UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

FACULTAD DE DERECHO

ESCUELA DE DERECHO

Responsabilidad administrativa de los bancos en los casos de phishing a propósito de las resoluciones brindadas por Indecopi

TESIS PARA OPTAR EL TÍTULO DE

ABOGADO

AUTOR

Andrea Denisse Torres Chavez

ASESOR

Armando Rafael Prieto Hormaza

https://orcid.org/**0000-0003-3084-6149**

Chiclayo, 2023

Responsabilidad administrativa de los bancos en los casos de phishing a propósito de las resoluciones brindadas por Indecopi

PRESENTADA POR

Andrea Denisse Torres Chavez

A la Facultad de Derecho de la
Universidad Católica Santo Toribio de Mogrovejo
para optar el título de

ABOGADO

APROBADA POR

Victor Javier Sanchez Seclen
PRESIDENTE

Blanca Lizbeth Carrasco Delgado
SECRETARIO

Armando Rafael Prieto Hormaza
VOCAL

Dedicatoria

Le dedico este trabajo a las personas que siempre creyeron en mí y fueron mí mayor soporte todo este tiempo.

Agradecimientos

A Dios, por siempre iluminar mí camino.

A mis padres, por brindarme su apoyo incondicional.

A mi hermana, por tenerme paciencia en mis amanecidas.

A mi profesor Carlos Tejada Lombardi, quien fue el que me motivó a seguir la presente investigación. Sus charlas, consejos y recomendaciones me enseñaron mucho.

Y, por su puesto, a todas las personas presentes en este proceso, por haber estado siempre.

INFORME DE ORIGINALIDAD

18%	18%	3%	11%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	3%
2	vlex.com.pe Fuente de Internet	2%
3	lpderecho.pe Fuente de Internet	1%
4	Submitted to Pontificia Universidad Catolica del Peru Trabajo del estudiante	1%
5	repositorio.usmp.edu.pe Fuente de Internet	1%
6	Submitted to Universidad San Ignacio de Loyola Trabajo del estudiante	1%
7	tesis.pucp.edu.pe Fuente de Internet	1%
8	tesis.usat.edu.pe	

Índice

Resumen

El incremento del uso de la tecnología, producto de la pandemia, ocasionó que las entidades financieras crearan nuevas formas de realizar transacciones bancarias mediante el uso de la banca por internet y aplicativos móviles, pero a la vez se generaron nuevas formas siniestros o fraudes cibernéticos, entre ellos el phishing. Los usuarios al verse afectados por estos sucesos acudieron al Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual, en adelante Indecopi, a interponer sus diversos reclamos por operaciones no reconocidas; sin embargo, esta entidad en sus resoluciones finales, analizaba el deber de idoneidad del proveedor financiero a partir del correcto ingreso de los datos confidenciales sin tomar en cuenta otras medidas de seguridad que a este tipo de servicios les competen, para así, finalmente, declarar responsable de su realización al consumidor. Por ello, la presente investigación analizó dichos criterios jurídicos ya establecidos, el deber de idoneidad, las normas complementarias de las entidades financieras y jurisprudencia a nivel internacional para finalmente establecer los criterios jurídicos adecuados mediante un precedente de observancia obligatoria que deberían seguir las resoluciones de Indecopi para determinar responsabilidad administrativa en este tipo de situaciones. Siendo un trabajo interpretativo, de tipo documental el cual, en su desarrollo, ha utilizado un modelo de investigación bibliográfica analizando resoluciones finales de este tribunal durante enero del 2020 – octubre del 2022.

Palabras clave: phishing, deber de idoneidad, medidas de seguridad, responsabilidad administrativa

Abstract

The increased use of technology, as a result of the pandemic, caused financial institutions to create new ways of carrying out banking transactions through the use of internet banking and mobile applications, but at the same time new sinister forms or cyber fraud were generated, like phishing. When users were affected by these events, they went to the National Institute for the Defense of Competition and Intellectual Property, hereinafter Indecopi, to file their various claims for unrecognized operations. However, this entity in its final resolutions, analyzed the duty of suitability of the financial provider based on the correct entry of confidential data without taking into account other security measures that are the responsibility of this type of services, in order to finally declare the consumer responsible for its realization. For this reason, the present investigation analyzed the legal criteria already established, the duty of suitability, the complementary regulations of financial institutions and jurisprudence at the international level to finally establish the appropriate legal criteria through a precedent of mandatory observance that Indecopi resolutions should follow to determine administrative responsibility in this type of situation. Being an interpretative work, of a documentary type which, in its development, has used a bibliographic research model analyzing final resolutions of this court during January 2020 - October 2022.

Keywords: phishing, duty of suitability, security measures, administrative responsibility.

Introducción

La modalidad de fraude cibernético: phising, según lo que menciona una encuesta realizada por la Organización Internacional de Policía Criminal (Interpol), por repercusiones de la COVID-19, se encuentra en un crecimiento constante dentro de las amenazas más importantes del sistema financiero, encontrándose incluso como dentro del sector de la ciberdelincuencia ocupando el primer lugar seguido por el malware/ransomware y por las violaciones de seguridad, mencionan que los ciberdelicuentes continuamente explotan nuevas tecnologías que se adapten a sus ataques de robo.

Aunado a ello, la importancia de su tratamiento jurídico proviene del hecho — tal como lo informa el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual —, que de los 75, 404 reclamos recibidos durante el periodo de enero del 2020 a marzo del 2021, el 47,75 % corresponde a la actividad bancaria y financiera, ocasionados en su mayoría por temas de consumos fraudulentos en las tarjetas de crédito y/o débito. Asimismo, se encuentra lo mencionado por la Superintendencia de Banca y Seguros (SBS) quien entre el periodo del 2018 y setiembre del 2022 recibió 22.214 denuncias contra las entidades del sistema financiero, lo cual sin ninguna duda bastante ha tenido que ver el impulso de la bancarización digital desde la aparición de la crisis sanitaria, siendo el año 2020 donde se registraron la mayor cantidad de casos.

De esta manera, la pandemia ocasionada por el virus Covid-19 ha conllevado a la aceleración del uso de la tecnología para el día a día de la vida de cada ciudadano, en el cual el sistema financiero no se ha encontrado exento pues este fue uno de los primeros en brindar diversas facilidades para los consumidores vía online con el fin de realizar transacciones bancarias ya sea desde un aplicativo móvil o el uso común de la laptop u ordenador personal pues en reemplazo de la forma presencial y directa del cliente al momento de realizar transacciones bancarias, se ha pasado al concepto de “mecanismos de autenticación” que, en otras palabras, significa la no necesidad de presencialidad como requisito de validez para realizar este tipo de acciones financieras.

Dicho desarrollo tecnológico y los nuevos servicios y productos que se brindan en el ciberespacio han traído consigo nuevos riesgos para los consumidores pues esta “facilidad” o “sencillez” también se ve reflejada en las nuevas formas de realización de fraudes por parte de los ladrones cibernéticos quienes han innovado en la forma de robo a través del envío de mensajes fenómeno denominado como “phishing”, el cual se caracteriza por ser

uno de los fraudes por Internet más peligrosos, complejos y masivos que se presentan en la industria financiera. Este consiste en el hurto de la identidad digital bancaria para asi poder obtener un lucro indebido, que se logra mediante el envío de un correo electrónico al cliente bancario –de forma engañosa- solicitándole al consumidor información personal o sensible sobre sus cuentas.

Después de todo lo desarrollado, estimamos que, de continuar con esta situación, el consumidor bancario se encuentra vulnerable ante este tipo de fraudes electrónicos pues, finalmente, a través de resoluciones de Indecopi se menciona que estos no "actuaron de forma diligente al resguardar su información personal"; pero, ¿qué sucede cuando estos actuan diligentemente y aun así son engañados por este tipo de fraude? ¿quién debe asumir sus consecuencias?, es decir, ¿a quién le corresponde asumir la pérdida del dinero apropiado por los delincuentes? Y, sobretodo, ¿cuáles son los criterios para determinar quien asume dicha responsabilidad?

Si pretendemos establecer que los consumidores bancarios son negligentes al caer en este tipo de fraude pues "no cumplimieron con su deber de resguardo al brindar su información personal a un tercero", estaríamos exonerando al banco de su responsabilidad como ente ventojoso de la relación comercial establecida. En efecto, no es incoherente considerar que quien ofrece el servicio es quien debe encargarse de gestionar y prever los riesgos típicos de su actividad profesional, maxime cuando nuestra legislación así se los exige a través de la implementación de medidas de seguridad en sus productos y/o servicios que brindan, obligaciones parcialmente consideradas por Indecopi quien, para determinar la responsabilidad ante este tipo de operaciones fraudulentas, solo toma en cuenta el cumplimiento de una de ellas.

En consecuencia, como hipótesis se plantea que si la modalidad de "phishing" es un patrón de fraude reiterativo hacia los consumidores y, por ende, constituye un riesgo típico de la actividad bancaria entonces las entidades financieras tendrán la obligación legal ante este tipo de situaciones de:

a) Asumir responsabilidad administrativa conforme a criterios jurídicos adecuados, tomando en cuenta sus obligaciones en conjunto que como tal le competen.

b) Encontrarse exoneradas de responsabilidad administrativa conforme a criterios jurídicos adecuados.

Revisión de Literatura

2.2. Bases Teóricas

2.2.1. Implicancias del phishing y su relación con el deber del banco de implementar medidas de seguridad.

Nuestro ordenamiento jurídico regula las operaciones del sistema financiero a través de la Superintendencia de Banca y Seguros, en adelante SBS, quien es el máximo ente supervisor de este sector empresarial siendo una institución constitucionalmente autónoma, así reconocida por el artículo 85 de nuestra carta magna, y con personería de derecho público que tiene como finalidad velar por los intereses del público en el ámbito financiero y de seguros, todo esto estipulado en el artículo 345 de la Ley N°26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros.

De esta manera, la SBS emite todas las normas concernientes entorno a la regulación de las entidades financieras, quienes tienen la labor de cumplir e implementar, como la Circular G-140-2009 la cual establece que para el desenvolvimiento de las entidades financieras dentro de nuestro sistema jurídico se debe mantener, establecer y documentar un Sistema de gestión de la seguridad de la información (SGSI) para así poder garantizar el acatamiento de una política de seguridad de información de usuarios o terceros propios de este sistema. Por ello, en base a esta normativa, a través de la Resolución N°504-2021, se aprobó el Reglamento para la gestión de seguridad de la información y ciberseguridad, el cual dispone que las empresas deben contar con un entorno seguro y confiable para la abasto de sus todos productos y servicios.

A través de este, desarrolla con mayor precisión las gestiones de ciberseguridad sobre temas que versan entorno al reporte interno de incidentes, vulnerabilidades, requisitos mínimos para su desenvolvimiento, protocolos de respuesta y/o recuperación frente a incidentes, entre otros; pero, es menester señalar lo mencionado en su artículo 19 donde prescribe que para el uso de las operaciones por canales digitales:

> “Se requiere de autenticación reforzada para aquellas acciones que puedan originar operaciones fraudulentas u otro abuso del servicio en perjuicio del cliente, como las operaciones a través de un canal digital que impliquen pagos o transferencia de fondos a terceros, (…), para lo cual se requiere:

a) **Utilizar una combinación de factores de autenticación,** según el literal j) del artículo 2 del presente Reglamento que, por lo menos, correspondan a dos categorías distintas y que sean independientes uno del otro.

b) **Generar un Código de autenticación mediante métodos criptográficos,** a partir de los datos específicos de cada operación, el cual debe utilizarse por única vez.

c) **Cuando la operación sea exitosa, notificar los datos de la operación al usuario**" (…). (El resaltado es nuestro)

En adición a ello, se promulgó el Reglamento de Tarjetas de Crédito y Débito, en adelante el Reglamento, en el cual a través del artículo 17 ha establecido diversas medidas de seguridad que deberán ser adoptadas como mínimo por las entidades bancarias e implementarlas dentro de sus sistemas a fin de evitar que sus usuarios sean víctimas de circunstancias que puedan afectar sus bienes jurídicos. En efecto, debido al carácter natural de la labor que desarrollan y "el riesgo al que se enfrentan en el manejo de recursos del público, especialmente de dinero, se encuentran en la obligación de adoptar mecanismos de seguridad indispensables para evitar la ocurrencia de siniestros ocasionados por asaltos bancarios, entre los cuales es razonable la implementación de dichos mecanismos".

En otras palabras, se entiende que las entidades financieras como entes expertas en el mercado que se desenvuelven para brindar un servicio idóneo estos tienen el deber, como una garantía legal, de contar con dichos mecanismos de seguridad. Como afirma Julio Campos, esta implementación dentro de los sistemas del banco, establece que el consumidor debe tener en cuenta que las instituciones financieras, en el desenvolvimiento de sus labores, son expertos en la formalización de sus servicios y los peligros que estos mismos pueden producir; de tal forma que, si bien la barrera de su actividad es elevada saben compensar el tema del riesgo o perjuicios que pueden estos mismos puedan generar.

A partir de este punto, se observa su relación implícita con el phishing pues al ser este uno de los fraudes por Internet más complejos y masivos alrededor de la industria bancaria, el cual, según la Audiencia Provincial de Madrid generalmente consiste en "la suplantación de identidad de un banco por parte del phiser con la finalidad de adquirir información confidencial del cliente para realizar operaciones por Internet", poniéndose

en relieve la responsabilidad de los bancos pues ante su acontecimiento, es imprescindible que este tipo de entidades cuenten con medidas de seguridad suficientes que permitan resguardar el patrimonio de los consumidores y, a su vez, advertir de su posible realización a través de los medios de comunicación que ha establecido con sus clientes.

Así pues, de cara a estas nuevas modalidades de fraude – phishing -, debemos tener en claro que, si bien es el ciberdelincuente quien, a través de engaños, convence al usuario para tener acceso a sus claves secretas y realizar el ilícito; esto no califica como una razón suficiente para considerar que dicha entidad se libera de responsabilidad al ver que el usuario trasgredió su deber de custodia.

Esto último justificado en la defensa que invocan los bancos pues mencionan que como fue el propio usuario quien accedió al link sospechoso y brindó sus datos sensibles sobre sus tarjetas es este quien debe ser el responsable; sin embargo, según se ha explicado, quien posee la obligación de implementar, intensificar o mejorar dichas medidas de seguridad para eludir los reiterados, constantes y previsibles atentados informáticos son las entidades financieras, quienes a través de diversas legislaciones advierten obligaciones a sobremanera que les competen dentro de su actuación profesional.

2.2.2. El deber de idoneidad frente al fraude cibernético phishing

El Código de Protección y defensa al consumidor, en su capítulo V referido específicamente a los Productos y Servicios Financieros, prescribe diversas obligaciones del proveedor que brinda dichos servicios y/o productos dentro del mercado financiero, además de, a su vez, precisar los derechos de los consumidores al momento de obtener un determinado servicio o producto, la información necesaria que deben recibir, publicidad, contratación y modificación contractual, imputación de pago, entre otros.

En este sentido, frente a esta lista de obligaciones que le competen a las entidades financieras, el deber de idoneidad se establece como un forma de ”cláusula general” la cual incorpora un conjunto de criterios que, a través del desarrollo de nuestra legislación, han permitido su aplicación en determinados casos en concreto, a partir de lo que se ha llamado *garantías en materia de consumo*.

Esta definida como aquella característica, términos o condiciones con los que cuenta un determinado servicio o producto; es decir, aquello que el proveedor ofrece al

consumidor debido a que una ley así se lo impone -garantía legal-, lo formuló de manera expresa en algún instrumento o documento informático -garantía explícita-, o bien por el uso y costumbre de un determinado servicio o producto encontrándose acorde a lo previamente ofertado -garantía implícita-. (Bellido, Y. 2018)

Ahora, en temas de servicios financieros, dichas garantías vinculadas al deber de idoneidad tienen una característica singular pues naturalmente los servicios ofrecidos de Banca por Internet, involucran tanto aspectos por contratación masiva y la adhesión a cláusulas generales de su contratación y posterior uso, como las obligaciones legales que se incorporan al servicio virtual que promulga la entidad financiera.

Por ello, dichas entidades no sólo se adhieren a lo establecido en el Codigo de Consumo, sino también a normas complementarias como La Ley de Protección Complementaria al Consumidor del Sistema financiero, el Reglamento de Tarjetas de Crédito y Débito, entre otras normas de menor jerarquía promulgadas por la Superintendencia de Banca y Seguros

Acorde a lo que menciona Gabriel Martín, siendo este un mercado excesivamente regulado, la magnitud de estas garantías legales aumenta ya que la trasgreción a cualquier elemento normativo puede determinar una contingencia de consumo y una trasgreción inoportuna hacia los usuarios.

De esta manera, si bien toda actividad empresarial tienen una disponibilidad libre de la oferta y demanda, pues nuestro sistema legislativo así lo dispone, debido a la relevancia de los servicios financieros y la norma tuitiva dirigida a estos usuarios, el derecho condiciona dicho principio de libertad permitiendo que exista una regulación de parámetros mínimos para el ofrecimiento de los servicios financieros. En este orden de ideas, es que es completamente exigible a cualquier servicio financiero dichas garantías establecidas alrededor de la legislación nacional; y, por tanto, considerar que ante su incumplimiento se contraviene directamente el deber de idoneidad.

Así, en relación al fraude cibernético phishing, se entiende que las entidades financieras, al ser proovedores del servicio, se encuentran obligadas a prestar los servicios y entregar los productos en las condiciones esperadas por el consumidor, de acuerdo a los términos comunicados y previsibles, destacando esta última parte pues les compete a estas entidades preever los posibles siniestros que puedan afectar o atentar contra los bienes juridicos que deben resguardar de los usuarios. Los hurtos, robos y estafas cibernéticas

son un riesgo de la actividad bancaria electrónica, los cuales tienen que estar minuciosamente gestionados para evitar daños al consumidor o cliente financiero y, de una indebida distribución de riesgo, conllevaría a asumir al consumidor el costo de dichas acciones delitivas.

El fraude cibernético phishing si bien se muestra como un tipo de fraude donde se le atribuye cierta "responsabilidad" al usuario pues fue este mismo quien facilitó sus claves secretas, que debía tener en custodia, hacia terceros; no se toma en cuenta el tema del engaño y de las obligaciones que inicialmente le competen al banco debido a las condiciones de un servicio idóneo a las que se encuentran sugestionados como son: verificar que quien realice dicha operación sea el titular de la tarjeta mediante factores de autenticación, clave digital, token, entre otros; analizar si las transacciones se encuentran dentro del consumo habitual del tarjetahabiente; alertar sobre movimientos inusuales mediante mensaje de texto, correo, entre otros; bloquear, en caso de verificar una acción fraudulenta, la cuenta para que así no se trasgreda el patrimonio del cliente, entre otros.

2.2.3. Criterios jurídicos utilizados por el Tribunal del INDECOPI en los casos de phishing para determinar la responsabilidad administrativa

En la última década, el Tribunal de INDECOPI para determinar la existencia de responsabilidad administrativa en este tipo de casos ha utilizado diversos criterios jurídicos, los cuales han ido evolucionando junto con el perfeccionamiento de la doctrina; pero, finalmente para dictar sus resoluciones, en su mayoría, ha promulgado fundamentarlas en dos obligaciones esenciales con el fin así establecer si el banco actuó o no de manera idónea y, por ende, al verificar que alguna de ellas no llegara a efectuarse determine la existencia de responsabilidad financiera o, según sea el caso, otorgarle la responsabilidad al usuario. Dichas obligaciones son:

2.2.3.1. Autorización del titular para la realización de la operación cuestionada

El Reglamento de Tarjetas de Crédito y Débito, en su artículo 17, sobre las medidas de seguridad respecto al monitoreo y realización de operaciones, menciona que debe existir, cuando sea aplicable, una presentación de un documento oficial de identidad o utilizar un mecanismo de autenticación de múltiple factor, el cual permita reconocer que efectivamente es el titular quien esta realizando dicha operación. Así, entiende que para la realización de cualquier operación financiera es necesario que se

acredite fehacientemente que quien realiza dicha operación sea el titular de la cuenta de la cual se harán cargos, giros, transferencias, solicitud de préstamos, entre otros.

En razón de ello, para establecer el parámetro de idoneidad en este tipo de casos es menester verificar que los mecanismos de seguridad implementados por los proveedores financieros hayan funcionado acorde a su función como tal, para así poder cuestionar si el servicio brindado fue o no un servicio idóneo. Ello pudiendo ser demostrado a través del ingreso de un código, firma electrónica, otra forma de inicio de sesión en la plataforma correspondiente, entre otros.

2.2.3.2. Obligaciones del consumidor

El consumidor a la vez que ha adquirido derechos, también deberes, por lo que a través de diversa jurisprudencia se ha comentado la responsabilidad que este tiene por ser el propietario de su tarjeta en cuanto a su conservación y la clave de identificación personal. Incluso, este tiene el deber de comunicar a la entidad financiera respecto de cualquier situación potencial de riesgo en el uso ilícito de su tarjeta, tal como su pérdida, sustracción o situaciones que podrían posibilitar su uso por un tercero no autorizado.

Estas mencionadas, a su vez, en casos de phishing como aquel deber de custodia que tiene el consumidor de resguardar su información secreta, datos confidenciales y claves de su tarjeta. Por ello, es que el Indecopi lo considera como un criterio para determinar responsabilidad en tanto que, menciona, fue este quien permitió que terceros accedan a su información confidencial de forma voluntaria.

2.3. Definición de Categorías Conceptuales

2.3.1. El Phishing

Según Jerry Féliz y Chris Hauck (2004), en la conferencia titulada “Sistema de Seguridad: La perspectiva de un Hacker”, definieron al phishing como el método a través del cual una persona puede imitar a una entidad de confianza u organismo financiero vía online con la finalidad de sustraer información del usuario quien se presenta como víctima ante este suceso. En otras palabras, se define a este tipo de fraude cibernético como el proceso por el cual una persona, vía online, mediante correo electrónico simula ser una institución financiera legítima para obtener información privada de los usuarios como: contraseñas, datos bancarios, entre otros.

Asimismo, menciona Flores Mendoza, que este puede verse desde dos sentidos: el sentido amplio y el sentido estricto, el primero se refiere al delito como un grupo de conductas que conllevan a provocar un desembolso patrimonial tanto al usuario como a la entidad financiera, siendo la característica esencial de esta el acceso eficaz a las claves de internet del usuario perjudicado, las cuales permitirán ingresar al portal digital de la entidad financiera sin el consentimiento del titular ni del banco; mientras que, por otro lado, el segundo, el cual ciñe su existencia al primer paso que es cuando el "phisher" accede indebidamente a la información.

Pero, una definición más precisa proporcionada por el Anti-Phishing Working Group es, que los ataques de phishing son:

> *"Formas de ingeniería social y subterfugios técnicos para robar los datos de identificación personal de consumidores y las credenciales de cuentas financieras. Estos ardides de ingeniería social se basan en correos electrónicos engañosos que conducen a los consumidores a sitios web falsos diseñados para estafar a los destinatarios para que divulguen datos financieros tales como números de tarjetas de crédito, nombres de usuario de cuentas, contraseñas y números de la seguridad social. Apropiándose de nombres comerciales de bancos, distribuidores y compañías de tarjetas de crédito, los phishers a menudo convencen a los destinatarios para que respondan". (Instituto Nacional de Tecnología de la Investigación, 2007)*

Por su parte, Balmaceda Hoyos (2009) propone que el 'phishing' – el cual significa una "pesca de claves", conjunción de las palabras en inglés 'password' y 'fishing'- se basa en el uso de las comunicaciones de Internet, mediante un e-mail, para adquirir toda la información financiera personal del consumidor. La cual, según Nicolás Oxman, puede constituir un medio para la realización de complejas o elaboradas formas de estafas informáticas, donde caracteriza su elemento informático: el Internet, como su plataforma de soporte operativo.

En conclusión, el phishing es una modalidad de fraude cibernético el cual se desarrolla a través del envío de un correo o mensaje electrónico por el "phiser" quien simula ser una institución legítima con el fin de así poder obtener datos secretos en relación a información financiera, personal, contraseñas, entre otros; pero que, termina

ejerciendo una forma de engaño para captar o robar la información del usuario víctima de este suceso.

2.3.2. El deber de idoneidad

A través del artículo 18 de la Ley N°29571 – Código del Protección y Defensa del Consumidor, el Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual – INDECOPI menciona que:

"Se entiende por idoneidad la correspondencia entre lo que un consumidor espera y lo que efectivamente recibe, en función a lo que se le hubiera ofrecido, la publicidad e información transmitida, las condiciones y circunstancias de las transacción, las características y naturaleza del producto o servicio, el precio, entre otros factores, atendiendo a las circunstancias del caso".

Esta misma entidad, mediante sus pronunciamientos, menciona que esta idoneidad se refiere tanto a las condiciones expresamente pactadas como, también a las expectativas generadas en el consumidor atendiendo a circunstancias propias que rodean el propio acto de consumo: la vulnerabilidad del consumidor, la asimetría en la relación de consumo, la posición que ostenta el proveedor dentro del mercado, la información proporcionada y, por último, la confianza o expectitivas que tenga el consumidor por el bien o servicio contratado.

En adición a ello, Rodolfo Salas (2010), define al deber de idoneidad como aquella obligación que poseen los proveedores de entregar los bienes y servicios que ofrecen en la forma exacta en como han sido ofertados o, en otras palabras, tal y como ellos se comprometieron mediante su oferta. De esta manera, se entiende al deber de idoneidad como parte de la expectativa de los consumidores, el cual fundamenta o justifica el deseo de adquirir dicho producto o servicio por parte del consumidor, entendiéndose a este como una obligación fundamental del proveedor de cumplir con lo previamente ofrecido en características como: duración, contenido, calidad, uso, entre otros.

Así pues, siguiendo lo que menciona Northcote, el deber de idoneidad se encuentra en la etapa de ejecución de la relación de consumo, pudiendo manifestarse tanto en la etapa de prestación de servicios como en la etapa de comercizaliación de algún producto. Si bien, en la doctrina, se ha criticado la amplitud que este principio pretende abarcar, en nuestro ordenamiento jurídico constituye una parte fundamental en la impartición de justicia en

las relaciones de consumo pues representa la naturaleza tutelar de defensa en beneficio de quienes se encuentran en una situación de asimetría informativa.

Cabe mencionar que, con respecto al sistema de tarjetas de crédito y/o débito, la entidad financiera emisora al igual que el establecimiento afiliado tendrán que cumplir con la idoneidad del servicio ante el usuario o consumidor financiero; rescatando que, únicamente las entidades financieras son las legalmente responsables en la totalidad de lo que versa sobre la seguridad del medio de pago, el bloqueo o activación de la tarjeta, el uso de la misma en sus distintas modalidades -vía online o presencial- y los medios de comunicación disponibles para sus usuarios.

Este deber de idoneidad también se entiende desde el principio de tipicidad en materia de los procedimientos administrativos de protección al consumidor pues, acorde menciona la Resolución Final N°0144-2022/CC2 - INDECOPI:

> "*Las normas de protección al consumidor se adscriben u operan como parte del derecho ordenador del mercado y requieren de tipos de infractores amplios, dada la versatilidad de las conductas que podrían adoptarse para evadir los derechos de los consumidores, siendo una constante en estos ordenamientos construir tipos infrectores de tal naturaleza, lo que no afecta el principio de tipicidad establecido por la Ley del Procedimiento Administrativo General, pues como también ha reconocido el Tribunal Constitucional para que se cumpla con el principio de tipicidad en materia administrativa basta que de la norma – que contiene una descripción general del supuesto de hecho – sea razonablemente posible extraer la conducta infractora a partir de criterios lógicos, técnicos o de experiencia."*

Es por ello, que el Colegiado mencionado, considera que no es posible establecer un catálogo de conductas infractoras para este deber idóneo; sino que a través de diversas de conductas, dentro de los límites establecidos en su propia definición, se puede constituir una infracción, toda vez que su análisis se realiza evaluando cada caso en concreto en temas relacionados al cumplimiento o adecuación entre lo esperado por el consumidor o lo ofrecido por el proveedor y lo realmente recibido; de tal manera que, si no existe una correspondencia, se entiende, existirá infracción.

2.3.3. Medidas de Seguridad en transacciones financieras por internet

Según Eugenio Cuello (1999), las medidas de seguridad se refieren a aquellos medios privativos, limitativos o preventivos de bienes jurídicos que son impuestos por el estado para ciertas circunstancias en concreto por un tiempo indeterminado pues, a través de estas se pretende resguardar los bienes jurídicos de los usuarios. Así, son entendidas como una solución rápida y vinculante para todas las entidades empresariales, pues se interpreta que, para la realización de alguna transacción o servicio ofrecido, deberan contar con el mínimo de medidas de seguridad establecidas en nuestra legislación nacional, permitiéndose implementar más de las exigidas si se pretende obtener una mayor seguridad, sobre todo si lo que se busca es velar por la mayor protección del consumidor.

Dichos requisitos mínimos se encuentran estipulados en diversos reglamentos de nuestra legislación, pero para efectos de la presente investigación nos centraremos en lo que establece la Resolución N°6523-2013 – Reglamento de Tarjetas de Crédito y Débito- promulgado por la Superintendencia de Banca y Seguros, en su artículo 17 pues menciona aquellas medidas de seguridad que se deben cumplir en respecto al monitoreo y la realización de operaciones con tarjetas:

"*Las empresas deben adoptar como mínimo las siquientes medidas de seguridad con respecto a las operaciones con tarjetas que realizan los usuarios:*

a) ***Contar con sistemas de monitorio de operaciones, que tengan como objetivo detectar aquellas operaciones que no corresponden al comportamiento habitual de consumo del usuario****. (…)*

e) Requerir al usuario la presentación de un documento oficial de identidad, cuando sea aplicable, o ***utilizar un mecanismo de autenticación de múltiple factor.*** *(…)*

f) En el caso de operaciones de retiro o disposición en efectivo, según corresponde, u otras con finalidad informativa sobre las operaciones realizadas u otra información similar, ***deberá requerirse la clave secreta del usuario, en cada oportunidad, sin importar el canal utilizado para tal efecto."*** (el subrayado es nuestro).

Siendo estas mandatos imperativos para todas las entidades financieras y bancarias pues deberán implementar formas de moritoreo en sus sistemas para las transacciones

financieras que deseen brindar ya sea de forma virtual o presencial para así poder detectar operaciones que no corresponden al comportamiento habitual de consumo del propietario de dicha tarjeta; además de tener que emplear un mecanismo de autenticación de múltiple factor que permita reconocer fehacientemente que quien está haciendo uso de la tarjeta sea, en efecto, el titular de la misma; y, requerir, indispensablemente, la clave secreta del usuario ya sea manifestada bajo el título de: "token digital", "clave digital", entre otros.

2.3.3. Responsabilidad administrativa del Proveedor

Si bien el término que alude "responsabilidad" es totalmente amplio ya que puede referirse a diversos ámbitos del derecho tanto desde el punto de vista obligacional, sancionabilidad, civilista, entre otros, en el presente caso nos referiremos a este aludiendo al campo específico del Derecho Administrativo pues aquí, según Carlos Rojas (2014), la responsabilidad recae en quien comete una conducta o un acto regulado dentro del marco legislativo de un procedimiento administrativo sancionador. Señala que, específicamente en esta situación, no sólo se trata de una indeminazación como tal sino, también, de una sanción dentro del marco de un procedimiento, el cual va a determinar una sanción en beneficio de la administración pública y, en ciertos casos, en una medida correctiva en favor del consumidor.

Esta responsabilidad, se encuentra fundamentada en el principio de causalidad regulado en nuestra legislación peruana en el inciso 8) del artículo 230 de la Ley N°2744, Ley del Procedimiento Administrativo General pues de esta nace la relación de causalidad entre la conducta del administrado y la infracción sancionable. Así, lo que pretende la responsabilidad administrativa es desincentivar aquellas conductas de los proveedores que configuran infracciones en las relaciones de consumo y para entender el alcance y la configuración de la responsabilidad administrativa de estos se debe evaluar el rubro o caso en particular, considerando tanto los términos y condiciones como las circunstancias del caso.

Asimismo, a través del artículo 104 de la Ley N°29571 – Código de Protección y Defensa del Consumidor, esta normativa se refiere a la responsabilidad del proveedor cuando existan estos supuestos:

"***El proveedor es administrativamente responsable por la falta de idoneidad o calidad, el riesgo injustificado o la omisión o defecto de información o cualquier otra***

infracción a lo establecido en el presente Código *y demás normas complementarias de protección al consumidor, sobre un producto o servicio determinado."* (el subrayado es nuestro)

Respecto a estos deberes esenciales mencionados, INDECOPI ha establecido diversos lineamientos en su jurisprudencia, enmarcando a la falta de idoneidad a aquella situación cuando no existe una similitud entre lo que el consumidor espera y lo que finalmente obtiene, pero a la vez lo que este espera dependerá de la cantidad y calidad de información recibida por parte del proovedor.

Así, como menciona Bullard, esta responsabilidad es sancionable pues las empresas no cumplieron con ofrecer servicios o bienes idóneos dentro de la expectativa tenida por un consumidor razonable. Destacando que, en el momento de evaluar la debida diligencia, se deberá tener en cuenta el ámbito empresarial, los bienes o servicios ofertando, la asimetría contractual, entre otros; para determinar si existe o no responsabilidad.

De esta manera, la configuración de responsabilidad constituye, de cierta manera, una garantía en favor de los consumidores con el fin de que así las empresas implementen y formen políticas de protección sostenibles pues dichos supuestos respaldaran la consolidación del proceso competitivo en el que los proovedores serán premiados por las elecciones en cumplimiento de esta normativa, o bien sancionados por sus malas prácticas en vulneración de estos supuestos.

Materiales y métodos

El presente trabajo investigativo es interpretativo, de tipo documental el cual, en su desarrollo, ha utilizado un modelo de investigación bibliográfica a nivel nacional e internacional, a través del método análitico, mediante el cual se interpretó la información y analizó los datos del objeto de estudio que versan específicamente en sus elementos esenciales (el deber de idóneidad, phishing, medidas de seguridad y responsabilidad administrativa del proveedor); la técnica de gabinete, también conocida como “fichaje”, con la cual se sistematizó las fuentes bibliográficas del fundamento teórico de la investigación (fichas textuales, de resumen y bibliográficas); y, finalmente, el análisis documental pues se analizó fuentes de información amplia como revistas, artículos, jurisprudencia, doctrina y tesis; orientados a la búsqueda de resultados para el problema planteado.

Cabe mencionar, que todo el método descrito involucra, en su progreso, la observación, descripción y redacción de la realidad problemática, planteamiento del problema y objetivos tanto generales como específicos, propuesta de la hipótesis, y, por último, la selección y recopilación de documentos sobre los cuales se ha realizado una revisión de manera exahustiva y rigurosa para escoger de forma sistemática lo más relevante para la investigación. Para finalizar, se realizó una lectura crítica aplicando la técnica del fichaje y el análisis documental de jurisprudencia, doctrina, artículos y libros electrónicos para la redacción del informe final con las conclusiones pertinentes.

Resultados y Discusión

4.1. Análisis desde la perspectiva de Indecopi respecto a las operaciones fraudulentas y su clasificación

De acuerdo a lo anteriormente mencionado, se entiende que una condición implícita dentro del deber idóneo de las entidades financieras es la garantía exigida a los proveedores de implementar, dentro de sus sistemas informáticos, medidas de seguridad que aseguren la protección del patrimonio de sus consumidores, considerándose, como parte del servicio prestado, la confianza que este le pueda atribuir a dichos sistemas de seguridad para la realización de cualquier operación mediante los recursos que esta le ofrezca como son la tarjeta de crédito, débito, banca por internet, entre otros.

Ahora bien, es común que en la dinámica de las relaciones comerciales existan diversos modos de efectuar transacciones financieras, y para poder establecer cuales medidas de seguridad le competen a cada una de estas es necesario constituir una clasificación jurídica la cual permita identificar fehacientemente el tipo de transacción y la forma de su realización.

De esta manera, el presente apartado se centrará en la clasificación realizada por Indecopi sobre dos tipos de operaciones financieras ya sea mediante el uso de la "tarjeta presente" o la "tarjeta no presente", siendo importante mencionar que para garantizar su correcta realización, en ambas situaciones, es imprescindible contar con la autorización válida del tarjetahabiente.

Con respecto a las transacciones bancarias con tarjeta presente, según el artículo 9 del Reglamento de Tarjetas de Crédito y Débito, para esta se requiere la presencia física de la tarjeta, la cual será auténticada por un terminal de venta también llamado POS por su siglas en inglés *Point of Sale*, en el cual se puede solicitar la clave secreta, la firma electrónica o la suscripción del orden de pago para que una operación pueda ser autorizada válidamente.

Si bien, en la actualidad, existen otras situaciones que no requieren que la tarjeta sea identificada por un terminal pues para su realización cuentan con un chip integrado o, en teléfonos modernos, con formas de *contactless*, siempre será necesaria la autenticación de la persona quien lo realiza.

Mientras que, respecto a las transacciones bancarias con tarjeta no presente, las condiciones exigidas cambian pues su realización se ejecuta a través de medios electrónicos como son vía banca por internet, Apps ofrecidas por el banco y otros medios que el mismo banco autorice, pasando de la condición de presencia física de la tarjeta a requerirse el ingreso de los datos impresos en esta misma como son los dieciséis dígitos, el código CVV, el nombre del tarjetahabiente, la fecha de vencimiento, o la clave dinámica, datos que permitirán identificar que es realmente el propietario de dicha tarjeta quien está realizando la transacción solicitada.

Por ello, ante el cuestionamiento por el consumidor de alguna de estas transacciones, será la entidad financiera quien deberá acreditar de manera indubitable que la operación realizada fue autorizada válidamente por el consumidor, en tanto que al proveedor, especialista en su mercado y sus sistemas de seguridad, se le ha asignado la carga de la prueba.

Cabe mencionar que, a estas medidas de seguridad se le añaden lo preescrito el artículo 17 del mismo Reglamento pues las entidades financieras, a su vez se encuentran obligadas a contar con sistemas de monitoreo respecto a las operaciones financieras, los cuales deben permitir, en principio, detectar aquellas transacciones que conformen parte del comportamiento habitual del consumidor y; además, ser capaces de identificar patrones de fraude y activar las alertas correspondientes para evitar su realización o, en su defecto, ser capaces de efectuar las acciones necesarias para resguardar el patrimonio de sus consumidores.

En consecuencia, el Indecopi reconoce que para poder determinar responsabilidad en casos de operaciones fraudulentas con tarjeta no presente primero se deberá analizar si la transacción cuestionada contó o no con la autorización válida del titular de la cuenta materia investigación, evaluando el correcto ingreso de los datos confidenciales o los dos factores de autenticación implementados en sus sistemas de seguridad; para luego, evaluar si es que dichas transacciones se encontraban o no dentro del parámetro habitual del consumidor.

No obstante, si bien el Indecopi brinda un análisis impecable y uniforme sobre los elementos para atribuir responsabilidad, cuando analiza los casos en concreto, estos no son considerados o, en el mayor de los casos, utiliza solo uno de estos criterios mencionados para atribuir responsabilidad.

4.2. Elementos que constituyen una ruptura del nexo causal para atribuir responsabilidad en casos de phishing

Esto último, demostrado a través de diversa jurisprudencia pues centrándonos en el caso materia de investigación conocido como phishing – o, en su similitud, smishing– este órgano colegiado evalúa el parámetro de idoneidad únicamente a partir del ingreso correcto de manera indubitable de los datos confidenciales del cliente, solamente haciendo alusión a este otro mecanismo de seguridad cuando el consumidor lo cuestiona en su denuncia, no siendo estos parte de una obligación exigible o imprescindible para evaluar la idóneidad del servicio ofrecido.

Es por ello que, si a través de la evaluación que realice Indecopi la entidad bancaria logra acreditar que las transacciones financieras se realizaron bajo parámetros de autorización "válidos", finalmente determina que el banco actuó diligentemente y, por ende, carece de responsabilidad obteniendo como resultado que las denuncias de los consumidores sean declaradas infundadas.

Por tener de ejemplo la Resolución Final N°1756-2022/CCI del Expediente N°0069-2022/PS2 menciona la obligación del banco de acreditar la correcta autorización de las operaciones financieras mediante canales electrónicos donde evalúan los factores de autenticación que mínimamente deben ser solicitados por este tipo de entidades como son el Token, clave de coordenadas, clave SMS, el número de tarjeta de crédito/débito o la clave secreta de internet previamente estipulada por el consumidor, para así mencionar que como estos fueron ingresados "válidamente" no se les puede atribuir responsabilidad.

O bien, la Resolución Final N°0496-2022/CC1 del Expediente N°2411-2021/PS2 mediante el cual mencionan que, como existen suficientes elementos de convicción que el Banco presentó con el propósito de acreditar el debido cumplimiento de las medidas de seguridad – refiriéndose únicamente al ingreso válido de los códigos de autenticación – es que establecen la imposibilidad de atribuirle responsabilidad al banco, pues, además, consideraron que la denunciante no cumplió con su deber de custodia al haber ingresado a un enlace web de dudosa procedencia, para luego brindarle información confidencial a terceros y así estos puedan realizar los hechos materia de denuncia.

Añadido a ello, lo expresamente señalado en la Resolución Final N°0286-2022/PS2 del Expediente N°0028-2022/PS2 donde menciona que *si bien el banco se encuentra obligado a adoptar medidas de seguridad para la autorización de operaciones con*

tarjeta no presente, ninguna acción resultará eficaz si el propio consumidor omite su deber de custodia; con el cual, afirma que si nos encontramos ante este tipo de fraudes cibernéticos será completa responsabilidad del consumidor su realización pues considera que este no fue suficientemente diligente al resguardar su información secreta y dejar que terceros accedan a su información. Incluso, menciona, que el consumidor pudo evitar el fraude si es que tomaba en cuenta la información compartida en la página oficial del banco respecto a la seguridad en las transacciones vía internet.

En efecto, Indecopi únicamente en los casos que el banco no ha podido demostrar que en el registro de sus sistemas las operaciones se realizaron con las contraseñas, información privada del consumidor, o en los casos que los retiros se produjeron luego del aviso de dichas operaciones, es que resuelve en favor del consumidor. Frente a ello nos cuestionamos ¿dicho deber de cuidado hasta donde debería considerarse?

Pues el consumidor, en este tipo de casos, es víctima de un tercero con conocimientos especializados y accionar doloso, no encontrándonos de acuerdo con que si "se hubiera revisado la información impartida por el Banco sobre los fraudes" se pudiera haber evitado, en tanto que la acción del consumidor sobre "entregar su información sensible a un tercero" no es excusa para no analizar si la entidad bancaria realmente ofreció un servicio idóneo a este, pues como ya se ha explicado en el supuesto de responsabilidad administrativa la carga de la prueba se le impone a la entidad bancaria.

Si partimos desde los origenes de la protección al consumidor tomando en cuenta tanto normativa constitucional como legislativa, el fin propio de la creación de el Indecopi es que este pueda fomentar en el mercado mejores decisiones de consumo, donde se garantice que estos puedan acceder a productos y servicios idóneos y que, a su vez, gocen de derechos y mecanismos efectivos para ello, por lo que no es posible afirmar que la "falta al deber de cuidado" sea considerado como un eximente de responsabilidad, cuando el Indecopi no ha evaluado todas las obligaciones que al proovedor bancario, en su situación beneficiosa de la relación comercial, les son exigidas y las cuales se encuentran incluidas dentro del parámetro de idoneidad del servicio que brindan.

Con ello no señalamos que el consumidor siempre debe ser exhimido de responsabilidad debido a su situación de desventaja pues, como afirma Alfredo Bullard, "asumir que el consumidor puede ser protegido en cualquier circunstancia, sin importar su nivel de diligencia, es asumir que tendrá una suerte de seguro contra su propia

irresponsabilidad"; sino que, se pretende que Indecopi para dictar sus fallos realice un análisis basado en todas las obligaciones que normativamente se les ha atribuido a este tipo de entidades.

Entre ellas el estudio detallado del comportamiento habitual del tarjetahabiente, implementar procedimientos complementarios para gestionar la activación de alertas por movimientos inusuales, identificar posibles patrones de fraude, entre otros; para que, con la evaluación de todo ello, se pueda determinar si realmente brindaron un servicio idóneo y por ende, que efectivamente carecen de responsabilidad.

4.3. Propuesta de Criterios Jurídicos que Indecopi debe considerar para determinar responsabilidad administrativa en casos de phishing

Ante este panorama resultaba imprescindible realizar un estudio que abarque esta problemática pues, en la actualidad, se ha convertido en uno de los ataques más comunes y engañosos de los medios digitales, el cual ha ocasionado daño en el patrimonio a más de un usuario financiero. Por lo que, finalmente, en este acápite se explicará la propuesta de criterios jurídicos para el análisis de responsabilidad a partir de la aplicación del artículo 17 estipulado en el Reglamento de Tarjetas de Crédito y Débito, para que así el Indecopi, ante este tipo de casos, configure a esta norma como una condición mínima legal al analizar el parámetro de idoneidad de los servicios financieros.

La mencionada norma alude a diversas obligaciones que el banco debe cumplir, entre ellas la de conocer el comportamiento habitual de consumo de cada uno de sus clientes mediante los productos contratados con el banco, en razón a que se encuentra en posición de monitorear el uso de dichos productos, pudiendo así conocer los movimientos realizados por el consumidor durante la relación de consumo. Este estipulado en el artículo 2 del mismo Reglamento entendido como aquel 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.*

De esta manera, la norma entiende al comportamiento habitual como la manera en que cada consumidor va creando su propio historial de consumo generado conforme a su uso y necesidades acordes a su actuar habitual, teniendo en cuenta que el comportamiento de consumo de los usuarios no obedece a un conjunto "inmutable y estático" de

operaciones, sino que este es, naturalmente dinámico y está en un constante desarrollo personal de cada cliente en particular.

En este sentido, lo que se evalúa es que cada sistema de monitoreo utilizado por la banca es que debe poder detectar de manera individualizada cuando una transacción no se encuentre acorde a dicho consumo habitual del tarjetahabiente y, en el mejor de los casos, identificar patrones de fraude. Esto último también considerado como parte de las medidas de seguridad, al cual se le reconoce como una suerte de "consecuencia" del comportamiento habitual de consumo pues aquí se encargará de identificar, del registro individual de cada tarjetahabiente, aquellas transacciones que se realizan dentro de un parámetro "sospechoso".

Refiriéndose a que cuando se realicen varias transacciones en un corto periodo de tiempo ya sea por diversos montos, lugares de realización, terceros beneficiarios, horario poco habitual, entre otros; es que detectará aquellas operaciones como ajenas al patrón de consumo habitual del usuario. Añadido a esto, están los procedimientos para gestionar alertas pues son los encargadas de advertir a los usuarios sobre los consumos realizados en su cuenta.

Dichos mecanismos de seguridad igualmente considerados como un parámetro de idoneidad dentro de las obligaciones bancarias para otros países como, por ejemplo, Chile el cual establece a través de la Ley Num 20.009 - Régimen de limitación de responsabilidad para titulares o usuarios de tarjetas de pago y transacciones electrónicas - en su artículo 06, las medidas de seguridad mínimas a considerar las cuales son:

i) Tener sistemas de monitoreo que tengan por finalidad detectar aquellas operaciones que no conformen parte del comportamiento habitual del usuario;
ii) Implementar procedimientos internos para gestionar las alertas generadas por dichos sistemas;
iii) Identificar patrones potenciales de fraude;
iv) Establecer controles y límites en los diversos canales de atención que permitan aminorar las pérdidas por fraude.

Mencionado específicamente en el mismo artículo que la falta o deficiencia de tales medidas debe considerarse de forma obligatoria para la determinación de responsabilidad

ante casos de operaciones no reconocidas que el usuario o un tercero afectado pudiera perseguir en contra de estas entidades.

Incluso en Argentina el cual, a través de su legislación, específicamente en el artículo 2 de la Comunicación "A" N°7175, ha considerado dentro de las responsabilidades que se le atribuyen a este tipo de entidades el deber de arbitrar los mecanismos de seguridad apropiados para así asegurar la transmisión y recepción de transacciones, además de ofrecer herramientas de mitigación de fraude a sus clientes y utilizar dichas herramientas para identificar patrones sospechosos y alertar a los usuarios.

Asimismo, el Banco Central de esta República ha establecido "Lineamientos sobre ciberseguridad", en el cual obliga a todo el sector financiero a establecer estrategias y adoptar un marco de ciberseguridad acorde a su tamaño, complejidad, perfil de riesgo, entre otros; quedando claro que para este país cada entidad bancaria tiene el deber de implementar medidas adecuadas para que sus servicios ya no solo reparen el daño causado por algún tipo de fraude; sino, además, que estos puedan prevenirlos y, de suceder, estos puedan minimizarse.

Añadido a esto, resulta conveniente tener en cuenta que en el Perú la economista Roxana Barrantes, Vocal de la Sala especializada en protección al consumidor del Tribunal de Indecopi, mediante sus votos singulares o discordantes en procedimientos administrativos donde se discute el uso fraudulento de tarjetas de crédito y la responsabilidad de las entidades del sistema financiero; acoge los criterios expuestos en los párrafos anteriores, fijando el parámetro de idoneidad a partir del comportamiento habitual de consumo del cliente como un criterio jurídico a considerar para determinar la existencia de responsabilidad por operaciones fraudulentas.

De esta forma, establece en las entidades financieras, el deber de observar la combinación de diversos factores tales como: frecuencia, monto, canal, entre otros, los cuales se puedan contrastar con las características propias del historial de consumo de cada cliente según el producto evaluado, frecuentemente mostrado en sus estados de cuenta, consulta de saldos, movimientos, los cuales permitirán detectar posibles operaciones de fraude con la finalidad de advertir al cliente sobre su realización, preservando su patrimonio.

Menciona que, además de revisar la cantidad de transacciones realizadas y que el cliente alega son operaciones no reconocidas, se debe tener en cuenta el monto de las mismas incluyendo indicadores que versen entorno al cotejo de la frecuencia, el canal en que se produjo dicha operación, incluso el tipo de moneda o tipo de transacción y, es recién en ese momento, tras haber realizado la respectiva evaluación, donde se puede determinar si era habitual o, en su defecto, ameritaba que la entidad advirtiera al titular de su realización.

Así, queda claro que constituye una obligación del proveedor de servicios financieros, ante un caso de operaciones fraudulentas, demostrar que las operaciones discutidas contaban con todas las medidas de seguridad exigidas por ley; es decir, que las transacciones cuestionadas se encontraban dentro del parámetro habitual de consumo que el tarjetahabiente realizaba, pues, de no ser así, dicho proveedor debió advertirlo y adoptar las acciones necesarias para evitar que tales transacciones se carguen a las cuentas del consumidor, según sea el caso.

Cabe señalar, que solo en los casos donde las operaciones no reconocidas correspondan al comportamiento habitual de consumo del cliente o, bien estas hayan sido alertadas o advertidas al consumidor de manera oportuna, será únicamente en esta situación que la concurrencia de los requisitos de validez constituirá una medida de seguridad adecuada para determinar la responsabilidad del consumidor.

Con el fin de ejemplificar, todo lo mencionado es pertinente realizar una comparación entre la forma en que se han venido resolviendo los casos con la forma en que se podrían resolver si se aplicara, detallado de la siguiente manera:

TABLA 1: Análisis de Resolución Final N°1 (Anexo 1)

<table>
<tr><th></th><th>Elementos</th><th>Como se resolvió</th><th>Como se podría resolver</th></tr>
<tr><td>Resolución Final N°1961-2022/CC1</td><td>Hechos Jurídicos</td><td colspan="2">

A las 10:30 horas del día 23 de setiembre del 2021 la Sra. Ramos recibió un correo electrónico de “SERPOST” solicitándole el pago de S/5.90 para cambiar la dirección de entrega de un paquete, por lo que ingresó al enlace que le enviaron apareciendo un cuadro para completar sus datos e ingresar el código de validación que recibió por mensaje de texto; siendo víctima de phishing.
A las 11:30 horas del mismo día, recibió una llamada del Banco informándole que había bloqueado su tarjeta temporalmente toda vez que se detectaron 04 (CUATRO) operaciones sospechosas, las cuales fueron:

<table>
<tr><th>Fecha</th><th>Hora</th><th>Monto</th></tr>
<tr><td>23/09/2021</td><td>10:38</td><td>US$ 1,791.18</td></tr>
<tr><td>23/09/2021</td><td>10:39</td><td>US$ 3,450.35</td></tr>
<tr><td>23/09/2021</td><td>10:41</td><td>US$ 1,512.63</td></tr>
<tr><td>23/09/2021</td><td>10:42</td><td>US$ 538.99</td></tr>
</table>

Ante ello, se comunicó con el Banco, vía telefónica y correo electrónico señalando que no realizó dichos movimientos y procedió a bloquear su tarjeta.
El Banco sólo canceló las 02 (DOS) últimas operaciones y considero como válidas las dos primeras respectivamente.
La denunciante agotó todas las vías administrativas para resolver su conflicto, sin embargo, esto no sucedió, por lo que el 14 de diciembre del 2021 denunció al Banco ante la entidad competente (Indecopi).

</td></tr>
</table>

<table>
<tr><td></td><td>Imputación de Cargos</td><td colspan="2">Presunta infracción a los artículos 18° y 19° de la Ley N°29571, Código de Protección y Defensa del Consumidor, en tanto que el proveedor denunciado no habría adoptado las medidas de seguridad pertinentes, al permitir que se procesen 02 (DOS) operaciones no reconocidas con cargo a la Tarjeta de Crédito N°4280********015 de titularidad de la denunciante, a pesar de que informó no las hubo efectuado. Las operaciones fueron las siguientes:
<table>
<tr><th>Fecha</th><th>Hora</th><th>Monto</th></tr>
<tr><td>23/09/2021</td><td>10:38</td><td>US$ 1 791,18</td></tr>
<tr><td>23/09/2021</td><td>10:39</td><td>US$ 3 450,35</td></tr>
</table></td></tr>
<tr><td></td><td>Fundamentos relevantes para determinar responsabilidad</td><td>Autorización de las operaciones

La Sala verificó, para sustentar la validez de las operaciones, los print de pantalla en los cuales se señala el ingreso manual de los datos confidenciales de la tarjeta como son el nombre, la fecha de caducidad y el código CVV2, de acuerdo con el rubro de “POS ETY 01.

Además del reporte “Chronological Journal” se puede verificar la fecha, hora y monto de cada operación, así como el número de tarjeta con la cual se realizó y el código de autorización para cada una de las operaciones, por lo que consideró fueron realizadas de forma válida.</td><td>Comportamiento habitual del tarjetahabiente

Si la Sala hubiera analizado el parámetro de idoneidad a partir del comportamiento habitual del cliente, hubiera observado el tipo de operaciones que realizaba dicho consumidor, la frecuencia entre operaciones, el monto o la moneda en que se realizó, y de no encontrarse acorde con el parámetro de consumo habitual, el Banco tenía la obligación de alertar de forma inmediata su realización.

Se debe precisar que la llamada realizada por el banco acredita que sí tiene la capacidad de identificar las operaciones de naturaleza distinta a las transacciones que habitualmente este realizaba.</td></tr>
<tr><td></td><td>Decisión</td><td>Declarar INFUNDADA la denuncia interpuesta por la Sra. Ramos contra el Banco de Crédito del Perú S.A. por presunta infracción a los artículos 18° y 19° de la Ley N°29571, Código de Protección al Consumidor.</td><td>Declarar FUNDADA la denuncia interpuesta por la Sra. Ramos contra el Banco de Crédito del Perú S.A. por la infracción a los artículos 18° y 19° de la Ley N°29571, Código de Protección al Consumidor en tanto que ha quedado acreditado que las medidas de seguridad no fueron debidamente adoptadas por el Banco.</td></tr>
</table>

En efecto, si se hubiera tomado en cuenta las otras medidas de seguridad, el Indecopi hubiera concluido que los *prints* presentados respecto a la autenticación del tarjetahabiente, no son suficientes para cumplir con el objetivo de la normativa señalada. De esta manera, si se lograra incluir estas medidas de seguridad de forma obligatoria, como parte del análisis del deber de idoneidad en los servicios financieros ante este tipo de casos se quebrantaría el nexo causal de atribución de responsabilidad administrativa al consumidor, en tanto que se podría demostrar que efectivamente el proveedor no brindó un servicio idóneo.

Esto pudiéndose hacer efectivo a través de lo dispuesto por el artículo 21 del Reglamento de Organización y Funciones del Indecopi, que menciona entre las funciones del tribunal, expedir precedentes de observancia obligatoria que interpreten de modo expreso el sentido y alcance de normas de competencia institucional; y, además, considerando el resguardo del principio de verdad material como una obligación de la autoridad administrativa de adoptar todas las medidas establecidas en ley para sustentar sus decisiones finales. Obteniendo como consecuencia que el ejercicio de la potestad discrecional tenga un límite.

Así, en atención a la presente investigación, se propone establecer un precedente de observancia obligatoria que uniformice los criterios objetivos, los cuales servirán de fundamento para la resolución de este tipo de controversias con el fin de brindar equidad y seguridad jurídica a los consumidores.

El texto del precedente que se propone sería el siguiente:

> *"Para evaluar la responsabilidad del proveedor en los procedimientos administrativos en materia de protección al consumidor derivados de denuncias sobre operaciones no reconocidas de tarjeta de crédito o débito por el consumidor, ya sean estas realizadas de manera física o por medios electrónicos; se seguirán los siguientes criterios:*
>
> - *La Comisión evaluará la adopción de medidas de seguridad necesarias tales como: implementar sistemas de monitoreo, procedimientos complementarios para gestión de alertas respecto a operaciones fraudulentas, analizar si estas se encontraban dentro de la conducta habitual de consumo de sus clientes, o las establecidas en nuestra*

normativa vigente, con el fin de integrarlas como parte del servicio idóneo brindado por este tipo de entidades.

Parar efectos de determinar el comportamiento habitual de un cliente, la Comisión deberá verificar el cumplimiento de diversos factores como: monto, frecuencia, canal, moneda, lugar, destino y otros que le fueran aplicables.

- *En tal sentido, la entidad financiera tiene la carga de probar ante la Comisión: i) Analizar la implementación de las medidas de seguridad descritas; ii) Evaluar si las transacciones cuestionadas atendían a lo usual o cotidiano dispuesto por el consumidor en operaciones anteriores e individualizadas; y, iii) De no encontrarse dentro del parámetro habitual de consumo, haber advertido tales operaciones de manera oportuna y eficiente al consumidor.*
- *De no acreditarse, el proveedor será responsable.*

De esta manera, no es necesario considerar la creación de una nueva norma o legislación para su cumplimiento pues el propio Reglamento del Indecopi nos brinda las herramientas necesarias para que el Tribunal efectúe un análisis uniforme en virtud de los fundamentos vertidos y con ello establecer este criterio de manera obligatoria para todos los casos de operaciones no reconocidas por los consumidores de servicios financieros. Revistiendo de un contenido más completo a la aplicación de estas medidas de seguridad en la idoneidad del servicio financiero.

A modo conclusión, no se pretende implementar más obligaciones financieras o, como se mencionó, establecer una regulación de manera legislativa sobre la determinación de responsabilidad para este tipo de casos en tanto que, sabemos, tratar de regular cada situación en específico de operaciones no reconocidas, encajaría este hecho delictivo a una sola resolución cuando se trata de un tema totalmente dinámico y cambiante. Por el contrario, lo que se pretende es que el análisis efectuado por el Indecopi sea a partir de la exigencia del actuar diligente por parte de las entidades financieras basado en el cumplimiento de todas las obligaciones asignadas para cada una de ellas.

Conclusiones

Los criterios jurídicos utilizados en las resoluciones del Tribunal del Indecopi en casos de phishing son: la autorización del titular para la realización de la operación cuestionada, a través de verificación del correcto ingreso de datos confidenciales como clave token, CVC, números de la tarjeta, entre otros; y, la obligación del consumidor de resguardar la información sensible de su tarjeta. Asimismo, de forma particular, en ciertos casos se analiza el comportamiento habitual del tarjetahabiente, pero solo cuando es a solicitud de parte.

La relación entre el fraude cibernético bajo la modalidad de phishing y la vulneración de las medidas de seguridad establecidas por los bancos para el uso de su banca por internet y aplicativos móviles se entiende a partir de que este es una forma de realización de operaciones no reconocidas por el consumidor y atendiendo al mandato de seguridad que el Reglamento de Tarjetas de Crédito y Débito ha impuesto en su artículo 17 para adoptar las medidas de seguridad en calidad de monitoreo de operaciones con el fin de detectar aquellas que no correspondan al comportamiento habitual del usuario. De esta manera, la entidad bancaria tuvo la obligación de haber informado, alertado o haber realizado alguna acción suficiente para haber evitado la realización de dicha operación no reconocida.

La responsabilidad administrativa de los bancos en casos de phishing se ve reflejada a nivel internacional pues tanto Chile como Argentina han establecido como un parámetro de idoneidad, en la condición de los servicios de este tipo de productos, el de implementar medidas de seguridad; estableciendo que, ante su incumplimiento, será total responsabilidad del proveedor la realización de alguna operación sospechosa o no reconocida que pudiera haber afectado el patrimonio del usuario. Aunado a ello, en nuestro país, Roxana Barrantes - Vocal de la Sala Especializada de Indecopi - a través de sus votos singulares y discordantes ha considerado establecer dichas medidas de seguridad como parte del servicio idóneo que el banco pretende brindar para determinar la existencia de responsabilidad.

La propuesta de criterios jurídicos que debe seguir el Indecopi para determinar la existencia de responsabilidad administrativa de los bancos en los casos de fraudes cibernéticos por la modalidad de phishing es considerar como un parámetro de idoneidad en el servicio financiero a las medidas de seguridad establecidas en la normativa nacional para evitar el menoscabo del patrimonio del consumidor. En consecuencia, este tipo de entidades tienen la obligación, de asumir responsabilidad administrativa conforme al precedente vinculante de observancia obligatoria planteado en la presente investigación.

Recomendaciones

En la presente investigación se recomienda implementar este precedente de observancia obligatoria en tanto que brinda un análisis más completo de las obligaciones financieras en cuanto a las medidas de seguridad que estas deben implementar en los servicios que ofrecen y su adecuada interpretación; además, de brindar uniformidad y seguridad jurídica a los consumidores en casos de operaciones no reconocidas ya sea en casos de tarjeta presente y no presente a nivel jurisprudencial.

Asimismo, se recomienda al Tribunal, emitir pronunciamientos teniendo en consideración todas las obligaciones que a este tipo de entidades se le han otorgado en aras de resguardar el principio de verdad material que se encuentra obligado, para así resguardar los bienes jurídicos protegidos del consumidor.

Se incentiva a los estudiantes a seguir investigando sobre este tema y las obligaciones de este tipo de entidades, las cuales podrían encontrarse inmersas o consideradas dentro del parámetro de idoneidad del servicio que estas brindan.

Referencias

Abad, G. (2021). *Análisis de la responsabilidad bancaria en casos de estafas electrónicas mediante redes sociales desde la óptica del derecho de consumo*. https://www.abogadovergara.com.ar/2021/05/analisis-de-la-responsabilidad-bancaria.html

Abad, G. (2021). *Responsabilidad bancarias ante estafas electrónicas. Medida cautelar a favor del consumidor*. *http://bit.ly/3W6Aytl*

Ananías, F. (2020). Análisis comparativo del phishing y responsabilidad civil de los bancos, previa y posterior a la entrada en vigencia de la Ley 21.234. Tesis de Magister en Derecho de la Empresa. Universidad del Desarrollo. https://repositorio.udd.cl/bitstream/handle/11447/4112/An%C3%A1lisis%20comparativo%20del%20phishing%20y%20responsabilidad%20civil%20de%20los%20bancos.pdf?sequence=1&isAllowed=y

Balcazar, W. (2017). Medidas de Seguridad que deberían incorporarse a fin de evitar operaciones no reconocidas en tarjetas de crédito y débito. Tesis de pregrado. Universidad Privada Antenor Orrego. Trujillo – Perú. pp. 63.

Balmaceda, G. (2009). *El delito de estafa informática. Editorial Leyer, Primera edición*, Colombia, Bogotá. pp. 21.

Bellido, Y. (2018). La idoneidad en las tarjetas de crédito: a propósito de las denuncias ante los órganos competentes de Indecopi durante los años 2013-2015. Tesis de maestría. Universidad Nacional Mayor de San Marcos. https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/9681/Bellido_ay.pdf?sequence=3

Campos, J. (2018). Instituto Pacífico: La responsabilidad civil de los bancos por el riesgo de phishing. N°52, 277-302. http://www.cccabogados.pe/wp-content/uploads/2020/01/La-responsabilidad-civil-de-los-bancos-por-el-riesgo-phishing.pdf

Casajuana. J. (2020). *Estafas digitales: Responsabilidad del Banco por Phishing. https://jlcasajuanaabogados.com/estafas-digitales-responsabilidad-del-banco-por-phishing/*

Cerrón, L. & Otros. (2019). *Lineamientos sobre Protección al Consumidor"* (1° ed). [EPub]. Lima, Perú: publicado por INDECOPI.

Chávez. J & Bustamante. V. (2021). *Las medidas de seguridad como componente del deber de idoneidad en la prestación de servicios financieros.* https://lpderecho.pe/medidas-seguridad-deber-idoneidad-prestacion-servicios-financieros/#_ft_n4

Circular N° G-140-2009, Gestión de la Seguridad de la información. (02 de abril de 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

Comunicación "A" N°7175-2020, Sistema Nacional de Pagos – Transferencias. (07 de diciembre del 2020). Argentina. https://www.bcra.gob.ar/Pdfs/comytexord/A7175.pdf

Comunicación "A" N°7249-2021, Protección de los Usuarios de Servicios Financieros. (31 de marzo del 2021). Argentina. https://www.bcra.gob.ar/Pdfs/Texord/t-pusf.pdf

De la Cruz, D. (2021). Operaciones financiadas por internet y su relación con la responsabilidad civil de los bancos en la provincia de Huaura-Huacho 2018. Tesis de Pregrado. http://repositorio.unjfsc.edu.pe/bitstream/handle/UNJFSC/4960/DIEGO%20ALBERTO%20DE%20LA%20CRUZ%20S%C3%81NCHEZ.pdf?sequence=1&isAllowed=y

Hernandez, A. (2008). Protección al Consumidor Financiero en el Ordenamiento Jurídico Colombiano. Tesis de pregrado. Pontificia Universidad Javeriana. https://repository.javeriana.edu.co/bitstream/handle/10554/16920/HernandezGomezAngelaMaria2008.pdf;sequence=1

Jiménez, R. (2019). *El principio de verdad material en el procedimiento administrativo. https://bit.ly/3Fp61RP*

Ley N°26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros. (06 de diciembre de 1996). https://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/8CEF5E01E937E76105257A0700610870/$FILE/26702.pdf

Ley Num. 20.009, Régimen de Limitación de Responsabilidad para Titulares o Usuarios de Tarjetas de Pago y Transacciones Electrónicas en caso de extravío, hurto, robo o fraude. (29 de mayo del 2020). Chile. https://www.cmfchile.cl/portal/principal/613/articles-29132_doc_pdf.pdf

Linares, L. (2020). El deber de idoneidad de las entidades bancarias de la región de la libertad en el fraude electrónico con tarjetas de crédito y débito. Tesis de Pregrado. Universidad Privada del Norte. https://repositorio.upn.edu.pe/bitstream/handle/11537/25849/TRABAJO_TOTAL.pdf?sequence=1&isAllowed=y

Marin, M. (2016). El phishing. *Universitat Jaume I.* http://repositori.uji.es/xmlui/bitstream/10234

Monar, V. (2019). La responsabilidad civil ante la seguridad de las transacciones electrónicas bancarias. Tesis de Magister. Colegio Universitario de Estudios Financieros. https://biblioteca.cunef.edu/files/documentos/TFM_Veronica_Monar_Gaibor.pdf

Muchaypiña, M. (2020). El deber de idoneidad, derecho inherente del consumidor Expediente N°1268-2015/CCI (Idoneidad). Tesis de pregrado. Universidad San Ignacio de Loyola. https://repositorio.usil.edu.pe/server/api/core/bitstreams/49866416-e8d0-48cc-ad0e-cd4aec7973c1/content#:~:text=La%20infracci%C3%B3n%20al%20deber%20de,sido%20puesto%20en%20el%20mercado.

Munita, R. & Aeda, C. (2021). Responsabilidad Civil de los Bancos por Fraudes informáticos a la luz de la Ley de Protección de los consumidores. Actualidad Jurídica N°42- Julio 2020. *Universidad del Desarrollo. https://derecho.udd.cl/actualidad-juridica/files/2021/01/AJ42-P73.pdf*

Namuche. E. (2021). *Pautas jurídicas frente a las operaciones bancarias no reconocidas y fraudulentas.* https://lpderecho.pe/consejos-operaciones-bancarias-no-reconocidas-fraudulentas/

Oxman, N. (2013). Estafas informáticas a través de Internet: A través de la imputación penal del "phishing" y el "pharming". Revista de derecho de la Pontificia Universidad Católica de Valparaíso. N°XLI, 211-262. https://scielo.conicyt.cl/pdf/rdpucv/n41/a07.pdf

Padilla, J. (2017). Responsabilidad de los establecimientos bancarios por el pago de cheques falsos o alterados en Colombia. https://revistas.uexternado.edu.co/index.php/derpri/article/view/5031/6857#info

Resolución de la S.B.S. N°3274-2017, Reglamento de Gestión de Conducta de Mercado del Sistema Financiero y modifican el Manual de Contabilidad paralas empresas del sistema financiero. https://elperuano.pe/NormasElperuano/2017/08/21/1556283-1/1556283-1.htm

Resolución Final N°0064-2022/SPC - INDECOPI (Lima). (12 de enero de 2021). Tribunal de Defensa de la Competencia y de la Propiedad Intelectual: Sala Especializada en Protección al Consumidor.

Resolución Final N°0098-2021/CC1 (Lima). (19 de enero del 2022). Comisión de Protección al Consumidor N°01: Sede Central.

Resolución Final N°0101-2021/SPC - INDECOPI (Lima). (14 de enero de 2021). Tribunal de Defensa de la Competencia y de la Propiedad Intelectual: Sala Especializada en Protección al Consumidor.

Resolución Final N°0286-2022/PS2 (Lima). (3 de marzo de 2022). Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor N°2: Sede Lima Sur.

Resolución Final N°0308-2022/PS2 (Lima). (8 de marzo de 2022). Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor N°2: Sede Lima Sur.

Resolución Final N°0496-2022/CC1 (Lima). (23 de febrero de 2022). Comisión de Protección al Consumidor N°1: Sede Central.

Resolución Final N°0658-2022/CC1 (Lima). (09 de marzo de 2022). Comisión de Protección al Consumidor N°1: Sede Central.

Resolución Final N°1156-2021/CC1 (Lima). (21 de mayo de 2022). Comisión de Protección al Consumidor N°1: Sede Central.

Resolución Final N°1349-2022/PS2 (Lima). (15 de septiembre de 2022). Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor N°2: Sede Lima Sur.

Resolución Final N°1756-2022/CC1 (Lima). (22 de junio de 2022). Comisión de Protección al Consumidor N°1: Sede Central.

Resolución Final N°191-2022/CC1 (Lima). (26 de enero de 2022). Comisión de Protección al Consumidor N°1: Sede Central.

Resolución Final N°1961-2022/CC1 (Lima). (13 de julio de 2022). Comisión de Protección al Consumidor N°1: Sede Central.

Resolución Final N°889-2022/CC1 (Lima). (30 de marzo del 2022). Comisión de Protección al Consumidor N°1: Sede Central.

Resolución SBS N° 6523-2013, modificado por la Resolución SBS 5570-2019, Reglamento de Tarjetas de Crédito y Débito. https://busquedas.elperuano.pe/normaslegales/modifican-reglamento-de-tarjetas-de-credito-y-debito-el-reg-resolucion-no-5570-2019-1831401-1/

Resolución SBS N°504-2021, modificado por la Resolución SBS 5570-2019, Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad. (19 de febrero de 2021) https://busquedas.elperuano.pe/normaslegales/aprueban-el-reglamento-para-la-gestion-de-la-seguridad-de-la-resolucion-no-504-2021-1929393-1/

Rojas, C. (2014). Responsabilidad Administrativa del Proveedor. Administración pública y control N°11, 38 – 45. https://www.lazoabogados.com.pe/wp-content/uploads/2014/12/Responsabilidad-Administrativa-del-proveedor-CRK.pdf.pdf

Ruth. C. (2022). *Fallo sin precedentes sobre phishing: brindar las claves bancarias voluntariamente no exime al banco de su responsabilidad.* https://www.infobae.com/sociedad/2022/10/14/fallo-sin-precedentes-sobre-phishing-brindar-las-claves-bancarias-voluntariamente-no-exime-al-banco-de-su-responsabilidad/

Salas, R. (2010) Algunos apuntes y reflexiones sobre la tutela de los derechos de los consumidores y la asimetría Informativa en el mercado. Foro Jurídico, (11), 182-193. https://revistas.pucp.edu.pe/index.php/forojuridico/article/view/18587

Silvestre, J. (2021). Informe Jurídico sobre Resolución N°2272-2018/SPC-INDECOPI. Tesis de Pregrado. Pontificia Universidad Católica del Perú. https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/18454/SILVESTRE_BERM%c3%9aDEZ_JULIA_KATTY%20%281%29.pdf?sequence=1&isAllowed=y

Zapana, Y. (2022). Análisis del deber de idoneidad de los proveedores que prestan servicios financieros en la ciudad de Puno, periodo 2019-2020. Tesis de pregrado. Universidad Nacional del Altiplano. http://repositorio.unap.edu.pe/bitstream/handle/UNAP/17567/Zapana_Castro_Yubel_Arassely.pdf?sequence=1&isAllowed=y

Anexos

Tabla 1: Análisis de Resolución Final N°1 (Anexo 1)

<table>
<tr><td rowspan="2">Resolución Final N°1961-2022/CC1</td><td>Elementos</td><td>Como se resolvió</td><td>Como se podría resolver</td></tr>
<tr><td>Hechos Jurídicos</td><td colspan="2">
- A las 10:30 horas del día 23 de setiembre del 2021 la Sra. Ramos recibió un correo electrónico de “SERPOST” solicitándole el pago de S/5.90 para cambiar la dirección de entrega de un paquete, por lo que ingresó al enlace que le enviaron apareciendo un cuadro para completar sus datos e ingresar el código de validación que recibió por mensaje de texto; siendo víctima de *phishing.*
- A las 11:30 horas del mismo día, recibió una llamada del Banco informándole que había bloqueado su tarjeta temporalmente toda vez que se detectaron 04 (CUATRO) operaciones sospechosas, las cuales fueron:
<table>
<tr><td>Fecha</td><td>Hora</td><td>Monto</td></tr>
<tr><td>23/09/2021</td><td>10:38</td><td>US$ 1,791.18</td></tr>
<tr><td>23/09/2021</td><td>10:39</td><td>US$ 3,450.35</td></tr>
<tr><td>23/09/2021</td><td>10:41</td><td>US$ 1,512.63</td></tr>
<tr><td>23/09/2021</td><td>10:42</td><td>US$ 538.99</td></tr>
</table>
- Ante ello, se comunicó con el Banco, vía telefónica y correo electrónico señalando que no realizó dichos movimientos y procedió a bloquear su tarjeta.
- El Banco sólo canceló las 02 (DOS) últimas operaciones y considero como válidas las dos primeras respectivamente.
- La denunciante agotó todas las vías administrativas para resolver su conflicto, sin embargo, esto no sucedió, por lo que el 14 de diciembre del 2021 denunció al Banco ante la entidad competente (Indecopi).
</td></tr>
</table>

<table>
<tr><td></td><td>Imputación de Cargos</td><td colspan="2">Presunta infracción a los artículos 18° y 19° de la Ley N°29571, Código de Protección y Defensa del Consumidor, en tanto que el proveedor denunciado no habría adoptado las medidas de seguridad pertinentes, al permitir que se procesen 02 (DOS) operaciones no reconocidas con cargo a la Tarjeta de Crédito N°4280********015 de titularidad de la denunciante, a pesar de que informó no las hubo efectuado. Las operaciones fueron las siguientes:
<table>
<tr><th>Fecha</th><th>Hora</th><th>Monto</th></tr>
<tr><td>23/09/2021</td><td>10:38</td><td>US$ 1 791,18</td></tr>
<tr><td>23/09/2021</td><td>10:39</td><td>US$ 3 450,35</td></tr>
</table></td></tr>
<tr><td></td><td>Fundamentos relevantes para determinar responsabilidad</td><td>Autorización de las operaciones

La Sala verificó, para sustentar la validez de las operaciones, los print de pantalla en los cuales se señala el ingreso manual de los datos confidenciales de la tarjeta como son el nombre, la fecha de caducidad y el código CVV2, de acuerdo con el rubro de “POS ETY 01.

Además del reporte “Chronological Journal” se puede verificar la fecha, hora y monto de cada operación, así como el número de tarjeta con la cual se realizó y el código de autorización para cada una de las operaciones, por lo que consideró fueron realizadas de forma válida.</td><td>Comportamiento habitual del tarjetahabiente

Si la Sala hubiera analizado el parámetro de idoneidad a partir del comportamiento habitual del cliente, hubiera observado el tipo de operaciones que realizaba dicho consumidor, la frecuencia entre operaciones, el monto o la moneda en que se realizó, y de no encontrarse acorde con el parámetro de consumo habitual, el Banco tenía la obligación de alertar de forma inmediata su realización.

Se debe precisar que la llamada realizada por el banco acredita que sí tiene la capacidad de identificar las operaciones de naturaleza distinta a las transacciones que habitualmente este realizaba.</td></tr>
<tr><td></td><td>Decisión</td><td>Declarar INFUNDADA la denuncia interpuesta por la Sra. Ramos contra el Banco de Crédito del Perú S.A. por presunta infracción a los artículos 18° y 19° de la Ley N°29571, Código de Protección al Consumidor.</td><td>Declarar FUNDADA la denuncia interpuesta por la Sra. Ramos contra el Banco de Crédito del Perú S.A. por la infracción a los artículos 18° y 19° de la Ley N°29571, Código de Protección al Consumidor en tanto que ha quedado acreditado que las medidas de seguridad no fueron debidamente adoptadas por el Banco.</td></tr>
</table>