitar la ejecución de operaciones fraudulentas, no se observa que todos los órganos resolutivos examinen el cumplimiento de esta obligación ni se identifica un criterio uniforme en su análisis; por lo que se sugiere añadir, al análisis de los puntos anteriormente mencionados, el cumplimiento del sistema de gestión de alertas, que consiste en establecer comunicación con el usuario ante la detección de una operación atípica o inusual a fin de que valide su ejecución o, en caso de que ello no sea posible, proceder con el bloqueo preventivo de la tarjeta.

[75] Resolución 2006-2023/SPC
[76] Resolución 1754 2022 (ORPS n.° 2)

G. Sobre el otorgamiento de medidas correctivas en los casos de operaciones no reconocidas

Existe el criterio generalizado[77] por parte de los órganos resolutivos de devolver el importe total de las operaciones no reconocidas como medida correctiva, cuando se demuestra que dichas operaciones no fueron válidamente realizadas o no cumplieron con el proceso de autenticación establecido por la normativa y la entidad financiera.

En contraste, en los casos de operaciones inusuales que fueron autenticadas de forma válida, se observa que varios de los órganos resolutivos tienen el criterio de no ordenar la devolución o extorno de la primera operación inusual, alegando que su procesamiento es necesario para activar alertas en los sistemas del banco, de tal manera que se evite la realización de las operaciones posteriores[78].

Este criterio es compartido por la Sala que deniega la devolución de la primera operación que debe generar la alerta y concede el extorno de las operaciones subsiguientes, siempre y cuando se demuestre que la primera operación fue válidamente efectuada.[79] En los casos en los que se encuentre en cuestionamiento una sola operación no reconocida, la Sala ha adoptado el criterio de no otorgar medida correctiva alguna en caso se acredite la validez de dicha operación, pues el sistema de monitoreo de las entidades financieras no es de naturaleza predictiva, sino que se construye con cada operación efectuada por el consumidor[80].

No obstante, otro criterio que adoptan los órganos resolutivos[81] consiste en que, si bien efectúan el análisis de validez de las operaciones y patrón de consumo del usuario, no diferencian las operaciones entre

77 Resoluciones 23-2022/PSO-INDECOPI-HRZ, 44-2023/PSO-INDECOPI-HRZ, 171 2023/PSO-INDECOPI-ICA, 3-2023/PSO-INDECOPI-CHT, 144-2023/PSO-INDECOPI-TAC, 85-2023/CPC-INDECOPI-ICA, 349-2023/CPC-INDECOPI-JUN, 76-2023/CPC-INDECOPI-PUN, 65-2022/CPC-INDECOPI-PUN, 58-2023/CPC-INDECOPI-TAC, 105-2023/CPC-INDECOPI-TAC, 1954-2023 (CPC n.° 1), 1773-2023 (CPC n.° 1), 323-2023/PSO-INDECOPI-LAM, 246-2023/PSO-ILN, 229-2023/CPC-INDECOPI-CAJ, 828-2022/CPC-INDECOPI-LAL, 447-2022/CPC-INDECOPI-LAM Y 310-2022/CPC-INDECOPI-LAM.

78 Resoluciones 171-2023/PSO-INDECOPI-ICA, 136-2023/PSO-INDECOPI-TAC Y 1725-2022 (ORPS n.° 2).

79 Resolución 2086-2023/SPC

80 Resolución 2006-2023/SPC

81 Resoluciones emitidas por el ORPS CUSCO, ORPS JUNÍN, ORPS LA LIBERTAD, 9-2023/PSO-INDECOPI-LOR, 77-2023/PSO-INDECOPI-LOR, 339-2023/CPC-INDECOPI-JUN, 274-2023/PSO-INDECOPI-SAM, 73-2023/PSO-ILN, 37-2023/CPC-INDECOPI-LAL

aquellas que debieron generar la alerta y las operaciones subsecuentes, por lo que dictan como medida correctiva la devolución de la totalidad del importe de las operaciones materia de cuestionamiento, es decir, tanto de aquellas que debieron generar la alerta en los sistemas del banco como de las operaciones posteriores, incluso, si se llegase a determinar que las primeras fueron válidamente efectuadas.

Otro supuesto para tener en cuenta, son los casos en que se cuestiona una única operación no reconocida procesada de manera válida, pero que no se ajusta al patrón de consumo habitual del consumidor. En estas situaciones, los órganos resolutivos han adoptado dos enfoques diferentes: algunos ordenan la devolución de dicha operación[82], mientras que otros deniegan la medida correctiva al considerar que esta operación es el punto de partida para la generación de alertas[83].

En conclusión, al analizar las resoluciones emitidas por los diversos órganos resolutivos, se evidencia que la mayoría ordena la devolución total de las operaciones no reconocidas cuando se demuestra que estas no fueron válidamente efectuadas. Sin embargo, surge una discrepancia de criterios cuando se demuestra que, si bien las operaciones fueron válidamente ejecutadas, no se ajustan al patrón de consumo del usuario. En estos casos, una buena parte de los órganos resolutivos considera la devolución solo de las operaciones subsiguientes a la primera operación inusual realizada de manera válida. La justificación detrás de este criterio consiste en que el sistema de monitoreo no tiene naturaleza predictiva, por lo que existe la necesidad de procesar la primera operación a fin de que, en caso se determine que es inusual, genere una alerta en los sistemas del banco, para evitar el procesamiento de posteriores operaciones no reconocidas.

En contraste, existe también el criterio de otros órganos resolutivos de considerar que, en el supuesto de que se determine que las operaciones son inusuales, se debe efectuar la devolución de la totalidad

[82] Resolución 1-2022/PSO-INDECOPI-CAJ
[83] Resolución 146-2023/PSO-INDECOPI-TAC

de los importes denunciados, sin importar si eran o no las primeras operaciones efectuadas.

Por otro lado, se ha notado que algunos órganos resolutivos del Indecopi ordenan la devolución de los intereses legales generados desde la ejecución de las operaciones fraudulentas hasta la fecha de emisión de la resolución. Esta medida correctiva se encuentra contemplada en el artículo 115 del Código y, junto con la devolución de los fondos sustraídos, podría proporcionar una solución más completa y reparadora para el usuario. Sin embargo, de la revisión de las resoluciones bajo análisis, se aprecia que esta medida no es adoptada uniformemente por todos los órganos resolutivos del Indecopi[84], lo que genera discrepancia en los pronunciamientos y podría generar una percepción de desigualdad en el trato a los usuarios, debido a que en situaciones similares no se les estaría brindando el mismo nivel de reparación. Cabe indicar que los intereses legales compensan el tiempo durante el cual el consumidor se vio privado de sus fondos como consecuencia de las operaciones fraudulentas efectuadas, y su devolución asegura que el usuario no solo reciba el monto sustraído, sino también una compensación justa por el perjuicio financiero sufrido durante el periodo en que no pudo disponer de su dinero.

En ese sentido, existe la necesidad de unificar un criterio respecto de la medida correctiva que el órgano resolutivo ordenará -es decir, si corresponde el extorno o devolución de las operaciones no reconocidas en su totalidad o solo de las subsiguientes a la operación que debe generar la alerta-, así como la devolución de los intereses legales generados, ya que la falta de predictibilidad al respecto genera incertidumbre tanto en los consumidores como en las entidades financieras, pues en muchos casos, la primera operación es la única cuestionada por el usuario, y la denegatoria de su devolución podría dejar al consumidor en una posición desfavorable. Por otra parte, la

[84] Resoluciones 10-2023-PSO-INDECOPI-CHT, 23-2022-PSO-INDECOPI-HRZ, 47-2022-PSO-INDECOPI-HRZ, 65-2022-CPC-INDECOPI-PUN, 74-2023-PSO-INDECOPI-LOR, 146-2023-PSO-INDECOPI-ICA, 182-2022-INDECOPI-CHT, 232-2022-PSO-INDECOPI-CAJ, 243-2022-INDECOPI-CHT, 246-2023-ILN-PSO, 274-2023-PSO-INDECOPI-SAM, 339-2023-INDECOPI-JUN y 828-2022-INDECOPI-LAL.

autoridad administrativa debe tener en cuenta que la decisión que tome tendrá consecuencias patrimoniales en el consumidor o usuario denunciante, por lo que la falta de un criterio unificado podría generar expectativas infundadas en el mismo, y su vez, impedir que las entidades financieras puedan anticipar y gestionar de manera consistente este tipo de situaciones.

H. Sobre la graduación de la sanción en los casos de operaciones no reconocidas

A partir del 15 de junio de 2021 entró en vigor el Decreto Supremo que aprueba la graduación, metodología y factores para la determinación de las multas que impongan los órganos resolutivos del Indecopi respecto de las infracciones sancionables en el ámbito de su competencia (2021). Dicha norma señala que la multa a imponer por infracciones al Código de Protección y Defensa del Consumidor se graduará con base en la fórmula "M = m x F" donde "m" representa la multa base y "F" la sumatoria de los factores agravantes y atenuantes, estableciendo la cuantía de la multa de acuerdo con un listado taxativo de infracciones y tomando en cuenta el tipo de empresa infractora.

De la revisión de las resoluciones materia de investigación, si bien se verifica que dicha norma es aplicada por casi todos los órganos resolutivos del Indecopi en materia de protección al consumidor[85], se observan algunas diferencias de criterio al momento de calcular la multa final.

En el caso del ORPS de Huaraz[86] se efectúa el cálculo de la sanción haciendo uso de las reglas establecidas en el Decreto Supremo 032-2021-PCM; no obstante, en algunos casos[87], se considera como criterio atenuante la baja cuantía de las operaciones denunciadas y el perjuicio patrimonial causado al denunciante, por lo que, en mérito del principio de razonabilidad, se sanciona al banco con una amonestación.

85 Con excepción del ORPS San Martín
86 Resolución 23-2022/PSO-INDECOPI-HRZ
87 Dicho criterio, no es aplicado en todas las resoluciones emitidas por dicho órgano, ya que en las resoluciones 40-2023/PSO-INDECOPI-HRZ y 44-2023/PSO-INDECOPI-HRZ, no se verifica el uso de dicha atenuante.

De manera similar, el ORPS de Lima Norte realiza el cálculo de la sanción a través del decreto supremo anteriormente mencionado, aplicando las atenuantes de acuerdo con lo establecido en dicha norma. No obstante, al momento de calcular el monto final de la sanción, citan el principio de razonabilidad (el cual, según dicho órgano, prescribe que la sanción a imponer debe generar incentivos para corregir las acciones contrarias al ordenamiento jurídico), por lo que determina finalmente imponer una amonestación[88] o una multa de menor cuantía a la calculada[89].

Por su parte, la CPC de Ancash Sede Chimbote[90] sigue un análisis similar, al tomar en consideración el principio de razonabilidad como atenuante y considerar que las sanciones a ser aplicadas deben ser proporcionales al incumplimiento calificado como infracción, por lo que determina finalmente sancionar al proveedor con una amonestación.

En el caso específico del ORPS de San Martín[91] la determinación de la sanción no se realiza mediante la aplicación de las reglas establecidas en la norma particular, sino que se lleva a cabo con los criterios señalados en el artículo 112 del Código de Protección y Defensa del Consumidor. En este sentido, sostiene que la graduación de la sanción se rige por el principio de razonabilidad, el cual implica que las autoridades deben asegurarse de que cometer la conducta infractora no resulte más beneficioso para el infractor que el cumplimiento de las normas legales vigentes.

Por otra parte, es importante destacar el criterio de la Sala[92] según el cual, ante la imposibilidad de categorizar la conducta infractora en los términos del Decreto Supremo, se debe efectuar una graduación de la sanción a imponer en atención a los criterios establecidos en el artículo 112 del Código. Dicho criterio fue aplicado por la CPC La Libertad[93], que sancionó a la entidad financiera tomando en cuenta los criterios

88 Resolución 73-2023/PSO-ILN
89 Resolución 246-2023/PSO-ILN
90 Resoluciones 243-2022/CPC-INDECOPI-CHT y 182-2022/CPC-INDECOPI-CHT
91 Resolución 274-2023//PSO-INDECOPI-SAM
92 Resoluciones 2006-2023/SPC y 2086-2023/SPC
93 Resolución 37-2023/CPC-INDECOPI-LAL

establecidos en el artículo 112 del Código, ya que no era posible graduar la sanción a través del Decreto Supremo.

En conclusión, se observa divergencia en los criterios aplicados por los órganos resolutivos del Indecopi en cuanto a la graduación de las sanciones en casos de operaciones no reconocidas. Aunque la mayoría de los órganos resolutivos utiliza los criterios establecidos en el Decreto Supremo 032-2021-PCM para calcular las multas, algunos de ellos introducen factores adicionales, como la cuantía de las operaciones denunciadas y el principio de razonabilidad.

En particular, se observa que algunos órganos resolutivos consideran la baja cuantía de las operaciones y aplican el criterio de razonabilidad, lo que resulta en la imposición de amonestaciones en lugar de multas. Esta interpretación no está contemplada como atenuante según el Decreto Supremo, por lo que constituye un criterio que está fuera de los parámetros establecidos en la norma específica.

Al respecto, consideramos que la aplicación de la sanción debe ceñirse estrictamente a lo establecido en el Decreto Supremo, ya que la conducta infractora consiste en la falta de adopción de medidas de seguridad, por lo que la imposición de sanciones pecuniarias no solo debe considerarse como un medio de punición, sino como una forma de incentivar a las empresas a mejorar sus sistemas de seguridad y prevenir la ejecución de operaciones fraudulentas; además, la graduación contemplada en la norma toma en cuenta el tamaño de las empresas infractoras y la afectación patrimonial al usuario, por lo que obedece a criterios objetivos y razonables.

4.1.2 Objetivo Específico N.° 2

A. Chile

En Chile, la Ley 19.496, Normas sobre protección de los derechos de los consumidores (2021) establece que las entidades financieras deben demostrar experticia y control en la relación que mantienen con los consumidores. Así, el artículo 3 literal d) garantiza el

derecho a la seguridad en el consumo, el cual puede ser vulnerado cuando el proveedor no adopta medidas de seguridad idóneas en la ejecución de pagos y transacciones electrónicas.

En esa línea, los artículos 12 y 23 de la misma ley señalan que el deber de seguridad implica que el proveedor debe entregar bienes y servicios de acuerdo con los términos ofrecidos, actuando con diligencia para prevenir perjuicios al consumidor por fallas en la calidad o seguridad del bien o servicio adquirido.

En adición con lo anterior, la Ley 20.009, que establece un régimen de limitación de responsabilidad para titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude (2005), se emitió a fin de conferir mayor protección a los usuarios de tarjetas e introdujo un nuevo tipo penal por uso fraudulento de las mismas (Escárate, 2015).

Según Bernal (2023) en un principio esta ley solo abordaba situaciones relacionadas con el extravío, hurto o robo de tarjetas de crédito, excluyendo a la tarjeta de débito y otros métodos de pago; sin embargo, a través de la Ley 21.234 (2020), se llevaron a cabo modificaciones para ampliar su alcance, incorporando a las tarjetas de pago en general y a las transacciones electrónicas, entendiéndose estas últimas como aquellas que se efectúan por medios electrónicos, incluyéndose las transacciones realizadas por medio de portales web u otras plataformas.

La norma y sus respectivas modificaciones establecen las reglas que deben seguir los titulares o usuarios de los medios de pago, así como los emisores de estos, en caso de que se presente una situación de pérdida, hurto, robo o fraude de la tarjeta de pago. A continuación, resumiremos algunas de las reglas que son relevantes para esta investigación:

Los titulares de medios de pago tienen la posibilidad de limitar su responsabilidad en situaciones de pérdida, hurto, robo o fraude, siempre

y cuando notifiquen al emisor de manera oportuna. Para garantizar este proceso, los emisores deben mantener canales de comunicación gratuitos y disponibles las 24 horas del día, todos los días del año, con el fin de recibir dichas notificaciones. Al recibir la notificación, la entidad emisora está obligada a proporcionar al usuario un código de seguimiento, bloquear el medio de pago y enviar la información pertinente a través de un medio acordado (artículo 2).

En el supuesto de que se utilicen los medios de pago después de haber realizado el aviso, el emisor asumirá la responsabilidad de dichas operaciones y sus consecuencias económicas (artículo 3). Sin embargo, si las operaciones se efectúan antes del aviso, el usuario tiene un plazo de 30 días hábiles después del aviso para reclamar al emisor por las operaciones no autorizadas, inclusive aquellas realizadas hasta 120 días antes del aviso (artículo 4).

Si el usuario desconoce la autorización de una operación, es responsabilidad del emisor demostrar su correcta autorización y registro. Sin embargo, el simple registro de las operaciones no será suficiente para demostrar la autorización del usuario ni su culpabilidad o negligencia, sin perjuicio de tomar acciones legales contra el autor del delito.

El emisor tiene la obligación de cancelar los cargos o restituir los fondos correspondientes a las operaciones reclamadas dentro de un plazo de 5 días hábiles si el monto total reclamado es igual o inferior a 35 unidades de fomento. Para montos superiores, deben cancelarse o restituirse 35 unidades en el mismo plazo y el resto en siete días adicionales. Sin embargo, si durante este tiempo el emisor recopila evidencia de dolo o culpa grave por parte del usuario, puede emprender ante el juez de policía local las acciones judiciales correspondientes.

En caso de que se determine mediante sentencia firme o ejecutoriada que el usuario ha participado en la comisión del delito, obtenido un beneficio ilícito o actuado con dolo o culpa grave facilitando su comisión, la cancelación o restitución de fondos queda sin efecto, sin perjuicio de las indemnizaciones correspondientes (artículo 5).

Además, los emisores, operadores, comercios y otras entidades afiliadas a sistemas de tarjetas de pago deben implementar medidas de seguridad para prevenir ilícitos y proteger la privacidad de los usuarios. Estas medidas incluyen implementar sistemas de monitoreo para detectar operaciones inusuales, instaurar procedimientos internos para gestionar alertas generadas por el monitoreo, identificar patrones de posibles fraudes e imponer límites y controles en los canales de atención para mitigar pérdidas por fraude, basados en criterios objetivos y no discriminatorios.

En conclusión y de acuerdo con Bernal (2023) en casos de extravío, hurto, robo o fraude, el usuario puede liberarse de responsabilidad sobre las operaciones con el aviso al proveedor, a menos que este último demuestre dolo o culpa grave y que ello se encuentre respaldado por una sentencia firme o ejecutoriada. Por tanto, los tribunales (Juzgados de Policía Local) adoptan una presunción de culpa en favor del usuario que informa oportunamente sobre las operaciones no reconocidas, por lo que la carga de la prueba se invierte, siendo responsabilidad del proveedor demostrar que la operación se realizó correctamente y con las medidas de seguridad adecuadas.

A.1 Acciones legales de los usuarios frente a operaciones no reconocidas

De acuerdo con las Leyes 20.009 y 19.496, las acciones que un usuario de servicios financieros afectado por operaciones fraudulentas puede iniciar con el propósito de determinar la responsabilidad de la entidad financiera son las siguientes: la acción infraccional, acción civil y acción de protección.

Siguiendo a Bernal (2023) la acción infraccional, tanto a nivel individual como colectivo, tiene como propósito determinar la responsabilidad de una entidad financiera por infringir las normas establecidas en la Ley 19.496. Aunque un consumidor puede buscar la

responsabilidad civil de la entidad financiera sin necesidad de presentar la denuncia o querella infraccional, es relevante señalar que esta última continuará su curso una vez iniciada. Es importante precisar que el consumidor es el titular de la acción infraccional; sin embargo, el SERNAC también puede ejercerla según lo establecido en la Ley 19.496 (Bernal, 2023).

Un ejemplo concreto de una acción infraccional se materializó con la Demanda Colectiva presentada por el SERNAC contra el Banco del Estado de Chile (Sentencia Rol n.° C-2126-2023, Juzgado Civil de Santiago, 2023). Esta demanda se originó debido a que numerosos consumidores fueron afectados por cargos indebidos y operaciones no reconocidas por clonación o suplantación de identidad y, pese a que formularon diversos reclamos, no hubo una gestión adecuada por parte del banco, lo que condujo a la presentación de la demanda.

El SERNAC argumentó que, aunque el banco afirmó que las operaciones eran correctas según los registros bancarios, la Ley N.° 20.009 establece que estos registros no son suficientes para demostrar la autorización del usuario, especialmente en casos de fraudes electrónicos. Además, se alegó que la entidad no actuó con la debida diligencia profesional ni implementó medidas de seguridad adecuadas para prevenir perjuicios a los consumidores. A la fecha, este procedimiento sigue en trámite.

Por otro lado, la acción civil, según Bernal (2023), tiene como objetivo reparar los perjuicios ocasionados al consumidor por la ejecución de las operaciones fraudulentas. En el ámbito de los servicios financieros, la responsabilidad civil es regulada por el régimen contractual, ya que la relación entre el consumidor y el proveedor financiero se establece mediante un contrato, generalmente de adhesión. Cabe indicar que, el deber de seguridad establecido en la Ley 19.496 y las obligaciones de la Ley 20.009, se aplican en este contexto.

La Ley N.° 19.496 establece el marco mínimo de comportamiento que una entidad financiera debe guardar respecto de sus

clientes, ya que el incumplimiento de las obligaciones adquiridas, lo hará responsable frente al consumidor, generando la obligación de indemnizar el daño causado.

Por otro lado, en cuanto a la exoneración de responsabilidad, la Ley 20.009 establece dos supuestos: a) si se acredita que la operación fue debidamente autorizada y registrada a nombre del usuario; y, b) si se demuestra la existencia de dolo o culpa grave en el consumidor. La existencia de dolo o culpa grave en el usuario implica generalmente conductas descuidadas que facilitan el fraude electrónico.

En la Sentencia Rol N.° 783-2020, Corte de Apelaciones de Santiago (2022), la pretensión del consumidor fue rechazada en todos sus extremos, pues se consideró que existió una falta de diligencia de su parte. Así, en los casos en los que se demuestre que la negligencia del consumidor ocasionó el fraude, la víctima debe asumir el costo total de los daños generados por el delito y, en consecuencia, se dictamina la exoneración de responsabilidad del proveedor o una rebaja a la indemnización por exposición imprudente al daño.

Por último, en la acción de protección se evidencia una predisposición de los tribunales superiores a admitir acciones basadas en la vulneración del derecho de propiedad consagrado en el artículo 19 N.º 24 de la Constitución Política de la República (Bernal, 2023). Por ejemplo, en la Sentencia Rol N.° 13407-2021, Corte de Apelaciones de Concepción (2022) se menciona que el banco al no asumir el perjuicio económico del consumidor estaría actuando de manera arbitraria y afectando directamente el patrimonio del cliente, lo cual vulnera el derecho establecido en el artículo 19 N.º 24 de la Constitución.

En relación con la posible concurrencia de acciones constitucionales y civiles en casos de fraudes bancarios, los tribunales han señalado que no se excluyen mutuamente, ya que la acción de protección constitucional puede ser procedente, sin que ello impida ejercer otros derechos ante la autoridad o tribunal correspondiente.

A.2 Jurisprudencia

De la revisión de la jurisprudencia emitida por los Juzgados de Policía Local, se verifica que un argumento utilizado para determinar la responsabilidad de la entidad financiera consiste en tomar en cuenta la especialidad y complejidad de los servicios que ofrecen, en tanto deben ser cuidadosos y eficientes respecto de las herramientas que ponen a disposición de sus clientes, sobre todo de forma previa a las transacciones defraudatorias. Por otro lado, se verifica que en estos casos se consideran como infracciones las disposiciones establecidas en el artículo 3, literal d, de la Ley 19.486, que impone la obligación de proporcionar al consumidor seguridad en el consumo de bienes y servicios, así como el deber de prevenir los riesgos que puedan afectarlos. Así, en caso se determine que las medidas de seguridad implementadas por el proveedor fueron insuficientes y que actuó con negligencia, se acoge la acción infraccional, condenándose a la entidad financiera al pago de una multa. Además, en el ámbito civil, una vez que se acoge la acción infraccional, se ordena también la devolución de las transacciones no autorizadas y se concede una indemnización por daño moral (Sentencia Rol N.° 10146-2021, 2° Juzgado de Policía Local de Talca, 2022).

Por otro lado, se establece que, en caso de que la entidad financiera alegue la presencia de dolo o culpa grave según lo establecido en el artículo 5 inciso tercero de la Ley 21.234, es responsabilidad del banco acreditar que el usuario autorizó las operaciones en cuestión y/o que participó en la comisión del delito, que obtuvo un beneficio ilícito, o que actuó con dolo o culpa, sin que baste el simple registro de las operaciones para probarlo (Sentencia Rol N.° 10-2023, Juzgado de Policía Local del Puerto Porvenir, 2023). Adicionalmente, la falta de acción inmediata del querellante al no notificar el robo de su tarjeta, pese a la notificación de los estados de cuenta al usuario en los que se verifica la ejecución de las operaciones no reconocidas, acarrea la responsabilidad del usuario. En esos casos, el juzgado rechaza tanto la denuncia infraccional como la demanda civil en todos sus aspectos

(Sentencia Rol N.° 1115-2020, 2° Juzgado de Policía Local de Talca, 2022).

En los casos de los recursos de protección formulados por los usuarios, se determina que la sustracción de los fondos del usuario por terceros, quienes realizaron operaciones fraudulentas utilizando los medios de pago contratados, afecta el derecho de propiedad. Por lo tanto, en los casos en los que el recurso sea acogido, se ordena al banco cancelar los cargos provenientes del fraude y restituir los fondos correspondientes (Sentencia Rol n.° 201-2022, Segunda Sala de la Corte de Apelaciones de La Serena, 2022).

Finalmente, en los casos de los procedimientos voluntarios colectivos, la Subdirección de Procedimientos Voluntarios Colectivos del SERNAC inicia procedimientos voluntarios por afectación al interés colectivo de los consumidores y posibles contravenciones a la Ley 19.496. Según el artículo 54P n.° 3 de la Ley 19.496, a través del cual se establece que las condiciones del acuerdo deben incluir una solución proporcional al daño causado, que involucre a todos los consumidores afectados y esté basada en elementos objetivos, como podría ser el reintegro de la totalidad del monto correspondiente a las operaciones fraudulentas, además de compensaciones adicionales por el costo del tiempo, la indisponibilidad financiera y el costo del reclamo (Resolución exenta n.° 727, 2020).

A.3 Análisis comparativo con las normas peruanas

El marco normativo y jurisprudencial relacionado con las operaciones financieras no reconocidas en Perú y Chile contiene similitudes y diferencias significativas respecto de cómo se establece la responsabilidad de la entidad financiera y de los consumidores.

Al igual que la normativa peruana, en Chile se limita la responsabilidad del consumidor luego del aviso de bloqueo, ya que las operaciones efectuadas luego del mismo son de responsabilidad exclusiva de la entidad bancaria. Asimismo, de manera similar al caso

peruano, en la normativa chilena se establece que la carga de la prueba de acreditar que la operación fue autorizada y registrada correctamente recae en el emisor de la tarjeta o medio de pago; no obstante, a diferencia de la normativa peruana, en la Ley 20.009 se señala de forma expresa que el registro de las operaciones no es suficiente para demostrar que el usuario autorizó la operación o que actuó con culpa o descuido.

Un punto importante es que la normativa chilena, al igual que la peruana, establece como obligación de las entidades financieras o emisoras de tarjetas la implementación de sistemas de monitoreo destinados a detectar operaciones inusuales, con el objetivo de identificar patrones de fraude. No obstante, de la revisión de las sentencias emitidas por los juzgados de policía, se aprecia que no se realiza una verificación del cumplimiento de dicha obligación a fin de determinar la responsabilidad de la entidad financiera, análisis que sí es efectuado en las resoluciones emitidas por el Indecopi y que, en muchos casos, es determinante para declarar la responsabilidad del banco.

Por otro lado, en el caso de las operaciones no reconocidas efectuadas antes del aviso al emisor por hurto, robo, extravió o fraude, la normativa chilena establece de forma expresa el deber de restitución que tiene el emisor de la tarjeta ante operaciones fraudulentas, el cual consiste en que si el monto reclamado es igual o inferior a 35 unidades de fomento debe restituir las operaciones en un plazo de 5 días hábiles y, si superan este monto, debe restituir las 35 unidades en el plazo de 5 días y el resto en 7 días adicionales. No obstante, si en el plazo anterior el emisor logra reunir pruebas que acrediten el dolo culpa grave del usuario, puede realizar las acciones judiciales ante el juez de policía local, para que, a través de una sentencia firme o ejecutoriada, determine la participación del usuario en la comisión de fraude, dolo o culpa grave. Por su parte, la normativa peruana no contempla la devolución automática de los fondos en casos de operaciones no reconocidas ni se establecen las medidas que las entidades emisoras podrían adoptar para obtener la restitución de dichos fondos en caso acrediten dolo, culpa grave o participación en la comisión del fraude por parte del usuario.

Otra diferencia es que en Chile no existe una autoridad administrativa que se encargue de tramitar procedimientos administrativos que determinen la comisión de una infracción en casos concretos de operaciones no reconocidas, que imponga sanciones y/o dicte medidas correctivas en favor del usuario, ya que estos casos se dilucidan directamente ante el Poder Judicial a través de los juzgados de policía local. Las acciones judiciales más comunes que puede interponer el usuario son la acción infraccional, que tiene por finalidad determinar la responsabilidad de la entidad, y la acción civil, que tiene por finalidad determinar la responsabilidad civil del proveedor y, de esa forma, obtener una indemnización por daños y perjuicios.

Los casos en los que se interpone tanto una acción infraccional como una civil, se asemejan a los procedimientos de denuncia administrativa tramitados ante el Indecopi, ya que a través de estos se efectúa un análisis de la responsabilidad de la entidad bancaria en los casos de operaciones no reconocidas y, de determinarse la comisión de una infracción, se imponen las sanciones y medidas correctivas en favor del usuario; sin embargo, en los procedimientos tramitados por el Indecopi, no es posible solicitar una indemnización por los daños y perjuicios ocasionados, por lo que debe ser solicitada por el usuario en la vía jurisdiccional correspondiente. Es importante mencionar en este punto que el Indecopi cuenta con facultades para otorgar medidas correctivas que, si bien no tienen carácter indemnizatorio, buscan retrotraer los efectos de la infracción, por lo que puede ordenarse la devolución de los montos cuestionados y de los intereses legales generados.

Es necesario precisar que, en Chile, los casos se analizan como infracciones al deber de seguridad contemplado en la Ley 19.496, el cual establece que el proveedor debe entregar bienes y servicios que se encuentren de acuerdo con lo ofrecido y actuar de forma diligente para evitar que se generen perjuicios a los consumidores por fallas que podrían tener sus propios productos o servicios. En Perú, el Indecopi analiza esta infracción como una falta al deber de idoneidad y no como

una falta al deber de seguridad contemplado en el artículo 25 de dicha norma. En resumen, la conducta de no adoptar las medidas de seguridad necesarias para evitar la ejecución de operaciones no reconocidas es tipificada por el Indecopi en el tipo infractor general del deber de idoneidad, lo que contrasta con la jurisprudencia chilena, en la que se aborda específicamente esta conducta como una presunta infracción al deber de seguridad.

Por otra parte, en la jurisprudencia chilena analizada, se observa que los órganos judiciales determinan como regla que la carga de la prueba recae en las entidades bancarias, pues los bancos tienen el deber de cuidado respecto de las herramientas o medios que ponen a disposición de los clientes; además, se resalta el rol preventivo que deben desempeñar las entidades financieras para evitar la ejecución de operaciones fraudulentas. Se precisa, además, que el emisor debe efectuar el abono o la restitución de las operaciones no reconocidas y, en caso se presente, acreditar el dolo o culpa grave por parte del usuario para que se deje sin efecto dicha devolución. No obstante, de la revisión de las sentencias, se observa que el juzgado es bastante riguroso en la presentación de pruebas para acreditar dichos supuestos, por lo que los casos en los que el juzgado ha rechazado la denuncia infraccional y la demanda civil por dolo o culpa grave de los consumidores son escasos.

Es importante destacar el rol que tiene SERNAC en la presentación de acciones infraccionales y en la gestión de procedimientos voluntarios colectivos ante afectaciones al interés colectivo de los consumidores, ya que a través de estos últimos la autoridad administrativa puede arribar a un acuerdo con la entidad financiera para la devolución del monto de las operaciones no reconocidas en favor de una colectividad de usuarios. En el caso peruano, no se cuenta con experiencias recientes de procedimientos de oficio iniciados en materia de operaciones no reconocidas en favor de una colectividad de consumidores ni de acciones judiciales iniciadas por el Indecopi u otra institución con dicho tenor, por lo que esta experiencia podría ser tomada en cuenta, a fin de que evaluar la posibilidad de iniciar

procedimientos de oficio o demandas ante el Poder Judicial por afectación a los intereses colectivos de consumidores en casos de operaciones no reconocidas.

En conclusión, en Chile se establece que, en los casos de operaciones fraudulentas, la entidad financiera solo podrá librarse de responsabilidad si logra acreditar dolo o culpa grave por parte del consumidor, e incluso cuenta con disposiciones legales que obligan a la entidad a la devolución de los fondos ante el reclamo del consumidor y que señalan expresamente que el solo registro de las operaciones no es suficiente para acreditar la responsabilidad del usuario.

En contraste, en Perú los usuarios deben iniciar un procedimiento ante el Indecopi a fin de obtener un pronunciamiento que ordene la restitución de fondos, pues no se contempla una norma que obligue a la entidad o emisor de la tarjeta a devolverlos de forma automática. Además, el dolo o la culpa grave del usuario en la comisión de operaciones fraudulentas no están contemplados de forma expresa como supuestos de exoneración de responsabilidad en la normativa.

Adicionalmente, desde la perspectiva jurisprudencial, el Indecopi realiza un análisis centrado en evaluar las medidas de seguridad adoptadas por la entidad financiera. Así, de acreditarse que la operación fue válidamente efectuada y que se implementaron las medidas de seguridad necesarias, el proveedor puede ser liberado de responsabilidad sin que se efectúe un análisis de la culpa grave o el dolo en los que podría haber incurrido el consumidor, aun si fue un factor determinante en la ejecución de las operaciones.

B. Colombia

En Colombia, de acuerdo con el artículo 56 de la Ley 1480 Estatuto del Consumidor (2011), los consumidores financieros pueden ejercer diversas acciones jurisdiccionales. Estas incluyen las acciones populares, que buscan proteger los intereses colectivos de los consumidores; las acciones de grupo, por medio de las cuales un grupo

de personas busca la reparación de perjuicios con una causa común; y la acción de protección al consumidor financiero. Las dos primeras se ejercen ante el juez competente, mientras que la tercera se presenta ante una autoridad administrativa con funciones jurisdiccionales, siendo la SFC la entidad a la que se le han otorgado dichas facultades.

La Superintendencia puede dictar sentencias fundamentadas en la ley con carácter definitivo. Las controversias que resuelve están relacionadas con la ejecución y el cumplimiento de las obligaciones contractuales entre los consumidores financieros y las entidades supervisadas (Superintendencia Financiera de Colombia, n.d.).

Las normas vigentes que la Superintendencia puede aplicar al abordar una controversia en la esfera financiera incluyen el Estatuto Orgánico del Sistema Financiero (1993); la Ley 1328, por la cual se dictan normas en materia financiera, de seguros, del mercado de valores y otras disposiciones (2009); el Decreto 2555, por el cual se recogen y reexpiden las normas en materia del sector financiero, asegurador y del mercado de valores y se dictan otras disposiciones (2010); la Circular Básica Jurídica 029/14 (2014) emitida por la Superintendencia Financiera de Colombia, entre otras regulaciones aplicables.

En el ámbito de la seguridad en el uso de medios electrónicos de transferencia y pago, Manjarrés (2023) señala que es fundamental que el consumidor financiero no revele datos confidenciales, como tarjetas, códigos y contraseñas, para prevenir accesos no autorizados a sus cuentas. Este deber de autoprotección, establecido desde 2009 por la Ley 1328, prescribe la diligencia del consumidor para evitar fraudes, por lo que su falta de cuidado puede eximir de responsabilidad a la entidad financiera en casos de fraude electrónico, de acuerdo con la jurisprudencia de los Tribunales Superiores y de la Delegatura de Funciones Jurisdiccionales de la SFC. Sin perjuicio de lo anterior, ante un posible incumplimiento al deber de diligencia por parte consumidor financiero, surge otro deber: la necesidad de notificar de inmediato al banco cualquier situación adversa, por lo que se espera que el

consumidor informe de manera pronta cuando sea víctima de alguna ocurrencia o tan pronto se entere de ella, con el fin de evitar la consumación de operaciones financieras (Manjarrés, 2023).

Sobre ello, la Corte Suprema de Justicia ha abordado esta temática al analizar el artículo 733 del Código de Comercio (1971), al referir que el aviso que realice el titular de una cuenta a la entidad bancaria de la pérdida o hurto de un cheque solo será oportuno si se realiza antes de que el cheque sea presentado para su pago (Sentencia Rad. 6909, 2003).

Por otra parte, de acuerdo con el artículo 7 de la Ley 1328 (2009), son deberes y obligaciones de la entidad financiera: entregar el producto o prestar el servicio de manera debida y garantizar adecuados estándares de seguridad y calidad en su prestación; asimismo, disponer de los medios electrónicos y controles idóneos para brindar de forma eficiente la seguridad a las transacciones.

De manera específica y en esa misma línea, el capítulo I del título II de la parte I de la Circular Básica Jurídica 029/14 (2014) contiene, entre otras, las siguientes reglas relacionadas a la seguridad y calidad del servicio proporcionado por las entidades bancarias durante la realización de operaciones:

En principio, es importante que la entidad garantice la protección de las claves de acceso a sus sistemas de información, evitando el uso de claves compartidas, genéricas o para grupos, y resguardando la debida identificación y autenticación en los dispositivos y sistemas de cómputo (artículo 2.3.3.1.6). Además, debe establecer procedimientos para el bloqueo de canales o medios en casos justificados o después de un determinado número de intentos fallidos de acceso por parte de un cliente, así como implementar medidas operativas y de seguridad para la reactivación de estos canales o instrumentos (artículo 2.3.3.1.12).

La entidad también está obligada a elaborar el perfil de las costumbres transaccionales de sus clientes y establecer procedimientos

para confirmar rápidamente operaciones que no se alineen con sus patrones usuales (artículo 2.3.3.1.13), así como informar y capacitar a los clientes sobre las medidas de seguridad que deben tomar al realizar operaciones a través de cada canal, incluyendo instrucciones para bloquear, reactivar y cancelar productos y servicios ofrecidos (artículo 2.3.3.2.8).

Además, debe promover y poner a disposición de los clientes mecanismos que disminuyan el riesgo de interceptación de información financiera durante cada sesión por terceras personas no autorizadas (artículo 2.3.4.9.3). En el caso de operaciones realizadas a través de Banca Móvil, la prestación del servicio debe incluir mecanismos de autenticación de 2 factores para todas las operaciones (artículo 2.3.4.11.1), así como implementar mecanismos de cifrado fuerte para el envío y recepción de información confidencial en operaciones individuales o acumuladas que superen un umbral específico (artículo 2.3.4.11.2).

En ese marco, Manjarrés (2023) señala que el banco tiene la responsabilidad de actuar como el profesional más experto y cuidadoso al implementar medidas de seguridad que protejan los depósitos de sus clientes contra riesgos, incluido el fraude electrónico. Según la jurisprudencia, en situaciones donde los consumidores pierden dinero debido a operaciones como retiros, transferencias y pagos, la entidad solo puede eximirse de responsabilidad civil si demuestra la culpa del titular de la cuenta en los eventos que conduzcan a la sustracción o uso indebido de los recursos (Providencia n.° SC5176, 2020) (Providencia n.° SC18614, 2016). Este criterio sostiene que, incluso en casos de culpa grave por parte del depositante, debido a un manejo descuidado y revelación de información confidencial, el banco no puede eximirse de responsabilidad si las operaciones cuestionadas no se ajustan al hábito transaccional del consumidor. Por lo tanto, el conocimiento del hábito del cliente y la adopción de medidas para detectar operaciones fuera de lo común son herramientas esenciales para prevenir y evitar los efectos perjudiciales del fraude.

Sobre ello, la Sentencia Rad. 2016-071307 (2017), emitida por la Delegatura para Funciones Jurisdiccionales de la SFC, establece que la conducta culposa del consumidor financiero se manifiesta al exponerse de manera determinante a situaciones de riesgo, incumpliendo sus obligaciones legales y contractuales. Esto ocurre cuando, de manera imprudente, por ejemplo, facilita a terceros la información personalísima necesaria para disponer de sus recursos al realizar operaciones por cajero automático. No obstante, la entidad financiera también incurre en responsabilidad si estas operaciones no se ajustan al perfil transaccional del consumidor, ya que la construcción de este constituye una obligación de orden reglamentario, cuyo incumplimiento contractual puede generar responsabilidad civil en el Banco.

En esa línea, la Sentencia SC18614 Rad. 05001-31-03-001-2008-00312-01 (2016) examinó detalladamente la responsabilidad bancaria en casos de fraudes electrónicos. Esta decisión unificó conceptos previamente desarrollados por la jurisprudencia de los Tribunales Superiores de Distrito Judicial, convirtiéndolos en doctrina vinculante para los jueces y magistrados en Colombia en litigios relacionados con operaciones a través de canales electrónicos (Manjarrés, 2023).

El fallo establece que el desconocimiento del hábito transaccional puede ser un criterio para atribuir responsabilidad civil a los bancos. Por otra parte, en situaciones donde el cliente impugna operaciones realizadas con sus depósitos, la entidad solo puede eximirse de responsabilidad si demuestra la culpa del cliente en el procesamiento o ejecución de las transacciones al haber incumplido con sus obligaciones contractuales de custodia y confidencialidad. Así, se reconoce también los riesgos inherentes a la actividad de comercio electrónico, los cuales deben ser asumidos por las entidades bancarias por la confianza depositada por sus clientes y al ser ellos quienes ponen al servicio de estos los servicios informáticos como parte de una estrategia de ampliación de oferta y cobertura de productos y servicios financieros, lo que, si bien requiere de una inversión para su operación y mantenimiento, genera un lucro para la entidad al atraer un número

mayor de clientes. Además, se exige legalmente a las entidades financieras el cumplimiento de los deberes de control, seguridad y diligencia en sus actividades, entre ellas, la de custodiar dinero proveniente del ahorro de sus clientes.

A este respecto, la Sentencia Rad. 2015-00206-01 (2016) señala que, en los casos en los que se demuestre la culpa grave del consumidor, y siempre que las operaciones impugnadas no correspondan con el hábito transaccional del afectado, la carga indemnizatoria será parcial, considerando que la revelación previa de información confidencial por parte del consumidor no exime completamente al banco de su responsabilidad, dando lugar a la aplicación de la concurrencia de culpas. La concurrencia no excluye la obligación de indemnizar a cargo del banco, pero permite al juzgador moderar la indemnización a reconocer al perjudicado.

De acuerdo con la Sentencia Exp. 214058750 (2015) la conducta culposa del consumidor financiero se evidencia al exponerse de manera determinante a situaciones de riesgo, incumpliendo sus obligaciones contractuales al descuidar la información necesaria para disponer de sus recursos. En ese contexto, el banco debe demostrar no solo la culpa grave de la víctima al permitir el acceso de terceros a la información necesaria para la realización de las operaciones, sino también que dichas operaciones se ajustaban a sus hábitos transaccionales, considerando algunos aspectos como los días en que el cliente suele realizar operaciones, la dirección I.P. normalmente utilizada (en caso se trate de operaciones realizadas por internet), el horario, la frecuencia usual y la naturaleza de la transacción.

Manjarrés (2023) indica, a la luz de la jurisprudencia anteriormente citada, que ni siquiera la conducta grave del consumidor financiero, al descuidar información confidencial, exime totalmente al banco de responsabilidad civil. En ese sentido, para graduar la responsabilidad civil del establecimiento bancario en casos de operaciones ilícitas, propone un análisis en tres etapas: la primera fase,

de carácter objetivo, implica verificar técnicamente que las operaciones rechazadas por el cliente hayan utilizado la información y claves exclusivas de este último. La segunda etapa, de índole subjetiva, se centra en evaluar el comportamiento contractual del consumidor frente a la operación electrónica, especialmente en cuanto a la revelación inapropiada de información confidencial. La tercera fase, de análisis objetivo, consiste en corroborar si la operación se ajusta al hábito transaccional del consumidor; así, en caso no se ajuste, se asigna una porción significativa de la culpa al banco, e incluso la obligación podría ser asignada totalmente a este si la culpa del consumidor no se encuentra calificada como grave.

En un reciente litigio, la Sala Civil del Tribunal Superior de Bogotá en la Sentencia Rad. 003-2021-01984-01 (2022) revocó las condenas impuestas a un banco por la Superintendencia Financiera de Colombia, que atribuía un 30 % de la responsabilidad indemnizatoria a la entidad. La decisión se basó en la falta de pruebas que demostraran un fallo en la seguridad del banco y precisó las conductas omisivas del consumidor, como no mantener protegidos sus equipos de cómputo, descuidar la actualización de antivirus y no establecer sistemas de alertas de transacciones. Adicionalmente, se mencionó que la transacción cuestionada se originó desde la IP del demandante, que las sumas transferidas estaban dentro del perfil transaccional y que no se evidenciaron fallas de seguridad en los sistemas del banco.

En la Providencia n.° STC12199 de la Rad. 11001-22-03-000-2022-01602-01 (2022) se consideró que el valor de las operaciones es determinante para evaluar si una operación es inusual, siendo que, en estos casos, corresponde a la entidad financiera aplicar las medidas de seguridad necesarias para la confirmación o el bloqueo de las operaciones, lo que evitaría una mayor afectación en los recursos del consumidor. En dicha sentencia se determinó que tanto el usuario como la entidad financiera facilitaron la realización de las operaciones reclamadas y, por tanto, contribuyeron a la ocurrencia del riesgo,

debiendo ambas partes asumir la responsabilidad de las transacciones objeto de reclamación.

En conclusión, cuando la conducta del cuentahabiente revela un movimiento irregular que supera su hábito transaccional y se evidencia una grave culpabilidad por parte del cliente, no se exime totalmente al banco de responsabilidad civil; sin embargo, se reduce la porción de la indemnización a cargo del banco mediante la teoría de la concurrencia de culpas. La determinación de la fracción del daño que no debe asumir el depositario recae en el juez, quien evaluará los medios de prueba y aplicará su criterio con base en la sana crítica y las reglas de la experiencia.

B.1 Análisis comparativo con las normas peruanas

En Colombia, los casos en los que un consumidor denuncia operaciones fraudulentas en sus productos financieros se discuten a través de acciones de protección que son resueltas por la SFC, que es una entidad administrativa que cuenta con funciones jurisdiccionales, por lo que puede dictar sentencias relacionadas con el cumplimiento de las obligaciones contractuales entre consumidores y entidades financieras.

En la jurisprudencia colombiana se precisa el cuidado y experticia con la que deben actuar las entidades financieras al implementar medidas de seguridad para proteger los depósitos que sus clientes efectúan contra riesgos como el fraude electrónico, siendo una de las medidas a adoptar el deber de verificar el hábito transaccional del consumidor. Ello se basa en el reconocimiento de que la actividad de comercio electrónico implica un riesgo inherente, el cual debe ser asumido por la entidad bancaria al ofrecer este tipo de herramientas o servicios en el mercado con el objetivo de generar un lucro mayor.

En esa línea, la Circular Básica Jurídica 029/14 (2014) establece el deber de la entidad financiera de elaborar el perfil transaccional del usuario y establecer procedimientos para la confirmación oportuna de operaciones que no se ajusten al mismo. Ello, se asemeja a la normativa

peruana que expresamente señala el deber de la entidad financiera de identificar patrones de consumo en las operaciones efectuadas por sus clientes.

De otro lado, en cuanto a la determinación de la responsabilidad de la entidad financiera en los casos de operaciones fraudulentas, la jurisprudencia peruana y colombiana han asumido un criterio similar. En Perú, se realiza un análisis de las medidas de seguridad adoptadas por el Banco, incluyendo el examen del patrón de consumo del usuario; de manera parecida, en la jurisprudencia colombiana se efectúa un análisis de las medidas de seguridad, lo que incluye también la verificación de los hábitos del cliente y de su perfil transaccional.

Sin perjuicio de lo anterior, en la jurisprudencia colombiana se establece que la entidad financiera podrá eximirse de responsabilidad si acredita la culpa del usuario en la realización de las operaciones no reconocidas o el incumplimiento de sus obligaciones de custodia y confidencialidad. Sin embargo, si bien la conducta culposa del usuario puede ser determinante en la exposición a situaciones de riesgo, ello no enerva la obligación que tiene la entidad financiera de realizar el análisis del perfil transaccional del consumidor y adoptar los requisitos mínimos de seguridad establecidos normativamente. Por tanto, en situaciones en las que se demuestre culpa grave del consumidor y, a su vez, que la entidad financiera no cumplió con las medidas de seguridad necesarias, nos encontraremos frente a un caso de concurrencia de culpas, en el que ambas partes deberán asumir las consecuencias patrimoniales de la pérdida.

En este sentido, la jurisprudencia colombiana difiere de la peruana, ya que en esta última se ha determinado que la responsabilidad por las operaciones fraudulentas recae en la entidad financiera incluso cuando se determine culpa por parte del usuario. Esto se fundamenta en el deber legal que tiene la entidad financiera de cumplir con las medidas de seguridad, incluyendo el análisis del correcto registro y autenticación de las operaciones y del patrón de consumo, por lo que, incluso en los

casos en los que se demuestre la culpa del consumidor, si la entidad financiera no acredita haber cumplido con sus deberes legales en la custodia y seguridad de las operaciones, se declarará fundada la denuncia a favor del consumidor y se responsabilizará en su totalidad a la entidad financiera por la realización de dichas operaciones.

En conclusión, el análisis del perfil transaccional del consumidor en Colombia es determinante al momento de analizar la responsabilidad de la entidad financiera en la realización de operaciones fraudulentas. Por tanto, si se determina que las operaciones se encontraban dentro de este perfil, se exime de culpa a la entidad financiera; de lo contrario, se le atribuye responsabilidad y debe asumir la pérdida de los fondos. De otro lado, de acreditarse la culpa grave del usuario, este deberá asumir una porción o porcentaje de la pérdida. Lo anterior, guarda similitud con la jurisprudencia peruana, que también otorga un papel determinante al análisis del patrón de consumo del usuario al momento de determinar la responsabilidad de la entidad financiera; no obstante, la jurisprudencia del Indecopi señala que, aun cuando se demuestre la culpa del usuario, la entidad financiera tiene el deber de adoptar las medidas de seguridad legalmente establecidas. Por tanto, si se comprueba el incumplimiento de estas obligaciones, la entidad financiera debe asumir la pérdida de los fondos.

C. España

Según Bernal (2023) la legislación española ha debido ajustarse a diversas directivas emanadas de la Unión Europea (UE), las cuales han establecido un marco común para todos los países miembros. La última Directiva del Parlamento Europeo y del Consejo, Directiva (UE) 2019/713, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión Marco 2001/413/JAI del Consejo (2019) se centró en combatir el fraude y la falsificación de medios de pago no monetarios. Esta directiva, acordada en Bruselas, buscó establecer un nivel mínimo para que los países de la UE procedan a regular el fraude y la falsificación de medios de pago.

Aunque la directiva aborda principalmente cuestiones de derecho penal, su importancia radica en la obligación de los estados miembros de proporcionar asistencia y apoyo a las víctimas afectadas por fraude o el uso indebido de sus datos personales. Además, se insta a los países a tomar medidas preventivas para reducir la incidencia de fraude, implementando campañas de información y programas educativos para concientizar a la población sobre los riesgos asociados con la falsificación de medios de pago distintos al efectivo.

En relación con la responsabilidad de los bancos ante delitos relacionados con fraudes bancarios, Calvo (2022) señala que, en la legislación española, existen dos posibles vías legales que pueden usar los consumidores víctimas de fraude informático: a) iniciar un procedimiento penal mediante denuncia o querella contra el presunto delincuente, y b) presentar una reclamación civil contra la entidad financiera alegando incumplimiento de sus obligaciones de vigilancia debida, según lo establecido en el Real Decreto-ley 19/2018, de servicios de pago y otras medidas urgentes en materia financiera (2018). Este decreto tiene como objetivo principal fortalecer la seguridad del usuario ante posibles fraudes derivados del uso indebido de medios de pago, estableciendo así normativas específicas en esta área (Bernal, 2023).

Para Calvo (2022) esta norma establece la responsabilidad cuasi-objetiva del proveedor, imputándosele directamente la responsabilidad, excepto en situaciones en las que se rompa la relación causal por fuerza mayor, fraude o negligencia grave del perjudicado. Por tanto, existe la presunción *iuris tantum* de que la víctima ha cumplido con sus obligaciones legales respecto del cuidado de sus credenciales, salvo que la entidad demuestre lo contrario (art. 3 y 44.1 del Real Decreto-ley 19/2018).

A mayor abundamiento, según Bernal (2023) el régimen de responsabilidad cuasi-objetiva[94] solo cesa si el ordenante o usuario actúa

[94] Según Blasco (como se citó en Bernal, 2023), la jurisprudencia española utiliza el término "responsabilidad cuasi-objetiva" para referirse a una responsabilidad de naturaleza objetiva, que contempla exenciones basadas en la culpa exclusiva de la víctima y la fuerza mayor.

de manera fraudulenta o incumple, deliberada o negligentemente, las obligaciones establecidas en el artículo 41 del Real Decreto-ley 19/2018. En tales casos, el proveedor debe demostrar que el incidente ocurrió debido a la conducta dolosa o gravemente negligente del cliente. Además, como alternativa a la vía judicial, los clientes pueden presentar reclamaciones ante los proveedores de servicios o recurrir a mediación o arbitraje, según lo establecido en los artículos 69 y 70 del Real Decreto-ley 19/2018.

La jurisprudencia sostiene que la responsabilidad del proveedor de servicios de banca online adopta un carácter cuasi-objetivo, lo que implica que la entidad asume el riesgo y, por ende, debe demostrar que la operación fue auténtica y que no se vio afectada por fallos técnicos o deficiencias, como ataques informáticos de naturaleza fraudulenta. Por tanto, en caso de omisión, deficiencia o mal funcionamiento de sus sistemas, el proveedor debe asumir la responsabilidad por los fallos de seguridad que pudiesen presentarse (Sentencia Roj. SAP A 632/2018, 2018).

En este punto, es importante mencionar que el Real Decreto-ley 19/2018 (2018) establece una serie de disposiciones que abordan el procedimiento a seguir en los casos de operaciones no reconocidas o fraudulentas en el ámbito de los servicios de pago. En primer lugar, según lo dispuesto en el artículo 40, se establece que los proveedores de servicios de pago tienen la facultad de bloquear un instrumento de pago en casos debidamente justificados, como situaciones relacionadas con la seguridad del instrumento o sospechas de uso no autorizado o fraudulento. Es importante que el proveedor notifique al titular del instrumento sobre el bloqueo de manera previa o, en caso de no ser factible, de forma inmediata luego de efectuado el bloqueo.

Asimismo, el artículo 41 detalla las responsabilidades del usuario de servicios de pago autorizado para utilizar un instrumento de pago, estableciéndose, entre ellas, que el usuario debe seguir las condiciones establecidas para la emisión y uso del instrumento, así como tomar

medidas adecuadas para proteger sus credenciales de seguridad personalizadas. En caso de pérdida, robo o uso no autorizado del instrumento de pago, el usuario debe notificar de inmediato al proveedor de servicios de pago o a la entidad designada para tal fin.

En lo concerniente a la seguridad de las credenciales, el artículo 42 establece que el proveedor de servicios de pago emisor del instrumento de pago debe asegurarse de que las credenciales de seguridad personalizadas sean accesibles únicamente para el usuario autorizado. Además, se requiere que el proveedor garantice la disponibilidad de medios adecuados y gratuitos para que el usuario pueda notificar operaciones no autorizadas y, cuando sea necesario, proporcionar de forma gratuita medios que permitan demostrar dicha comunicación durante un período de 18 meses.

Por otro lado, el artículo 43 establece que el proveedor de servicios de pago rectificará una operación no autorizada o ejecutada incorrectamente únicamente si el usuario comunica el problema sin demora injustificada, tan pronto como tenga conocimiento de las operaciones objeto de reclamación, dentro de un plazo máximo de trece meses a partir de la fecha en que se realizó el adeudo.

En esa línea, el artículo 44, numeral 1, establece que si un usuario de servicios de pago niega haber autorizado una operación de pago o alega que esta se realizó de manera incorrecta, el proveedor de servicios de pago debe demostrar que la operación fue autenticada, registrada y contabilizada, y que no fue afectada por fallas técnicas u otras deficiencias del servicio. Por otro lado, el numeral 2 indica que el simple registro por parte del proveedor de la utilización del instrumento de pago no será suficiente para probar la autorización de la operación por parte del ordenante o su participación en un acto fraudulento, incumplimiento deliberado o negligencia grave en sus obligaciones. Finalmente, el numeral 3 especifica que es responsabilidad del proveedor de servicios de pago demostrar que el usuario del servicio cometió fraude o negligencia grave.

Adicionalmente, el artículo 45 establece que, si se lleva a cabo una operación no autorizada, el proveedor de servicios de pago reembolsará el monto de la operación de manera inmediata o, como máximo, al finalizar el siguiente día hábil después de que haya observado o sido notificado sobre la operación, a menos que tenga motivos razonables para sospechar fraude y comunique estos motivos por escrito al Banco de España.

Finalmente, el artículo 46 establece que el ordenante (consumidor) puede ser responsable de hasta 50 euros en pérdidas por operaciones no autorizadas si se utilizó un instrumento de pago extraviado, sustraído o apropiado por un tercero, a menos que no pudiera detectarlo antes del pago o la pérdida sea atribuible al proveedor de servicios de pago. Además, el ordenante soportará las pérdidas derivadas de operaciones de pago no autorizadas si incurrió en ellas por haber actuado de manera fraudulenta o por haber incumplido, de forma deliberada o por negligencia grave las obligaciones mencionadas en el artículo 41.

Sin embargo, quedará libre de responsabilidad en caso de sustracción, extravío o apropiación indebida de un instrumento de pago si las operaciones se realizaron de forma no presencial usando solo los datos impresos en la tarjeta, siempre que no se haya producido fraude o negligencia grave en la custodia del instrumento y las credenciales de seguridad, y se haya notificado de inmediato dicha situación. En caso de que el proveedor no requiera autenticación reforzada, el ordenante solo será responsable de soportar las consecuencias económicas en caso se demuestre que actuó de forma fraudulenta. Si el beneficiario o el proveedor de servicios de pago no aceptan la autenticación reforzada, deben reembolsar el importe al proveedor del ordenante. Excepto en casos de fraude, el ordenante no asumirá consecuencia económica alguna por la utilización, de manera posterior a la notificación referida en el artículo 41, de un instrumento de pago extraviado o sustraído.

C.1 Jurisprudencia

En las Sentencias Roj. SAP M 7327/2022 (2022) y Roj. SAP PO 496/2023 (2023) se menciona que, la negligencia exigida para responsabilizar al cliente debe surgir de una conducta caracterizada por una significativa falta de diligencia, por lo que no será considerada como tal aquella que fue inducida por el engaño de un delincuente profesional. En ese sentido, el usuario que fue víctima de engaño a través de phishing no puede considerarse negligente de manera grave, ya que se trata de un método de fraude difícil de detectar para un cliente promedio. A mayor detalle, en la Sentencia Roj. SAP S 1267/2023 (2023) se mencionó la sofisticación de la modalidad de estafa de *"phishing"* y su capacidad de imitar el lenguaje, formato e imagen de las entidades financieras a las que suplantan, de modo que inducen fácilmente a error a la víctima.

En la Sentencia Roj. SAP M 7327/2022 (2022) se cita también el Reglamento Delegado (UE) 2018/389 (2017), que señala la necesidad de que las entidades financieras implementen tecnología *antiphishing* para detectar y cerrar páginas clonadas que podrían comprometer las credenciales del usuario. Además, se establece la necesidad de una conducta activa y tecnológica por parte de la entidad financiera para evitar situaciones de fraude, la cual no debe limitarse a la simplemente informativa o divulgativa.

A mayor abundamiento, en la Sentencia Roj. SJPI 1022/2023 (2023) se indica que la entidad bancaria debe adoptar tecnología avanzada para garantizar la seguridad en operaciones online, ya que la responsabilidad de custodiar las credenciales no recae únicamente en el cliente, sino también en la entidad que debe implementar medidas activas para prevenir situaciones de fraude.

En este punto, se cita la Sentencia Roj. SAP M 6240/2015 (2015) en la que se menciona que, salvo actuación fraudulenta, incumplimiento deliberado o negligencia grave del ordenante (Art. 32), la responsabilidad será del proveedor del servicio de pago, lo que supone que a él le corresponde la carga de la prueba de que la orden de pago "no

se vio afectada por un fallo técnico o cualquier otra deficiencia". Además, la responsabilidad contemplada en la Ley se considera como cuasi-objetiva ya que la entidad bancaria solo es exonerada si prueba la culpa grave del ordenante.

En la Sentencia Roj. SAP B 6560/2023 (2023) el tribunal concluyó que, según la normativa legal, el proveedor de servicios de pago es responsable de la restitución al ordenante por operaciones no autorizadas, salvo excepciones. Una de estas excepciones consiste en que la responsabilidad recaerá en el ordenante en casos de actuación fraudulenta, negligencia grave o incumplimiento de sus obligaciones. Dicha norma va acompañada de la obligación de la carga de la prueba, la cual recae sobre el proveedor de servicios de pago, a quien le corresponde demostrar fraude o negligencia grave por parte del usuario.

La negligencia que atribuye responsabilidad al cliente es la que surge de una falta considerable de diligencia, lo que implica que la conducta se realiza por iniciativa del usuario y no como resultado del engaño al que pudo haber sido inducido. En ese sentido, no se considerará negligencia grave cuando el usuario no logre identificar mensajes fraudulentos o páginas web falsas, ya que para una persona sin conocimientos especializados puede ser difícil detectarlos. En contraste, las entidades financieras tienen la obligación de adoptar medidas de seguridad y mecanismos de supervisión para prevenir operaciones fraudulentas, siendo su responsabilidad implementar tecnología que permita la detección oportuna de fraudes como el *phishing* (Sentencia Roj. SAP PO 496/2023, 2023). En resumen, a fin de definir la negligencia grave es pertinente citar la Sentencia Roj. SAP C 481/2023 (2023), en la cual se precisa que "[l]a negligencia grave supone una falta de la diligencia más elemental que consiste en no hacer lo que todos hacen".

Cabe indicar que, en la Sentencia Roj. SAP O 2047/2023 (2023) se señala que, el análisis para determinar la responsabilidad de la entidad financiera no debe basarse esencialmente en los registros del banco, ya

que ello contraviene al artículo 44 de la Ley, que indica que el registro por el proveedor de servicios sobre el uso del instrumento de pago no constituye prueba suficiente de que la operación fue autorizada por el ordenante, ni de que este haya actuado de manera fraudulenta o incumplido deliberada o negligentemente alguna de sus obligaciones.

Finalmente, es importante mencionar que existen casos en los que se atribuye la responsabilidad de las operaciones al consumidor por haber obrado con imprudencia al introducir el código de autorización para realizar la operación sin leer el mensaje y al haberse revelado que el demandante ingresó a la APP auténtica de la entidad, lo que generaba dudas sobre si realizó la transferencia de modo involuntario (Sentencia Roj. SAP S 1277/2023, 2023).

C.2 Análisis comparativo con las normas peruanas

En España, los casos de operaciones no reconocidas se discuten ante el Poder Judicial; no obstante, los consumidores tienen la opción de recurrir a la mediación, arbitraje o realizar una reclamación directamente al proveedor de servicios. Este sistema difiere del modelo peruano, en el que, si bien los consumidores pueden accionar a través de las vías jurisdiccionales correspondientes o arribar a un acuerdo con los proveedores a través de mecanismos alternativos de solución de conflictos, la resolución de casos de operaciones no reconocidas es dirimida *prima facie* por el Indecopi, que es una autoridad administrativa.

Por otro lado, al igual que la normativa peruana, la española establece la obligación de la entidad financiera de realizar el bloqueo del instrumento de pago en situaciones debidamente justificadas, es decir, ante casos de presunto uso fraudulento o no autorizado de la tarjeta. En tales casos, tiene el deber de comunicarse con el consumidor para informarle previamente del bloqueo y de los motivos del mismo, si no puede entablar contacto, tiene que informarle de ello inmediatamente después de realizado el bloqueo.

De otra parte, se aprecia que la legislación española señala que el usuario tendrá derecho a la rectificación de una operación no autorizada o ejecutada incorrectamente por parte del proveedor de servicios de pago solo si comunica sin demora injustificada a la entidad financiera dentro de un plazo máximo de 13 meses contado desde la fecha del adeudo. Incluso se establece el procedimiento que el consumidor deberá seguir en los casos de pérdidas derivadas por operaciones no autorizadas efectuadas como consecuencia de extravío, pérdida, sustracción o apropiación indebida, señalando que el consumidor estará obligado a soportar hasta un máximo de 50 euros, salvo que no le resultase posible detectar ello con anterioridad al pago o cuando la pérdida sea atribuible al proveedor. Este punto difiere de la legislación peruana, en la que no se establece un supuesto de rectificación automática por parte de las entidades que brindan servicios de pago, ya que el consumidor previamente debe recurrir ante una autoridad administrativa o judicial para que ordene la devolución del monto de las operaciones no reconocidas, previa evaluación de la responsabilidad de los proveedores involucrados.

Otro aspecto importante por mencionar es que la normativa española señala que la entidad financiera tiene que probar que la operación fue autenticada y registrada sin fallos técnicos u otras deficiencias que pudieran presentarse en la prestación del servicio. Sin embargo, se establece de forma expresa que el registro de la utilización del instrumento de pago no será suficiente para acreditar que el usuario autorizó las operaciones o que actuó de forma fraudulenta, con negligencia grave o que incumplió deliberadamente sus obligaciones legales. Ello, se diferencia de la legislación peruana, en la que no existe una norma que establezca de forma expresa la insuficiencia del registro de las operaciones en los sistemas internos del banco para acreditar la autorización o actuación negligente del usuario; por el contrario, se verifica que, en las resoluciones emitidas por el Indecopi, un aspecto que se analiza al momento de evaluar la responsabilidad administrativa de la

entidad, y que en muchos casos suele ser determinante, es la correcta autenticación o registro de las operaciones en los sistemas de la entidad.

En relación con la jurisprudencia española, las sentencias tienen el criterio de que, en los casos de servicios de banca por internet, la responsabilidad de la entidad adopta un carácter cuasi-objetivo. Este régimen consiste en que la entidad bancaria solo será exonerada de responsabilidad si logra acreditar que el usuario actuó de forma fraudulenta, con negligencia grave o que incumplió deliberadamente sus obligaciones legales. Dicho criterio, se basa en que, al poner a disposición del cliente estos servicios, la entidad financiera asume el riesgo por la utilización de los mismos, por lo que le corresponde demostrar la autenticidad de la operación y que esta no se vio afectada por fallos técnicos o deficiencias en sus sistemas.

Adicionalmente, la jurisprudencia señala que, para que se considere la existencia de negligencia grave por parte del consumidor, esta debe surgir de una significativa falta de diligencia y no de la inducción al engaño por parte de un delincuente profesional, cuya detección no está al alcance de una persona media. Además, se aprecia que las sentencias establecen la obligación de la entidad financiera de adoptar tecnología avanzada para la custodia de las credenciales del cliente, así como para detectar y cerrar páginas clonadas que podrían comprometer la seguridad de sus usuarios de forma preventiva. Por tanto, la falta de diligencia y la falta de adopción de medidas preventivas también la harían responsable de la comisión de dichas operaciones.

Este criterio difiere del adoptado por el Indecopi, en el que suele darse un rol determinante a la correcta autenticación o registro de las operaciones materia de denuncia, así como al análisis del patrón de consumo del usuario. Para los órganos resolutivos del Indecopi, si el proveedor acredita el cumplimiento de la adopción de las medidas de seguridad legalmente establecidas es liberado de responsabilidad, sin que sea trascendental el grado de responsabilidad que el usuario pudo tener en la ejecución de dichas operaciones. En contraste, como se señaló

anteriormente, en España se presume la responsabilidad del proveedor a menos que demuestre la negligencia grave, fraude o incumplimiento de las obligaciones legalmente establecidas del consumidor, siendo este el único caso en el que será liberado de responsabilidad.

4.1.3 Objetivo Específico N.° 3

A través del tercer objetivo, buscamos proponer recomendaciones o lecciones que puedan ser implementadas para mejorar la predictibilidad de los pronunciamientos del Indecopi en casos de operaciones fraudulentas realizadas por internet. En este sentido, consideramos que es importante que el Indecopi establezca un precedente de observancia obligatoria o lineamientos que sirvan como referencia para los órganos resolutivos al momento de dictar decisiones en estos casos, ya que ello permitiría una mayor uniformidad en las resoluciones, brindando mayor seguridad jurídica a los administrados. A continuación, presentamos algunos de los lineamientos que podrían ser considerados tomando en cuenta los resultados obtenidos en los objetivos específicos 1 y 2 de la presente investigación:

- La carga de probar la adopción de las medidas de seguridad durante la ejecución de las operaciones bancarias efectuadas por internet recae en el proveedor, debido a que se encuentra en una posición más favorable y cuenta con más información que el usuario.
- Se recomienda un análisis inicial de la validez de las operaciones (correcto enrolamiento y autenticación), seguido por la evaluación del patrón de consumo del usuario a fin de detectar operaciones inusuales e identificar conductas fraudulentas.
- Al analizar la validez de las operaciones efectuadas por Banca Móvil y Banca por Internet, deberá verificarse la condición activa de la tarjeta, la afiliación o habilitación del canal utilizado, el correcto enrolamiento del usuario, así como, se deberá tomar en cuenta las obligaciones establecidas en el Reglamento de Gestión de la Seguridad de la Información y la Ciberseguridad respecto de la autenticación reforzada para operaciones efectuadas por canal digital que hubiesen sido efectuadas a partir del 2 de julio de 2022.

- En el caso de operaciones efectuadas por comercios electrónicos, se debe adoptar un criterio uniforme para determinar si las operaciones efectuadas a través de comercios electrónicos deben aplicar la autenticación reforzada.
- Se debe solicitar información del patrón de consumo del usuario de un periodo de al menos seis meses y como máximo un año antes de la ejecución de la operación no reconocida. Asimismo, al analizar el patrón de consumo del usuario, se deben evaluar de forma integral y sistemática factores como el canal, frecuencia, tipo de comercio, moneda, lugar, límite operacional, importe, etc.
- Se debe evaluar la generación de alertas en el sistema de monitoreo tras la materialización de más de una operación inusual en un periodo específico. No obstante, debe tomarse en cuenta que la activación de alertas exige la materialización de más de una operación inusual, ya que el sistema de monitoreo no tiene una naturaleza preventiva. También, se debe evaluar que la entidad financiera haya establecido mecanismos de comunicación inmediata al usuario ante la detección de una operación atípica o inusual, con la finalidad de validar su ejecución, y, si no es posible establecer contacto con este, proceder con el bloqueo preventivo de la tarjeta.
- En cuanto a las medidas correctivas, se sugiere la devolución total de los fondos si se demuestra que no fueron realizadas válidamente, de otro lado, si las operaciones se ajustan al patrón de consumo, pero se demuestra que son fraudulentas, solo deberán devolverse las subsiguientes a la primera operación inusual. Además, como medida correctiva complementaria debe ordenarse la devolución de los intereses legales generados hasta la fecha de la devolución efectiva de los fondos sustraídos.
- La graduación de la sanción en los casos de operaciones fraudulentas debe realizarse aplicando las fórmulas y factores establecidos en el Decreto Supremo 032-2021-PCM.

4.1.4 Objetivo General

El problema de la falta de predictibilidad en los pronunciamientos del Indecopi en casos de operaciones no reconocidas es un desafío que afecta la

seguridad jurídica de los usuarios administrados en nuestro país. Esta situación se agrava por el hecho de que los métodos fraudulentos para sustraer dinero de las cuentas bancarias evolucionan de manera constante, lo que genera una brecha entre los avances tecnológicos de los delincuentes y las medidas de seguridad implementadas por las entidades bancarias. Como consecuencia, los usuarios se encuentran en un estado de vulnerabilidad, lo que exige que tanto las entidades financieras como las instituciones del estado adopten una posición más proactiva y eficiente.

En este sentido, es necesario que el Indecopi cuente con criterios predictivos a nivel nacional que garanticen un tratamiento equitativo de los casos de operaciones fraudulentas realizadas a través de internet. La predictibilidad en los pronunciamientos no solo otorga seguridad jurídica, sino que también contribuye a incrementar la confianza de los usuarios en las instituciones encargadas de proteger sus derechos. Además, resulta imperativo actualizar la legislación vigente para que esté alineada con las tendencias internacionales y contemple las mejores prácticas de la legislación comparada.

Desde el punto de vista normativo, se sugiere la implementación de una legislación que se mantenga a la vanguardia en materia de seguridad bancaria y protección al consumidor. Dicha legislación debe incluir medidas que evolucionen junto con los avances tecnológicos, garantizando que las entidades financieras cumplan con estándares mínimos de seguridad.

Por otro lado, es necesario que tanto el Indecopi como la SBS, en el marco de sus competencias, asuman un rol más proactivo. Ello implica una mayor fiscalización del cumplimiento de las normas por parte de las entidades financieras, así como el desarrollo de políticas preventivas y de concientización sobre el fraude bancario.

Dicho esto, es fundamental que el marco normativo tenga la flexibilidad necesaria para adaptarse a la realidad cambiante de los avances tecnológicos, sin perder de vista la importancia de mantener un enfoque centrado en la protección de los derechos de los consumidores. En ese sentido, a continuación, presentamos algunas consideraciones extraídas de la legislación comparada analizada en el marco de la presente investigación; es importante indicar que

consideramos que su análisis y debate es importante a fin de contar con un marco normativo que se adapte a la realidad y permita luchar de forma efectiva ante casos de fraude bancario:

- La SBS y el Indecopi, de acuerdo con sus competencias y atribuciones, deben evaluar la implementación de procedimientos de oficio para salvaguardar el interés colectivo de los consumidores afectados por operaciones no reconocidas y/o para verificar el cumplimiento efectivo de las disposiciones normativas relativas a medidas de seguridad, ello incluye revisar si las medidas de seguridad de las entidades financieras están actualizadas de acuerdo con la normativa de la materia y son efectivas contra fraudes, o evaluar la interposición de demandas ante el Poder Judicial por afectación a los intereses colectivos de consumidores en casos de operaciones no reconocidas.
- Debe incluirse una disposición que establezca la obligación de las entidades financieras de reembolsar los fondos sustraídos o realizar la rectificación automática ante operaciones fraudulentas, cuando el consumidor presente un reclamo, salvo que se acredite dolo, culpa grave o participación en el fraude por parte del usuario, y siempre que el consumidor haya notificado sin demora a la entidad financiera sobre la ocurrencia del fraude.
- No obstante, aun en caso se verifique la culpa grave del usuario, si se demuestra que la omisión del deber de adoptar las medidas de seguridad pertinentes de parte de la entidad bancaria coadyuvó en la ejecución de las operaciones no reconocidas se debe determinar que existe una situación de responsabilidad compartida, por lo que se debe establecer qué porcentaje de la responsabilidad recae en la entidad financiera y qué porcentaje en el usuario.
- Además, se debe especificar normativamente que el simple registro de las operaciones no es suficiente para acreditar que el usuario autorizó las operaciones o que actuó de manera fraudulenta o negligente.
- Se debe evaluar también la incorporación de una disposición que considere la falta de diligencia en la adopción de medidas preventivas ante fraude

informático por parte de la entidad financiera como un factor de responsabilidad.

4.2 Discusión

Respecto del primer objetivo específico, se observa que los órganos resolutivos del Indecopi no son predictivos en la resolución de casos relacionados con operaciones fraudulentas realizadas a través de internet durante los años 2022 y 2023. Ello, se evidencia al verificar que carecen de un criterio unificado al momento de analizar el parámetro de idoneidad de las medidas de seguridad adoptadas por la entidad financiera, así como al ordenar medidas correctivas o imponer sanciones.

Si bien se encontraron puntos de coincidencia en aspectos, como: (i) el hecho de que la negligencia o la falta de diligencia del consumidor en el uso de su tarjeta no es un factor determinante para exonerar de responsabilidad a la entidad financiera, ya que, aunque el comportamiento del consumidor haya sido decisivo en la ejecución de las operaciones fraudulentas, la entidad debe acreditar el cumplimiento de sus obligaciones legales y contractuales; de no hacerlo, asume la responsabilidad por dichas operaciones; y, (ii) respecto a que la carga de la prueba recaerá siempre en el proveedor, que debe demostrar la validez de las operaciones, así como su conformidad con el patrón de consumo del usuario; ello no enerva el hecho de que no cuenten con un criterio unificado en las seis categorías restantes.

Respecto al análisis del cumplimiento del deber de idoneidad de las medidas de seguridad adoptadas por la entidad financiera, se observaron discrepancias en los criterios adoptados por los órganos resolutivos. Algunos órganos examinan primero la validez de las operaciones para luego verificar el cumplimiento del deber de monitoreo y detección de operaciones inusuales por parte de la entidad bancaria. En cambio, otros verifican, en principio, si la entidad llevó a cabo el monitoreo y detección de operaciones inusuales y, posteriormente, analizan la validez de la operación. Esta variabilidad de criterios puede influir en el resultado final de los casos, ya que el orden en la aplicación de estos filtros afecta la determinación de la responsabilidad del proveedor, en tanto algunos órganos consideran suficiente la acreditación correcta del registro de las operaciones en los sistemas del banco para exonerarlo de responsabilidad, mientras que otros solo analizan si las operaciones se ajustaban al

patrón de consumo habitual del usuario e infundan la denuncia si dicha condición se acredita.

Por otro lado, en cuanto al análisis de la validez de las operaciones, se verifica que los criterios aplicables varían dependiendo del tipo de canal utilizado. Al respecto, se constató la falta de un criterio unificado que identifique los filtros que la autoridad debe evaluar para determinar el correcto enrolamiento y autenticación de las operaciones, ya que algunas resoluciones establecen filtros detallados, mientras que otras simplemente analizan si la operación cuestionada se realizó con el uso de información confidencial. En este sentido, es necesario que la autoridad establezca criterios definidos para determinar si la operación se realizó de manera válida.

De otra parte, se aprecia que existe discrepancia de criterios al requerir los estados de cuenta para analizar patrones de fraude, puesto que no se ha establecido el plazo o período que debe ser analizado para determinar si la operación se ajusta al patrón de consumo del usuario. En este punto, es importante mencionar, además, que los órganos resolutivos carecen de un criterio uniforme para identificar las operaciones que no se ajustan al comportamiento habitual del consumidor, en tanto no se encuentran definidos los factores que deben evaluarse para determinar habitualidad de las operaciones. Además, se verifica que mientras que algunos órganos prefieren examinar cada operación de manera individual, otros realizan un análisis integral, contrastando estas operaciones con el historial de comportamiento del usuario. En ese sentido, se hace necesario que el análisis de habitualidad parta de un examen integral que considere diversas circunstancias y factores para la detección de operaciones sospechosas a fin de que no se afecte la fluidez de las transacciones financieras legítimas de los clientes.

Con respecto a la generación de alertas, se aprecia una tendencia entre los órganos resolutivos de considerar que la primera operación es la que debe generar la alerta a fin de establecer comunicación con el consumidor y confirmar su autorización para proceder con su ejecución. Sin embargo, al revisar las resoluciones, se observa que no todas evalúan el cumplimiento de la obligación de la entidad de contactar al usuario antes de proceder con el bloqueo preventivo de la tarjeta. Por lo tanto, es fundamental que se establezcan criterios uniformes en relación con el cumplimiento del deber de generación y gestión de alertas para garantizar una respuesta efectiva ante posibles transacciones fraudulentas.

En cuanto al otorgamiento de medidas correctivas, también se evidencian discrepancias cuando se determina que las operaciones se realizaron de manera válida pero no obedecen a patrones de fraude. Algunos órganos resolutivos ordenan la devolución solo de las operaciones subsiguientes a la primera operación que fue realizada de forma válida, ya que consideran que el sistema de monitoreo no tiene una naturaleza predictiva, por lo que es necesario procesar la primera operación para que sirva como base para generar la alerta en los sistemas del banco. En contraste, otros órganos resolutivos ordenan la devolución de la totalidad de las operaciones, incluyendo la primera. Esta divergencia de criterios puede generar inconsistencia en las decisiones de la autoridad y afectar la igualdad en el tratamiento de los casos de operaciones no reconocidas, tomando en cuenta que la decisión que se adopte en este punto tiene consecuencias patrimoniales en las partes del procedimiento.

Por otro lado, en relación con la graduación de la sanción, también se observa una discrepancia en los criterios utilizados por los órganos resolutivos, ya que algunos consideran como criterios atenuantes el monto de las operaciones realizadas y el principio de razonabilidad, y optan por amonestar al proveedor o imponer una sanción más baja que la establecida en el Decreto Supremo 32-2021-PCM, por lo que es necesario unificar los criterios también en este punto para garantizar una mayor coherencia y predictibilidad en las decisiones del Indecopi.

Respecto del segundo objetivo, se observa que en Chile, Colombia y España, no se cuenta con una autoridad administrativa que tenga facultades para determinar, a través de un procedimiento administrativo, la responsabilidad de las entidades financieras en los casos de operaciones no reconocidas, sino que dichas cuestiones se dilucidan directamente ante el Poder Judicial, por lo que, además de obtener la devolución de las operaciones no reconocidas, el consumidor podría obtener una indemnización por los daños y perjuicios ocasionados.

En la jurisprudencia chilena, se establece que la entidad financiera tiene el deber de restituir las operaciones no autorizadas al usuario; siendo que, si logra acreditar dolo, culpa grave o la participación del usuario en el fraude, puede iniciar las acciones judiciales ante el juez de policía local para ser liberado de responsabilidad y obtener el recupero de dichos fondos. Es decir, en los casos de operaciones fraudulentas, el usuario obtiene la restitución de los fondos de forma directa, sin tener que recurrir previamente

a la autoridad administrativa o judicial para que ordene la restitución de los mismos, ello obedece a que, para la normativa chilena, es insuficiente que la operación se encuentre correctamente registrada para determinar la falta de responsabilidad de la entidad financiera, por lo que solo se la libera de responsabilidad si logra acreditar que la conducta del usuario fue determinante para la ejecución de las operaciones no reconocidas, y que incurrió en culpa grave, dolo o participó en los actos fraudulentos.

Por otro lado, en la jurisprudencia colombiana, se menciona el deber de las entidades financieras de verificar el hábito transaccional del consumidor, por lo que, incluso en casos de culpa grave, es deber del banco acreditar el cumplimiento de dicha obligación. En este punto, se establece el sistema de concurrencia de culpas, que consiste en que la conducta culposa del usuario puede ser determinante en la exposición al riesgo ante una operación fraudulenta. En tales casos, se determina la responsabilidad parcial del consumidor y se le responsabiliza por la pérdida de los fondos en una porción o porcentaje. Es decir, la responsabilidad por una operación no reconocida puede ser compartida entre la entidad y el usuario, dependiendo de las circunstancias del caso y de la contribución de cada parte en la ejecución de la operación.

En España, existe la presunción *iuris tantum* de que el consumidor ha cumplido con sus obligaciones legales relacionadas con el resguardo de sus credenciales; por lo tanto, corresponde a la entidad financiera demostrar que la actuación fraudulenta, negligencia grave o incumplimiento de las obligaciones provienen del usuario. Asimismo, la entidad financiera debe probar que la operación fue autenticada, registrada y contabilizada sin fallos técnicos u otras deficiencias que puedan presentarse en la prestación del servicio; sin embargo, es importante tener en cuenta que el solo registro del uso del instrumento de pago no es suficiente para acreditar la correcta autorización del usuario en la ejecución de las operaciones.

De lo anterior, se aprecia que el tratamiento de los casos de operaciones no reconocidas en otros países se fundamenta en el hecho de que las entidades financieras son las proveedoras del servicio de operaciones bancarias por internet, por lo que son ellas quienes deben asumir el riesgo inherente a la prestación de dicho servicio. Además, en la jurisprudencia se les exige realizar acciones preventivas para evitar la vulneración de sus sistemas y permanecer a la vanguardia en la protección de sus clientes contra posibles estafas. En este contexto, se presume la responsabilidad de la

entidad financiera en casos de operaciones fraudulentas efectuadas por internet, a menos que pueda demostrar la actuación dolosa, culpa grave, negligencia o participación del usuario en el fraude. Es decir, la entidad tendrá la carga de probar su actuación diligente durante la ejecución de las operaciones y de demostrar que fue el cliente quien incurrió en conductas que contribuyeron al fraude. En el caso peruano, si bien la autoridad resolutiva impone a la entidad financiera la carga de la prueba de demostrar la correcta realización de las operaciones y el cumplimiento de sus deberes de monitoreo y seguridad, es más indulgente al momento de determinar su responsabilidad, ya que, si acredita el cumplimiento de sus obligaciones legales, se le exonera de responsabilidad y se impone al usuario la carga de asumir el costo de las operaciones no reconocidas.

Sin embargo, dada la rápida evolución de la tecnología y la sofisticación de los métodos empleados por los delincuentes cibernéticos, así como la vulnerabilidad de los usuarios frente a estas situaciones, podría considerarse inadecuado que los consumidores asuman la responsabilidad por la realización de tales transacciones, a menos que se demuestre su culpa grave, dolo o participación en el fraude. En este sentido, además de acreditar que las operaciones fueron correctamente validadas y se cumplió con el deber de monitoreo y gestión de alertas, la entidad financiera debería probar la participación en el fraude, negligencia grave o dolo del usuario en la ejecución de las operaciones y, de no poder demostrar su culpabilidad, asumir la pérdida de los fondos, o en los casos de concurrencia de culpas, compartir con el consumidor la responsabilidad por las operaciones no autorizadas.

Cabe indicar que, al asumir una carga de la prueba más rigurosa, las entidades financieras se verán incentivadas a implementar y mantener medidas de seguridad más efectivas, para evitar posibles sanciones por parte de la autoridad administrativa. Ello podría incluir la mejora de los sistemas de autenticación, mayor proactividad en la vigilancia de actividades sospechosas y la actualización constante de sus protocolos de seguridad para hacer frente a nuevas amenazas cibernéticas.

Respecto al tercer objetivo específico, se elaboró un modelo de lineamiento que podría implementarse para mejorar los pronunciamientos del Indecopi en casos de operaciones fraudulentas realizadas por internet. Este modelo se basa en los resultados obtenidos en la presente investigación y aborda las principales discrepancias identificadas en la jurisprudencia analizada, así como algunas modificaciones

normativas e iniciativas que podrían implementarse, a fin de promover una mayor responsabilidad de las entidades financieras en la prevención de fraudes y mejorar la protección de los derechos de los consumidores usuarios de los servicios financieros (anexo 4).

CONCLUSIONES

- Se evidencia que los pronunciamientos del Indecopi emitidos a nivel nacional en materia de operaciones fraudulentas efectuadas por internet durante los años 2022 a 2023 no son predictivos, ya que los órganos resolutivos presentan criterios diferentes al momento de evaluar la responsabilidad de la entidad financiera y se verifica que no existe un criterio unificado al analizar los parámetros de idoneidad que las medidas de seguridad implementadas por las entidades financieras deben cumplir. Además, respecto del otorgamiento de las medidas correctivas, se observa una evidente discrepancia de criterios en cuanto a la devolución o extorno de las operaciones fraudulentas, así como sobre la devolución de los intereses legales generados; de igual manera, al momento de graduar la sanción, se aprecia que algunos órganos han optado por utilizar criterios diferentes a los establecidos en el Decreto Supremo 32-2021-PCM.

- En Chile, Colombia y España, los casos de operaciones bancarias no reconocidas se resuelven en la vía judicial, ya sea a través del Poder Judicial o de órganos administrativos con facultades jurisdiccionales; por consiguiente, los consumidores pueden demandar, además de la devolución del importe de las operaciones, una indemnización por los daños y perjuicios ocasionados. En Perú, aunque el consumidor final cuenta con la vía judicial para satisfacer sus pretensiones, también puede recurrir ante el Indecopi, que es una autoridad administrativa, y obtener la devolución del importe de las operaciones, previa evaluación de la responsabilidad del proveedor denunciado.

  Por otro lado, en la jurisprudencia sobre operaciones fraudulentas de estos países, se observa que las entidades financieras únicamente pueden exonerarse o atenuar su responsabilidad si logran acreditar que el consumidor actuó con culpa grave, dolo, negligencia grave o si se demuestra que participó en las conductas fraudulentas; por tanto, el simple registro de las operaciones no reconocidas en los sistemas de las entidades financieras no es suficiente para acreditar la autorización del consumidor en la ejecución de las operaciones. Esto contrasta con la jurisprudencia del Indecopi, que considera suficiente que la entidad bancaria demuestre la validación o autenticación correcta de las operaciones y el cumplimiento de sus deberes de monitoreo y seguridad para ser liberada de responsabilidad.

- Es necesario que el Indecopi establezca lineamientos en casos de operaciones no reconocidas, de tal manera que sea utilizado por los órganos resolutivos al momento de resolver. Sobre la base de los resultados de la presente investigación, consideramos que los siguientes criterios deben ser tomados en cuenta al momento de resolver estos casos: (i) la responsabilidad de acreditar el correcto procesamiento de las operaciones recae en el proveedor; (ii) se recomienda un análisis inicial de la validez de la operación, seguido por la evaluación del patrón de consumo del usuario en un periodo de seis meses a un año previo a la operación no reconocida; (iii) al analizar la validez de las operaciones, deberá verificarse la habilitación del canal utilizado, así como el correcto enrolamiento y autenticación, (iv) al analizar el patrón de consumo del usuario, se deben evaluar de forma integral diversos factores y activar alertas tras la primera operación inusual; (v) se sugiere la devolución total de los fondos si se demuestra que el usuario no realizó válidamente las operaciones, de otro lado, si las operaciones no se ajustan al patrón de consumo, pero fueron válidas, solo se devolverán las subsiguientes a la primera operación inusual, y (v) las sanciones deben imponerse de conformidad con el Decreto Supremo 32-2021-PCM.

- Es fundamental que el marco normativo tenga la flexibilidad necesaria para adaptarse a la realidad cambiante de los avances tecnológicos. Por tanto, resulta imperativo actualizar la legislación vigente para que esté alineada con las tendencias internacionales y contemple las mejores prácticas de la legislación comparada. En ese sentido, se propone lo siguiente: (i) La SBS e Indecopi deben implementar procedimientos de oficio para proteger a los consumidores ante operaciones no reconocidas y verificar que las entidades financieras cumplan con medidas de seguridad actualizadas; (ii) las entidades financieras deberían estar obligadas a reembolsar los fondos sustraídos o corregir automáticamente operaciones fraudulentas tras el reclamo del usuario, salvo dolo, culpa grave o participación en el fraude del consumidor, y siempre que el fraude haya sido notificado sin demora; (iii) asimismo, el simple registro de una operación no puede ser suficiente para probar que fue autorizada por el usuario; y, (iv) finalmente, se sugiere incluir una disposición que considere la falta de medidas preventivas como un factor de responsabilidad de las entidades financieras.

RECOMENDACIONES

- Se recomienda a los órganos resolutivos del Indecopi que unifiquen sus criterios a nivel nacional al evaluar los parámetros de idoneidad con los que las medidas de seguridad implementadas por las entidades financieras deben contar, especialmente, en lo que se refiere a la autenticación de las operaciones, la evaluación del patrón de consumo del usuario y la gestión de alertas generadas por el sistema de monitoreo de operaciones; asimismo, se sugiere establecer criterios claros y uniformes en el otorgamiento de medidas correctivas y graduación de las sanciones, ya que la unificación de criterios es fundamental para fortalecer la confianza de los administrados en los procedimientos administrativos sancionadores tramitados por el Indecopi y permitirá mejorar la predictibilidad de las decisiones emitidas por los diversos órganos resolutivos.
- Ante el constante avance tecnológico y la creciente vulnerabilidad del usuario frente a posibles situaciones de fraude resulta imperativo adoptar un nuevo enfoque en la legislación, que considere la responsabilidad de las entidades financieras en casos de fraude informático como una presunción inicial, de la cual solo podrán liberarse si logran demostrar la existencia de culpa grave, dolo o participación del usuario en el fraude.
- Es necesario evaluar la introducción de disposiciones normativas que dispongan la devolución automática de operaciones no autorizadas por parte de la entidad financiera, siempre que el consumidor notifique sin demora injustificada a la entidad financiera ante una situación de fraude. Asimismo, debe considerarse la incorporación de una disposición que determine que el registro de la utilización del instrumento de pago no es suficiente para acreditar que el usuario autorizó las operaciones o que actuó de manera fraudulenta o negligente.
- Se recomienda al Indecopi y a la SBS, en el marco de sus competencias y atribuciones, la implementación de procedimientos colectivos voluntarios o el inicio de procedimientos sancionadores de oficio que tengan por finalidad salvaguardar el interés colectivo o difuso de los consumidores víctimas de operaciones fraudulentas o para verificar el cumplimiento efectivo de las disposiciones relativas a medidas de seguridad contenidas en la normativa vigente.

BIBLIOGRAFÍA

Abad, J., y Reyes, M. (2022). *Transacciones fraudulentas y delitos informáticos* [Tesis para optar el título de abogado, Universidad Privada de Trujillo]. http://repositorio.uprit.edu.pe/handle/UPRIT/38/browse?value=REYES+CORCINO%2C+MARITZA+JOVANNAytype=author

Aware. (2019). *How financial institutions secure mobile banking with biometric technology*. https://www.aware.com/blog-securing-mobile-banking-biometric-technology/

Balcazar, W. (2017). *Medidas de seguridad que deberían incorporarse a fin de evitar operaciones no reconocidas en tarjetas de crédito y débito* [Tesis para obtener el título profesional de abogado, Universidad Privada Antenor Orrego]. https://repositorio.upao.edu.pe/handle/20.500.12759/3314

Banga, L., y Pillai, S. (2021). Impact of Behavioural Biometrics on Mobile Banking System. *Journal of Physics: Conference Series*, *1964*(6), 062109. https://doi.org/10.1088/1742-6596/1964/6/062109

Begazo, F., y Vela, V. (2022). *Aplicación de criterios tuitivos en la determinación de responsabilidad administrativa derivada de relaciones financieras de consumo afectadas por fraudes informáticos tramitados ante Indecopi-OR-Arequipa (2019-2021)* [Tesis para optar el título profesional de Abogado, Universidad Nacional de San Agustín de Arequipa]. http://hdl.handle.net/20.500.12773/15592

Bernal, C. (2023). *La responsabilidad de los proveedores de productos y servicios financieros por el uso de tarjetas de pago y transacciones electrónicas de carácter ilícito* [Tesis de Maestría, Universidad de Chile]. https://repositorio.uchile.cl/handle/2250/196134

Blossiers, J. (2016). *Para conocer el derecho bancario*. Grupo Editorial Lex y Iuris.

Broseta, M. (1994). *Manual de Derecho Mercantil*. Editorial Tecnos S.A.

Cabrera, M., y Quintana, R. (2013). *Derecho Administrativo y Derecho Procesal Administrativo*. Ediciones Legales.

Cairampoma, A. (2014). La regulación de los precedentes administrativos en el ordenamiento jurídico peruano. *Derecho PUCP, 73*. https://doi.org/10.18800/derechopucp.201402.014

Calvo, M. (2022). La responsabilidad civil de los bancos en los delitos de estafa por "phishing." *Actualidad Jurídica Iberoamericana, 18*. https://dialnet.unirioja.es/servlet/articulo?codigo=8947777

Camacho, M. (2019). *Derecho Económico, Financiero y Bancario*. Editora y Librería Jurídica Grijley E.I.R.L.

Castillo, J. (2018). *El delito informático y su implicación en el patrimonio económico en Colombia* [Especialización en Administración de la Seguridad, Universidad Militar Nueva Granada]. http://hdl.handle.net/10654/17914

Coello, D. (2019). *Identificación biométrica. La seguridad del futuro*. Openbank Open News Blog. https://www.openbank.es/open-news/identificadores-biometricos/

De Romaña, G. (2022). *Análisis del sistema regulatorio en los servicios de telefonía e internet fija y móvil y su necesidad de permanente revisión y cambio, Perú 2021* [Tesis de Maestría, Escuela de Postgrado San Francisco Xavier SFX]. http://repositorio.sfx.edu.pe/handle/SFX/76

Divito, F. (2021). *Skimming y phishing de tarjetas de crédito o débito: ¿actos preparatorios o principio de ejecución de la defraudación cometida mediante tarjeta falsificada o el uso de sus datos?* [Tesis de Maestría, Universidad de San Andrés]. http://hdl.handle.net/10908/18343

Duran, J. (2020). *Principales características, modos de perpetración y vulneración de la seguridad informática a través de la modalidad carding* [Especialización en seguridad informática, Universidad Nacional Abierta y a Distancia "UNAD"]. https://repository.unad.edu.co/handle/10596/34366

Escárate, N. (2015). *Análisis del delito de uso fraudulento de tarjeta de crédito o débito contenido en la Ley 20.009* [Tesis para optar el grado de Licenciada en Ciencias Jurídicas y Sociales, Universidad de Chile]. https://repositorio.uchile.cl/handle/2250/132589

Figueroa, H. (2010). *Derecho del Mercado Financiero*. Editora y Librería Jurídica Grijley E.I.R.L.

Gobierno del Perú. (2024). *Conocer más sobre las billeteras digitales disponibles en el Perú*. Plataforma Digital Única Del Estado Peruano. https://www.gob.pe/14930-conocer-mas-sobre-las-billeteras%20-digitales-disponibles-en-el-peru

Guzmán, C. (2013). *Manual del Procedimiento Administrativo General*. Pacífico Editores S.A.C.

Hernández, J. (2020). *La responsabilidad de las entidades financieras por fraudes electrónicos* [Trabajo de Maestría, Universidad Pontificia Bolivariana]. http://hdl.handle.net/20.500.11912/6161

Hernández, R., Fernández, C., y Baptista, M. del P. (2014). *Metodología de la investigación*. McGRAW-HILL y S. A. INTERAMERICANA EDITORES.

Huamán, L. (2017). *Procedimiento Administrativo General Comentado*. Jurista Editores E.I.R.L.

Linares, L. (2020). *El deber de idoneidad de las entidades bancarias de la región La Libertad en el fraude electrónico con tarjetas de crédito y débito* [Tesis para optar el título profesional de Abogada, Universidad Privada del Norte]. https://hdl.handle.net/11537/25849

López, P. (2015). *¿Qué es el vishing?* BBVA. https://www.bbva.com/es/innovacion/vishing-la-imaginacion-los-estafadores-no-limites/

Lozano, A. (2008). El perfil financiero: una estrategia para detectar el lavado de activos. *Revista Criminalidad, 50*(2). https://dialnet.unirioja.es/servlet/articulo?codigo=5744723yinfo=resumen

Manjarrés, J. (2023). *Responsabilidad civil de los establecimientos bancarios por la utilización fraudulenta de canales electrónicos de disposición de depósitos y su relación con los hábitos transaccionales de los consumidores financieros* [Tesis de Maestría, Universidad Externado de Colombia]. https://doi.org/10.57998/bdigital/handle.001.169

Mayer, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Ius et Praxis*, *24*(1), 159–206. https://doi.org/10.4067/S0718-00122018000100159

Mayer, L., y Oliver, G. (2020). El delito de fraude informático: concepto y delimitación. In *Revista chilena de derecho y tecnología*, *9*(1), 151–185. https://www.scielo.cl/scielo.php?script=sci_arttextypid=S0719-25842020000100151

Meza, P. (2012). *El estándar de consumidor razonable aplicado en los consumos fraudulentos generados por clonación* [Tesis para optar por el Título de Abogado, Pontificia Universidad Católica del Perú]. https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/1668

Misra, S., Thakur, S., Ghosh, M., y Saha, S. K. (2020). An Autoencoder Based Model for Detecting Fraudulent Credit Card Transaction. *Procedia Computer Science*, *167*, 254–262. https://doi.org/10.1016/j.procs.2020.03.219

Mora, C. (2020). *Criterios para resolver casos de operaciones no reconocidas efectuadas mediante el uso de tarjetas de crédito o débito* [Trabajo Académico para optar el título de Segunda Especialidad en Derecho de Protección al Consumidor, Pontificia Universidad Católica del Perú]. http://hdl.handle.net/20.500.12404/1668

Morales, M., y Prieto, L. (2021). *Eficiencia de la protección al consumidor financiero en el fraude de tarjetas de crédito* [Tesis para optar el título de abogado, Universidad Santo Tomás]. http://hdl.handle.net/11634/42995

Morón, J. (2018). *Comentarios a la Ley del Procedimiento Administrativo General*. Gaceta Jurídica.

Oxman, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del “phishing” y el “pharming.” *Revista de derecho*, 41, 211–262. https://dx.doi.org/10.4067/S0718-68512013000200007

Pareja, J. (2022). *Algunas críticas a las medidas de seguridad en materia de patrón de consumo en el empleo de tarjetas de pago* [Trabajo Académico para optar el título de Segunda Especialidad en Derecho de Protección al Consumidor,

Pontificia Universidad Católica del Perú]. http://hdl.handle.net/20.500.12404/24583

Patrón, C. (2011). *Protección al Consumidor en los Servicios Financieros*. Ediciones Caballero Bustamante S.A.C.

Peláez-Ypanaqué, R. (2014). La naturaleza del procedimiento de protección al consumidor del Indecopi y la oportunidad de desistimiento en aquel. *IUS ET PRAXIS, Revista de La Facultad de Derecho de La Universidad de Lima*, *45*. https://doi.org/10.26439/iusetpraxis2014.n045.376

Perú Retail. (2023). *No solo Yape y Plin: Conoce las billeteras digitales disponibles en Perú y en qué se diferencian*. Perú Retail. https://www.peru-retail.com/no-solo-yape-y-plin-conoce-las-billeteras-digitales-disponibles-en-peru-y-en-que-se-diferencian/

Pineda, J. (2008). *Investigación Jurídica.* Editorial Pacífico.

Ponce, J. (2022). *La clonación de tarjetas de créditos y débitos, su implicancia como delito informático en el Perú* [Tesis para optar el título profesional de Abogado, Universidad Peruana Las Américas]. http://repositorio.ulasamericas.edu.pe/handle/upa/2715

Puémape, D. (2013). *Tratado Elemental Derecho Bancario Peruano*. Aries Editores.

Quispe, N. (2021). *Análisis del plan de mejora en el proceso de atención de reclamos de operaciones no reconocidas en una entidad bancaria* [Tesis para optar el Título de Licenciado en Administración de Empresas, Universidad de Piura]. https://hdl.handle.net/11042/4876

Ruiz, M., Borboa, M., y Rodríguez, J. (2013). El enfoque mixto de investigación en los estudios fiscales. In *Revista Académica de Investigación*, *13*, 10–11. https://dialnet.unirioja.es/servlet/articulo?codigo=7325416

San Miguel, V. (2019). *La tarjeta de crédito en el sistema financiero peruano como un mecanismo de acceso al crédito: límites y posibilidades* [Universidad de Lima]. https://doi.org/10.26439/ulima.tesis/8043

Santander. (2020). *¿Qué es la banca digital?* Santander. https://www.santander.com/es/stories/que-es-la-banca-digital

Scotiabank. (2023, August 17). *¿Qué es el CVV dinámico?* Scotiabank. https://ayuda.scotiabank.com.mx/article/que-es-el-cvv-dinamico

Semana. (2014). *Los tipos de robos que hacen a través de las tarjetas*. https://www.semana.com/credito/articulo/los-robos-pueden-hacer-tarjetas/53157/

Sifuentes, R. (2022). *La predictibilidad del comportamiento habitual de consumo en el marco del análisis de operaciones no reconocidas realizadas con tarjetas de crédito y/o débito* [Trabajo Académico para optar el título de Segunda Especialidad, Pontificia Universidad Católica del Perú] http://hdl.handle.net/20.500.12404/24567

Silvestre, J. (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 para optar el título de Segunda Especialidad, Pontificia Universidad Católica del Perú]. http://hdl.handle.net/20.500.12404/21054

Stucchi, P., Bezada, J., y García, Ó. (2021). *Manual de Derecho del Consumo aplicado a los Servicios Bancarios*. Palestra Editores.

Superintendencia Financiera de Colombia. (n.d.). Lo que usted debe saber sobre funciones Jurisdiccionales de la Superintendencia Financiera de Colombia en materia de protección al consumidor financiero. *Superintendencia Financiera de Colombia*. Superintendencia Financiera de Colombia. Recuperado el 24 de febrero de 2024, de https://im.sura-am.com/sites/default/files/2020-10/ABC%20Negocios%20Fiduciarios.pdf

Tirado, J. (2015). El desistimiento del denunciante en el procedimiento administrativo sancionador. *PRAECEPTUM, 2*. http://hdl.handle.net/11724/7723

Ventura, M. (2021). *La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima, 2020* [Tesis para optar el título profesional de Abogada, Universidad Privada del Norte]. https://repositorio.upn.edu.pe/handle/11537/28942

ANEXOS

Anexo 1. Matriz de consistencia

PROBLEMA	OBJETIVOS	VARIABLES	DIMENSIONES	INDICADORES	METODOLOGÍA
GENERAL	**GENERAL**	**VARIABLES INDEPENDIENTES:** Pronunciamientos del Indecopi emitidos a nivel nacional en materia de operaciones fraudulentas	Instancia administrativa	➢ Primera instancia: OPS, CPC ➢ Segunda instancia: CPC, OPS, SPC	
			Tipo de servicio utilizado	➢ Banca móvil ➢ Banca por internet ➢ Compras por internet	**ENFOQUE:**
¿Cuál es la problemática jurídica subyacente en la predictibilidad de los pronunciamientos del Indecopi emitidos a nivel nacional en materia de operaciones fraudulentas efectuadas por internet durante los años 2022 a 2023?	Analizar la problemática jurídica subyacente en la predictibilidad de los pronunciamientos del Indecopi emitidos a nivel nacional en materia de operaciones fraudulentas efectuadas por internet durante los años 2022 a 2023.		Competencia territorial	➢ Lima: OPS1, CC1, OPS Lima Norte, CPC Lima Norte, SPC ➢ Regiones: Ancash - Sede Chimbote, Arequipa, Cajamarca, Cusco, Ica, Junín, La Libertad, Lambayeque, Loreto, Piura, Puno, San Martín y Tacna	Cualitativo **TIPO DE INVESTIGACIÓN:** Descriptiva, comparativa y aplicada
ESPECÍFICOS	**ESPECÍFICOS**	Pronunciamientos emitidos en materia de operaciones fraudulentas por organismos similares de otros países	España	➢ Legislación ➢ Criterios jurisprudenciales	**MÉTODO DE INVESTIGACIÓN:** Descriptivo Observación directa Análisis de contenido
¿Son predictivos los pronunciamientos del Indecopi emitidos a nivel nacional en materia de operaciones fraudulentas tanto en primera como segunda instancia administrativa durante los años 2022 a 2023?	Determinar si los pronunciamientos del Indecopi emitidos a nivel nacional en materia de operaciones fraudulentas tanto en primera como segunda instancia administrativa durante los años 2022 a 2023 son predictivos.		Colombia	➢ Legislación ➢ Criterios jurisprudenciales	
			Chile	➢ Legislación ➢ Criterios jurisprudenciales	
¿Cuáles son las similitudes y diferencias entre los pronunciamientos emitidos en otros países, como España, Colombia y Chile, en casos de operaciones fraudulentas efectuadas por internet y los pronunciamientos emitidos por el Indecopi?	Comparar los pronunciamientos emitidos en otros países como España, Colombia y Chile para resolver controversias en materia de operaciones bancarias fraudulentas con los pronunciamientos emitidos por el Indecopi.	Propuesta de lineamiento y/o modificación legislativa	Elaboración de lineamiento y/o propuesta de modificación legislativas	➢ Lineamiento ➢ Propuesta de modificación legislativa	**TÉCNICAS:** Observación documental Análisis de contenido
			Análisis de la idoneidad y pertinencia de medidas de seguridad y monitoreo adoptadas	➢ Análisis de validez de la operación ➢ Análisis del patrón de consumo ➢ Gestión y emisión de alertas	**INSTRUMENTOS:** Fichas de observación Fichas de análisis de contenido
¿Cuáles son las recomendaciones o lecciones que pueden implementarse para mejorar la predictibilidad de los pronunciamientos del Indecopi en casos de operaciones fraudulentas efectuadas por internet?	Establecer recomendaciones o lecciones que puedan implementarse para mejorar la predictibilidad de los pronunciamientos del Indecopi en casos de operaciones fraudulentas efectuadas por internet.	**VARIABLE DEPENDIENTE:** Grado de predictibilidad	Medida correctiva	➢ Reparadora ➢ Complementaria	
			Sanción	➢ Multa ➢ Amonestación	

Anexo 2. Ficha de observación

FICHA DE OBSERVACIÓN
CATEGORÍA
REGISTRO
BIBLIOGRAFÍA
TEMA
FECHA Y LUGAR
REGISTRO:

Anexo 3. Ficha de análisis

FICHA DE ANÁLISIS

Instrucciones: Registrar la conducta o actividad observada conforme a cada ítem, marcando con una X el espacio disponible o completando los espacios en blanco.

I. **Ítems de observación:**

1. Expediente N.°
2. Instancia:
3. Número de resolución:
4. Fecha:
5. Órgano Resolutivo:
6. Denunciado:
7. Sentido: (FUNDADO / INFUNDADO)
8. Tipo de servicio utilizado: Banca móvil, Banca por internet, Compras por internet
9. Al análisis del fondo de la denuncia
    - Criterio sobre la carga de la prueba
    - Criterio sobre la responsabilidad del usuario o consumidor titular de los instrumentos de pago
    - Criterio sobre las medidas de seguridad implementadas por las entidades financieras
    - Criterio sobre la validación de operaciones en canales virtuales
    - Criterio sobre la valoración del patrón de consumo
    - Criterio sobre la gestión de alertas generadas por el sistema de monitoreo de operaciones
10. Medidas correctivas
11. Tipo de sanción impuesta

Anexo 4. Lineamientos para la resolución de casos de operaciones bancarias no reconocidas

I. Criterios Generales

Responsabilidad del proveedor:

La negligencia o falta de diligencia del consumidor no constituye un factor determinante para exonerar de responsabilidad a la entidad bancaria. En consecuencia, la autoridad deberá verificar si el proveedor adoptó las medidas de seguridad legal y contractualmente establecidas durante la ejecución de las operaciones bancarias cuestionadas, independientemente de si la conducta negligente del consumidor pudo haber facilitado la realización de dichas operaciones.

Carga probatoria:

La carga de probar el correcto y válido registro y procesamiento de las operaciones, así como la adopción de medidas de seguridad, recaerá en el proveedor, quien se encuentra en una posición más favorable y cuenta con más información que el usuario.

II. Evaluación de la idoneidad de las medidas de seguridad

Medidas de Seguridad:

Se deberá realizar un análisis inicial de la validez de las operaciones (correcto enrolamiento y autenticación), seguido por la evaluación del patrón de consumo del usuario a fin de detectar operaciones inusuales e identificar conductas fraudulentas. Siendo que, si las operaciones no fueron válidamente procesadas o autenticadas, esto podría indicar un defecto o falla en los sistemas de la entidad; en tal caso, la responsabilidad recaería únicamente en la entidad bancaria, al tener la obligación de mantener actualizados sus sistemas internos y de supervisar el funcionamiento de los mismos para asegurar el correcto proceso de autenticación del usuario y registro de las operaciones, a fin de evitar cualquier tipo de falla que pudiera comprometer la seguridad de las operaciones.

Validación y Autenticación de Operaciones

- **Operaciones efectuadas por Banca Móvil o Banca por Internet**

Los órganos resolutivos deben evaluar los siguientes aspectos al abordar la correcta validación y/o autenticación de las operaciones efectuadas por Banca Móvil o Banca por Internet:

(i) la condición activa de la tarjeta al momento de las operaciones;

(ii) la afiliación o habilitación del canal a través del cual se realizaron las operaciones;

(iii) el correcto enrolamiento del usuario a la Banca por Internet o Banca Móvil, que consiste en la verificación de la identidad del usuario, la implementación de las medidas necesarias para reducir la posibilidad de suplantación, así como la generación de credenciales y su asignación al usuario; y,

(iv) según el Reglamento de Gestión de la Seguridad de la Información y la Ciberseguridad se deberá verificar la implementación de la autenticación reforzada para operaciones efectuadas por canal digital, para tal efecto, se debe analizar:

- la utilización de, por lo menos, 2 factores de autenticación que correspondan a categorías distintas y sean independientes uno del otro; salvo que se trate de una operación exenta de utilizar la autenticación reforzada.
- la implementación de un control ante ataques de hombre en el medio, que puede incluir un código generado mediante métodos criptográficos, cuyo uso debe ser por única vez; y,
- la notificación al usuario de los datos de la operación exitosa.

- **Operaciones efectuadas por Comercios Electrónicos**

Las operaciones realizadas a través de este canal según el Reglamento de Gestión de la Seguridad de la Información y la Ciberseguridad no están exentas de implementar la autenticación reforzada. Así, para acreditar la implementación del primer factor de autenticación, el proveedor puede demostrar que la operación se realizó con los datos consignados en el plástico, incluyendo el número de tarjeta, fecha de

vencimiento o CVV. La implementación del segundo factor de autenticación es opcional para el proveedor y podría ser omitido bajo su responsabilidad, siempre y cuando cumpla con las condiciones establecidas para la exención de la autenticación reforzada, según lo dispuesto en el artículo 20 del Reglamento de Gestión de la Seguridad de la Información y la Ciberseguridad.

Cabe indicar que, en estos casos, se debe verificar si en el contrato se estipuló la posibilidad de realizar operaciones en comercios electrónicos o la efectiva habilitación del producto (tarjeta) para efectuar compras a través de comercios electrónicos desde páginas web y/o aplicaciones de dispositivos móviles distintos a los provistos por la entidad financiera.

III. Análisis del patrón de consumo del usuario

Periodo de Evaluación

El órgano resolutivo debe solicitar información del patrón de consumo del usuario de un periodo de al menos seis meses y como máximo un año antes de la ejecución de la operación no reconocida, ya que ello permitirá observar la formación del patrón de consumo sin recurrir a información demasiado antigua ni insuficiente.

Factores para analizar el patrón de consumo del usuario

Se deberá realizar un análisis integral y sistemático del historial de consumo del usuario considerando diversos criterios como canal, frecuencia, tipo de comercio, tipo de moneda, lugar o establecimiento, límite operacional, horario y tipo de operación, importe, entre otros, ya que de esta forma se garantizará una evaluación más completa y objetiva del comportamiento del consumidor, a fin de evitar la imposición de restricciones indebidas que podrían afectar la autonomía y fluidez de las transacciones financieras legítimas de los clientes.

IV. Sistema de Gestión de Alertas

Generación de alertas

Se debe evaluar la generación de alertas en el sistema de monitoreo tras la materialización de más de una operación inusual en un periodo específico. No obstante, debe tomarse en cuenta que la activación de alertas exige la materialización de más de

una operación inusual en un periodo específico, ya que el sistema de monitoreo no tiene una naturaleza preventiva.

Comunicación activa con el consumidor

Se debe evaluar que la entidad financiera haya establecido mecanismos de comunicación inmediata al usuario ante la detección de una operación atípica o inusual, con la finalidad de validar su ejecución, y, si no es posible establecer contacto con este, proceder con el bloqueo preventivo de la tarjeta, de conformidad con lo establecido en el artículo22 del Reglamento de Tarjetas de Crédito y Débito.

V. Medidas correctivas y sanciones

Devolución de Fondos

Se deberá ordenar la devolución del importe total de las operaciones no reconocidas como medida correctiva, cuando se demuestre que las operaciones cuestionadas no fueron válidamente realizadas o no cumplieron con el proceso de autenticación establecido por la normativa y la entidad financiera.

En caso se demuestre la validez de las operaciones, pero que estas no se ajustan al patrón de consumo del usuario, corresponderá la devolución solo de las operaciones subsiguientes a la primera operación inusual realizada de manera válida, puesto que el sistema de monitoreo no tiene naturaleza predictiva, por lo que existe la necesidad de procesar la primera operación a fin de que, en caso se determine que es inusual, genere una alerta en los sistemas del banco, para evitar el procesamiento de posteriores operaciones no reconocidas.

De otro lado, como medida correctiva complementaria deberá ordenarse la devolución de los intereses legales generados hasta la fecha de emisión de la resolución final.

Imposición de sanciones

La graduación de la sanción en los casos de operaciones fraudulentas debe realizarse aplicando las fórmulas y factores establecidos en el Decreto Supremo 032-2021-PCM. Debe considerarse que la imposición de sanciones pecuniarias en estos casos no solo debe tomarse como un medio de punición, sino como una forma de

incentivar a las empresas a mejorar sus sistemas de seguridad y prevenir la ejecución de operaciones fraudulentas; además, la graduación contemplada en la norma toma en cuenta el tamaño de las empresas infractoras y la afectación patrimonial al usuario, por lo que obedece a criterios objetivos y razonables.

VI. Lecciones extraídas de la comparativa internacional

Lecciones extraídas de la legislación y jurisprudencia chilena

- La SBS y el Indecopi, de acuerdo con sus competencias y atribuciones, deben evaluar la implementación de procedimientos de oficio para salvaguardar el interés colectivo de los consumidores afectados por operaciones no reconocidas y/o para verificar el cumplimiento efectivo de las disposiciones normativas relativas a medidas de seguridad, ello incluye revisar si las medidas de seguridad de las entidades financieras están actualizadas de acuerdo con la normativa de la materia y son efectivas contra fraudes, o evaluar la interposición de demandas ante el Poder Judicial por afectación a los intereses colectivos de consumidores en casos de operaciones no reconocidas.
- Debe añadirse una disposición que establezca el deber de las entidades financieras de devolver los fondos sustraídos por la ejecución de operaciones fraudulentas ante el reclamo del consumidor, a menos que se acredite dolo o culpa grave por parte del usuario.
- Además, se debe especificar normativamente que el simple registro de las operaciones no es suficiente para acreditar la responsabilidad del usuario.

Lecciones extraídas de la legislación y jurisprudencia colombiana

- Evaluar la introducción de una disposición normativa que establezca que la entidad financiera puede ser parcialmente exonerada de responsabilidad si se demuestra que el usuario actuó con dolo o culpa grave, pero solo en la medida en que esta culpa haya contribuido a la ejecución de las operaciones fraudulentas. Es decir, si se demuestra la culpa grave del usuario, pero, por otro lado, se demuestra que la entidad bancaria no adoptó las medidas de seguridad pertinentes, se debe determinar que existe una situación de responsabilidad compartida, por lo que corresponde establecer los porcentajes de responsabilidad que recaen en la entidad financiera y en el usuario.

Lecciones extraídas de la legislación y jurisprudencia española

- Evaluar la implementación de una disposición que establezca que la responsabilidad de la entidad financiera en casos de operaciones no reconocidas tiene un carácter cuasiobjetivo, eximiéndosele de responsabilidad solo si se demuestra que el usuario actuó de manera fraudulenta, con negligencia grave, o incumplió deliberadamente sus obligaciones legales. En consecuencia, la entidad financiera podría ser parcialmente exonerada de responsabilidad si se demuestra que el usuario actuó con dolo o negligencia grave, pero solo en la medida en que esta culpa haya contribuido a la ejecución de las operaciones fraudulentas.
- Evaluar la incorporación normativa de un procedimiento que permita la rectificación automática de operaciones no autorizadas por parte de la entidad financiera, siempre que el consumidor notifique esta situación sin demora injustificada a la entidad.
- Evaluar la introducción de una disposición que determine que el registro de la utilización del instrumento de pago no es suficiente para acreditar que el usuario autorizó las operaciones o que actuó de manera fraudulenta o negligente.
- Evaluar la incorporación de una disposición que considere la falta de diligencia en la adopción de medidas preventivas por parte de la entidad financiera como un factor de responsabilidad en caso de operaciones fraudulentas.

Anexo 5. Listado de resoluciones del Indecopi revisadas durante la ejecución de la investigación

N.°	N.° DE RESOLUCIÓN	FECHA	INSTANCIA	ÓRGANO RESOLUTIVO	DENUNCIADO	TIPO DE SERVICIO	SENTIDO	MEDIDA CORRECTIVA	SANCIÓN
1	0023-2022	06/04/2023	DENUNCIA	ORPS DE ANCASH SEDE HUARAZ	BANCO INTERNACIONAL DEL PERÚ S.A.A. - INTERBANK	BANCA MÓVIL	FUNDADO	SÍ	AMONESTACIÓN
2	0040-2023	08/05/2023	DENUNCIA	ORPS DE ANCASH SEDE HUARAZ	BANCO DE LA NACIÓN	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.78 UIT
3	0044-2023	01/06/2023	DENUNCIA	ORPS DE ANCASH SEDE HUARAZ	BANCO DE LA NACIÓN	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.49 UIT
4	0001-2022	06/01/2022	DENUNCIA	ORPS DE ANCASH SEDE HUARAZ	SCOTIABANK PERU S.A.A.	BANCA POR INTERNET	INFUNDADO	NO APLICA	NO APLICA
5	0001-2022	04/01/2022	DENUNCIA	ORPS DE CAJAMARCA	BANCO RIPLEY PERU S.A.	BANCA POR INTERNET	FUNDADO	SÍ	MULTA 0.5 UIT
6	0006-2022	07/01/2022	DENUNCIA	ORPS DE CAJAMARCA	BANCO RIPLEY PERÚ S.A.	COMPRAS POR INTERNET	INFUNDADO	NO APLICA	NO APLICA
7	0007-2022	07/01/2022	DENUNCIA	ORPS DE CAJAMARCA	BANCO RIPLEY PERÚ S.A.	COMPRAS POR INTERNET	FUNDADO	SÍ	MULTA 3.49 UIT
8	0232-2022	09/08/2022	DENUNCIA	ORPS DE CAJAMARCA	BANCO DE LA NACIÓN	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.49 UIT
9	0412-2023	26/07/2023	DENUNCIA	ORPS DE CUSCO	BANCO BBVA PERÚ	BANCA POR INTERNET	FUNDADO	SÍ	MULTA 3.49 UIT
10	0432-2023	04/08/2023	DENUNCIA	ORPS DE CUSCO	BANCO DE CREDITO DEL PERU	COMPRAS POR INTERNET	FUNDADO	SÍ	MULTA 3.78 UIT
11	0419-2023	02/08/2023	DENUNCIA	ORPS DE CUSCO	BANCO BBVA PERÚ	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.49 UIT
12	0302-2023	30/05/2023	DENUNCIA	ORPS DE CUSCO	BANCO INTERNACIONAL DEL PERÚ-INTERBANK	COMPRAS POR INTERNET	FUNDADO	SÍ	MULTA 3.49 UIT
13	0303-2023	30/05/2023	DENUNCIA	ORPS DE	FINANCIERA OH S.A.	COMPRAS	FUNDADO	SÍ	MULTA

				CUSCO		POR INTERNET			3.78 UIT
14	0171-2023	10/08/2023	DENUNCIA	ORPS DE ICA	BANCO DE CREDITO DEL PERÚ S.A.	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.49 UIT
15	0172-2023	10/08/2023	DENUNCIA	ORPS DE ICA	BANCO INTERNACIONAL DEL PERÚ S.A.A. INTERBANK	COMPRAS POR INTERNET	FUNDADO	SÍ	MULTA 3.49 UIT
16	0146-2023	04/07/2023	DENUNCIA	ORPS DE ICA	SCOTIABANK PERÚ S.A.A.	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.78 UIT
17	0121-2023	05/06/2023	DENUNCIA	ORPS DE ICA	FINANCIERA OH! S.A. O FINANCIERA OH S.A	COMPRAS POR INTERNET	FUNDADO	SÍ	MULTA 3.49 UIT
18	024-2023	21/02/2023	DENUNCIA	ORPS DE ICA	BANCO DE CREDITO DEL PERU S.A.	BANCA POR INTERNET	FUNDADO	SÍ	MULTA 3.78 UIT
19	0620-2022	27/12/2022	DENUNCIA	ORPS DE JUNÍN	CAJA MUNICIPAL DE AHORRO Y CRÉDITO DE PIURA S.A.C.	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.49 UIT
20	0598-2022	05/12/2022	DENUNCIA	ORPS DE JUNÍN	BANCO DE LA NACIÓN	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.49 UIT
21	0575-2022	25/11/2022	DENUNCIA	ORPS DE JUNÍN	SCOTIABANK PERÚ S.A.A.	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.49 UIT
22	565-2022	21/11/2022	DENUNCIA	ORPS DE JUNÍN	BANCO INTERNACIONAL DEL PERÚ S.A.A. – INTERBANK	BANCA POR INTERNET	FUNDADO	SÍ	MULTA 3.49 UIT
23	050-2023	24/01/2024	DENUNCIA	ORPS DE JUNÍN	CAJA MUNICIPAL DE AHORRO Y CRÉDITO DE PIURA S.A.C.	BANCA POR INTERNET	FUNDADO	SÍ	MULTA 3.78 UIT
24	0010-2023	08/02/2023	DENUNCIA	ORPS DE ANCASH - SEDE CHIMBOTE	SCOTIABANK PERÚ S.A.A.	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.49 UIT
25	0003-2023	11/01/2023	DENUNCIA	ORPS DE ANCASH - SEDE CHIMBOTE	FINANCIERA OH S.A.	BANCA POR INTERNET	INFUNDADO	NO APLICA	NO APLICA
26	0004-2023	04/01/2023	DENUNCIA	ORPS DE LA LIBERTAD	BANCO DE CRÉDITO DEL PERÚ S.A.	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.49 UIT
27	0323-2023	24/03/2023	DENUNCIA	ORPS DE	SCOTIABANK PERÚ	BANCA	FUNDADO	SÍ	MULTA

				LAMBAYEQUE	S.A.A.	MÓVIL			3.49 UIT
28	0562-2022	21/07/2022	DENUNCIA	ORPS DE LAMBAYEQUE	BANCO DE LA NACION	BANCA MÓVIL	INFUNDADO	NO APLICA	NO APLICA
29	102-2023	01/09/2023	DENUNCIA	ORPS DE PUNO	SCOTIABANK PERÚ SOCIEDAD ANÓNIMA	BANCA MÓVIL	INFUNDADO	NO APLICA	NO APLICA
30	72-2023	15/06/2023	DENUNCIA	ORPS DE PUNO	BANCO INTERNACIONAL DEL PERÚ S.A.A. - INTERBANK	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.78 UIT
31	0144-2023	03/08/2023	DENUNCIA	ORPS DE TACNA	BANCO INTERNACIONAL DEL PERÚ S.A.A. - INTERBANK	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.49 UIT
32	0146-2023	01/08/2023	DENUNCIA	ORPS DE TACNA	FINANCIERA OH S.A.	COMPRAS POR INTERNET	INFUNDADO	NO APLICA	NO APLICA
33	0136-2023	19/07/2023	DENUNCIA	ORPS DE TACNA	SCOTIABANK PERÚ S.A.A.	COMPRAS POR INTERNET	FUNDADO	SÍ	MULTA 3.78 UIT
34	1912-2022	22/12/2022	DENUNCIA	ORPS N.° 2 – SEDE CENTRAL	BANCO BBVA PERÚ	BANCA POR INTERNET	FUNDADO	SÍ	MULTA 4.01 UIT
35	1754-2022	01/12/2022	DENUNCIA	ORPS N.° 2 – SEDE CENTRAL	BANCO BBVA PERÚ	COMPRAS POR INTERNET	FUNDADO	SÍ	MULTA 3.49 UIT
36	1725-2022	25/11/2022	DENUNCIA	ORPS N.° 2 – SEDE CENTRAL	BANCO INTERNACIONAL DEL PERÚ S.A.A. – INTERBANK	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.78 UIT
37	0073-2023	19/01/2023	DENUNCIA	ORPS DE LIMA NORTE	BANCO DE CREDITO DEL PERU	COMPRAS POR INTERNET	FUNDADO	SÍ	AMONESTACIÓN
38	0246-2023	10/03/2023	DENUNCIA	ORPS DE LIMA NORTE	BANCO INTERNACIONAL DEL PERÚ S.A.A. – INTERBANK	BANCA MÓVIL	FUNDADO	SÍ	MULTA 2 UIT
39	0243-2022	22/12/2022	APELACIÓN	COMISIÓN DE LA ORI ANCASH SEDE CHIMBOTE	BANCO DE LA NACIÓN	BANCA MÓVIL	FUNDADO	SÍ	AMONESTACIÓN
40	0182-2022	21/10/2022	APELACIÓN	COMISIÓN DE	BANCO DE LA NACIÓN	BANCA	FUNDADO	SÍ	AMONESTA

				LA ORI ANCASH SEDE CHIMBOTE		MÓVIL			CIÓN
41	0229-2023	14/08/2023	APELACIÓN	CPC CAJAMARCA	CMAC PIURA S.A.C.	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.49 UIT
42	0160-2023	25/05/2023	APELACIÓN	CPC CAJAMARCA	BANCO DE LA NACIÓN	BANCA MÓVIL	INFUNDADO	NO APLICA	NO APLICA
43	363-2023	17/07/2023	APELACIÓN	CPC CUSCO	BANCO DE LA NACIÓN	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.78 UIT
44	549-2022	12/09/2022	DENUNCIA	CPC CUSCO	BANCO BBVA PERÚ	COMPRAS POR INTERNET	FUNDADO	SÍ	MULTA 11.6 UIT
45	195-2023	17/04/2023	APELACIÓN	CPC CUSCO	BANCO DE CRÉDITO DEL PERÚ	CAJERO AUTOMÁTICO	FUNDADO	NO	MULTA 3.78 UIT
46	063-2023	09/03/2023	APELACIÓN	CPC ICA	BANCO INTERNACIONAL DEL PERÚ S.A.A.- INTERBANK	BANCA MÓVIL	INFUNDADO	NO APLICA	NO APLICA
47	339-2023	11/08/2023	DENUNCIA	CPC JUNÍN	SCOTIABANK PERÚ S.A.A.	BANCA MÓVIL	FUNDADO	SÍ	MULTA 22.97 UIT
48	349-2023	11/08/2023	DENUNCIA	CPC JUNÍN	CAJA MUNICIPAL DE AHORRO Y CRÉDITO PIURA S.A.C.	BANCA MÓVIL	FUNDADO	SÍ	MULTA 11.6 UIT
49	0037-2023	12/01/2023	DENUNCIA	CPC LA LIBERTAD	BANCO GNB PERU S.A.	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3 UIT
50	0828-2022	17/11/2022	APELACIÓN	CPC LA LIBERTAD	BANCO DE LA NACIÓN	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.49 UIT
51	0951-2022	15/12/2022	APELACIÓN	CPC LA LIBERTAD	BANCO BBVA PERU	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.78 UIT
52	0447-2022	01/08/2023	DENUNCIA	CPC LAMBAYEQUE	BANCO DE LA NACIÓN	BANCA MÓVIL	FUNDADO	SÍ	MULTA 6.89 UIT
53	0310-2022	23/05/2022	APELACIÓN	CPC LAMBAYEQUE	BANCO BBVA PERU	BANCA POR INTERNET	FUNDADO	SÍ	MULTA 11.60 UIT
54	076-2023	15/08/2023	APELACIÓN	CPC DE PUNO	BANCO DE LA NACIÓN	CAJERO AUTOMÁTICO	FUNDADO	SÍ	MULTA 3.49 UIT
55	077-2023	15/08/2023	APELACIÓN	CPC DE PUNO	FINANCIERA OH SOCIEDAD ANÓNIMA	COMPRAS POR INTERNET	INFUNDADO	NO APLICA	NO APLICA

56	065-2022	12-07-2022	APELACIÓN	CPC PUNO	BANCO DE LA NACIÓN	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.78
57	0058-2023	29-03-2023	DENUNCIA	CPC TACNA	BANCO BBVA PERÚ S.A.	COMPRAS POR INTERNET	FUNDADO	SÍ	MULTA 11.6
58	0105-2023	28-06-2023	DENUNCIA	CPC TACNA	MIBANCO - BANCO DE LA MICROEMPRESA S.A.	BANCA MÓVIL	FUNDADO	SÍ	MULTA 6.89
59	0026-2023	14-02-2023	APELACIÓN	CPC TACNA	BANCO DE LA NACIÓN	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.49 UIT
60	1954-2023	16-08-2023	DENUNCIA	CPC N.° 1	SCOTIABANK PERÚ S.A.A.	BANCA MÓVIL	FUNDADO	SÍ	MULTA 22.97 UIT
61	1775-2023	26-07-2023	DENUNCIA	CPC N.° 1	BANCO INTERNACIONAL DEL PERÚ S.A.A. – INTERBANK	BANCA MÓVIL	FUNDADO	SÍ	MULTA 0.49 UIT
62	1773-2023	26-07-2023	DENUNCIA	CPC N.° 1	BANCO INTERNACIONAL DEL PERÚ S.A.A. – INTERBANK	COMPRAS POR INTERNET	FUNDADO	SÍ	MULTA 2.82 UIT
63	0488-2023	11-08-2023	APELACIÓN	ILN-CPC	BANCO DE CRÉDITO DEL PERÚ	BANCA MÓVIL	FUNDADO	SÍ	MULTA 0.50 UIT
64	0298-2023	26-05-2023	APELACIÓN	ILN-CPC	BANCO DE LA NACIÓN	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3 UIT
65	0590-2022	29-11-2022	DENUNCIA	ORPS DE AREQUIPA	BANCO RIPLEY PERÚ S.A.	COMPRAS POR INTERNET	FUNDADO	SÍ	AMONESTACIÓN
66	074-2023	26-04-2023	DENUNCIA	ORPS DE LORETO	SCOTIABANK PERÚ S.A.A.	BANCA MÓVIL	FUNDADO	SÍ	MULTA 3.78
67	009-2023	20-01-2023	DENUNCIA	ORPS DE LORETO	BANCO DE CRÉDITO DEL PERÚ	COMPRAS POR INTERNET	FUNDADO	SÍ	MULTA 4.01 UIT
68	077-2023	03-05-2022	DENUNCIA	ORPS LORETO	BANCO BBVA PERÚ S.A.	BANCO POR INTERNET	FUNDADO	SÍ	MULTA 4.01 UIT
69	501-2023	01-06-2023	DENUNCIA	ORPS PIURA	BANCO INTERNACIONAL DEL PERÚ - INTERBANK	BANCA MÓVIL	INFUNDADO	SÍ	MULTA 3.49 UIT
70	2144-2023	09-08-2023	APELACIÓN	SPC	BANCO BBVA PERÚ S.A.	COMPRAS POR INTERNET	FUNDADO	NO	MULTA AMONESTACIÓN
71	2086-2023	02-08-2023	APELACIÓN	SPC	SCOTIABANK PERÚ	BANCO POR	FUNDADO	NO	MULTA

					S.A.A.	INTERNET			22.97 UIT
72	2006-2023	24-07-2023	APELACIÓN	SPC	BANCO BBVA PERÚ S.A.	BANCA MÓVIL	FUNDADO	NO	MULTA 4 UIT
73	1841-2023	06-07-2023	APELACIÓN	SPC	BANCO DE CRÉDITO DEL PERÚ S.A.	BANCA POR INTERNET	INFUNDADO	NO APLICA	NO APLICA
74	274-2023	18-10-2023	DENUNCIA	ORPS DE SAN MARTÍN	SCOTIABANK PERU S.A.A.	BANCA MÓVIL	FUNDADO	SÍ	MULTA 1 UIT

Anexo 6. Legislación

Perú

Circular G-140-2009, Gestión de la seguridad de la información, Pub. L. No. Circular G-140-2009, Diario El Peruano (2009). https://www.sbs.gob.pe/Portals/0/jer/Auto_Nuevas_Empresas/Normas_Comunes/9.%20Gesti%C3%B3n%20de%20la%20Seguridad%20de%20la%20Informaci%C3%B3n_Circ.%20SBS%20G-140-2009.pdf

Código de Protección y Defensa del Consumidor, Pub. L. No. Ley 29571, Diario El Peruano (2010). https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H682697

Decreto Supremo que aprueba la graduación, metodología y factores para la determinación de las multas que impongan los órganos resolutivos del Indecopi respecto de las infracciones sancionables en el ámbito de su competencia, Pub. L. No. Decreto Supremo 032-2021-PCM, Diario El Peruano (2021). https://repositorio.indecopi.gob.pe/bitstream/handle/11724/8067/DS.032-2021-PCM.pdf?sequence=1&isAllowed=y

Reglamento de gestión de la seguridad de la información y la ciberseguridad, Pub. L. No. Resolución S.B.S. N.° 504-2021, Diario El Peruano (2021). https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1277430

Reglamento de Tarjetas de Crédito y Débito, Pub. L. No. Resolución SBS 6523-2013, Diario El Peruano (2013). https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1089323

T.U.O. de La Ley 27444, Ley Del Procedimiento Administrativo General, Pub. L. No. Decreto Supremo 004-2019-JUS, Diario El Peruano (2019). https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1226958

Chile

Ley 19496, que establece normas sobre protección de los derechos de los consumidores, Pub. L. No. D.F.L. Núm. 3 (2021). https://www.bcn.cl/leychile/navegar?idNorma=1160403

Ley 20009, que establece un régimen de limitación de responsabilidad para titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude, Pub. L. No. Ley 20009 (2005). https://www.bcn.cl/leychile/navegar?idNorma=236736

Ley 21234, que limita la responsabilidad de los titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude, Pub. L. No. Ley 21234 (2020). https://www.bcn.cl/leychile/navegar?i=1145840

Resolución Exenta n.° 727, que contiene los términos del acuerdo y declara el término favorable del procedimiento voluntario colectivo entre el SERNAC y Scotiabank Chile S.A. (2020). https://www.sernac.cl/portal/609/w3-propertyvalue-64485.html#recuadros_articulo_1768_group_pvid_67130

Colombia

Circular Básica Jurídica 029/14, Pub. L. No. C.E. 029/14 (2014). https://www.superfinanciera.gov.co/jsp/10083443

Código de Comercio, Pub. L. No. Decreto 410, Diario Oficial de Colombia (1971). http://www.secretariasenado.gov.co/senado/basedoc/codigo_comercio.html#1

Decreto 2555, por el cual se recogen y reexpiden las normas en materia del sector financiero, asegurador y del mercado de valores y se dictan otras disposiciones., Pub. L. No. Decreto 2555, Diario Oficial de Colombia (2010).

Estatuto Orgánico del Sistema Financiero, Pub. L. No. Decreto Ley 663, Diario Oficial de Colombia (1993). http://www.secretariasenado.gov.co/senado/basedoc/estatuto_organico_sistema_financiero.html

Ley 1328, por la cual se dictan normas en materia financiera, de seguros, del mercado de valores y otras disposiciones, Pub. L. No. Ley 1328, Diario Oficial de Colombia (2009). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36841

Ley 1480, Estatuto del Consumidor, Pub. L. No. Ley 1480, Diario Oficial de Colombia (2011).

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=44306#:~:text=Esta%20ley%20tiene%20como%20objetivos,para%20su%20salud%20y%20seguridad.

España

Directiva 2015/2366, Sobre servicios de pago en el mercado interior, Pub. L. No. 2015/2366, Agencia Estatal Boletín Oficial del Estado (2015). https://www.boe.es/buscar/doc.php?id=DOUE-L-2015-82575Directiva

Directiva (UE) 2019/713, Sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión Marco 2001/413/JAI Del Consejo, Pub. L. No. Directiva (UE) 2019/713 (2019). https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX%3A32019L0713

Real Decreto-Ley 19/2018, de servicios de pago y otras medidas urgentes en materia financiera (2018). https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16036

Reglamento Delegado (UE) 2018/389, Diario Oficial de la Unión Europea (2017). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018R0389&qid=1696344687089

Anexo 7. Jurisprudencia

Perú

Resolución 0004-2010/SC2-INDECOPI (2010).
https://servicio.indecopi.gob.pe/buscadorResoluciones/

Resolución 0022-2020/SPC-INDECOPI (2020).
https://servicio.indecopi.gob.pe/buscadorResoluciones/

Resolución 0023-2020/SPC-INDECOPI (2020).
https://servicio.indecopi.gob.pe/buscadorResoluciones/

Resolución 2609-2022/SPC-INDECOPI (2022).
https://servicio.indecopi.gob.pe/buscadorResoluciones/

Chile

Sentencia Rol N.° 10-2023, Juzgado de Policía Local Del Puerto Porvenir (2023).
https://www.sernac.cl/sentencias/app/public/

Sentencia Rol n.° 201-2022, Segunda Sala de La Corte de Apelaciones de La Serena (2022). https://www.sernac.cl/sentencias/app/public/

Sentencia Rol N.° 783-2020, Corte de Apelaciones de Santiago (2022).
https://oficinajudicialvirtual.pjud.cl/indexN.php

Sentencia Rol N.° 1115-2020, 2° Juzgado de Policía Local de Talca (2022).
https://www.sernac.cl/sentencias/app/public/

Sentencia Rol N.° 10146-2021, 2° Juzgado de Policía Local de Talca (2022).

https://www.sernac.cl/sentencias/app/public/

Sentencia Rol n.° C-2126-2023, Juzgado Civil de Santiago (2023).
https://www.sernac.cl/sentencias/app/public/

Sentencia Rol N.º 13407-2021, Corte de Apelaciones de Concepción (2022).
https://oficinajudicialvirtual.pjud.cl/home/index.php

Colombia

Sentencia Exp. 214058750 (2015).
http://consultajurisprudencial.ramajudicial.gov.co:8080/WebRelatoria/csj/index.xhtml

Sentencia Rad. 003-2021-01984-01 (2022).
http://consultajurisprudencial.ramajudicial.gov.co:8080/WebRelatoria/csj/index.xhtml

Sentencia Rad. 2015-00206-01 (2016).
http://consultajurisprudencial.ramajudicial.gov.co:8080/WebRelatoria/csj/index.xhtml

Providencia n.° SC5176 de La Rad. 11001-31-03-028-2006-00466-01 (2020).
http://consultajurisprudencial.ramajudicial.gov.co:8080/WebRelatoria/csj/index.xhtml

Providencia n.° SC18614 de La Rad. 05001-31-03-001-2008-00312-01 (2016).
http://consultajurisprudencial.ramajudicial.gov.co:8080/WebRelatoria/csj/index.xhtml

Providencia n.° STC12199 de La Rad. 11001-22-03-000-2022-01602-01 (2022).
http://consultajurisprudencial.ramajudicial.gov.co:8080/WebRelatoria/csj/index.xhtml

Sentencia Rad. 6909 (2003).
https://consultaprocesos.ramajudicial.gov.co/Procesos/NumeroRadicacion

Sentencia Rad. 2016071307 (2017).
http://consultajurisprudencial.ramajudicial.gov.co:8080/WebRelatoria/csj/index.xhtml

Sentencia SC18614 de La Rad. 05001-31-03-001-2008-00312-01 (2016).
https://consultaprocesos.ramajudicial.gov.co/Procesos/NumeroRadicacion

España

Sentencia Roj. SAP A 632/2018 (2018).
https://www.poderjudicial.es/search/indexAN.jsp

Sentencia Roj. SAP A 1571/2023 (2023).
https://www.poderjudicial.es/search/indexAN.jsp

Sentencia Roj. SAP B 6560/2023 (2023).
https://www.poderjudicial.es/search/indexAN.jsp

Sentencia Roj. SAP C 481/2023 (2023).
https://www.poderjudicial.es/search/indexAN.jsp

Sentencia Roj. SAP M 6240/2015 (2015).
https://www.poderjudicial.es/search/indexAN.jsp

Sentencia Roj. SAP M 7327/2022 (2022).
https://www.poderjudicial.es/search/indexAN.jsp

Sentencia Roj. SAP O 2047/2023 (2023).
https://www.poderjudicial.es/search/indexAN.jsp

Sentencia Roj. SAP PO 496/2023 (2023).
https://www.poderjudicial.es/search/indexAN.jsp

Sentencia Roj. SAP S 1267/2023 (2023).
https://www.poderjudicial.es/search/indexAN.jsp

Sentencia Roj. SAP S 1277/2023 (2023).
https://www.poderjudicial.es/search/indexAN.jsp

Sentencia Roj. SJPI 1022/2023 (2023).
https://www.poderjudicial.es/search/indexAN.jsp

Anexo 8. Fichas de observación de jurisprudencia comparada

FICHA DE OBSERVACIÓN	
CATEGORÍA	**Sentencia (Chile)**
TEMA	Sentencia Rol N.° 10146-2021, 2° Juzgado de Policía Local de Talca (2022)

REGISTRO:

En agosto de 2021, el demandante sufrió el robo de su billetera, la cual contenía su tarjeta de cuenta RUT. Posteriormente, al recibir correos electrónicos que mostraban transacciones no autorizadas, se comunicó con el banco para realizar un reclamo y solicitar la devolución de su dinero, pero el banco denegó la solicitud y procedió con el bloqueo de su tarjeta. El demandante alegó que el banco infringió los artículos 3 literales b, d y e, 12 y 24 de la Ley 19.496 y buscó una indemnización por daño emergente y moral, intereses, reajustes y costas. En respuesta, el banco argumentó que las transacciones cuestionadas fueron realizadas sin errores en sus sistemas de seguridad, y que cada transacción genera códigos únicos y cuenta con un complejo sistema de almacenamiento de datos, procesador y software.

Al respecto, en Juzgado señala que las operaciones involucraron retiros en cajero automático y compras en establecimientos por un monto significativo, por lo que existen fundadas sospechas de un ilícito -lo que concuerda con lo relatado por el consumidor en su denuncia-; además, el banco notificó al cliente después de efectuadas las operaciones, por lo que recién a partir de ese momento pudo percatarse del fraude.

Así, la sentencia indica que el banco no actuó conforme a los estándares comerciales necesarios, los cuales, teniendo en cuenta la especialidad y complejidad de los servicios que ofrecen, deben ser cuidadosos y eficientes respecto de las herramientas que ponen a disposición de sus clientes, sobre todo de forma previa a las transacciones defraudatorias.

Por tanto, se colige que se infringieron las disposiciones establecidas en el artículo 3, literal d, de la Ley 19.486, que impone la obligación de proporcionar al consumidor seguridad en el consumo de bienes y servicios, así como el deber de prevenir los riesgos que puedan afectarlos. Además, se hace referencia al artículo 12, que establece la obligación del proveedor de respetar los términos, condiciones o

modalidades acordadas en la prestación del servicio, y al artículo 23, que señala como infracción la actuación negligente del proveedor que cause perjuicio al consumidor debido a fallos o deficiencias en la calidad del servicio.

En este contexto, el Juzgado concluye que las medidas de seguridad implementadas por el proveedor fueron insuficientes y que actuó con negligencia, por lo que se acoge la acción infraccional, condenándose al Banco del Estado de Chile, conforme a lo dispuesto en el artículo 50 C inciso final y 50 D de la Ley 19.496, a pagar una multa en beneficio municipal ascendente a 20 UTM (Unidad Tributaria Mensual) por infracción a los artículos 3 letra d), 12 y 23 de la Ley 19.496 En el ámbito civil, tras haberse acogido la acción infraccional, la sentencia ordena también la devolución de las transacciones no autorizadas y concede una indemnización por daño moral. Finalmente, establece una orden de reclusión diurna para el representante del banco en caso no cumpla con el pago de la multa dentro del plazo establecido.

FICHA DE OBSERVACIÓN	
CATEGORÍA	**Sentencia (Chile)**
TEMA	Sentencia Rol N.° 10-2023, Juzgado de Policía Local del Puerto Porvenir (2023)

REGISTRO:

En este caso, el Banco del Estado de Chile interpuso una querella infraccional contra el señor Silva, alegando la presencia de dolo o culpa grave según lo establecido en el artículo 5 inciso tercero de la Ley 21.234. El Banco señala en su denuncia que el señor Silva se contactó telefónicamente el 22 de diciembre de 2022 para denunciar un siniestro del cual fue víctima, solicitando la restitución del monto defraudado al no haber realizado ni autorizado tres transferencias electrónicas realizadas a diferentes destinatarios, por lo que el banco, cumpliendo con lo dispuesto en el artículo 5 de la Ley 21.234, realizó el abono normativo de 35 UF sin reconocer responsabilidad.

El banco sostiene que, tras una investigación interna, se concluyó que las operaciones denunciadas por el señor Silva derivaron de una conducta dolosa o asimilable a culpa grave, ya que entregó claves a un tercero, quien se hizo pasar por ejecutivo del banco y le indicó que existían devoluciones de dinero pendientes. Así, el banco alega negligencia por parte del señor Silva, ya que hizo caso omiso a las campañas

informativas destinadas a prevenir este tipo de situaciones. En ese sentido, solicita se declare la existencia de dolo o culpa por parte del querellado, se deje sin efecto la cancelación de cargos efectuada por el Banco y se ordene la restitución del abono de 35 UF; además, interpone una acción civil por indemnización de daños contra el señor Silva.

Al respecto, según lo dispuesto en los incisos 5 y 6 del artículo 4 de la Ley 21.234, es responsabilidad del banco acreditar que el usuario autorizó las operaciones en cuestión y/o que participó en la comisión del delito, que obtuvo un beneficio ilícito, o que actuó con dolo o culpa, sin que baste el simple registro de las operaciones para probar ello.

En este contexto, el juzgado considera que las pruebas presentadas por el banco fueron insuficientes para respaldar su hipótesis, ya que no se demostró ningún vínculo entre los beneficiarios de las transferencias y el querellado, lo que impedía al juzgado constatar la existencia de algún beneficio o facilitación de fraude por parte de este último. Por lo tanto, la querella infraccional presentada por el banco contra el señor Silva fue rechazada, ya que no se pudo acreditar que incurrió en alguna de las conductas descritas en los artículos 4 y 5 de la Ley 21.234; en consecuencia, se desestimó también la demanda civil interpuesta por el banco.

FICHA DE OBSERVACIÓN	
CATEGORÍA	**Sentencia (Chile)**
TEMA	Sentencia Rol n.° 201-2022, Segunda Sala de la Corte de Apelaciones de La Serena (2022)

REGISTRO:

La señora Molina presentó un Recurso de Protección contra el Banco luego de ser víctima de fraude en enero de 2022. La denunciante alegó que terceros realizaron operaciones no autorizadas desde sus cuentas y tarjetas de crédito, incluyendo compras y transferencias que no correspondían a su comportamiento habitual, sin que se emitieran alertas sobre estas transacciones. Así, al tomar conocimiento de las operaciones, de inmediato contactó al Banco, bloqueó sus cuentas y denunció el fraude, solicitando la no realización de pagos asociados a estas transacciones.

A pesar de su reclamo, el Banco solo le devolvió parcialmente los cargos

fraudulentos, alegando que las medidas de seguridad se habían cumplido; por tal motivo, la señora Molina interpuso una acción de protección en mérito al artículo 5 de la Ley 21.234, que establece la cancelación o restitución de cargos en casos de fraude. Sin embargo, el banco rechazó la devolución total, argumentando que el fraude no estaba probado, ya que las transacciones se llevaron a cabo con la confirmación del cliente y siguiendo los protocolos de seguridad.

El juzgado determinó que el banco actuó ilegal y arbitrariamente al no acoger completamente el reclamo de la señora Molina, vulnerando su derecho de propiedad; además, señaló que era claro que se configuró un fraude que afectó a la querellante, ya que terceros realizaron operaciones fraudulentas utilizando los medios de pago que contrató.

Precisó también que el banco rechazó parcialmente la cancelación de cargos y la restitución de los fondos, siendo esta decisión arbitraria y caprichosa. En consecuencia, el recurso de protección presentado por la señora Molina fue acogido, ordenándose al banco cancelar los cargos provenientes del fraude y restituir los fondos correspondientes.

FICHA DE OBSERVACIÓN	
CATEGORÍA	**Sentencia (Chile)**
TEMA	Sentencia Rol N.° 1115-2020, 2° Juzgado de Policía Local de Talca (2022)

REGISTRO:

El señor Carvajal presentó una denuncia infraccional (infracción a los artículos 3, letra d y e, 23 y 24 de la Ley 19.496) y una demanda civil contra Banco Itaú Corpbanca, alegando que fue víctima de un robo de su tarjeta de crédito que resultó en compras no autorizadas por más de $2 millones entre enero y marzo de 2020. El querellante argumentó que el banco no le notificó de inmediato sobre estas transacciones fraudulentas, enterándose meses después de los cargos realizados, por lo que solicitó una indemnización de $24,085,059 por daño emergente y moral, más intereses, reajustes y costas.

El juzgado consideró que el señor Carvajal, como titular de la tarjeta, era responsable de su custodia y que fue negligente al no notificar inmediatamente al banco sobre el

extravío. También señaló que las transacciones reclamadas se llevaron a cabo durante tres meses sin que el querellante revisara sus estados de cuenta, lo que contribuyó a su falta de conocimiento sobre las compras fraudulentas; cabe indicar que, el banco presentó como pruebas el envío de los estados de cuenta al correo del señor Carvajal y los registros de consultas de saldo y pagos durante los meses en cuestión.

El juzgado concluyó que no se acreditó un actuar negligente por parte del banco, sino que la responsabilidad recaía en la falta de acción inmediata del querellante al no notificar el robo de su tarjeta, además, el propio querellante afirmó haberse enterado de las compras recién el 4 de marzo de 2020, a pesar de que el banco notificó las transacciones a través de los estados de cuenta enviados a su correo y del portal de usuario en su página web institucional, lo que indica que, pese a que tuvo acceso a la información, el usuario no actuó de inmediato. Por lo tanto, el juzgado rechazó tanto la denuncia infraccional como la demanda civil en todos sus aspectos.

FICHA DE OBSERVACIÓN	
CATEGORÍA	**Sentencia (Chile)**
TEMA	Resolución exenta n.° 727, que contiene los términos del acuerdo y declara el término favorable del procedimiento voluntario colectivo entre el SERNAC y Scotiabank Chile S.A. (2020)

REGISTRO:

El 13 de abril de 2020, la Subdirección de Procedimientos Voluntarios Colectivos del SERNAC emitió una resolución para iniciar un procedimiento voluntario colectivo con Scotiabank Chile S.A. debido a indicios de afectación al interés colectivo de los consumidores y posibles contravenciones a la Ley 19.496.

Este acuerdo tiene por finalidad beneficiar a los consumidores clientes de Scotiabank Chile que fueron perjudicados por operaciones y pagos desconocidos realizados con tarjetas de crédito a través del comercio electrónico de "AIRBNB" desde agosto de 2018 hasta noviembre de 2019. El total de consumidores beneficiados era de 841, por un monto aproximado de $325,863,775 pesos más $37,952 pesos.

Según el artículo 54P n.° 3 de la Ley 19.496, la resolución que establece las condiciones del acuerdo debe incluir una solución proporcional al daño causado, que

involucre a todos los consumidores afectados y esté basada en elementos objetivos. En consecuencia, en dicha resolución se declaró el término favorable del procedimiento voluntario colectivo y se determinó que el Banco reintegrará la totalidad del monto correspondiente a los fraudes alegados, además de compensaciones adicionales a los consumidores afectados por el costo del tiempo, la indisponibilidad financiera y el costo del reclamo.

FICHA DE OBSERVACIÓN	
CATEGORÍA	**Providencia (Colombia)**
TEMA	Providencia n.° STC12199 de la Rad. 11001-22-03-000-2022-01602-01 (2022)

REGISTRO:

En el presente caso, un consumidor financiero denunció a Bancolombia S.A. por el uso no autorizado de su tarjeta de crédito de la franquicia American Express. En términos generales, el demandante alega que su tarjeta fue robada en Miami el 4 de febrero de 2022, efectuándose movimientos al día siguiente que no fueron autorizados por él, no corresponden a su perfil transaccional y, a pesar de informar al banco sobre ello el 5 de febrero de 2022, la reclamación resultó desfavorable.

La Superintendencia Financiera, en primera instancia, dictaminó que Bancolombia S.A. era responsable del 40% de las transacciones realizadas el 5 de febrero de 2022 y lo condenó a eliminar dicho porcentaje de transacciones, así como a reliquidar la obligación crediticia. En esta sentencia, se atribuyó al consumidor parte de la responsabilidad, ya que perdió su tarjeta, no brindó aviso oportuno al Banco y no interpuso una denuncia respecto al robo del que fue víctima, pese a no haber acreditado que se encontraba en algún estado de indefensión. Además, luego de arribar a la conclusión de que el cuidado y custodia de la tarjeta son responsabilidad del titular, la SFC determinó que la entidad financiera tiene el deber de elaborar el perfil transaccional de las costumbres de sus clientes y establecer procedimientos para la validación oportuna de las operaciones que no se ajustan a sus hábitos.

En segunda instancia, se determinó que era responsabilidad del Banco desplegar una conducta destinada a confirmar si las operaciones fueron realizadas por el titular o en su defecto bloquear las mismas, ya que estos movimientos constituían situaciones

inusuales no por el canal, el horario o el número de operaciones, sino solamente por el valor. En ese sentido, colige que el Banco debió aplicar las medidas de seguridad mínimas para la confirmación o el bloqueo de las operaciones, lo que hubiera evitado una mayor afectación en los recursos del consumidor.

En conclusión, la Corte confirmó el pronunciamiento emitido por la Superintendencia y determinó que las conductas de ambas partes facilitaron la realización de las operaciones reclamadas y, por tanto, contribuyeron en la ocurrencia del riesgo, por lo que deben asumir las consecuencias patrimoniales de la pérdida. Así, se asignó al Banco un 40% de responsabilidad en las transacciones objeto de reclamación, mientras que el resto recae en la parte demandante.

FICHA DE OBSERVACIÓN	
CATEGORÍA	**Sentencia (España)**
TEMA	Sentencia Roj. SAP M 7327/2022 (2022)

REGISTRO:

En esta sentencia, el demandante impugna los retiros fraudulentos de efectivo realizados por un tercero con cargo a su cuenta, argumentando que no habría incurrido en negligencia grave, ya que el método fraudulento utilizado era complejo y difícilmente detectable. Se cita la Directiva 2015/2366, sobre servicios de pago en el mercado interior (2015), que menciona que, la negligencia exigida para responsabilizar al cliente debe surgir de una conducta caracterizada por una significativa falta de diligencia, por lo que no será considerada como tal aquella que fue inducida por el engaño de un delincuente profesional.

La sentencia sostiene que el demandante no puede considerarse negligente de manera grave, ya que el método de fraude empleado, el phishing, era difícil de detectar para un cliente con sus características. La complejidad del engaño, evidenciada por la forma en que se denominaba al banco en el SMS y los errores gramaticales en el texto de dicho mensaje, no eran suficientes para que el demandante detectara el fraude. En contraste, se enfatiza la responsabilidad exigida a la entidad demandada, proveedora del servicio, que debió adoptar medidas de seguridad y mecanismos de supervisión para detectar operaciones fraudulentas.

En este fallo, se cita el Reglamento Delegado (UE) 2018/389 (2017), que señala la

necesidad de que las entidades financieras implementen tecnología antiphishing para detectar y cerrar páginas clonadas que podrían comprometer las credenciales del usuario. Además, se establece la necesidad de una conducta activa y tecnológica por parte de la entidad financiera para evitar situaciones de fraude, la cual no debe limitarse a la simplemente informativa o divulgativa.

FICHA DE OBSERVACIÓN	
CATEGORÍA	**Sentencia (España)**
TEMA	Sentencia Roj. SAP B 6560/2023 (2023)

REGISTRO:

En este caso, S.GOL, S.L. interpuso una demanda contra Banco Bilbao Vizcaya Argentaria S.A. (BBVA) por incumplimiento de un contrato de cuenta corriente bancaria debido a una transferencia no autorizada. S.GOL alegó que recibió un correo electrónico con un burofax que llevó a la descarga de archivos adjuntos, los cuales, al no poder visualizarlos, eliminó. Posteriormente, al acceder a su cuenta del Banco, le aparecía un mensaje de advertencia de seguridad, en el que le solicitaban su token móvil, por lo que procedió a escribirlo; no obstante, al ver que la página no se abría, verificó las cuentas mediante su teléfono encontrando una transferencia no autorizada de 3.000 €. A pesar de denunciar el incidente, el BBVA no anuló la transferencia y se negó a asumir los perjuicios por el fraude cometido.

En respuesta, BBVA argumentó que la responsabilidad no recaía sobre ellos, ya que S.GOL descargó troyanos y expuso sus claves de banca en línea. Señaló que la responsabilidad de la entidad no era ilimitada y no cubría supuestos de negligencia de sus clientes cuando estos exponían sus claves a terceros, por lo que la demanda debía desestimarse.

El tribunal concluyó que, según la normativa legal, el proveedor de servicios de pago es responsable de la restitución al ordenante en casos de operaciones no autorizadas, salvo excepciones. Una de estas excepciones consiste en que la responsabilidad recaerá en el ordenante en casos de actuación fraudulenta, negligencia grave o incumplimiento de las obligaciones del artículo 41, entre las que se incluyen la de tomar medidas razonables a fin de proteger sus credenciales de seguridad personalizadas. Dicha norma va acompañada de la obligación de la carga de la

prueba, la cual recae sobre el proveedor de servicios de pago, a quien le corresponde demostrar fraude o negligencia grave por parte del usuario.

A fin de definir la negligencia grave se cita la Sentencia Roj. SAP C 481/2023 (2023), en la cual se precisa que "[l]a negligencia grave supone una falta de la diligencia más elemental que consiste en no hacer lo que todos hacen", y la Sentencia Roj. SAP PO 496/2023 (2023) que señala lo siguiente:

[l]a negligencia que hace responder al cliente es la que se deriva de una conducta caracterizada por un grado significativo de falta de diligencia, lo que supone que la misma surge o se produce por iniciativa del usuario, no como consecuencia del engaño al que haya podido ser inducido por un delincuente profesional.

En este caso, el tribunal determinó que la actuación de S.GOL no constituía negligencia grave, ya que no podía prever la existencia de algún virus malicioso en el dispositivo. Además, subrayó la complejidad del método de "phishing", cuyas consecuencias dañosas no están al alcance de una persona promedio y, por tanto, es responsabilidad de la entidad financiera el dotarse de tecnología adecuada a fin de evitar la ejecución de operaciones fraudulentas. En consecuencia, se desestimó el recurso de apelación de BBVA y se confirmó la sentencia del Juzgado de Primera Instancia, que ordenó a BBVA la devolución del importe transferido.

FICHA DE OBSERVACIÓN	
CATEGORÍA	**Sentencia (España)**
TEMA	Sentencia Roj. SAP S 1277/2023 (2023)

REGISTRO:

El accionante presentó una demanda contra BBVA por una transferencia no autorizada de 9.987 € realizada desde su cuenta corriente. Alegó que, mientras consultaba su cuenta a través de la APP de BBVA, introdujo un código solicitado en la pantalla de actualización del módulo de seguridad, sin percatarse de que se trataba de una estafa. El juzgado de primera instancia desestimó la demanda, considerando la negligencia grave del demandante, quien introdujo el código solicitado sin leer el mensaje con la mínima atención, el cual constituye un elemento de seguridad adicional al realizar una transferencia.

En el recurso de apelación, el accionante argumentó error en la valoración de la

prueba y la incorrecta aplicación de la Ley de protección de pagos. La sentencia de apelación confirmó el pronunciamiento de primera instancia, basándose en la imprudencia del demandante al introducir el código de autorización para realizar la operación sin leer el mensaje, al haberse revelado, de los medios probatorios obrantes, que al parecer el accionante ingresó a la APP auténtica de la entidad, desde donde introdujo el código solicitado, lo que generaba dudas sobre si el actor realizó la transferencia de modo involuntario, conforme a lo alegado en su demanda.

FICHA DE OBSERVACIÓN	
CATEGORÍA	**Sentencia (España)**
TEMA	Sentencia Roj. SAP S 1267/2023 (2023)

REGISTRO:

Las accionantes presentaron una demanda contra Liberbank (hoy UNICAJA) por diversas operaciones realizadas sin su autorización después de recibir un mensaje aparentemente del banco que solicitaba ingresar a un enlace para confirmar una transferencia a favor de una de las demandantes en agosto de 2020. El demandado reconoció el fraude, pero argumentó la negligencia de la demandante al pinchar el enlace y autenticar las operaciones. El juzgado de primera instancia estimó la demanda, condenando a la entidad al pago de 23.240 € y 2.000 € más intereses legales.

En el recurso de apelación, UNICAJA alegó negligencia de la demandante al pinchar el enlace y sostuvo que los mensajes eran burdos porque la dirección del remitente no se parecía a la de Liberbank, por lo que su contenido no podía hacer caer en un error a una persona que obrase con una mínima precaución y diligencia. La sentencia de apelación desestimó el recurso, considerando que la entidad asumió la existencia del fraude y que la demandante fue víctima de "phishing", lo que la excluiría del supuesto de negligencia grave.

La sentencia destacó que la entidad no implementó medidas suficientes para proteger a sus clientes de ataques cibernéticos, ya que, en casos de "phishing", el usuario pierde el control de sus credenciales, no pudiendo imputársele negligencia, incluso si pinchó inicialmente el enlace sin precaución. Se mencionó la sofisticación de esta modalidad de estafa y su capacidad de imitar el lenguaje, formato e imagen de las

entidades financieras a las que suplantan, de modo que inducen fácilmente a error a la víctima; asimismo, se señaló la incapacidad de la entidad para detectar el fraude a pesar de que las múltiples operaciones se efectuaron en un corto período.

En consecuencia, se confirmó la responsabilidad de UNICAJA por incumplimiento de sus obligaciones relacionadas con implementar medidas de seguridad para los medios de pago.

FICHA DE OBSERVACIÓN	
CATEGORÍA	**Sentencia (España)**
TEMA	Sentencia Roj. SAP O 2047/2023 (2023)

REGISTRO:

En este caso, el accionante presentó una demanda contra Caja Rural de Asturias solicitando el reintegro de 5.996,83 euros por operaciones fraudulentas realizadas a través de la aplicación Ruralvía. Estas operaciones fueron producto de un fraude de phishing, en el que el demandante recibió mensajes SMS falsos que le indicaban activar un nuevo sistema de seguridad por lo que debía introducir los datos bancarios que le fueron requeridos.

La sentencia de primera instancia desestimó la demanda, argumentando que la ejecución de las operaciones implicó una doble autenticación por parte del demandante. Así, aunque había caído en el engaño de la página falsa a través de un SMS que simulaba ser de Caja Rural, posteriormente recibió otro SMS solicitando la introducción de un código para activar el servicio de biometría, a pesar de no haber solicitado tal activación. La sentencia concluyó que el demandante incumplió el deber de no facilitar sus datos, posibilitando al ciberdelincuente realizar las operaciones.

En la sentencia de segunda instancia, se analizó si el usuario proporcionó la clave SMS para activar el servicio de biometría, permitiendo así las operaciones fraudulentas. Al respecto, el Banco mencionó que el sistema de autenticación implementado para la realización de transferencias, requiere, en primer lugar, del número de usuario personal y de la clave de banca en línea y, en segundo lugar, de la aprobación a través de un segundo factor de autenticación que consiste en el envío de push (mensaje enviado al dispositivo del usuario para poner en su conocimiento la operación) y la firma, ya sea mediante biometría o a través del ingreso del código

facilitado por la entidad para la realización de cada una de las operaciones.

En el caso en concreto, el denunciante utilizaba el código facilitado para cada operación, pero modificó tal mecanismo por el sistema de biometría; luego, el código fue remitido mediante SMS al teléfono del accionante y este lo facilitó al defraudador. No obstante, dicho análisis se basa esencialmente en los registros del banco, lo que contraviene al artículo 44 de la Ley, que señala que el registro por el proveedor de servicios de pago sobre el uso del instrumento de pago no constituye prueba suficiente de que la operación de pago fue autorizada por el ordenante, ni de que este haya actuado de manera fraudulenta o incumplido deliberada o negligentemente alguna de sus obligaciones.

En tal sentido, la Sala considera que la única negligencia imputable al consumidor consiste en haber confiado en el SMS recibido en su móvil y en haber consignado las claves de acceso de su usuario en la página web a la que fue redireccionado, lo que no puede considerarse como negligencia grave. En conclusión, la sentencia de apelación revocó la decisión anterior y estimó la demanda de Don Raimundo, condenando a Caja Rural a pagarle 5.996,83 euros más intereses legales e imponiéndose las costas procesales a la demandada.

FICHA DE OBSERVACIÓN	
CATEGORÍA	**Sentencia (España)**
TEMA	Sentencia Roj. SJPI 1022/2023 (2023)

REGISTRO:

En este caso, la demandante interpuso una acción de reclamación contra el BBVA. Alega que la entidad bancaria incumplió sus obligaciones como proveedor de servicios de pago relacionadas con la autenticación reforzada de clientes y la seguridad en servicios financieros.

La demandante sostiene que fue víctima de fraude mediante el método "smishing", ya que recibió un mensaje de texto falso del BBVA, el cual se encontraba dentro de la línea de conversación que mantiene con BBVA. En dicho mensaje se le comunicaba la aceptación de una operación que presuntamente había realizado y se añadía un enlace web para, supuestamente, cancelarla en caso de no reconocerla, por lo que introdujo su usuario y contraseña en el enlace fraudulento. Posteriormente, recibió

mensajes de alerta a través de la aplicación móvil, en los que se le informaba de dos accesos no autorizados a sus cuentas bancarias desde dos móviles desconocidos. En ese momento, recibió una llamada en su teléfono de un supuesto encargado de protección al cliente de BBVA, quien le informó que alguien intentaba ingresar a su banca móvil, por lo que debía desinstalar la aplicación. Tras colgar e instalar nuevamente la aplicación, comprobó que se realizaron cargos fraudulentos en sus cuentas; por lo que presentó una reclamación al banco; sin embargo, el banco no restituyó todas las cantidades defraudadas.

El banco, por su parte, alega que la demandante actuó con negligencia grave al revelar sus datos de acceso y códigos de seguridad, ya que las transacciones fueron autorizadas correctamente, por lo que la responsabilidad recae en la demandante por no proteger adecuadamente sus credenciales.

El juzgado analiza el caso y determina que la demandante no incurrió en negligencia grave al caer en el fraude dada la complejidad del método "phishing" y concluye que la entidad bancaria no implementó medidas suficientes para prevenir este tipo de fraude, responsabilizándola por el perjuicio sufrido por la demandante.

Se enfatiza que la entidad bancaria debería haber adoptado tecnología avanzada para garantizar la seguridad en operaciones online, ya que la responsabilidad de custodiar las credenciales no recae únicamente en el cliente, sino también en la entidad que debe implementar medidas activas para prevenir situaciones de fraude.

Se cita la Sentencia Roj. SAP M 6240/2015 (2015), en la que se menciona que, “salvo actuación fraudulenta, incumplimiento deliberado o negligencia grave del ordenante (Art. 32), la responsabilidad será del proveedor del servicio de pago, lo que supone que a él le corresponde la carga de la prueba de que la orden de pago "no se vio afectada por un fallo técnico o cualquier otra deficiencia". Se argumenta, además, que la responsabilidad contemplada en la Ley es cuasi-objetiva ya que la entidad bancaria solo es exonerada si prueba la culpa grave del ordenante.

Se menciona también la Sentencia Roj. SAP PO 496/2023 (2023), que indica que la negligencia que atribuye responsabilidad al cliente es la que surge de una falta considerable de diligencia, lo que implica que la conducta se realiza por iniciativa del usuario y no como resultado del engaño al que pudo haber sido inducido. En ese sentido, la Sala concluye que en el caso concreto no se aprecia negligencia grave por parte de la demandante en el cumplimiento de sus obligaciones de protección respecto

de sus credenciales, ya que, para una persona no experta, no es fácil detectar que el mensaje recibido es fraudulento o que la página web a la que accedió es falsa. Por el contrario, respecto de la entidad financiera, se establece que incumplió con sus deberes de diligencia en la prevención del fraude por phishing, al no haber adoptado una serie de medidas de seguridad ni haberse dotado de mecanismos de supervisión que permitieran detectar operaciones fraudulentas en la prestación de servicios de pago, como, por ejemplo, adoptar mayores garantías para evitar que un tercero, sin autorización del titular de la cuenta, pueda modificar el canal para el intercambio de comunicaciones; en consecuencia, sería responsable del perjuicio total sufrido por la demandante. En ese sentido, el juzgado estimó sustancialmente la demanda, condenando al BBVA a pagar a la demandante la suma reclamada más los intereses legales.

Anexo 9. Declaración jurada de autenticidad de tesis

Universidad Nacional del Altiplano Puno | Vicerrectorado de Investigación | Repositorio Institucional

DECLARACIÓN JURADA DE AUTENTICIDAD DE TESIS

Por el presente documento, Yo **RAISA VEROSCA LIMACHE FRISANCHO** identificado(a) con N° DNI: **72182627** en mi condición de egresado(a) de la:
MAESTRÍA EN DERECHO CON MENCIÓN EN DERECHO ADMINISTRATIVO Y GERENCIA PUBLICA
con código de matrícula N° 172005, informo que he elaborado la tesis denominada:
LA FALTA DE PREDICTIBILIDAD DE LOS PRONUNCIAMIENTOS DEL INDECOPI EN MATERIA DE OPERACIONES FRAUDULENTAS EFECTUADAS POR INTERNET

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y no existe plagio/copia de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como suyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

En caso de incumplimiento de esta declaración, me someto a las disposiciones legales vigentes y a las sanciones correspondientes de igual forma me someto a las sanciones establecidas en las Directivas y otras normas internas, así como las que me alcancen del Código Civil y Normas Legales conexas por el incumplimiento del presente compromiso

Puno, 10 de Diciembre del 2024.

FIRMA (Obligatorio)

Huella

Anexo 10. Autorización de depósito de tesis en el Repositorio Institucional

Universidad Nacional del Altiplano Puno | Vicerrectorado de Investigación | Repositorio Institucional

AUTORIZACIÓN PARA EL DEPÓSITO DE TESIS O TRABAJO DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL

Por el presente documento, Yo **RAISA VEROSCA LIMACHE FRISANCHO** identificado(a) con N° DNI: **72182627**, en mi condición de egresado(a) del **Programa de Maestría o Doctorado:**
MAESTRÍA EN DERECHO CON MENCIÓN EN DERECHO ADMINISTRATIVO Y GERENCIA PUBLICA,
informo que he elaborado la tesis denominada:

LA FALTA DE PREDICTIBILIDAD DE LOS PRONUNCIAMIENTOS DEL INDECOPI EN MATERIA DE OPERACIONES FRAUDULENTAS EFECTUADAS POR INTERNET

para la obtención de ☒ **Grado.**

Por medio del presente documento, afirmo y garantizo ser el legítimo, único y exclusivo titular de todos los derechos de propiedad intelectual sobre los documentos arriba mencionados, las obras, los contenidos, los productos y/o las creaciones en general (en adelante, los "Contenidos") que serán incluidos en el repositorio institucional de la Universidad Nacional del Altiplano de Puno.

También, doy seguridad de que los contenidos entregados se encuentran libres de toda contraseña, restricción o medida tecnológica de protección, con la finalidad de permitir que se puedan leer, descargar, reproducir, distribuir, imprimir, buscar y enlazar los textos completos, sin limitación alguna.

Autorizo a la Universidad Nacional del Altiplano de Puno a publicar los Contenidos en el Repositorio Institucional y, en consecuencia, en el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, sobre la base de lo establecido en la Ley N° 30035, sus normas reglamentarias, modificatorias, sustitutorias y conexas, y de acuerdo con las políticas de acceso abierto que la Universidad aplique en relación con sus Repositorios Institucionales. Autorizo expresamente toda consulta y uso de los Contenidos, por parte de cualquier persona, por el tiempo de duración de los derechos patrimoniales de autor y derechos conexos, a título gratuito y a nivel mundial.

En consecuencia, la Universidad tendrá la posibilidad de divulgar y difundir los Contenidos, de manera total o parcial, sin limitación alguna y sin derecho a pago de contraprestación, remuneración ni regalía alguna a favor mío; en los medios, canales y plataformas que la Universidad y/o el Estado de la República del Perú determinen, a nivel mundial, sin restricción geográfica alguna y de manera indefinida, pudiendo crear y/o extraer los metadatos sobre los Contenidos, e incluir los Contenidos en los índices y buscadores que estimen necesarios para promover su difusión.

Autorizo que los Contenidos sean puestos a disposición del público a través de la siguiente licencia:

Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional. Para ver una copia de esta licencia, visita: https://creativecommons.org/licenses/by-nc-sa/4.0/

En señal de conformidad, suscribo el presente documento.

Puno, 10 de Diciembre del 2024.

FIRMA (Obligatorio)

Huella