Universidad Femenina del Sagrado Corazón

Facultad de Derecho

Escuela Profesional de Derecho

RESPONSABILIDAD DE LAS ENTIDADES FINANCIERAS EN LA PROTECCIÓN DEL CONSUMIDOR FINANCIERO EN CASOS DE PHISHING

Tesis presentada por:

DEMMY NICOLLE VARGAS LÓPEZ
Cód. ORCID: 0009-0005-8032-0884

Para obtener el Título Profesional de Abogada

Línea de Investigación: Derecho civil patrimonial, empresarial y responsabilidad social empresarial

Asesora
Mg. Karolina Kira Kriete Urruchi
Cód. ORCID: 0000-0003-3641-0258

Lima – Perú

2025

Los miembros del jurado han aprobado el estilo y el contenido de la tesis sustentada por:

DEMMY NICOLLE VARGAS LÓPEZ

KAROLINA KIRA KRIETE URRUCHI

Asesor: Nombre(s) y Apellidos

LILIANA MICAELA SEMINARIO MENDEZ

Presidente de Jurado: Nombre(s) y Apellidos

MILLITZA CLARA FRANCISKOVIC INGUNZA

Miembro de Jurado 1: Nombre(s) y Apellidos

KAROLINA KIRA KRIETE URRUCHI

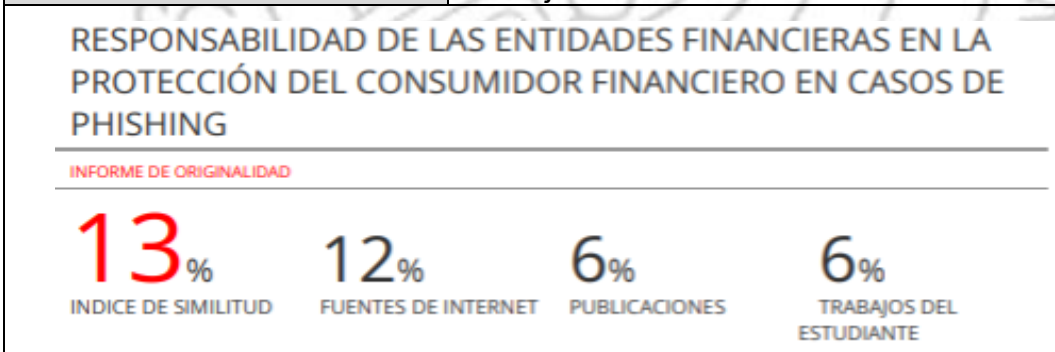
Miembro de Jurado 2: Nombre(s) y Apellidos

LILIANA MICAELA SEMINARIO MENDEZ

Nombre y apellidos del Decano(a)
Decano de la Facultad de Derecho

DECLARATORIA DE ORIGINALIDAD DEL ASESOR

Facultad:	Facultad de Derecho
Escuela profesional:	Escuela Profesional de Derecho
Dependencia al que pertenece el docente asesor:	Departamento de Ciencias Jurídicas
Docente asesor que verifica la originalidad:	Karolina Kira Kriete Urruchi
ORCID:	0000-0003-3641-0258
Título del documento:	RESPONSABILIDAD DE LAS ENTIDADES FINANCIERAS EN LA PROTECCIÓN DEL CONSUMIDOR FINANCIERO EN CASOS DE PHISHING
Autora del documento:	Demmy Nicolle Vargas López
Mecanismo utilizado para detección de originalidad:	Software Turnitin
N.º de trabajo en Turnitin: (10 dígitos)	2656181475
Porcentaje de similitud detectado:	13%
Fuentes originales de lassimilitudes detectadas:	Fuentes de internet = 12% Publicaciones = 6% Trabajos del estudiante = 6%



El docente asesor declara ha revisado el informe de similitud y expresa que el porcentaje señalado cumple con las “Normas Internas de Investigación e Innovación” establecidas por la Universidad Femenina del Sagrado Corazón.

Fecha de aplicación en Turnitin:	24-04-2025

RESUMEN

El phishing es una amenaza en continua evolución, que afecta a los consumidores financieros, por lo que, las entidades financieras se ven obligadas a implementar estrategias de prevención más rigurosas. El objetivo de la investigación es analizar la relación entre la responsabilidad de las entidades financieras y la protección del consumidor financiero en casos de phishing. Se siguió como línea metodológica el enfoque cualitativo, bajo el tipo de investigación de carácter básica, ceñido al diseño no experimental, cuyo nivel fue descriptivo. La técnica implementada para recolectar datos fue el análisis documental, a través del uso y comparación de resoluciones administrativas emitidas por Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual sobre casos vinculados al phishing en el año 2024, lo que permitió hacer una comparación y análisis entre 28 resoluciones emitidas en el 2024 por el INDECOPI, de las cuales se evaluaron 11 resoluciones, las cuales permitieron abordar el objeto de la presente investigación. Los hallazgos demostraron, que las conductas materia de sanción se relacionan mayormente con el principio de idoneidad y la obligación de los proveedores, regulado en los artículos 18 y 19 del Código de Protección y Defensa del Consumidor (Ley N° 29571). Igualmente, se evidencia en las diferentes Resoluciones la falta de medidas de seguridad adecuadas, así como la ausencia de respuesta oportuna como negativa de las entidades para asumir su responsabilidad. Por lo que, se concluye que las entidades financieras no cumplen con su obligación de poner a disposición de sus usuarios productos idóneos, es decir que sean seguros, ya que sus sistemas de seguridad carecen de los estándares de seguridad establecidos por la normativa actual, e incluso dichos estándares no se encuentran actualizados de acuerdo con los avances de la tecnología moderna, lo que facilita la desprotección de los consumidores financieros en casos de phishing.

Palabras clave: phishing, idoneidad, entidades financieras, consumidores, responsabilidad administrativa

ABSTRACT

Phishing is a constantly evolving threat that affects financial consumers, forcing financial institutions to implement more rigorous prevention strategies. The objective of this research is to analyze the relationship between the liability of financial institutions and the protection of financial consumers in cases of phishing. A qualitative approach was followed as a methodological line, under a basic research type, limited to a non-experimental design, with a descriptive level. The technique implemented to collect data was documentary analysis, through the use and comparison of administrative resolutions issued by the National Institute for the Defense of Competition and the Protection of Intellectual Property

on cases related to phishing in 2024. This allowed for a comparison and analysis of 28 resolutions issued in 2024 by INDECOPI. Of these, 11 resolutions were evaluated, which allowed us to address the objective of this research. The findings demonstrated that the conduct subject to sanctions is largely related to the principle of suitability and the obligations of providers, regulated in Articles 18 and 19 of the Consumer Protection and Defense Code (Law 29571). Likewise, the various Resolutions demonstrate a lack of adequate security measures, as well as a lack of timely responses and the entities' refusal to assume their responsibility. Therefore, it is concluded that financial institutions are failing to fulfill their obligation to provide their users with suitable, i.e., safe, products, since their security systems lack the security standards established by current regulations, and these standards are not even updated in accordance with advances in modern technology, which facilitates the vulnerability of financial consumers in cases of phishing.

Keywords: phishing, suitability, financial institutions, consumers, administrative responsibility

RECONOCIMIENTOS

La presente investigación no se habría concretado sin la oportunidad que me dio la facultad de derecho, para poder ejercer como secigrista en el Ministerio Público, de dicha experiencia logre recabar información e involucrarme en la problemática que desarrolla esta tesis. De igual forma, a la plana docente de la facultad, que siempre priorizaron la enseñanza de las materias en base los valores que debe tener todo buen abogado, así como también, me inculcaron el amor por el derecho en sus diversas ramas

DEDICATORIA

A mis padres, que siempre me impulsan a seguir adelante y no rendirme frente a las adversidades;

A mi abuela que me inculcó el hábito de la lectura y el estudio, pese a que no podrá dar lectura a mi tesis, estoy segura de que estaría orgullosa;

A mi abuelo que nunca dejó de preocuparse en mi alimentación y descanso; gracias por sus consejos y cuidados diarios; y

A mi hermana que siempre me levanto la moral, en esas amanecidas propias de la carrera.

ÍNDICE

LISTA DE TABLAS

Página

LISTA DE FIGURAS

INTRODUCCIÓN

Las entidades financieras actualmente enfrentan desafíos relacionados a los fraudes de tipo cibernéticos, pues cada vez estos suceden con más frecuencias y con diferentes mecanismos que superan las barreras de seguridad, tanto de las que ofrecen las entidades financieras como de parte de las que aplican los consumidores financieros. Por lo que, desde una perspectiva legal, la responsabilidad adquiere un tratamiento distinto que va a depender del contexto o del hecho ocurrido. De tal forma, que la posible responsabilidad de estas entidades financieras cuando ocurre un ciberdelito se deriva de las obligaciones que impone la ley a todas estas empresas, en lo concerniente a su deber de protección y resguardo de los datos informáticos de sus usuarios y siempre y cuando se logre corroborar que el consumidor no ha permitido la operación no reconocida.

En este contexto existen diferentes formas que utilizan los ciberdelincuentes para consumar el hecho delictivo, entre ellos se encuentra el phishing, uno de los delitos con más incidencias. Esto posiblemente ocurra debido al uso frecuente de los servicios en línea que ofrecen las entidades financieras. No obstante, cuando ocurren estos hechos, sin la participación indirecta o directa por parte de los usuarios, la responsabilidad de las entidades consiste en hacer la devolución de la cantidad extraída, sin autorización, de manera inmediata, debido a que la responsabilidad de la víctima en estos casos solo se toma en cuenta en caso de que se compruebe como negligencia grave.

Cabe mencionar, que las entidades financieras señalan que vienen haciendo esfuerzos para optimizar la seguridad digital de sus bancas digitales;

sin embargo, sus procesos de autenticación y prevención de fraudes, son percibidas como insuficientes, lo cual se ha reflejado en el volumen de reclamos de los usuarios, quienes han cuestionado a la vez el papel que deben asumir las instituciones financieras ante la protección sus datos informáticos y de sus ahorros. A efectos de analizar, como la autoridad administrativa viene resolviendo y con el fin de evidenciar las conductas de las entidades financieras que son sancionadas en la vía administrativa se realiza un análisis de resoluciones emitidas por el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI en el 2024, que versan sobre el phishing, lo que permite describir la realidad actual y demostrar si las entidades financieras realizan medidas suficientes para proteger a sus usuarios.

Por ello, el presente estudio indaga sobre la responsabilidad de las entidades financieras en la protección de los consumidores frente al phishing. Por consiguiente, se origina la siguiente interrogante que guía la investigación ¿Cómo se relaciona la responsabilidad de las entidades financieras con la protección del consumidor financiero en casos de phishing?

CAPÍTULO I: EL PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento del problema

El phishing es una amenaza en continua evolución que afecta tanto a las entidades bancarias y financieras como a sus clientes, demandando un enfoque preventivo y medidas proactivas para salvaguardar la seguridad y confidencialidad de la información financiera. Las técnicas de phishing, cada vez más complejas y creativas, dificultan su detección, lo que obliga a las entidades bancarias a implementar estrategias de prevención más rigurosas, a fin de mitigar el riesgo relacionado a la divulgación de datos sensibles de sus usuarios (Serrano, 2024).

En España, el phishing se ha convertido en una amenaza creciente para los consumidores financieros, exponiéndolos a fraudes que afectan sus patrimonios. La dificultad principal radica en determinar si las operaciones fueron realmente autorizadas por los titulares, lo que complica la asignación de responsabilidad. A pesar de los avances regulatorios, las entidades financieras no siempre implementan medidas suficientes de protección ni responden de manera adecuada ante los fraudes, dejando a los consumidores desprotegidos frente a la suplantación de identidad y la pérdida de dinero (Estancona, 2023).

En 2023, a nivel mundial el phishing financiero continuó siendo una amenaza relevante, representando el 27.32% de los ataques dirigidos a usuarios corporativos y el 30.68% a usuarios domésticos. Las tiendas en línea fueron el señuelo más utilizado, abarcando el 41.65% de los intentos de phishing financiero, además, las páginas de phishing que usaron el nombre de PayPal alcanzaron el 54.78% de los ataques dirigidos a sistemas de pago electrónico;

en suma, se señaló un aumento del 16% en los ataques relacionados con criptomonedas, con 5.84 millones de detecciones en 2023, frente a 5.04 millones en 2022 (Kaspersky, 2024)

En el 2023, Perú registró 31.5 millones de ataques de phishing, ocupando el tercer lugar en Latinoamérica después de Brasil con 134 millones y México con 43 millones, lo que se atribuye al aumento del uso de la banca en línea, especialmente durante la pandemia de COVID-19. Las restricciones sociales impulsaron el uso de servicios digitales para compras y pagos, y actualmente, con el aumento de los viajes y la popularización de aplicaciones de pago y herramientas de inteligencia artificial, los ataques han continuado en ascenso (Flores, 2023).

Por otra parte, en Argentina la proliferación de estafas electrónicas, especialmente durante la pandemia, ha dejado a los consumidores bancarios completamente desprotegidos, siendo el phishing la modalidad más utilizada. Las entidades bancarias han fallado en reforzar las medidas de seguridad y prevención, incumpliendo su obligación de proteger los datos personales y económicos de los clientes, a pesar de que esto está claramente establecido en la Constitución. La falta de acción, pone en riesgo la seguridad de los usuarios y agrava la situación ya que, la constante evolución de los ciberdelincuentes ha sido ignorada por las instituciones, lo que justifica la necesidad de aplicar sanciones y daños punitivos (Carril, 2022).

En Costa Rica, el phishing ha emergido como uno de los fraudes electrónicos más comunes, perjudicando a los consumidores mediante la ingeniería social; a pesar de los esfuerzos de las entidades financieras por mitigar los ataques cibernéticos, los estafadores perfeccionan constantemente

sus métodos. El Tribunal Contencioso Administrativo y la Corte Suprema han sostenido que los bancos deben asumir responsabilidad objetiva, dada su capacidad y recursos para prevenir estos riesgos, sin embargo, las entidades financieras a menudo no logran ofrecer la seguridad suficiente (Espinoza, 2023).

En Perú, las entidades financieras no han logrado implementar programas de cumplimiento normativos efectivos para combatir el phishing, lo que deja a los consumidores expuestos a fraudes. La escasa colaboración entre la Superintendencia de Banca, y Seguros (SBS) y la Superintendencia del Mercado de Valores (SMV), agrava la situación, impidiendo una acción conjunta frente a los ataques. Además, la integración insuficiente de tecnologías de seguridad, como la inteligencia artificial, impide prevenir de manera efectiva los fraudes (Diaz y Goitia, 2024).

Asimismo, en Lima Centro, durante 2022, más de 9,500 personas fueron víctimas de ciberataques, con el phishing como una de las modalidades más comunes, según la Fiscalía Especializada en Ciberdelincuencia. A nivel nacional, el Indecopi, a través de la Dirección de la Autoridad Nacional de Protección del Consumidor, recibió más de 200 reportes de phishing, con La Libertad y Arequipa como las regiones con mayor cantidad de denuncias. Además, el Indecopi investiga estos casos bajo la premisa de falta de idoneidad de las empresas financieras en operaciones no reconocidas, aunque el phishing ya es reconocido como un delito en sí mismo (Saenz, 2023).

El creciente uso de las tecnologías de la información y la comunicación (TIC) ha generado una creciente proliferación de delitos informáticos, lo que ha complicado al Derecho Penal para abordar nuevas formas de criminalidad. A pesar de los esfuerzos por parte de los gobiernos, las regulaciones no han

logrado mitigar eficazmente los riesgos asociados. En la banca peruana, los delitos como el fraude informático, *phishing, sim swapping* y ciberataques continúan en aumento, mostrando que las medidas de seguridad aún son insuficientes (Arméstar y Toche, 2024).

En al ámbito local, la creciente amenaza del phishing afecta a los consumidores financieros, exponiéndolos a fraudes y pérdidas económicas. Las entidades financieras, aunque tienen protocolos de seguridad, no siempre logran prevenir o alertar a tiempo a sus clientes sobre estos riesgos. Los síntomas de este problema incluyen transacciones no autorizadas, llamadas sospechosas y correos electrónicos falsos que buscan robar datos sensibles. La causa principal de esta vulnerabilidad reside en la limitada o inexistente formación en educación financiera y la insuficiente protección digital por parte de algunas instituciones. Asimismo, la escasa capacidad de respuesta ante incidentes también agrava el impacto en los usuarios.

Las consecuencias son graves, con muchos consumidores perdiendo grandes sumas de dinero, lo que afecta su confianza en las entidades bancarias y en el sistema financiero en general. Esta situación puede llevar a un incremento de la desconfianza y a una caída en el uso de servicios digitales financieros. Si no se implementan políticas más estrictas y mejores sistemas de alerta, el pronóstico es que el phishing continuará creciendo, afectando tanto la estabilidad económica de los consumidores como la integridad de las instituciones financieras.

A pesar de los esfuerzos realizados por algunas entidades financieras para fortalecer la seguridad digital, la percepción general es que las medidas preventivas y correctivas aún son insuficientes, lo que ha incrementado las

quejas de los usuarios y cuestionado el rol de estas instituciones en la protección del consumidor financiero. La presente investigación busca explorar la responsabilidad de las entidades financieras en la protección de los consumidores frente al phishing, examinando las políticas y acciones implementadas, así como las experiencias y percepciones de los afectados.

1.1.2 Problema general

¿Cómo se relaciona la responsabilidad administrativa de las entidades financieras con la protección del consumidor financiero en casos de phishing?

1.1.3 Problemas específicos

¿Cómo está resolviendo la autoridad administrativa (INDECOPI) los casos de phishing vinculados a la falta de responsabilidad de las entidades financieras?

¿Como se sanciona administrativamente a las entidades financieras al desproteger a los consumidores en casos de phishing?

1.2 Objetivos de la investigación

1.2.2 Objetivo general

Analizar la relación entre la responsabilidad de las entidades financieras con la protección del consumidor financiero en casos de phishing.

1.2.3 Objetivos específicos

Analizar el actuar de la autoridad administrativa (INDECOPI) frente a la resolución de casos de phishing vinculados a la falta de responsabilidad de las entidades financieras.

Determinar las sanciones administrativas que reciben las entidades financieras al desproteger a los consumidores en casos de phishing.

1.3 Hipótesis

Las entidades financieras son responsables de la protección de los datos de sus usuarios frente a los casos de phishing, puesto que es su deber implementar y reforzar sus medidas de seguridad para evitar que puedan ser víctimas de ataques cibernéticos. Sin embargo, esta no es asumida de manera efectiva, lo que provoca una protección insuficiente al consumidor financiero y genera inestabilidad y desconfianza en ese sector, por lo que es necesario que la normativa vigente se actualice y fortalezca a las entidades administrativas correspondientes.

1.4 Importancia de la investigación

La investigación es de gran importancia en el actual contexto de digitalización del sector financiero, donde delitos como el phishing amenazan a los consumidores. Este tipo de fraude, consiste en obtener información confidencial engañando a los usuarios, lo que viene generando pérdidas significativas y socavando la confianza en el sistema bancario. El estudio de dicha problemática es esencial, porque examina la responsabilidad administrativa de las entidades financieras en la protección de sus clientes frente a estos delitos.

Aunque existen normativas en Perú para salvaguardar los derechos de los consumidores, hay desafíos en su implementación; puesto que, muchos afectados por phishing, no reciben la compensación adecuada, lo que amerita análisis y sanciones por parte de las entidades públicas correspondientes. Comprender cómo las entidades financieras gestionan y protegen a sus usuarios es clave para cumplir con la normativa vigente y mejorar sus políticas de seguridad.

1.5 Justificación de la investigación

A nivel teórico, esta investigación se justifica en el marco normativo y teórico que regula la responsabilidad administrativa de las entidades financieras respecto a la protección de los consumidores financieros. Se basa en los principios de responsabilidad administrativa, que determinan las obligaciones y deberes de las instituciones financieras hacia sus clientes, especialmente en lo que respecta a la prevención y mitigación de fraudes cibernéticos, como el phishing. Conforme a estas bases teóricas, se realiza un análisis sobre el balance entre los derechos del consumidor y las responsabilidades que asumen los bancos al implementar servicios digitales, ante los delitos cibernéticos.

A nivel práctico, este estudio tiene significativa relevancia, dado que el phishing es uno de los fraudes cibernéticos más extendidos que afecta a los usuarios financieros. La investigación pretende ofrecer recomendaciones precisas para optimizar las políticas y medidas de seguridad de las entidades bancarias en Perú, además de fortalecer los mecanismos de compensación y reclamos para los consumidores víctimas de este tipo de delito.

A nivel metodológico, la investigación es novedosa debido a que aporta instrumentos de recolección de datos, al poder analizar y comparar resoluciones administrativas que poseen como factor común el phishing y que son de carácter público, lo que ha permitido identificar el criterio que utiliza la autoridad administrativa para resolver estos casos. Se aplica un enfoque correlacional explicativo, que permite identificar la influencia de la responsabilidad de las entidades financieras en la protección del consumidor financiero en casos de phishing, puesto que a falta de la primera se origina la desprotección de los consumidores y por tanto no se detecta ni detiene el phishing. Por lo que, la

relevancia del tema, permitirá que surjan nuevas interrogantes, debido a que la constante evolución de los ciberdelitos de carácter financiero continuará en auge si no se modifican y aumentan en rigurosidad la normativa legal peruana.

1.6 Delimitación de la investigación

- Espacial: Perú

- Documental: Resoluciones emitidas por Indecopi en el 2024 sobre phishing

- Temporal: Año 2024

1.7 Limitaciones de la investigación

Durante el proceso, se identificó algunas situaciones que produjeron limitaciones a la presente investigación, como es el caso de la falta de definición formal o legal del concepto y la modalidad del phishing, así como su correcta identificación por parte de la autoridad administrativa, ya que, al ser un nuevo delito, en las resoluciones materia de análisis se ha identificado que no se posee una sola definición del término phishing, sino que, por el contrario se confunde los actos que constituyen phishing con otros delitos informáticos.

Aunado a ello, la investigación, al envolver una modalidad de ciberdelito, requiere de un manejo y comprensión de terminología informática, es decir temas que no se vinculan a mi formación académica como autora, lo que ha constituido una limitación para la presente investigación. Por lo que, la falta de uniformidad sobre el concepto del phishing y la falta de conocimiento en temas informáticos, fueron la principal limitante, ya que dificulto la comparación y el análisis de la investigación.

1.8 Matriz de Consistencia

Tabla 1

Matriz de consistencia

Problema	Objetivo	Marco Teórico	Metodología
Problema General ¿Cómo se relaciona la responsabilidad de las entidades financieras con la protección del consumidor financiero en casos de phishing?	**Objetivo General** Analizar la relación entre la responsabilidad de las entidades financieras y la protección del consumidor financiero en casos de phishing.	Phishing - Delito informático - Convenio de Budapest - Protección de datos informáticos Responsabilidad de las entidades financieras	**Enfoque:** Cualitativa **Método:** Deductivo, exegético, analítico y dogmático. **Tipo:** Documental **Nivel:** Descriptivo

Problemas específicos ¿Cómo está resolviendo la autoridad administrativa (INDECOPI) los casos de phishing vinculados a la falta de responsabilidad de las entidades financieras? ¿Cómo se sanciona administrativamente a las entidades financieras al desproteger a los consumidores en casos de phishing?	**Objetivos específicos** Analizar el actuar de la autoridad administrativa (INDECOPI) frente a la resolución de casos de phishing vinculados a la falta de responsabilidad de las entidades financieras. Determinar las sanciones administrativas que reciben las entidades financieras al desproteger a los consumidores en casos de phishing.	- Responsabilidad administrativa Protección del consumidor financiero - Deber de idoneidad - Obligación de los proveedores	**Diseño:** No experimental-Teoría fundamentada. **Participantes:** Resoluciones emitidas por Indecopi en el 2024. **Técnica:** análisis documental. **Instrumento:** Cuadro comparativo de las resoluciones administrativas emitidas por el Indecopi en el 2024.

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes de la investigación

2.1.1 Antecedentes internacionales

Carril (2022) realizó un estudio orientado a indagar sobre la responsabilidad de las entidades bancarias ante el estallido de las estafas de tipo electrónicas que en su mayoría ocurrieron en clientes que son consumidores de servicios bancarios. Para tal fin, se realizó una revisión documental en donde se detallaron los deberes que debe brindar el banco en lo que respecta a seguridad y prevención a sus clientes como obligación en el marco del contrato de consumo; se detallan casos en los cuales la circunstancias y conducta de la entidad bancaria no estuvo a la altura de lo que se esperaba, lo cual dio origen a la judicialización. Se concluyó que, ante la configuración de la falta en lo referente a la prevención y seguridad que la entidad financiera debe cumplir en el marco del contrato de consumo, se señala que el daño punitivo se considera absolutamente procedente, debido a que la sanción punitiva en el derecho concerniente al consumidor en el contexto argentino establece que mediante la protección resguardada por la Ley Nro. 24.240 atribuida al Estado, las empresas proveedoras no deben reiterar conductas que vulneren los bienes jurídicos tutelados por la normativa en cuestión.

Espinoza (2023) refiere en su artículo que tanto el Tribunal Contencioso Administrativo y el sustento de la Corte Suprema de Justicia de Costa Rica coinciden en la misma línea de pensamiento con el transcurrir del tiempo, en la cual atribuyen responsabilidad objetiva a las entidades bancarias basadas en la teoría del riesgo asociadas, a su vez, al artículo 35 de la Ley N°.7472 y en toda la normativa en general. En tal sentido, la configuración de dicho criterio se

produce cuando se vulnera el compromiso de protección y seguridad garantizados por las instituciones y reflejados en los servicios brindados a los usuarios, en las que se consideran los factores inherentes a la responsabilidad objetiva. En conclusión, bajo la figura de responsabilidad objetiva, la carga de la prueba se revierte, con la finalidad de que la entidad bancaria sea quien se ocupe del conjunto de pruebas. Cabe mencionar que, la entidad financiera ciertamente ejecuta actividades mercantiles conforme a ley, pero que origina cierto riesgo, es el que asume la responsabilidad civil objetiva al tomar en cuenta que omite elementos concernientes a dolo y culpa, debido a que el riesgo y el daño son los únicos aspectos imputados. Empero, el banco puede finalizar la relación causal una vez que se pueda demostrar una causa eximente, entre las que se mencionan como acción realizada por tercero, imputación a la víctima o fuerza mayor.

Estancona (2023) en su estudio realizado en España, con el fin de analizar desde la perspectiva doctrinal y jurisprudencial, buscó dilucidar la controversia sobre los fraudes en los servicios de pago que han sido contratados por personas naturales o jurídicas, a través de contratos con las entidades financieras y que fueron víctimas de fraudes virtuales. Por lo tanto, mediante una metodología cualitativa, se empleó el análisis documental y entrevista a expertos, obteniéndose que la dificultad más relevante de absolver para la entidad financiera es establecer protocolos de responsabilidad respecto a la clasificación de la operación de pago, en otras palabras, respaldos que verifiquen si los movimientos son autorizadas por el titular de la cuenta, por tanto, se debe alinear a la normativa concerniente a servicios de pago y otras medidas urgentes, creado para generar un entorno seguro al uso de servicios de pagos digitales.

Se concluyó que el régimen de responsabilidad es cuasi-objetivo porque las entidades bancarias, como proveedores de servicios de pago, son responsables siempre en cuanto la regularización de seguridad no ha sido ejecutada de forma correcta, teniendo deficiencias en la diligencia en su actuación, de caso contrario, se realiza la imputación al cliente de una falta de autoprotección, a menos que se considere un engaño perceptible fácilmente.

Calvo (2023) presenta en su artículo, el objetivo de analizar concerniente a la responsabilidad que asumen las entidades bancarias frente los delitos informáticos de estafa por phishing. Para tal fin, realizó una revisión documental fundamentándose en un hecho problemático donde la persona que fue víctima de este delito consideró gestionar el reclamo a la entidad a fin de recuperar el dinero sustraído, todo ello sucede debido a que tuvo dificultad para identificar y localizar al delincuente. Desde el análisis general se obtuvo, que las entidades bancarias actualmente ofrecen servicios que cuentan con seguridad garantizada y al mismo tiempo son confiables, sin embargo, los hechos ocurridos de esta naturaleza ponen en duda la eficacia de los métodos de seguridad por el aumento de acciones fraudulentas, en las cuales no se notifica los movimientos relacionados en las cuentas de los usuarios, tal como fue este caso, donde lo requerimientos de los clientes reales fueron fácilmente vulnerados, por tanto el fallo fue a favor del consumidor. Se concluyó que la normativa referente a los servicios de pago, si el cliente niega haber autorizado una transacción, se presume automáticamente la falta de autorización.

Hernández (2020) en un artículo tuvo como objetivo analizar la validez de la sentencia SC18614-2016 de la Corte Suprema de Justicia, que estableció un régimen objetivo de responsabilidad en el fraude bancario por medios

electrónicos. La sentencia se centró en la diligencia debida de los bancos, limitando los medios de defensa y excluyendo las causales de exoneración de responsabilidad, sin considerar la naturaleza contractual de la relación, las responsabilidades de seguridad de cada parte ni las regulaciones del comercio electrónico. En respuesta a esto, se propuso una interpretación más integral del ordenamiento jurídico, sugiriendo que, en el análisis de fraudes en el sistema financiero se tomaran en cuenta todos los elementos relacionados con la operación. Finalmente, se concluyó que la responsabilidad por fraudes electrónicos bancarios debía resolverse según el cumplimiento de los deberes de diligencia de ambas partes, aplicando criterios subjetivos en lugar de criterios de responsabilidad objetiva.

2.1.2 Antecedentes nacionales

Aedo y Huamanciza (2023) plantearon en su estudio determinar la necesidad de incluir la responsabilidad civil solidaria de las entidades bancarias en la Ley N° 30096 respecto al delito de phishing, con el fin de prevenir la ocurrencia de este tipo de delito. La investigación adoptó un enfoque cualitativo, con un tipo de investigación básica y un diseño de investigación basado en la teoría fundamentada. El enfoque permitió corroborar información proveniente de teorías previamente consolidadas, a través de la utilización de guías y herramientas para la recolección de datos. Como resultado, se demuestra que los entrevistados estan de acuerdo con que las entidades financieras asuman responsabilidad civil, aún cuando existe una ley para regular los delitos de phishing, ya que la misma no está adecuada del todo para hacer frente a este tipo de fraude. Se llegó a la conclusión de que existe responsabilidad civil solidaria por parte de las entidades bancarias en casos de phishing. Por lo tanto,

se recomienda modificar la Ley N° 30096 para incluir a las entidades bancarias como responsables civiles solidarios en este tipo de delito.

Torres (2023) en su estudio analizó los criterios jurídicos sobre el deber de idoneidad del correcto ingreso de los datos confidenciales, las normas complementarias de las entidades bancarias y jurisprudencia desde la perspectiva internacional a fin de establecer los criterios de tipo jurídicos apropiados a través de un precedente de observancia obligatoria que deben seguir las resoluciones establecidas por el Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual (INDECOPI) para asignar responsabilidad administrativa en casos de fraude por siniestros o phishing. Siguiendo la metodología interpretativa de tipo documental, se consideró el modelo bibliográfico para analizar resoluciones finales de un tribunal. En este caso, los clientes de la entidad bancaria acudieron a INDECOPI, para realizar las denuncias correspondientes, por operaciones que estos no reconocieron haber realizado. Por otro lado, el parámetro de idoneidad para ser establecido como tal, es necesario verificar que los mecanismos referidos a la seguridad que implementa la entidad financiera hayan funcionado. En conclusión, los criterios legales que el Tribunal del Indecopi emplea en casos de phishing incluyen la verificación de la autorización del titular de la tarjeta para realizar la transacción, lo que implica comprobar si se ingresaron correctamente datos confidenciales.

Ramírez (2023) en su trabajo de investigación busca determinar cómo favorece la modificación del Código Penal frente a la responsabilidad de terceros involucrados en delitos informáticos en las instituciones financieras realizados en la Corte Superior de Piura en el periodo 2022. Para ello, aplica el enfoque descriptivo-analítico sobre la legislación actual y las brechas concernientes a la

gestión de ciberdelitos, aplicando a su vez entrevistas a expertos en la temática. Los hallazgos demuestran que a nivel internacional existen diversas formas de abordar los ciberdelitos, lo cual depende de las características legislativas propias de cada país. No obstante, debido a que este tipo de delito puede ser ejecutado desde otros países, es crucial la contribución internacional a fin de establecer alianzas de cooperación para la prevención y persecución. Por otra parte, el 80% de los juristas especialistas entrevistados coinciden en la insuficiencia relacionada a las sanciones que se aplican a terceros involucrados, dado que son consideradas no disuasorias. A la luz de lo mencionado se concluye que, es esencial implementar una estrategia legislativa de carácter integral y con suficiente adaptabilidad, que enfrente la complejidad y dinamismo que actualmente presenta la ciberdelincuencia, particularmente en el sector bancario.

Paredes y Silva (2021) tuvieron el objetivo en su investigación de examinar cómo la responsabilidad civil de los bancos debe aplicarse al delito de fraude informático phishing durante COVID-19 en Lima. El enfoque cualitativo, de tipo básico, nivel descriptivo y diseño de teoría fundamentada sirvió de base para ello, permitiendo la recopilación de conclusiones a partir de diversas fuentes de análisis documental, que luego se apoyaron en el uso de guías de entrevista con expertos en la materia. Esto condujo al siguiente resultado y conclusión: en Lima, en el 2020, se decidió que los bancos eran responsables civiles por el delito de phishing por fraude informático durante la pandemia del COVID-19. Dado que los bancos son las principales organizaciones que utilizan plataformas digitales, debería aplicarse de manera imparcial. Aunque en la actualidad algunos usuarios prefieren ponerse en contacto con un banco, la pandemia y las

nuevas medidas que sólo están disponibles a través de la banca por Internet han hecho que los usuarios sean los únicos responsables de los problemas informáticos.

Sihui y Unchupaico (2024), investigaron sobre la forma de afectación de la falta de incorporación de la responsabilidad penal en las entidades del sistema financiero frente al fraude informático al sujeto agraviado, dado que el acceso brindado a nuevos medios digitales bancarios no garantiza que los usuarios cuenten con la seguridad adecuada, vulnerando así los derechos de estos. Para desarrollar este estudio utilizaron como metodología el enfoque cualitativo. Los resultados demostraron que prevalece la ausencia de implementación de responsabilidad penal hacia las entidades bancarias concerniente a delitos de fraude informático debido a la carencia de sistemas de seguridad y conocimientos por parte de los clientes que utilizan el servicio digital brindado por las entidades financieras. Por lo tanto, se concluyó que las razones de atribuir responsabilidad penal a las entidades bancarias sobre delitos de fraude informático tienen su base en los art. 1°, 2 y 8° de la Ley N° 30096, cuyo soporte es la Resolución S.B.S. N° 04036- 2022 en su artículo 14.3 que instaura las medidas de protección del sistema financiero; no obstante se encuentra un vacío puesto que no se indica de manera clara las obligaciones y responsabilidades administrativas y/o penales de las entidades de este sistema.

Bermúdez y Flores (2024) analizaron cómo la legislación actual de Protección de Datos Personales (PDP) contribuye a la vulneración del derecho a la intimidad en el sistema financiero de la ciudad de Lima en el país de Perú durante el 2023. Por medio de un enfoque cualitativo, aplicando el método socio-jurídico, se realizó el análisis de normativas, así como de casos de jurisprudencia

del derecho comparado, además de las opiniones expresadas en las entrevistas de los especialistas en derecho administrativo sancionador. De igual modo, los instrumentos utilizados se enmarcaron en la entrevista y Resoluciones Directorales de la Autoridad Nacional de Protección de Datos (ANPDP). Los hallazgos demostraron que la normativa de P.D.P. actualizada en Perú exhibe carencias significativas que posibilitan la vulneración al derecho referido a la intimidad de las entidades del sector financiero-bancario. Por consiguiente, se concluye desde la perspectiva del derecho comparado que, se debe adoptar elementos del Reglamento General de Protección de Datos (RGPD) y la optimización en la aplicación de la normativa disponible son cruciales para reforzar la protección de datos en Perú.

2.2 Bases teóricas

2.2.1 Phishing

El Phishing es considerado como una de las formas de delinquir a través de las redes digitales, por tanto, está enfocado como un ciberdelito por medio del cual los llamados ciberdelincuentes hacen uso del correo electrónico de manera engañosa, es decir, envían mensajes que aparentemente son generados por las entidades financieras u otros organismos legítimos, en busca de obtener datos de tipo personal o informáticos para llevar a cabo el fraude (Vargas, 2023).

Para Rosero (2021), el phishing es una amenaza persistente que no desaparecerá, por lo que las medidas necesarias para estar preparados incluyen reformas en las leyes, asignación de más recursos a las áreas correspondientes, formación continua a los usuarios del sector público y privado, campañas con un lenguaje claro para todos los usuarios, y concientizarlos sobre los riesgos

presentes. La identificación y prevención del phishing es crucial para minimizar el impacto económico y financiero, como la pérdida de patrimonio y los ingresos de los usuarios, además de reducir la confianza en las transacciones a través de canales electrónicos, lo que a su vez tiene un efecto adverso en la actividad económica y financiera, y desmotiva a los usuarios a utilizar dichos canales.

En el contexto peruano, Barahona (2023) refiere que a pesar de que el *phishing* está tipificado y existen leyes que lo penalizan, como la Ley N° 30096 y la Ley N° 30171, no todos los casos son castigados, ya que con el progreso de la tecnología han surgido nuevas formas de cometer delitos, por tanto, las modalidades están creciendo y diversificándose, involucrando fraudes en línea que buscan engañar a autoridades o clientes, haciéndose pasar por entidades legítimas.

En tal sentido, se sostiene que en cuanto a la naturaleza jurídica o delictiva que debe asignarse al *phishing*, es importante considerar dos aspectos: en primer lugar, deben considerarse como delitos de peligro, ya que el bien jurídico que se protege es la seguridad informática. En segundo lugar, cuando las acciones de los ciberdelincuentes agravan la situación, el fiscal debe modificar la clasificación jurídica a delitos de resultados para garantizar la protección del usuario (Barahona, 2023).

Finalmente, Tomalá (2024) expresa que la formación y el aprendizaje constante acerca del *phishing* son esenciales, puesto que los usuarios que cuentan con la información adecuada y los recursos necesarios, demuestran una capacidad mucho mayor para reconocer y enfrentar mensajes de *phishing* y otros fraudes. Es así que, en una organización, los colaboradores que participan de manera habitual en programas de sensibilización no solo incrementan su

habilidad para identificar intentos fraudulentos, sino que también adoptan mejores hábitos de seguridad digital, como comprobar la autenticidad de los mensajes y emplear software de seguridad actualizado.

Del mismo modo, es referido como el principal medio utilizado por los ciberdelincuentes en el cual el fraude incluye medios digitales en línea que se utilizan diariamente por los consumidores. Ciertamente, el correo electrónico es la vía más común para iniciar con el delito; sin embargo, otros casos se han dado mediante otros canales de comunicación como redes sociales, sitios web, mensajería instantánea, así como los mensajes de texto enviados vía telefónica e incluso suelen hacerse a través de las llamadas de voz, los cuales no tienen normativas que responsabilicen al autor, sino generalmente son perfiles falsos que actúan bajo la responsabilidad del consumidor (Grimes, 2024). Resaltando que la mayoría de las veces en que ocurren estos delitos, la víctima da parte de la situación fraudulenta una vez que se ha causado el perjuicio económico, en este caso procede a comprobar que no fue su responsabilidad, sino el hecho atribuido al desconocimiento o convencimiento de la contraparte delictiva (Vargas, 2023).

2.2.1.1 Delito informático.

Dicha denominación se refiere a acciones ilícitas ejecutadas por medio de las herramientas que se enmarcan en las nuevas tecnologías. Al mismo tiempo se incluyen aquellos hechos donde intervienen las nuevas tecnologías con carácter de medio o bien jurídico protegido, a través de los cuales los criminales ejecutan delitos valiéndose del potencial que proveen las tecnologías de información y comunicación (TIC) superando los espacios fronterizos (Dalgo, 2022).

Por otra parte, debido al avance vertiginoso de las TIC, es necesario ampliar la definición de “delito informático” a fin de brindar soluciones normativas penales, puesto que, así como avanza la tecnología al mismo paso avanza la delincuencia en este contexto. Por tanto, se asume en su conceptualización como delitos informáticos las conductas ilícitas, que ocurran por acción u omisión, que sean típicas, antijurídicas y además culpables que afecten diferentes bienes de tipo tecnológico o que para llevarse a cabo esta acción ilícita sea esencial, utilizar cualquier herramienta tecnológica (Rincón, 2023).

En la normativa peruana, la Ley N° 30171 (2014) realizó modificaciones en la Ley N° 30096 concerniente a los delitos informáticos en este país y cuyo objeto presentando en el Artículo 1, refiere la prevención y sanción que deben ser aplicadas a las acciones de tipo ilícitas que inciden en sistemas informáticos, así como en otros bienes de carácter jurídico y que mantengan relevancia penal, las cuales son cometidas a través de la utilización de herramientas, equipos y todo lo que se relacione con medios tecnológicos de información o de comunicación, todo ello con el fin de reforzar la seguridad ante la ciberdelincuencia.

En consecuencia, los delitos informáticos relacionados con las entidades financieras en la protección del consumidor financiero en casos de phishing son contemplados en el Capítulo II de la Ley N° 30096 (2023) y prescribe los delitos contra datos y sistemas informáticos, haciendo referencia en primer lugar al denominado acceso ilícito descrito en el artículo 2 de la mencionada ley, señalando la sanción penal de aquellas personas cuyas conductas accedan a parte o a todo un sistema informático, de forma que vulnere las medidas de seguridad. Por otro lado, está el delito de atentado a la integridad de datos

informáticos, al cual refiere en su Artículo 3, y que establece las acciones que deben ser sancionadas cuando de manera deliberada e ilegal se ocasionan daños a los datos informáticos como dañar, introducir, borrar, deteriorar, alterar, suprimir o inaccesibilidad a los mismos.

También destacan en esta misma perspectiva el artículo 4 referido al atentado a la integridad de sistemas informáticos de la Ley N° 30096 (2023), indicando la sanción penal para quien de formas deliberada e ilegal consiga inutilizar un sistema informático parcial o totalmente, asimismo a quien obstaculice o entorpezca su funcionalidad y prestación de servicio. En los artículos mencionados, la instauración del delito informático tiene como finalidad proteger, desde la mirada jurídica, los datos informáticos, los cuales son considerados como un bien fundamental en las TIC (Rincón, 2023).

En los artículos mencionados, la instauración del delito informático tiene la finalidad de proteger, desde la mirada jurídica, datos informáticos de los consumidores, por ello, son considerados como un bien substancialmente de las llamadas TIC, explicando la naturaleza de delito informático (Rincón, 2023).

2.2.1.2 Convenio de Budapest.

Es considerado un instrumento donde se establecen acuerdos de carácter vinculante y cuyo alcance se da de forma internacional, a través del cual se pretende brindar protección desde escenarios internacionales a las amenazas de la ciberdelincuencia, todo ello considerando que este flagelo se caracteriza por su deslocalización, es decir puede ocurrir en un lugar, pero ser originado en otro. Por tanto, de manera comunitaria puede combatirse este delito que circula por medio de las redes (Rincón, 2023).

Bajo esta mirada, el Convenio sobre la Ciberdelincuencia realizado en

Budapest en el 2001, del cual forman parte los Estados miembros del Consejo de Europa y otros Estados signatarios, resalta la urgencia de adoptar una política en materia penal común con el fin de brindar protección necesaria a nivel internacional frente a la ciberdelincuencia. Así, este Convenio, en vista de la velocidad y profundidad de cambios que ha originado la continua digitalización en las redes informáticas, adopta una legislación adecuada en función de optimizar la cooperación internacional para prevenir los delitos informáticos.

Dentro de los vectores de este Convenio se consideran los delitos contra la integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos; además de los delitos informáticos con mayor prevalencia en casos de responsabilidad de las entidades financieras en la protección del consumidor financiero. Del mismo modo, en su contenido se encuentra lo concerniente a las amenazas en los espacios cibernéticos, así como las diferentes especificidades de nuevos delitos.

En el contexto peruano, se destaca la ratificación del Convenio sobre la Ciberdelincuencia a través del Decreto Supremo N° 010-2019-RE, el cual asume el compromiso efectivo de combatir los delitos informáticos y la necesidad de establecer alianzas cooperativas internacionales para la atención rápida de los ciberdelitos en materia penal.

2.2.1.3 Protección de datos informáticos.

Actualmente, se considera como un factor crucial para el funcionamiento de las entidades, debido a que la labor se enmarcar en el manejo de datos y, por tanto, es esencial que se garantice la protección e integridad ante los riesgos que existen en el contexto digital. Por ello, para evitar la suplantación de identidad o estafas, es necesario implementar medidas de seguridad que sean

aplicadas para los diferentes dispositivos electrónicos y medios digitales en los que se comparte información tanto personal como de las entidades (Ministerio Público Fiscalía de la Nación [MPFN], 2024).

Así mismo, el gobierno peruano establece la Ley N° 29733 - Ley de Protección de Datos Personales, para generar un sistema jurídico de protección al usuario al momento de utilizar alguna aplicación o sistema externo. Esta normativa busca garantizar la fluctuación de la información consentida y legal, pero existen limitaciones como lo indica el artículo 14 en el que se enfatiza que las entidades públicas tienen permitido transferir información según el ámbito comercial, más no los datos personales de sus trabajadores. Al mismo tiempo, en el artículo 18 manifiesta que solo el titular de la información tiene autorización para brindar datos detallados y si esto no se respeta existen represalias legales y jurídicas que respaldan al ciudadano (El Peruano, 2024).

No obstante, la ley antes citada, tiene un alcance limitado ante la protección de datos personales debido a la inexistencia de un extracto legal que tome en cuenta el uso de tecnología fuera de los ámbitos laborales públicos y privados. Esta situación deja desprotegidos a las personas ante perfiladores en estafas bancaria que utilizan los datos personales de los usuarios (Blume, 2021).

La finalidad de las leyes promulgadas en relación a la protección de datos personales es recopilar información correspondiente a sus actividades comerciales, legales y jurídicas de una persona, proporcionar información limitada según los diversos tratamientos, el registro actualizado de un ciudadano y la seguridad de recepción, alcance y transferencia de estos datos. Por lo tanto, las normativas impuestas en la actualidad buscan garantizar el uso adecuado y suscrito en la ley de los datos necesarios para actividades laborales, académicas

y judiciales. Su principal objetivo es otorgar tranquilidad y seguridad a los ciudadanos respecto al uso de su información (Quiroga, 2021).

2.2.2 Responsabilidad de las entidades bancarias

Corresponde en el deber de diligencia y seguridad hacia los consumidores, donde las instituciones financieras están obligadas a proteger los datos de sus clientes, tanto personales como financieros; lo cual abarca la correcta administración de los fondos que capta, la protección de intereses de los usuarios y seguridad del sistema financiero en general, para evitar casos donde el delincuente engaña al usuario para que revele información confidencial; por ende, los bancos deben reforzar la seguridad de los sistemas y plataformas digitales que utilizan sus clientes, evitando que terceros se apropien de sus datos para cometer delitos financieros (Diaz et al., 2022).

Flores (2023), señala que, para la prevención de delitos informáticos, la SBS emite una serie de regulaciones y recomendaciones que todas las entidades financieras deben cumplir. Esto se debe a que, aunque en el contexto del delito, su rol principal sería el de sujeto pasivo o como una de las víctimas.

Mientras que, para Estancona (2023), en casos de fraude como el *phishing*, la responsabilidad de la entidad financiera puede variar dependiendo de si se puede demostrar que el banco ha actuado con negligencia o no, esto respaldado bajo el acuerdo con el marco legal. Si el banco no implementó las medidas necesarias para prevenir el fraude, podría considerarse responsable por los daños sufridos por el cliente; sin embargo, si la entidad bancaria prueba que ha actuado con la debida diligencia y que la culpa recae en el usuario por no tomar las precauciones necesarias, como ignorar advertencias de seguridad o compartir información sensible, su responsabilidad podría quedar exonerada.

Finalmente, Flores (2023) señala que, respecto a la responsabilidad que debe asumir una entidad financiera frente a la comisión de un delito informático, se subraya la necesidad de contar con una norma de aplicación amplia y un alto nivel de protección. Entonces, considera que esta característica de cobertura es algo que actualmente falta en nuestra legislación peruana sobre delitos informáticos, la cual es restrictiva y requiere mayor desarrollo y contenido.

Cabe destacar que, la ciberseguridad en el sector bancario hace referencia a las estrategias, medidas y tecnologías implementadas para proteger los sistemas, redes y datos contra riesgos cibernéticos, como phishing, malware y ataques de ingeniería social. Dado que los bancos dependen de tecnologías avanzadas para ofrecer sus servicios, resulta esencial gestionar los riesgos mediante la anticipación de amenazas y la implementación de planes de contingencia. De este modo, se garantiza la protección de la información y la continuidad de las operaciones, lo que, a su vez, asegura la confianza de los clientes y el buen funcionamiento del sector financiero (Revilla et al., 2024).

Asimismo, la inteligencia artificial (IA) se ha convertido en una herramienta clave en la ciberseguridad, destacándose por su capacidad de analizar grandes volúmenes de datos, identificar patrones y adaptarse autónomamente a nuevas amenazas. Su aplicación abarca diversas áreas críticas, como la detección de malware, donde analiza programas y archivos para identificar comportamientos sospechosos como virus, troyanos y ransomware. Además, la IA monitorea el comportamiento de usuarios y sistemas para detectar accesos no autorizados o movimientos laterales en redes. En la detección de intrusiones, utiliza algoritmos avanzados para analizar el tráfico en tiempo real y responder a actividades maliciosas. Asimismo, facilita la gestión de vulnerabilidades mediante la

evaluación de configuraciones de seguridad y el análisis de código para identificar fallos (Tenorio, 2021).

2.2.2.1 Responsabilidad administrativa.

La regulación de las normativas de la Superintendencia de Banca y Seguros (SBS), la Ley del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros y AFPS - Ley N° 26702, y otras autoridades financieras y administrativas como INDECOPI, se consideran como los estándares de seguridad y protección de datos exigidos por la ley, que busca proteger al consumidor y prevenir posibles fraudes, asegurando que las entidades financieras actúen con transparencia y responsabilidad, la cual consiste en la implementación de políticas estrictas de ciberseguridad, así como programas de educación y concientización para sus clientes; por tanto, actúa como una herramienta preventiva y correctiva en la lucha contra el phishing.

Una de las principales responsabilidades administrativas de las entidades bancarias es el cumplimiento de las normas de prevención del lavado de activos y financiamiento del terrorismo, por ende deben implementar sistemas de monitoreo para detectar y reportar operaciones sospechosas a la SBS y la Unidad de Inteligencia Financiera - UIF, lo que incluye la capacitación continua de su personal en identificación de riesgos y la elaboración de informes periódicos, en suma, deben implementar políticas internas de reclamaciones para garantizar que los consumidores puedan reportar de manera efectiva cualquier problema relacionado con sus productos o servicios (Carranza y Alcántara, 2022).

Por tanto, entre las medidas clave que deben implementar los bancos se

encuentran políticas estrictas que incluyen el uso de tecnologías de cifrado, seguimiento en tiempo real de transacciones, y sistemas para detectar fraudes, además, las entidades están obligadas a realizar auditorías periódicas para evaluar la efectividad de estas medidas y a actualizar sus protocolos de seguridad de acuerdo con las nuevas amenazas cibernéticas, todo ello alineado a evitar sanciones pueden incluir multas, suspensiones de licencias o la implementación obligatoria de nuevas medidas de seguridad (Carril, 2022).

En relación a los reclamos de usuarios financieros todas las responsabilidades de las instituciones financieras deben alinearse con las directrices de la SBS, que incluyen la estabilidad financiera, la solidez financiera, el comportamiento adecuado en el mercado y el buen funcionamiento del Sistema Privado de Pensiones (Flores, 2023).

El procedimiento de reclamos por parte del consumidor es el siguiente: Indecopi posee competencia primaria para conceder protección a los consumidores financieros y la SBS consigna los casos de los usuarios por medio de la plataforma PLAVIR. Seguidamente, la oficina de Indecopi emite información al usuario indicando las vías disponibles para reclamos ante la SBS. Ahora bien, en el caso en que las denuncias sean efectuadas ante Indecopi, pero con competencia de la SBS, se procede a declararla improcedente. Por todo ello, es esencial que se implemente a la mayor brevedad la ventanilla única de reclamos que actualmente se encuentra proyectada por Indecopi (Palomino, 2023).

En este contexto, la Plataforma de Atención Virtual de Reclamos (PLAVIR), desarrollada por la SBS, se define como una herramienta digital que permite a los consumidores financieros presentar y dar seguimiento a sus

reclamos relacionados con productos y servicios financieros, tales como incumplimiento de contratos, cobros indebidos, prácticas desleales y errores en servicios bancarios. Entre los beneficios de la plataforma se destacan su acceso remoto y eficiente, lo que facilita la gestión de reclamos; la transparencia, ya que los usuarios pueden monitorear el estado de sus casos; y su capacidad para fomentar buenas prácticas entre las entidades financieras. Además, PLAVIR actúa como mediador, asegurando una resolución justa y protegiendo los derechos de los consumidores (Superintendencia de Banca , Seguros y AFP, 2023).

2.2.3 Protección del consumidor financiero

Proteger al consumidor financiero es una de las principales funciones que debe cumplir el Estado, promoviendo acciones y mecanismos que sirvan de orientación y prevención para solucionar conflictos, al mismo tiempo que efectúa mejoras de tipo técnico-normativas. Todo ello se realiza a través del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI, el cual pone, a su vez, a disposición el Sistema Nacional Integrado de Protección al Consumidor. Estas organizaciones consideran los criterios normativos y procedimentales que van a guiar las acciones de las entidades públicas, incluyendo a los consumidores y empresarios. De esta manera, se pretende reforzar el cumplimiento normativo relacionado a la promoción de la defensa y protección del consumidor en el territorio peruano (INDECOPI, 2024).

Por otro lado, se tiene el Código de Protección y Defensa del Consumidor en el marco de la Ley N.º 29571 (2010); siendo así, en el artículo 81 del capítulo

quinto referido a productos o servicios financieros, señala que la protección al consumidor financiero tiene su respaldo en el presente cuerpo normativo, toda vez que las organizaciones bajo supervisión de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones se rigen igualmente por el mismo cuerpo normativo. Al mismo tiempo el consumidor cuenta con la normativa especial que se estableció en la Ley N.º 28587, Ley Complementaria a la Ley de Protección al Consumidor en lo referente a Servicios Financieros, así como a preceptos normativos expuestos para reforzar su cumplimiento.

Es importante señalar que, el consumidor financiero es la persona que establece una relación con instituciones financieras autorizadas por el Estado para acceder a productos y servicios especializados. Su especificidad radica en que estos productos y servicios no solo buscan su beneficio individual, sino también el de su grupo familiar o social. No obstante, debido a la asimetría informativa entre el consumidor y el proveedor, el Estado interviene para otorgarle protección. Así, se busca equilibrar la relación contractual y garantizar un marco regulado que promueva la equidad y la seguridad en las transacciones financieras (Machuca, 2021).

Debido a esta desigualdad, la Ley de Protección y Defensa del Consumidor en Perú, establece las disposiciones sobre la responsabilidad de los proveedores de bienes y servicios, es decir, regula los derechos de los consumidores en relación con productos defectuosos y servicios que no cumplen con las expectativas razonables, según lo acordado o conforme a las normativas aplicables. De acuerdo con el artículo, los proveedores deben asumir la responsabilidad por los daños causados a los consumidores debido a productos

defectuosos o servicios mal prestados. Además, deben ofrecer una solución adecuada, que puede incluir la reparación, reposición o devolución del dinero (Chávez, 2023).

2.2.3.1 Deber de idoneidad.

Respecto a este deber, consiste en otorgar a los consumidores lo que esperan por parte de los proveedores de servicios financieros con respecto al servicio ofrecido. Dentro del marco legal, se considera que las características de seguridad e idoneidad sean adecuadas y cumplan con lo estipulado en los contratos realizados; por lo tanto, asegura que las herramientas financieras prioricen la satisfacción de las necesidades del consumidor, respetando la capacidad económica y nivel de comprensión (Chawla y Kumar, 2021).

Del mismo modo, se fundamenta en la transparencia, la responsabilidad y la confianza, pilares esenciales para fomentar relaciones justas entre las entidades financieras y los consumidores, contribuyendo a un mercado más equitativo y ético. Y también funciona como un principio de restricción para proteger a los usuarios de prácticas injustas, como la información engañosa o la comercialización de productos inadecuados (Richards y Hartzog, 2021).

2.2.3.2 Obligación de los proveedores.

Todo proveedor vinculado al sector de entidades financieras está sujeto a cumplir una serie de requerimientos que garanticen la seguridad, transparencia y buen funcionamiento de los servicios. Por ello, los proveedores deben respetar las leyes, así como las regulaciones financieras sobre la protección de datos y evitar fraudes, mantener la seguridad y confiabilidad de la información financiera, la calidad del servicio y la supervisión y auditoría (Raygada, 2023).

Por lo tanto, los controles de auditoría permiten a las entidades financieras reconocer y mantener el funcionamiento del sistema de seguridad. Su protocolo consiste en tener un control de las autorizaciones y aprobaciones mediante una serie de informes sobre las actividades operativas, su finalidad radica en evitar la filtración de información financiera. Además, el control interno garantiza el nivel de seguridad y confiabilidad de la información personal de los clientes (Cumbicos et al., 2023)

Una de las obligaciones más importantes para los proveedores financieros es garantizar la seguridad de los datos del usuario otorgando una serie de estrategias que controlan los ciberataques, los cuáles utilizan brechas informáticas para copiar, borrar o reescribir información y aprovechar la vulnerabilidad de las personas (Flores-Álava y Mena-Hernández, 2023).

La Ley de Transparencia y Acceso a la Información Pública – Ley N° 27806, promulgado en 2002 con el fin de promover la transparencia de los actos que realiza el Estado y regular el acceso a la información, específicamente en el artículo 5 indica que las entidades financieras pueden hacer uso de la imagen e información sustancial y relevante respecto a las funciones del empleado, el funcionamiento y procedimiento internos de la entidad, asegurando que los ciudadanos accedan fácilmente a la información clara sobre la gestión pública. Asimismo, la disposición en el compromiso de garantizar transparencia en la difusión de información donde los datos de las entidades proveedoras, montos comprometidos y calidad de productos y servicios ofrecidos permite que los consumidores indirectos conozcan los tratos con diversas entidades, garantizando el cumplimiento de la obligación de los proveedores y beneficiando

a los ciudadanos que dependen de estos servicios o productos (Congreso de la República, 2024).

En consecuencia, el tratamiento de datos personales es de suma importancia para las entidades financieras que buscan mantener y generar un nivel de confianza mayor con sus clientes. Puesto que, su principal preocupación es la sustracción de datos personales y realizar actividades ilícitas. Ante ello, los proveedores emplean una red de seguridad en cuanto a experiencia digital y conexión en sus plataformas, evitando una serie de estafas y apropiación de datos personales que afectan a los usuarios (Niño, 2022).

2.2.4 Marco Jurídico

2.2.4.1. Doctrina

El phishing es una modalidad de fraude cibernético que se distingue por utilizar técnicas de manipulación psicológica para inducir a las personas a entregar información confidencial sobre su actividad bancaria como la obtención de los dígitos de tarjetas de crédito, los medios empleados son las fuentes de internet como correos electrónicos fraudulentos o páginas web falsificadas, la cuales causan confusiones en los consumidores, al verlas como legítimas generando una ilusión de confianza (Mayer y Calderón, 2020). Por ende, la estrategia central del phishing es replicar la apariencia y funcionamiento de entidades confiables, como bancos o plataformas de servicios donde se elabora un escenario mediante llamada, navegación o mensaje de texto que convenza a la víctima de interactuar sin sospecha, logrando que de manera involuntaria proporcione datos sensibles, para dar pase al fraude (Vazquez, 2021).

Bajo el enfoque de protección al consumidor, el phishing representa un

peligro para la seguridad de la información personal y patrimonial de los usuarios, lo cual, puede incluir desde el acceso no autorizado a cuentas bancarias hasta la pérdida de identidades digitales, lo que conlleva graves consecuencias económicas y sociales; por ende, diversos países ha implementado en sus leyes y normativas regulaciones específicas destinadas a proteger a los usuarios ante este tipo de fraudes, obligando a las entidades bancarias que manejan datos personales a adoptar medidas de seguridad robustas, lo cual, busca que las víctimas dispongan de herramientas legales para denunciar los incidentes y obtener reparación por los daños causados, sin embargo, a la par promueven la responsabilidad del usuario para seguir los protocolos de seguridad y eduquen a los consumidores sobre cómo prevenir estos engaños (Estancona, 2023).

Por último, la colaboración público-privada en la lucha contra los ciberataques, especialmente el phishing**,** se basa en normativas europeas como la Directiva NIS 1 y su actualización NIS 2, las cuales establecen medidas de ciberseguridad para sectores esenciales y servicios digitales con el propósito de proteger infraestructuras críticas. Asimismo, el Reglamento UE 2019/881 (Cybersecurity Act) impulsa la certificación de ciberseguridad en productos y servicios TIC, fortaleciendo así la confianza digital. En el caso de Italia, normativas como el DL 105/2019, que define el Perímetro de Seguridad Cibernética, y el DL 82/2021, que creó la Agencia para la Ciberseguridad Nacional (ACN), han reforzado la cooperación entre el sector público y privado. A su vez, estas regulaciones han facilitado la creación de centros de intercambio de información (ISAC) y la participación de empresas especializadas en la respuesta a incidentes. Por otro lado, la estrategia italiana pone un énfasis particular en la educación y concientización pública sobre el phishing,

promoviendo una cultura de seguridad cibernética que contribuye a prevenir engaños y fortalecer la resiliencia digital (Previti, 2023).

2.2.4.2 Jurisprudencia

La sentencia 1100-2020 del Tribunal Constitucional del Perú aborda un caso de fraude informático relacionado con phishing. En este fallo, se examina cómo la víctima fue engañada para que proporcionara su información personal y bancaria. El Tribunal tipifica el fraude informático y señala que el uso de tecnologías digitales para cometer este tipo de delitos constituye un agravante. La decisión ratifica la condena del acusado, subrayando la responsabilidad penal en crímenes que comprometen la seguridad informática y la confianza pública (Tribunal constitucional, 2020).

2.2.4.3 Código de Protección y Defensa del Consumidor (2023)

La presente investigación, se centra en ciertos artículos del Código, relevantes y muy repetitivos en las resoluciones analizadas, los cuales se procederán a abordar.

El artículo 18, refiere que la idoneidad es la relación que existe entre las expectativas del consumidor y lo que recibe, en función de lo que se promete ofrecer por medio de sistemas publicitarios tomando en cuenta las condiciones y situaciones de la transacción, al mismo tiempo contempla las características, así como la naturaleza del producto o servicio que se ofrece, también se considera el precio, entre otros elementos, atendiendo a las diversas circunstancias que presente el caso (Código de Protección y Defensa del Consumidor [CPDC], 2023).

Por otro lado, para evaluar la idoneidad se considera la naturaleza y

aptitud del producto o servicio para satisfacer las necesidades que han dado paso a su ubicación en el mercado. Del mismo modo, la responsabilidad que debe asumir el proveedor en casos en que sea necesario frente al consumidor no dejan de ser eximidas, aun cuando el Estado autorice la producción o prestación en concordancia con lo ofrecido (CPDC, 2023).

En este mismo orden de ideas, se encuentra el artículo 19, que aborda la obligación que tienen los proveedores. Entre ellos, está el dar respuesta por la excelencia de los productos y servicios ofrecidos, igualmente se toma en consideración la autenticidad que presentan las marcas y leyendas referido al producto, o del signo que sirve de respaldo al prestador del servicio, así como por falta de aceptación a razón de la discordancia entre lo prometido por la publicidad y lo recibido; igualmente por la fecha de expiración y contenido del producto marcado en su envase, en lo que corresponda (CPDC, 2023).

Otro elemento de relevancia es el presentado en el artículo 25, sobre el deber general correspondiente a la seguridad, puesto que lo ofrecido en un mercado no debe implicar riesgos de salud o de cualquier otra índole, entre ellos de seguridad de forma injustificada a los consumidores o a sus bienes. Cabe señalar que, el Código de Protección y Defensa del Consumidor establece que los productos o servicios ofrecidos en el mercado deben ser seguros para los consumidores cuando se utilizan de acuerdo con su propósito o de manera normal (CPDC, 2023).

En este sentido, no deben implicar riesgos innecesarios o no informados que puedan afectar la salud, la seguridad de los consumidores o causar daño a sus bienes. En consecuencia, los productos deben ser diseñados y fabricados de manera que no representen un peligro para las personas cuando se utilicen

correctamente (Instituto Nacional de Defensa de la Competencia y de la Protección, 2023).

A modo de cierre, el marco normativo de protección al consumidor se basa en varios principios fundamentales. El principio de protección ante prácticas engañosas o discriminatorias salvaguarda a los consumidores de acciones fraudulentas o perjudiciales. A su vez, el principio de prevención de riesgos busca garantizar la seguridad de los productos y servicios. Asimismo, el principio de información precisa permite a los consumidores tomar decisiones fundamentadas. Además, se reconoce el derecho de acceso a mecanismos de reclamo para hacer valer sus derechos de manera efectiva. Por otro lado, el principio de interpretación en favor del consumidor establece que, en caso de duda en la aplicación de normas o contratos, debe prevalecer su protección. Finalmente, ante una violación a la Ley de Defensa del Consumidor, se garantiza el derecho a solicitar reparación o indemnización por daños y perjuicios derivados de la mala calidad de bienes o servicios adquiridos (Viteri et al., 2024).

2.2.4.4 Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad

En el artículo 3 acerca del Sistema de gestión de seguridad de la información y Ciberseguridad (SGSI-C), aprobado el 19 de febrero de 2021 con el objetivo de solicitar a las diversas empresas que utilicen estrategias para mejorar su confiabilidad y establecer un entorno seguro entre los productos y servicios brindados a los usuarios. Su finalidad está en reducir el número de riesgos de seguridad respecto a la información del producto y sus procesamientos, resguardando la información de la empresa y sus clientes. Por

lo tanto, en el apartado 3.1. expresa que es el grupo de política y cuestiones procedimentales, así como roles y responsabilidades diseñadas a fin de identificar y brindar protección a los activos relacionados con la información, también para hacer la detección de eventos relacionados con la seguridad, asimismo prevé respuesta y la recuperación ante acontecimientos de ciberseguridad (Resolucion SBS Nº504, 2021).

A su vez, la ciberseguridad se fundamenta en tres requisitos esenciales: confidencialidad, integridad y disponibilidad. Sin embargo, la administración del Estado tiene la obligación de adoptar medidas razonables para proteger los sistemas de información de las instituciones públicas, las organizaciones y los ciudadanos contra ciberataques, además de asumir la responsabilidad por los daños derivados de incidentes de ciberseguridad. En este sentido, la evolución tecnológica ha generado nuevos desafíos, ya que el internet de las cosas amplía la conectividad a diversos dispositivos, mientras que la computación en la nube conlleva una pérdida de control sobre la información compartida. Asimismo, la convergencia tecnológica, aunque impulsa la innovación, también aumenta los riesgos asociados (Rodríguez y Moreno, 2024).

En este sentido, el reglamento asigna responsabilidades claras para fortalecer las funciones del directorio, la gerencia, el comité de riesgos y la gestión de seguridad de la información y ciberseguridad. Establece tres niveles de proporcionalidad: régimen general, simplificado y reforzado, cuya aplicación depende del tamaño, la naturaleza y la complejidad de las operaciones de la entidad. Además, requiere la implementación de un programa de ciberseguridad basado en un marco de referencia internacional, que debe abordar funciones clave como identificación, protección, detección, respuesta y recuperación, con

el objetivo de mejorar las capacidades en este ámbito. También establece la obligación de notificar a la Superintendencia cualquier incidente de ciberseguridad que pueda causar un impacto adverso significativo. Asimismo, la empresa debe contar con la información necesaria para actuar oportunamente ante amenazas y gestionar vulnerabilidades, lo que puede incluir acuerdos con otras empresas del sector o con terceros relevantes (Melgar, 2023).

2.2.4.5. Constitución Política del Perú

La carta magna, promulgada por primera vez en 1823, tiene como finalidad, establecer una serie de normativas respaldadas por el estado sobre las cuestiones legislativas, ejecutivas y judiciales del país. Asimismo, por su superioridad normativa, consagra la defensa del consumidor, en su artículo 65, estableciendo que para la defensa de los usuarios se garantiza el derecho que toda persona tiene a la información en lo concerniente a recursos disponibles en el mercado para su consumo. De igual manera, protege la salud y la seguridad de la ciudadanía (Constitución Política del Perú, 1993).

Como punto de partida, la constitución establece como política pública el derecho de los consumidores a acceder a información clara y veraz, promoviendo su difusión y asegurando su respeto tanto por los sectores público como privado. El objetivo es garantizar la transparencia en el mercado, permitiendo que los consumidores tomen decisiones de consumo de manera libre, informada y responsable. De esta forma, se busca que la información proporcionada sea adecuada, favoreciendo la protección de los derechos del consumidor y su capacidad para tomar decisiones fundamentadas (Chávez, 2023).

2.2.4.6. Ley del Procedimiento Administrativo General

La Ley del Procedimiento Administrativo General (LPAG) se promulgó el 11 de abril del 2001, pero fue modificada el 4 de mayo de 2022, en ella se establece mejores condiciones reguladoras para la implementación y aprobación de procesos administrativos y de prestación en servicios de ámbitos diversos. Por lo tanto, la LPAG tienen como finalidad regular los procesos administrativos de los usuarios en las distintas entidades. En el artículo 3, señala el objetivo de implantar el régimen de carácter legal dirigido a que la Administración Pública proteja el interés general, asegurando el cumplimiento de derechos e intereses de los administrados, acorde a los cuerpos jurídicos, sobre todo el constitucional (Ley N° 27444, 2001).

En ese sentido, la presente ley establece el régimen de procedimientos administrativos comunes aplicables a todas las entidades y órganos del Estado, tanto de naturaleza administrativa como jurisdiccional, incluyendo entidades autónomas y personas jurídicas de derecho público que ejerzan funciones administrativas. Su propósito es garantizar el cumplimiento de los principios que rigen la actuación de la Administración Pública, entre ellos la legalidad, el impulso de oficio, la razonabilidad, la imparcialidad, el informalismo, la veracidad, la celeridad, la eficacia, la participación, la simplicidad, la uniformidad, la responsabilidad y el ejercicio legítimo del poder. Así, la ley asegura que las decisiones administrativas se adopten dentro de un marco legal coherente, alineado con los valores constitucionales y orientado a la protección de los derechos de los administrados (Ministerio de Justicia y Derechos Humanos, 2021).

2.2.4.7 Reglamento de Tarjetas de Crédito y Débito

El reglamento de Tarjetas de Crédito y Débito, aprobado mediante Resolución S.B.S. N.º 6523 -2013, fue actualizado el 26 de junio de 2024 con el objetivo de mejorar las definiciones, el contenido mínimo de los estados de cuenta y la resolución del contrato de tarjeta de crédito para los usuarios. Su finalidad está en establecer las normativas que evitan el sobreendeudamiento, los robos de datos y fraudes. Este reglamento indica en el artículo 23 como responsable para demostrar la autenticación y registro de las operaciones le concierne a la entidad financiera, ante el rechazo que ocurra de una transacción por parte del cliente (Resolución SBS N° 02286-2024, 2024).

Inicialmente, el Reglamento de Tarjetas de Crédito y Débito se define como un conjunto de normas que regulan la emisión, el uso y la operación de estos medios de pago, estableciendo los derechos y responsabilidades de emisores, tarjetahabientes y establecimientos afiliados. Su objetivo es garantizar un uso seguro y transparente, por lo que define aspectos como las condiciones de contratación, la seguridad en las transacciones, la prevención de fraudes, los procedimientos de reclamación y las reglas para la cancelación o suspensión de las tarjetas. Aunque este reglamento varía según la legislación de cada país, su propósito es proteger tanto a los usuarios como a las entidades financieras (Hernández, 2020).

En cuanto a, la cláusula del reglamento establece que los servicios adicionales de las tarjetas de crédito que se encuentran desactivados de forma predeterminada. El cliente asume la responsabilidad de solicitar su activación si así lo desea, y podrá desactivarlos en cualquier momento, en concordancia con lo dispuesto en el Reglamento de Tarjetas de Crédito y Débito (La

Superintendencia de Banca,Seguros y AFP, 2022).

2.2.4.8. Ley complementaria a la Ley de protección al consumidor, en materia de servicios financieros

La ley N° 28587, promulgada en el 2005, tiene como finalidad, el proteger a los usuarios de las empresas del sistema financiero que se encuentran reguladas por la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS). Por tanto, esta normativa establece las cláusulas generales de contratación y sus modificaciones, el cobro y difusión de los interés o comisiones y faculta a la SBS a implementar normas contra las cláusulas abusivas. Dicha normativa es importante para la investigación, porque permite reconocer que el Código de Protección y Defensa del consumidor, no contiene todo lo necesario para proteger a los consumidores financieros, puesto que, al tratarse de temas económicos, su regulación legal puede omitir ciertas variables importantes. Sin embargo, la ley fue promulgada en el 2005, lo que implica que no posee artículos que regulen los temas sobre ciberseguridad. Al respecto, es importante señalar que, los delitos informáticos comprenden una amplia gama de actividades ilegales, que incluyen desde el hacking y el phishing hasta la distribución de malware y el ciberacoso. En este contexto, es importante destacar la evolución constante de las técnicas y métodos utilizados por los ciberdelincuentes, quienes adoptan nuevas estrategias y tecnologías para vulnerar sistemas de información, lo que incrementa la complejidad de su detección y prevención (Cuenca y Núñez, 2024).

2.3 Estado del arte

Ayuhandika et al., (2023) estudiaron cómo es la responsabilidad bancaria

y la protección jurídica de los bancos por la pérdida de saldos de cuentas debida a delitos de suplantación de identidad. Esta investigación, a través de un método descriptivo cualitativo normativo, en base a los resultados, establece las siguientes conclusiones: en el delito de phishing experimentado por los usuarios, el banco puede ser plenamente responsable si el cliente puede demostrar que no hubo negligencia de su parte, sino un error del sistema de seguridad existente por parte del banco. Además de responsabilizarse por las pérdidas sufridas por los clientes, la entidad debe mejorar el sistema de seguridad para prevenir los delitos de suplantación de identidad. Este estudio es un aporte relevante debido a que el delito en el que ocurre el fraude es el phishing, al mismo tiempo la responsabilidad se asigna a la entidad bancaria, se muestra que la misma debe mejorar sus sistemas de seguridad aportando confianza a sus clientes.

Zhang et al., (2023) estudiaron cómo influye el phishing en el sector bancario chino. Aplicaron un método de análisis estadístico y el Modelo de Ecuaciones Estructurales (SEM). Los hallazgos mostraron que el grado de implicación de las fuerzas de seguridad pública, así como la función que ejecutan los operadores de telecomunicaciones, al igual que las iniciativas normativas relativas y las premisas de gobernanza cooperativa son esenciales para establecer límites a la tasa de aparición del phishing y los ciberdelitos relacionados, los cuales suponen un reto para el desarrollo del sector bancario chino. Motivo por el cual el estudio sirve de guía para considerar algunas iniciativas de carácter colaborativo para la lucha contra el phishing.

Flores et al., (2024) analizaron el phishing, como un delito informático presente desde 1996, caracterizado por el envío de correos electrónicos fraudulentos con el fin de obtener información personal de manera engañosa. A

través de un enfoque cualitativo que combina los métodos analítico-sintético e inductivo-deductivo, y utilizando el análisis documental y entrevistas, los resultados del estudio concluyen que la falta de una normativa específica sobre el phishing vulnera derechos constitucionales y genera un vacío legal que dificulta una protección efectiva contra esta amenaza digital en constante evolución. En este sentido, el estudio resalta la necesidad de tipificar el phishing dentro de la legislación ecuatoriana, con el fin de fortalecer la seguridad jurídica y garantizar una respuesta legal adecuada frente a este delito.

Castillo et al., (2021) estudiaron el derecho a la protección de los datos informáticos personales en relación con las cuentas bancarias de personas naturales en Cuba, así como el papel del secreto bancario como una manifestación práctica de esta protección dentro de las instituciones financieras. Para ello, aplicaron métodos teóricos y empíricos, combinados con herramientas de análisis lógico como la síntesis, la abstracción, la generalización, la inducción y la deducción. El estudio se basó en un diagnóstico normativo y práctico realizado en varias provincias de Cuba, a partir del cual se caracterizó el grado de cumplimiento del derecho a la protección de los datos personales en el ámbito bancario del país. Como resultado, la investigación ofrece una guía para futuros estudios y posibles mejoras destinadas a fortalecer la seguridad de los datos personales en un contexto cada vez más globalizado y digitalizado.

Alva et al., (2022) analizaron la relación de consumo entre las entidades financieras supervisadas por la Superintendencia Financiera y los consumidores, con un enfoque en la protección de estos últimos frente a posibles abusos o restricciones a sus derechos, aplicando el método dogmático-jurídico. Los resultados evidenciaron que la regulación y supervisión actuales presentan

deficiencias, lo que permite la persistencia de prácticas abusivas. En consecuencia, concluyeron que es necesaria una intervención más efectiva por parte del legislador y la Superintendencia Financiera para fortalecer la protección del consumidor financiero en Colombia. Asimismo, el estudio resalta la importancia de la información como una herramienta clave para equilibrar la relación entre proveedores y consumidores financieros.

Vélez y Reyes (2023) analizaron la evolución de la protección de los derechos de los consumidores en Ecuador, identificando los desafíos actuales y proponiendo medidas para fortalecer el marco legal. La investigación se fundamenta en una metodología integral que abarca el análisis documental, el estudio de la jurisprudencia, la comparación con normativas internacionales, así como el análisis cualitativo y cuantitativo de datos. A partir de los resultados obtenidos, se concluyó que es necesario fortalecer la protección del consumidor en Ecuador mediante la actualización de la legislación, la educación del consumidor, la protección de datos personales y la cooperación internacional. En este sentido, el estudio ofrece una guía útil para mejorar la protección del consumidor, centrándose en la actualización legislativa, la educación y la protección de datos.

Mendoza et al., (2020) analizó la importancia de la autenticación multifactor para reducir el riesgo de robo de información y dinero, a través de una revisión de seis métodos de autenticación, entre ellos la huella dactilar y el reconocimiento facial. Con base en los resultados obtenidos, se concluye que la implementación de estos sistemas en los sitios web de empresas del sector financiero se ha vuelto esencial para garantizar la seguridad de la información de los clientes y prevenir fraudes. En este contexto, el estudio proporciona una

base relevante para futuras investigaciones orientadas a fortalecer la autenticación multifactor y su papel en la protección de datos.

Reyes et al., (2023) analizaron el control de accesos mediante el modelo de autenticación de doble factor, basado en la combinación de una contraseña y un dispositivo con capacidad criptográfica. Para ello, se aplicó un esquema seguro de autenticación multifactor en la nube. Los hallazgos revelaron un bajo nivel de conocimiento y uso de medidas de seguridad digital, como la autenticación de doble factor, las VPN y los autenticadores de seguridad. Además, la mayoría de los encuestados percibe los pagos en línea como poco seguros y desconoce términos clave como phishing. Se concluye que los profesionales independientes poseen un mayor conocimiento en seguridad informática. Por ello, esta investigación contribuirá a la implementación de medidas que fortalezcan la seguridad digital.

CAPÍTULO III: MÉTODO

3.1. Tipo, diseño y método de investigación

Se trabajó bajo un enfoque cualitativo, debido a que la misma explora, describe y trata de generar entendimiento a partir de las experiencias de los participantes lo cual permite contextualizar y profundizar el entorno (Hernández y Mendoza, 2018). Asimismo, su característica principal es la observación; por consiguiente, el investigador busca comprender el fenómeno de manera que sus observaciones e interpretaciones estén orientadas a entender las interacciones de los componentes dentro de todo el sistema de forma contextualizada (Paragua et al., 2022).

Así pues, el enfoque cualitativo, ofrece un conocimiento holístico, el cual tiene como ventaja que brinda una perspectiva integral y completa del fenómeno en análisis (Paragua et al., 2022). Por ende, el implementarla, permitió una mayor comprensión de la responsabilidad de las entidades financieras en la protección del consumidor financiero en casos de phishing.

El tipo de investigación básica es aquella que está orientada a ampliar y consolidar los conocimientos teóricos adquiridos sobre ciertas temáticas partiendo de la curiosidad científica y siendo la base para estudios aplicados (Ñaupas et al., 2018). Del mismo modo, se la conoce también como investigación pura y en esta es posible proponer tesis con objetivos exploratorios, descriptivos o incluso correlacionales (Hadi et al., 2023). En consecuencia, este tipo de investigación fue básica, en tanto que, profundizó en el conocimiento consolidando con puertas a generar nuevo conocimiento en lo que respecta la responsabilidad de las entidades financieras en la protección del consumidor financiero en casos de phishing.

El presente estudio estuvo ceñido a un diseño no experimental, siendo propio de estos diseños el que los investigadores se limiten a ser observadores del fenómeno que se desea estudiar sin realizar modificación alguna de las variables de estudio (Ñaupas et al., 2018). Por ende, se aplicó el diseño citado, debido a que el objetivo ha sido la recopilación de datos.

El nivel descriptivo en una investigación refiere a que en esta se analizarán las características de un objeto de estudio o fenómeno presente; de tal manera que se describe o explica la situación de un individuo, objeto, fenómeno, problema, etc., en el momento actual (Paragua et al., 2022). Por otra parte, Hadi et al., (2023), señala que las investigaciones de nivel descriptivo pueden brindar la oportunidad de anticipar un suceso y formular hipótesis, aunque sean de manera básica. No obstante, es necesario poseer la base teórica adecuada, junto con antecedentes que proporcionen un panorama claro de lo que podría suceder.

En tal sentido, el presente estudio se catalogó bajo el nivel descriptivo porque se centró en registrar las propiedades y particularidades de un fenómeno, lo cual resulta crucial para ofrecer un panorama íntegro y detallado de la vivencia de los participantes (Silvestre y Huamán, 2019). A su vez, también fue de nivel correlacional, debido a que buscó establecer relaciones entre dos o más elementos que se pretenden investigar (Ñaupas et al., 2018).

Para el presente estudio se utilizará el método científico, caracterizado por ser riguroso para el estudio porque establece estándares precisos para la interpretación y permite proporcionar generalidades en los resultados (Hernández y Mendoza, 2018). El método inductivo procedimiento de investigación en el que se parte de un hecho particular para desarrollar un

razonamiento o principio más general (Ñaupas et al., 2018).

Vinculado a lo mencionado, el método inductivo en este estudio permitió comprender fenómenos a partir del análisis de información específica recopilada por medio de las resoluciones emitidas por INDECOPI y realizar comparaciones con las normativas sobre la responsabilidad de las entidades financieras en el contexto del phishing. De tal manera este método permite comprender desde una mirada holística y contextualizada el fenómeno, siendo crucial en la temática tan compleja como la protección y seguridad financiera.

3.2. Participantes

Los participantes forman parte de los elementos que se desean observar y a su vez presentan características comunes (Córdova, 2019). Y siendo una investigación cualitativa cuya base se centra en el análisis, los participantes fueron las resoluciones emitidas por Indecopi en el 2024 referente a la responsabilidad de las entidades bancarias, protección al consumidor y ciberdelitos como phishing. De tal manera que se consideraron 28 resoluciones de la totalidad de resoluciones emitidas.

3.3. Técnicas e instrumentos para el recojo de información

La técnica de recolección de datos que se utilizó en esta investigación cualitativa fue el análisis documental. En el caso del análisis documental, el instrumento elegido fue la ficha de análisis documental, siendo la ficha un instrumento práctico cuya utilidad radica en la simplicidad para registrar información de interés (Ñaupas et al., 2018). Por lo tanto, en la ficha se presentará lo relacionado a la referencia bibliográfica, el tipo de documento, objetivo del mismo, resumen de contenido, las categorías de análisis, el aporte al tema de investigación, las conclusiones claves y reflexión crítica.

CAPÍTULO IV: RESULTADOS

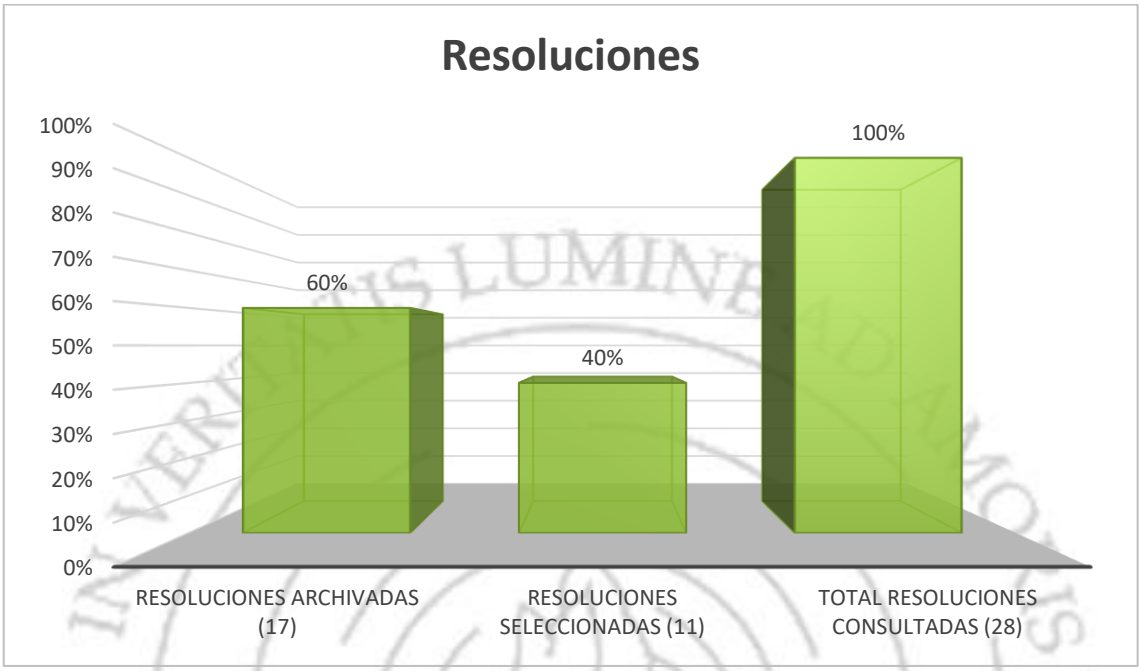
4.1. Análisis de las resoluciones

Cabe mencionar que para este apartado se han considerado 28 resoluciones emitidas por el INDECOPI en el 2024, seleccionadas bajo el criterio de su relevancia en la responsabilidad de las entidades financieras en casos de phishing; es decir que, abordan la protección del consumidor financiero y la idoneidad del servicio bancario en casos de phishing. Asimismo, los hechos materia de denuncia, que dieron origen al procedimiento administrativo, originan que la autoridad administrativa (INDECOPI) determine una infracción o un pronunciamiento relevante en relación a la protección contra el phishing; dentro de las resoluciones destacaban casos donde se impusieron sanciones, se discutía la ruptura del nexo causal o se establecieron criterios administrativos sobre la diligencia bancaria.

Por tanto, del 100 % (28 resoluciones) de resoluciones analizadas, se ha considerado solo el 40 %, es decir, solo las resoluciones donde se identificó que la responsabilidad de *phishing* radicaba en la entidad bancaria. Por ello, las resoluciones restantes, que configuran el 60 %, fueron excluidas por haber sido archivadas (17 resoluciones), debido a que INDECOPI determinó como fallo que los denunciantes remitieron su información a terceros, contribuyendo al acceso indebido en sus cuentas bancarias, aunque los bancos no alertaron sobre las transacciones de manera proactiva, este tipo de operaciones se considera ejecutada a través de los mecanismos de autenticación establecidos, por tanto, se alega la inexistencia de errores en el sistema bancario, lo que genera que dichos fallos no beneficien a la presente investigación.

Figura 1

Representación gráfica de las resoluciones consultadas



Fuente: Elaboración propia

4.1.1. Consideraciones de las resoluciones archivadas

Del análisis, se constató que las consideraciones para archivar las Resoluciones (motivo por el cual fueron excluidas de la investigación al no encontrar responsabilidad en las entidades involucradas), en su mayoría se produjo por lo siguiente:

- La ruptura de nexo causal por imprudencia del consumidor (10), destacando resoluciones como Resolución Final N° 0283-2024/PS2, Resolución Final N° 0432-2024/PS2, y Resolución Final N° 1328-2024/PS2, en suma, las 10 resoluciones archivadas se asociaron a que el consumidor facilitó voluntariamente el acceso a su cuenta bancaria, ingresaron información personal a portales web fraudulentos o que

compartieron sus accesos a terceros. Por tanto, INDECOPI, absolvió a las entidades financieras de la responsabilidad frente al fraude, estableciendo que dicha responsabilidad recaía netamente en los consumidores.

- Se demostró la responsabilidad del usuario (2), donde en la Resolución Final N° 0283-2024/PS2, fue archivado porque se verificó que la afectada había autorizado la operación sin percatarse, por lo que no se podía culpar al banco, similar a la Resolución Final N° 1035-2024/PS2, donde se comprobó que las credenciales del usuario estuvieron correctas y no hubo fallas en la seguridad proporcionada por el banco.

- La entidad no dio respuesta al reclamo en el plazo establecido y recibió sanción por ello, más no por el phishing (1); siendo el caso de la Resolución Final N° 1735-2024/PS2, donde no se determinó fraude por parte del banco.

- Se verifico que las infracciones habían sido denunciadas, tramitadas y resueltas bajo otro expediente (4), como la resolución Final N° 2472-2024/CC1 y la Resolución Final N° 0379-2024/PS2 y Resolución Final N° 1177-2024/PS1 (donde ya había sido justificado la denuncia), asimismo, la Resolución Final N° 0561-2024/PS1 donde ya se había determinado correctamente la invalidación de la cobertura del seguro.

4.1.2. Resoluciones analizadas y seleccionadas

Por consiguiente, el 40 % de las resoluciones analizadas, representa un total de 11 resoluciones, las cuales han sido registradas en INDECOPI como

delito de phishing. Además, en estas resoluciones queda demostrado que el consumidor no recibió llamadas, ni invitaciones a través de sus correos o páginas web para interactuar, tampoco entregó datos, ni accedió a algún link o web en el cual otorgara datos personales; siendo que solo se evidenció que, en su instrumento bancario, sea cuenta o tarjeta de débito o crédito se realizó una transacción no reconocida por él.

A efectos de identificar las similitudes y diferencias entre las resoluciones analizadas, se procedió a realizar un cuadro comparativo, donde se podrá visualizar: la entidad financiera denunciada, la ciudad de origen del proceso, el valor del perjuicio, el tipo de cuenta vulnerada, las conductas materia de sanción, los artículos del código de protección y defensa del consumidor vulnerados, el valor de la multa interpuesta a la entidad financiera, las costas y costos, las medidas correctivas, de ser el caso, el allanamiento de las entidades financieras denunciadas y su registro en el sistema de infracciones y sanciones del INDECOPI; lo que se adjunta a la presente :

RESOLUCIÓN N°	RESOLUCIÓN FINAL N° 014-2024/PS0-INDECOPI-SAM	RESOLUCIÓN FINAL 0084-2024/PS0-INDECOPI-CAJ	RESOLUCIÓN FINAL N° 093-2024/CPC-INDECOPI-PUN	RESOLUCIÓN 119-2024/ILN-CPC	RESOLUCIÓN FINAL N° 523-2024/INDECOPI-AQP		RESOLUCIÓN FINAL N° 668-2024/PS0-INDECOPI-CUS	RESOLUCIÓN FINAL N° 765-2024/PS0-INDECOPI-PIU	RESOLUCIÓN FINAL N° 0926-2024/CC1	RESOLUCIÓN FINAL N° 1055-2024/PS2	RESOLUCIÓN FINAL N° 1177-2024/PS1		RESOLUCIÓN FINAL Nº 2548-2024/CC1	
ENTIDAD FINANCIERA	Banco de la Nación	Banco de la Nación	Banco de la nación	Scotiabank	BCP	Pacifico Seguros	INTERBANK	Banco de la Nación	CMAC PIURA	Scotiabank	BNP PARIBAS CARDIF S.A. COMPAÑÍA DE SEGUROS Y REASEGUROS		BANCO DE CRÉDITO DEL PERÚ S.A	
CIUDAD	Tarapoto	Cajamarca	Puno	Lima – Los Olivos	Arequipa		Cusco	Piura	Lima	Lima Sur	Lima		Lima	
VALOR DEL PERJUICIO	S/ 4,000.00	S/ 1,300.00	S/ 4,350.00	S/ 3 000,00	a S/. 67 378.00	USD$ 5 362.20	S/ 10,870.00	S/ 5,835.05	S/7 545,00	US$ 1 902,91	S/ 1 000,00 - Tarjeta de Crédito del Banco Falabella	S/ 3 000,00,- operaciones no reconocidas realizadas con otras tarjetas	S/ 4 800,00	S/ 1 100,00
TIPO DE CUENTA	Cuenta de ahorros	Cuenta de ahorros	cuenta de ahorros	Tarjeta de débito /cuenta de ahorros	Tarjeta de crédito	Tarjeta de crédito	Tarjeta de crédito	cuenta de ahorros	Cuenta CTS	Tarjeta de crédito	Tarjeta de crédito - Poliza N° 41171701202		Cuenta de ahorro	
CONDUCTA MATERIA DE SANCION	- No se adoptó las medidas de seguridad necesarias, al permitir que se realice una operación no reconocida	-Se debitó indebidamente S/ 1300.00 de la cuenta de ahorros n° 04-**********3562 del denunciante -No cumplió con desbloquear la cuenta de ahorros, pese a que los reclamos, habían concluido. - No se acreditó que haya cumplido con atender, dentro del plazo legal establecido, el reclamo.	-No se adoptaron las medidas de seguridad necesarias, relacionadas a la validez de las operaciones y al comportamiento habitual de consumo del denunciante, al permitir un consumo no reconocido	-No haber adoptado ni aplicado las medidas de seguridad necesarias a efectos de evitar que se realice un consumo virtual	Se habría atribuido indebidamente al denunciante una deuda	-Se habría negado indebidamente a hacer efectiva la cobertura del seguro de protección de la tarjeta de crédito	-Se acredito que no cumplió con su deber de idoneidad, al no haber adoptado las medidas de seguridad respecto de las operaciones no reconocidas	-Se atribuyo una operación (transferencia) no reconocida por la denunciante	No se otorgó la garantía adecuada por los proveedores de que adoptarán las medidas de seguridad que fueran necesarias para garantizar que el patrimonio de los consumidores se encuentre debidamente resguardado.	-La operación fue procesada, pese a que se solicitó su anulación y bloqueó su tarjeta de crédito -El Banco no aplicó las medidas de seguridad pertinentes	-No se cumplió con brindar a la denunciante la cobertura de uso indebido de sus tarjetas de débito o crédito como consecuencia de phishing		-No se adoptaron las medidas de seguridad, al permitir que se realice una operación no reconocida	
CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR	artículo 19°	artículo 19 y 88	artículo 19°	artículo 19°	Art. 56° literal b)	artículo 19	artículo 19°	18° y 19°	artículos 1° literal c), 18° y 19°	artículos 1° literal c), 18° y 19°	artículo 19		artículos 1° literal c), 18° y 19°	
MULTA	(01) UIT	3.49 UIT	a 3.49 UIT	3 UIT	11.60 UIT	6.89 UIT		3.78 UIT	3,78 UIT		-		3,49 UIT	3,49 UIT
COSTAS Y COSTOS	S/ 36.00	S/ 36.00	S/ 36.00	S/ 36.00			S/ 36.00	S/ 36.00	S/ 36.00	S/ 36.00	S/ 36.00		S/ 36.00	
MEDIDAS CORRECTIVAS	devolver la suma de S/ 4,000.00 soles	-Devolución de los S/ 1300.00 -Desbloquear la cuenta de ahorros	-Devolución y/o abono por el importe de S/ 4,350.00 e	-Devolución y/o abono por el importe	- Dejar de atribuir al denunciante la deuda	- Cumplir con dar cobertura a la poliza del seguro de protección de la tarjeta de crédito	-Devolución y/o abono por el importe	-Devolución y/o abono por el importe	-Devolución y/o abono por el importe	extornar	otorgar la cobertura de uso indebido de sus tarjetas de débito o crédito		devolver en la Cuenta de ahorros los importes	
Allanamiento de la E.F.										SI	SI			
Registro de infracciones y sanciones del INDECOPI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI		SI	

4.1.3. Sanciones

Dentro del análisis de estas resoluciones se encontraron como entidades financieras sancionadas, a 7 empresas, teniendo como predominante al Banco de la Nación con 4 casos, seguida de Scotiabank con 2 registros y otras entidades como el Banco de Crédito del Perú, Pacífico Seguros, INTERBANK; CMAC Piura, BNP Paribas Cardif S.A. Compañía de seguros y Reaseguros, presentan un caso cada una.

4.1.4. Caracterización de las entidades financieras

Del mismo modo, se observa que la ciudad donde se dieron más hechos fue en Lima con 5 casos, seguida por ciudades como Tarapoto, Cajamarca, Puno, Arequipa, Cusco y Piura. Por otro lado, el valor de los perjuicios estuvo enmarcado en montos que van desde S/ 1,300.00 hasta S/ 67 378.00. Asimismo, el instrumento más utilizado para realizar el fraude fue a través de cuentas de ahorro o tarjetas de débito, registrándose dicha modalidad en 6 de las resoluciones analizadas, seguido de tarjeta de crédito con 5 casos y otro instrumento menos utilizado fue la cuenta CTS.

4.1.5. Conductas materia de sanción

Las conductas materia de sanción están relacionadas con el deber de idoneidad, debido a que no se tomaron en cuenta, las medidas de seguridad que son esenciales para permitir la transacción, incluyendo la ausencia de validez de las operaciones, así como monitoreo del comportamiento habitual de consumo del denunciante, la atribución de operaciones no reconocidas, entre otras.

También se observó el incumplimiento de atención del reclamo dentro del plazo legal establecido (Resolución Final 0084-2024/PS0-INDECOPI-CAJ).

4.1.6. Artículos y normativa vulneradas

En cuanto a los artículos del Código de Protección y Defensa del Consumidor con mayor predominancia fue el artículo 19 presente en las 11 resoluciones, debido a que el delito de phishing vulnera esencialmente la calidad del servicio e idoneidad que ofrecen las entidades financieras, ya que su deber es el de prevalecer y salvaguardar el dinero de sus usuarios, lo que claramente incumplen al dejar que se produzca el phishing. De igual forma, el artículo 18 estuvo presente en 4 casos, puesto que regula el deber de idoneidad, entendido como lo que esperan los usuarios recibir de sus proveedores, es decir de la entidad financiera, y en los casos materia de análisis, sería el segundo artículo más vulnerado, ya que los usuarios no reciben el cuidado y salvaguarda que suponen deberían recibir de dichas entidades, a las cuales confían sus ahorros. Por último, el artículo 56 regula las medidas comerciales coercitivas, ya que, en una resolución, el caso materia de denuncia involucraba un aumento en la línea de crédito del denunciante sin haber brindado su previa autorización y el articulo 88 regula el deber de las entidades financieras de resolver los reclamos que impongan los usuarios, sancionándose con este artículo a una entidad bancaria que no respondió a tiempo el reclamo del denunciante frente al cobro indebido de su tarjeta.

4.1.7. Multas

Las multas impuestas, variaron según la responsabilidad de la entidad financiera entre 01 UIT hasta 11.60 UIT siendo esta ultima la más alta. Al respecto, se debe señalar que el valor de la multa, se calculó en base al artículo

del código vulnerado y el perjuicio económico ocasionado, siendo que el deber de idoneidad regulado en el artículo 18 y la obligación de los proveedores regulado en el artículo 19, poseen las sanciones más bajas, desde 1 UIT hasta 6.89 UIT. Y el artículo 56 que regula los métodos comerciales coercitivos, posee la sanción más alta, por la cantidad de 11.60 UIT, esto en razón a que el denunciante nunca habría aceptado la contratación de un nuevo producto (ampliación de línea de crédito) y en tanto se habría obligado al consumidor a asumir prestaciones que no había solicitado ni aceptado voluntariamente, produciendo dicha acción una multa más elevada.

4.1.8. Costas y Costos

Las costas y costos se mantuvieron en S/ 36, puesto que es el monto que se paga ante INDECOPI para presentar una denuncia. Asimismo, las medidas correctivas con mayor presencia fueron las devoluciones y/o abonos y el desbloqueo de cuentas y en menor presencia, se encuentra el dejar de atribuir una deuda al denunciante (tarjeta de crédito).

De igual forma, se evidenció formulación de allanamiento en dos resoluciones (Resolución Final N° 1055-2024/PS2 y Resolución Final N° 1177-2024/PS1), lo que implica que las entidades financieras reconocían abiertamente los hechos materia de denuncia y asumían su falta de idoneidad para con el servicio ofrecido y la vulneración a sus obligaciones como proveedores.

4.1.9. Registro de sanciones

Igualmente, todas las resoluciones analizadas dispusieron que las entidades financieras sancionadas queden registradas ante el sistema de infracciones y sanciones del INDECOPI, debido a que se inició un proceso en su contra por el incumplimiento de las normas de protección al consumidor.

4.2. De las resoluciones

La Resolución Final N.º 523-2024/INDECOPI-AQP establece una sanción significativa al Banco de Crédito del Perú y a Pacífico Seguros, con multas de 11.60 UIT y 6.89 UIT, respectivamente, debido a la asignación errónea de una deuda de S/. 67,378.00 a un cliente y la negativa de la aseguradora a reconocer la cobertura del seguro de tarjeta de crédito, resaltando que la responsabilidad bancaria no respaldaba la gravedad del incumplimiento en la verificación de la autenticidad de los cargos y su impacto en la estabilidad económica del consumidor. Por lo tanto, la falta de justificación de la deuda perjudicó directamente la situación financiera del afectado, lo que pone en evidencia la responsabilidad respecto a la gestión adecuada de sus registros, reafirmando la necesidad de mecanismos de control estrictos para evitar errores administrativos que comprometan la confianza de los usuarios y subraya la obligación de las entidades de actuar con diligencia y transparencia en sus operaciones.

Asimismo, la Resolución Final N.º 093-2024/CPC-INDECOPI-PUN impone una multa de 3.49 UIT al Banco de la Nación debido a su omisión en la verificación de seguridad en una transacción de S/. 4,350.00, la cual el usuario no reconoció, por tanto, la responsabilidad bancaria acorde con el artículo 19° del Código de Protección y Defensa del Consumidor, exigía a la entidad financiera implementar mecanismos de seguridad efectivos para evitar operaciones fraudulentas, por tanto, la responsabilidad de la entidad radicó en falta de supervisión y monitoreo en movimientos inusuales, evidenciando deficiencias en los protocolos de autenticación del banco, lo que expone a los clientes a riesgos financieros, por lo cual, el fallo enfatizó que la idoneidad en los servicios financieros es un derecho fundamental del consumidor.

Complementariamente, la Resolución Final N.º 765-2024/PS0-INDECOPI-PIU impone una sanción de 3.78 UIT al Banco de la Nación debido a su negligencia en la validación de una transferencia por S/. 5,835.05, que terminó siendo acreditada en una cuenta ajena sin la autorización del titular, teniendo como fallo evidencias de fallas estructurales en los protocolos de seguridad bancaria, reflejando una gestión ineficaz en la verificación de transacciones inusuales, por tanto, la responsabilidad radicaba en la falta de mecanismos de autenticación reforzada y supervisión adecuada de los movimientos financieros del cliente, por tanto, existió una operación fraudulenta sin alertas ni validaciones previas, debido a que la resolución subraya la responsabilidad de los bancos en proteger los fondos de sus clientes, evitando la materialización de fraudes por fallos administrativos.

Por otra parte, la Resolución Final N.º 0926-2024/CC1 establece una sanción de 3.78 UIT hacia el CMAC Piura, además del reintegro por la suma de S/. 7,545.00 a una usuaria afectada por phishing; puesto que, la responsabilidad de la entidad financiera fue deficiente en la implementación de los controles adecuados en los sistemas de monitoreo bancario que respaldan los mecanismos de seguridad, el caso destaca por la falta de análisis en el patrón de consumo de la cliente ante una operación inusual. La decisión del INDECOPI enfatiza que el banco debe responsabilizarse de los protocolos de detección de fraudes y mejorar la supervisión de operaciones fuera de los hábitos financieros de sus clientes. A su vez, reafirma protocolos detallados y rigurosos en el control de la banca digital, destacando la importancia del monitoreo continuo del comportamiento financiero de los usuarios.

En caso similar, se encuentra la situación de la Resolución Final N.º 014-2024/PS0-INDECOPI-SAM que impone una sanción de 1 UIT al Banco de la Nación por falta de implementación de mecanismos de seguridad, concernientes a la necesidad de fortalecer los protocolos de autenticación y supervisión de transacciones electrónicas, asegurando rigurosamente una verificación de cualquier movimiento sospechoso. Asimismo, refuerza cumplir los protocolos de diligencia como ejercer responsabilidad en la prevención de fraudes, previniendo estos atentados con el empleo actualizado de tecnologías que permitan identificar patrones habituales de los movimientos de los clientes. Por lo cual, el fallo destacó que es la entidad financiera quien se responsabiliza de la protección a la confianza y estabilidad del manejo de las cuentas bancarias.

Acorde con la Resolución Final N.º 1055-2024/PS2, misma que establece que, Scotiabank debe asumir el pago de costas procesales luego de reconocer su responsabilidad por no establecer mejor sus protocolos en un caso de phishing, debido a que se evidenciaron deficiencias en sus mecanismos de seguridad, ya que es recurrente la exposición a fraudes electrónicos y la necesidad de que exista un sistema de autenticación para movimientos sospechosos, sin infringir en los derechos del consumidor. Por tanto, el fallo respalda que la entidad admite su error bajo el argumento de falta de actualización en las medidas adecuadas para detectar y bloquear la operación fraudulenta a tiempo, he impone que la obligación de las instituciones financieras es proteger a sus clientes de ciberataques, estableciendo controles más estrictos y educando a los usuarios sobre prácticas seguras.

Por otro lado, la Resolución Final N.º 1177-2024/PS1 impone una amonestación a BNP PARIBAS CARDIF S.A. COMPAÑÍA DE SEGUROS Y

REASEGUROS debido a su negativa de brindar la cobertura correspondiente ante un caso de phishing, destacando la falta de responsabilidad ante la obligación de proteger a los asegurados frente a fraudes cibernéticos. Aunque, el caso no llegó a la imposición de una multa económica, enfatiza que las aseguradoras deben garantizar una idoneidad de pólizas efectivas que cumplan términos de seguridad en los servicios ofrecidos. En base a ello, INDECOPI evidencia la importancia de que cualquier entidad bancaria o financiera debe estructurar sus protocolos con el fin de ser claros y acorde a normativas para atender reclamos relacionados con fraudes electrónicos, enfatizando que todos los clientes no queden desprotegidos frente al delito de phishing o cualquier nuevo delito cibernético.

Asimismo, se consideró la Resolución 119-2024/ILN-CPC (Scotiabank), donde la Comisión del INDECOPI determinó que la entidad bancaria no adoptó las medidas de seguridad necesarias, porque la transacción fue ejecutada sin mecanismos de autenticación requeridos basados en la confirmación de un correo, por ende, encontraron fallos en la seguridad del banco que justificaron su responsabilidad. En base a ello, se estableció que la denunciante, había sido perjudicada, ya que no reconocía los movimientos en su tarjeta de crédito, teniendo condiciones suficientes para declararse un cauce de fraude.

En suma, la Resolución Final N.º 2548-2024/CC1 aborda un caso en el que el Banco de Crédito del Perú fue denunciado por el cargo indebido de dos operaciones en la tarjeta de crédito del denunciante, quien alegó haber sido víctima de phishing. Por tanto, el argumento se basó en que el banco no implementó medidas de seguridad suficientes, ya que permitió la realización de estas operaciones sin alertar al cliente sobre accesos desde dispositivos ajenos,

pese a que la víctima tenía desactivadas las compras por internet, lo que indicaba una falla en la validación del perfil de consumo del usuario. Por ello, el fallo consistió en que el banco se responsabilizaba en devolver en la cuenta de ahorros el monto del incidente, y de igual forma, fue sancionado con una multa de 3,49 UIT.

Por otro lado, la Resolución Final N.º 668-2024/PS0-INDECOPI-CUS abordó un caso de phishing que afectó al denunciante, cliente del banco Interbank, quien detectó 43 consumos no reconocidos en su tarjeta de crédito. Dentro del caso, se estableció que la entidad financiera carecía de medidas de seguridad suficientes para prevenir el fraude, permitiendo transacciones sospechosas sin alertar al usuario, por tanto, el denunciante solicitó la devolución del monto defraudado y el pago de costas procesales, en base a ello se demostró que la entidad se responsabilizó administrativamente de la cobertura total del seguro, asimismo, se ordenaron medidas correctivas para reforzar la seguridad y prevenir futuros casos de phishing.

También, un caso similar fue la Resolución Final 0084-2024/PS0-INDECOPI-CAJ, la cual, se pronunció sobre la responsabilidad del Banco de la Nación en un caso sobre incumplimiento de un débito en la cuenta de ahorros del cliente, donde se evaluó la idoneidad del servicio financiero y se impuso una sanción administrativa, porque el banco no cumplió con su deber de diligencia en la gestión de las operaciones generando un perjuicio al consumidor. En este caso, la falta de medidas de seguridad en el desbloqueo de la cuenta de ahorros y el no atender el reclamo en el tiempo establecido, se establecieron como acciones que configuraron el fallo.

Tal como se evidencia en la Resolución Final N.º 0926-2024/CC1, Resolución Final N° 1055-2024/PS2 y Resolución Final N.º 2548-2024/CC1 en la cual se constata que la entidad financiera no acreditó el uso de las medidas de seguridad señaladas en el Reglamento de Ciberseguridad, aun cuando la Superintendencia de Banca, Seguros y AFP (SBS) brinda una serie de normativas a las cuales las entidades financieras deben apegarse a fin de garantizar todo lo concerniente a la seguridad y protección del usuario al momento de llevar a cabo transacciones.

Del mismo modo, se demuestra que los usuarios no son informados ante los cambios en los sistemas de seguridad, tal como se observa en la Resolución Final N.º 1177-2024/PS1 donde se señala que la entidad no cumplió con ofrecer a la denunciante información acerca de la cobertura de uso indebido de sus tarjetas de débito/crédito, teniendo como resultado, la estafa a través de las modalidades de phishing. Por lo tanto, se nota la ausencia de información en lo concerniente a los riesgos que el phishing acarrea y además de la manera cómo los usuarios pueden proteger su información personal.

Cabe mencionar que, en las denuncias queda demostrado que las entidades financieras en ocasiones obvian alguno de los procesos a seguir para evitar los fraudes digitales, como la autenticación biométrica y el uso de tokens para acceder a cuentas en línea. Agregando a lo anterior, también se suele omitir el monitoreo de actividades sospechosas, en las cuales se detectan transacciones inusuales y alertan a los usuarios acerca de las acciones potencialmente fraudulentas. Así se expone en la Resolución Final N.º 014-2024/PS0-INDECOPI-SAM donde en los documentos presentados por la entidad financiera no se registra información notable que describa a una operación

financiera por medio de la Banca Móvil; en otras palabras, en los documentos no se comprueba el ingreso de la Clave de usuario para acceder desde internet (6 dígitos) - Clave TOKEN/SMS, elementos imprescindibles de seguridad en estas operaciones, incurriendo en infracción al artículo 19° del Código de Protección y Defensa del Consumidor.

También se pudo corroborar por medio de la Resolución Final N.º 093-2024/CPC-INDECOPI-PUN, la ausencia de protocolos establecidos para dar respuesta de manera rápida ante incidentes de phishing. Por lo que, la entidad ante este hecho debió detectar la transacción como operación inusual o sospechosa al patrón de consumo del usuario y pronunciar la alerta respectiva.

Es importante mencionar que las medidas de seguridad son insuficientes, aun cuando las entidades financieras, aseguran implementar sistemas tecnológicos de seguridad, la efectividad de estas medidas es cuestionada al demostrarse que en las resoluciones señalan que la protección brindada, así como la información para prevenir fraudes no es oportuna y apropiada, lo cual deja en duda la capacidad de estas entidades para amparar los datos informáticos de sus clientes.

CAPÍTULO V: DISCUSIÓN DE RESULTADOS

Teniendo en cuenta las resoluciones analizadas, se ha identificado que las entidades financieras son responsables frente a la protección del consumidor financiero en casos de phishing, debido a que existen obligaciones de carácter legal que se enmarcan en la responsabilidad legal que deben brindar las entidades para proteger los datos informáticos y los fondos de sus clientes, es así, que la falta de medidas de seguridad viene conllevando sanciones y repercusiones legales.

Lo mencionado encuentra coincidencia con Carril (2022) quien señala que desde el plano axiológico se valora la tendencia relevante en la jurisprudencia de hacer cumplir el deber de seguridad y prevención que tienen las entidades bancarias relacionado con los usuarios de sus servicios, consagrados además de manera explícita en la Constitución Nacional como en las demás Leyes y Códigos. Los hallazgos demuestran según el dictamen que emitió el Ministerio Público, en lo concerniente a los incumplimientos de la entidad bancaria que sostienen el daño punitivo, que existió destrato hacia el usuario, ya que no fue atendido el reclamo que este hizo por medio de diferentes vías dispuestas por la misma entidad, lo cual se traduce en una conducta fuera del marco de la normativa referida al trato digno hacia el consumidor.

De igual forma, de las resoluciones analizadas, se evidenció que existe un marco legal en el contexto peruano, donde se derivan las obligaciones que deben cumplir las entidades financieras que manejan datos personales y confidenciales a través de la tecnología, garantizando la seguridad de la información de sus consumidores. Del mismo modo se evidenció que esta normativa, no se está cumpliendo de manera correcta, debido a que las

entidades financieras en ocasiones hacen caso omiso a su responsabilidad pues la implementación de medidas es inadecuada, lo cual vulnera el principio de idoneidad al estar ausente la protección de datos de sus usuarios. Todo ello demuestra, a su vez, que existe incumplimiento de la adopción de políticas de seguridad, así como de actualizaciones periódicas de sus sistemas de seguridad, conllevando a que no se cumplan los protocolos previstos para las transacciones u operaciones de los consumidores.

De este modo, similar son los hallazgos de Carril (2022) quien evidencia que la responsabilidad de las entidades financieras se hace más notoria toda vez que, frente al hecho de las diferentes estafas electrónicas, los consumidores sienten vulnerados el principio de idoneidad representado en la seguridad y protección de sus intereses económicos. Asimismo, demuestra que la entidad financiera según lo emitido por el Alto Tribunal, debió brindar información clara y precisa sobre los peligros o riesgos que pueden generarse al utilizar el home banking para operaciones con su cuenta. Por lo tanto, se percibe la usencia de información oportuna y veraz durante la relación que el consumidor establece con la entidad.

En este mismo contexto, la responsabilidad de las entidades financieras en cuanto a la protección del consumidor se respalda en el Código de Protección y Defensa del Consumidor - Ley N.º 29571 (2010); específicamente en el artículo 81 del capítulo quinto concerniente a productos o servicios financieros, menciona que la protección al consumidor financiero se ampara en el presente cuerpo normativo, dado que las organizaciones bajo supervisión de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones se administran igualmente siguiendo las mismas normativas. A la vez el usuario

financiero cuenta con la normativa de carácter especial que se instituyó en la Ley N.º 28587, Ley Complementaria a la Ley de Protección al Consumidor en lo relativo a Servicios Financieros, junto a las normas ostentadas para reforzar su cumplimiento.

Por otro lado, la responsabilidad de las entidades financieras en lo referente a la protección contra el phishing es esencial para que el usuario del sistema financiero confíe en los servicios que este ofrece. En este sentido, el hecho de que el banco no asuma su responsabilidad en un primer llamado o acuse a los clientes de otorgar sus datos, hace que estos perciban que las entidades no están tomando las precauciones fundamentales que garanticen la seguridad, lo que genera duda en hacer uso de sus servicios.

Este hecho basado en la usencia de responsabilidad va en contra de lo señalado en el artículo 65 de la Constitución del Perú (1993) donde se otorga reconocimiento al derecho que poseen los consumidores concernientes a recibir información precisa acerca de los productos en el mercado. Armoniza a su vez con Durand (2019) quien subraya la importancia de la protección del consumidor en un entorno económico social de mercado, siendo el consumidor el usuario final de todas las operaciones comerciales. Del mismo modo señala que, en países como el Perú, aun se observa la ausencia de institucionalidad en lo referente a la normativa y la articulación para llevar a cabo un trabajo coherente entre los organismos a quienes les compete la protección del consumidor. Por ello es necesario ir más allá, es decir, otorgar participación a los empresarios y a las entidades financieras, para que la evolución de las normativas puedan ser afines a la realidad de cada uno de los actores involucrados: Estado, consumidor, empresa y entidades financieras.

Bajo esta misma línea, la autoridad administrativa viene resolviendo los casos interpuestos contra entidades financieras por el delito de phishing, bajo el criterio primordial de que no se vulnere “el nexo causal”, es decir que el consumidor o usuario no haya contribuido de ninguna forma a consumar el phishing. Motivo por el cual, más del 50% de resoluciones emitidas en el 2024 sobre phishing son archivadas, debido a la falta de conocimiento de los ciudadanos sobre el phishing, por la excesiva confianza que se tiene a las entidades financieras respecto a sus sistemas de seguridad y por la falta de actualización del marco normativo respecto a los ciberataques.

Al respecto, Ramírez (2023) concuerda en la urgencia de adecuar el marco legal para brindar una respuesta más robusta y sistematizada por parte de las entidades financieras frente a los fraudes por phishing. Dado que la valoración realizada en un 80% por juristas especialistas a las sanciones que fueron aplicadas a terceros, tomadas como no disuasorias develaron ser insuficientes, lo cual marca la importancia de hacer una revisión para potenciar las penas, aspecto que robustecerá tanto la prevención como el castigo que deben recibir los delitos informáticos.

En consecuencia, lo mencionado por Pérez (2021) sirve de soporte o fundamento, debido a que establece que las entidades tienen la obligación de enmendar el daño causado por una acción u omisión, dando lugar a que el usuario víctima de fraude puede demandar una compensación económica, indemnizando así las pérdidas sufridas. Esta responsabilidad parte de garantizar la seguridad de las transacciones financieras y dar respuesta oportunamente ante la ocurrencia de los fraudes informáticos.

De acuerdo a los resultados obtenido en lo concerniente a la responsabilidad de las entidades bancarias frente al phishing, se pudo observar que las entidades financieras actualmente se encuentran en un punto crítico, aun cuando han implementado sistemas tecnológicos de seguridad que tienen como fin garantizar la protección de los usuarios al momento de realizar operaciones, por lo que, se denota una debilidad en cuanto a los diferentes procesos que deben seguir, lo cual quedó demostrado en las diferentes resoluciones analizadas.

Esto coincide con lo encontrado en los hallazgos de Calvo (2023) quien a nivel internacional demostró la sentencia dictada a una entidad financiera por no haber conseguido autorizar el cumplimiento de los convenios acerca de las diligencia exigibles en lo concerniente a la autentificación de las transacciones de pago, así como para disponer de la tecnología anti phishing adecuada que permitieran identificar y detecta las páginas que habían sido clonadas de las oficiales propias y proceder cerrarlas o eliminarlas. En este sentido, se observa la ineficacia de los métodos de seguridad y la usencia de notificaciones referida a los movimientos en las cuentas de los usuarios. Además, el componente fáctico concluyente para la condena a la entidad financiera se basó en la imposibilidad de demostrar que la transacción falsa se realizará desde la dirección IP acostumbrada del usuario; en este caso la entidad bancaria debe poseer mecanismos de seguridad de alto nivel para verificar al momento en que se produce la operación, que esta se está llevando a cabo de una IP que no es la que habitualmente suele conectarse el cliente, siendo esta una señal de alarma para que entidad este atenta y bloquear o no aceptar el movimiento bancario.

Caso similar demuestra Torres (2023) quien señala que dentro de los criterios legales que se emplean en caso de phishing según el Tribunal del Indecopi se enmarca en acciones como verficar la autorización del titular del instrumento financiero para realizar las diferentes operaciones, esto implica comprobar el ingreso de datos de forma correcta y que estos sean los confidenciales. Lo mencoinado ambién se respalda en el Convenido de Budapest (2001) señalando como ciberdelitos aquellos que vulneran la seguridad de la información, entre estos menciona a la confidencialidad, integridad y disponibilidad. En otras palabras, las entidades deben garantizar que sólo los usuarios autorizados pueden acceder a la información, ya sea para modificarla o eliminarla, igualmente que el ususario cuente con la información cuando sea necesario.

Asimismo, dadas las características de los fallos, respecto a la responsabilidad administrativa de las entidades financieras en las resoluciones analizadas, se puede decir que la responsabilidad que asumen frente a los casos de phishing, carece de idoneidad debido a que se observa que estas entidades generalmente tienden a evadir responsabilidad ante los fraudes que los usuarios sufren, evidenciando que dicho actuar contraviene con lo esperado por los mismos usuarios.

Aunado a ello, se observó que el principio de idoneidad no se le ha dado la importancia que requiere, puesto que se implementan medidas de seguridad inapropiadas, es decir, si bien las entidades mantienen protocolos de seguridad en su infraestructura tecnológica, como autenticación en dos pasos, esta no ha sido suficientes si no se cumple con comunicar de manera efectiva a los usuarios. Por ello, es relevante que este principio se configure con sistemas que

detecten fraudes en tiempo real, debido a que ello está contribuyendo al incumplimiento de dicho principio.

Este hallazgo se adhiere a lo evidenciado por Espinoza (2023) en su estudio donde sobresale que una parte del criterio menciona que los mecanismos de garantía brindados al cliente, deben suministrarse no solo dentro de los límites informáticos de la propia entidad financiera, sino también en el procesos o pasos de acceso a este sistema, todo ello como parte del servicio. De acuerdo a lo mencionado la responsabilidad se atribuye a la entidad como consecuencia del riesgo y de la poca seguridad que tiene el sistema. De igual manera, Estancona (2023) coincide en que la institución no cuenta con las medidas de seguridad que ofrece en el contrato de servicio, además en la operación no reconocida la entidad no realizó las acciones necesarias para la seguridad como el consentimiento escrito, llamada de comprobación al cliente, ni otro procedimiento que conlleve a la confirmación de la transacción.

Las afirmaciones anteriores se respaldan en los postulados de Rincón (2023) quien sustenta que el avance acelerado de las Tecnologías de las Comunicaciones, obliga a optimizar las soluciones normativas de carácter penal, es decir que estas regulaciones vayan a la par de los avances tecnológicos y apegados a las leyes internacionales. Agregando a lo anterior, en Perú queda ratificado el Convenio sobre la Ciberdelincuencia a través del Decreto Supremo N° 010-2019-RE (2019), otorgando importancia al compromiso dirigido a hacer frente a los delitos informáticos y la necesidad de instaurar alianzas cooperativas a nivel internacional para generar una atención eficaz de los ciberdelitos en materia penal.

Por tanto, los hallazgos encontrados en este estudio y en los previos, encuentran su fundamento en lo postulado por Barahona (2023), quien afirma sobre el carácter jurídico o delictivo que debe otorgársele al *phishing* considerar a este como delito de peligro, dado que el bien jurídico a protegerse se trata de la seguridad informática. Por consiguiente, al momento en que las acciones de los ciberdelincuentes agravan la situación, el fiscal ha de modificar la clasificación jurídica a delitos de resultados a fin de garantizar la protección del consumidor.

La responsabilidad de las entidades frente al phishing requiere mayor atención y una mejora constante, se observa en las resoluciones una cantidad de normativas que buscan brindar solución y protección a los consumidores; sin embargo, no se cumple con la proactividad de estas medidas, puesto que se evidencia que hay incumplimiento en acciones para educar y proteger a sus usuarios, al mismo tiempo, no se menciona en ningún criterio que, la entidad haya presentado actualizaciones en sus sistemas de seguridad, lo cual es esencial, en vista del rápido avance de las diferentes formas para aplicar phishing.

En este contexto, (Bermúdez y Flores, 2024) sirven de respaldo a lo encontrado, puesto que sus hallazgos constataron que la normativa de Protección de Datos Personales actualizada en Perú presenta carencias importantes que facilitan la vulneración al derecho concerniente a la intimidad de las entidades del sector financiero. Cabe mencionar que la jurisprudencia peruana La Ley N° 30171 (2014) modificó en Ley N° 30096 referida a los delitos informáticos en este país en su Artículo 1, mencionando la prevención y sanción que deben aplicarse a las acciones de carácter ilícitas que inciden en sistemas

informáticos, así como en otros bienes de tipo jurídico y que tienen relevancia penal, cometidas a través de la utilización de herramientas, equipos y todo lo que se relaciones con medios tecnológicos con el fin de reforzar la seguridad ante la ciberdelincuencia.

Por su parte, Aedo y Huamanciza (2023) resaltan la importancia de fortalecer la protección al consumidor financiero mediante la modificación de la ley, asegurando que las entidades bancarias asuman responsabilidad en dichos casos. Por otro lado, Hernández (2020) coincide en subrayar la importancia de las entidades financieras en cumplir con deberes de diligencia en la protección de los consumidores ante fraudes electrónicos como el phishing. Además, establece que la responsabilidad debe evaluarse de manera subjetiva, lo que refuerza la necesidad de una supervisión más rigurosa en la seguridad de las transacciones.

Por último, queda demostrado y se confirma a través de la contrastación con los estudios previos que la responsabilidad de las entidades bancarias en Lima frente a los casos de phishing no es asumida de manera efectiva, lo que provoca una protección insuficiente al consumidor financiero.

CONCLUSIONES

- Se concluye que la falta de información clara y oportuna a los usuarios sobre los riesgos del phishing y las medidas de protección de sus datos personales pone de manifiesto una deficiencia significativa en las prácticas de seguridad adoptadas por las entidades financieras. Las resoluciones presentadas evidencian que no se cumplen adecuadamente los protocolos de seguridad establecidos, como la autenticación biométrica, el uso de tokens y el monitoreo de actividades sospechosas. Además, se observa la omisión de procedimientos esenciales para la protección de los usuarios frente a fraudes digitales. Esta situación demuestra una desconexión en las obligaciones de las entidades financieras de garantizar la idoneidad y la transparencia en los servicios que ofrecen, afectando directamente la confianza y seguridad de los consumidores.
- Asimismo, luego de analizar las resoluciones, se tiene que varias entidades financieras no cumplieron con los estándares de seguridad necesarios para proteger a los usuarios frente a fraudes, lo que resultó en perjuicios económicos significativos. Además, Lima se destacó como la ciudad con mayor incidencia de estos hechos, y los fraudes se cometieron principalmente a través de cuentas de ahorro y tarjetas de débito.
- De igual forma, de las resoluciones materia de análisis, se concluye que la falta de medidas de ciberseguridad conlleva a sanciones y repercusiones legales contra las entidades financieras, por lo que, la prevención de los casos sobre el delito de phishing debe garantizarse con normativas nacionales respecto a la actualización de protocolos que brinden seguridad a los clientes, así como la orientación a los mismos sobre fraudes digitales.

- Teniendo en cuenta la normativa analizada, se concluye que la responsabilidad de las entidades financieras en la protección del consumidor financiero, no se encuentra debidamente actualizado en base al avance tecnológico. Pese a que existe un amplio marco legal, como lo es el Código de Protección y Defensa del Consumidor, particularmente en la Ley N.º 29571 (2010), que regula los productos y servicios financieros, siendo que su artículo 81, subraya el compromiso de las organizaciones supervisadas por la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones de adherir a las mismas normativas para garantizar la protección de los usuarios financieros y además, la Ley N.º 28587, ley Complementaria a la Ley de Protección al Consumidor en lo relativo a Servicios Financieros, refuerza la aplicación de estas regulaciones, proporcionando un marco normativo especial para asegurar que las entidades financieras cumplan con sus obligaciones y brinden un entorno seguro y transparente para los consumidores. La realidad demuestra que la implementación de medidas de seguridad sigue siendo inadecuada e ineficiente, vulnerando el principio de idoneidad, debido a que la mayoría de casos analizados, inician con algún método fraudulento que conduce a los consumidores a riesgos de phishing; teniendo en cuenta que la normativa de Perú no se encuentra actualizada y por tanto no refuerza la supervisión y la adopción de protocolos, las entidades financieras no están cumpliendo de manera proactiva con la actualización de sus sistemas de seguridad ni con la educación a sus usuarios sobre los riesgos de fraude informático.

- Igualmente, las resoluciones demostraron, la falta de respuesta oportuna como negativa de los bancos a asumir su responsabilidad ante las operaciones

no reconocidas por los consumidores vinculadas a casos de phishing, genera desconfianza contra las entidades financieras; por tanto, todo lo que se necesita para evitar o disminuir estos casos, radica en protocolos de seguridad de las entidades financieras hacia los usuarios, resaltando la necesidad de implementar estrategias efectivas para mejorar la seguridad mediante la comunicación con los clientes. Estos casos requieren una respuesta más rigurosa y sistematizada por parte de las entidades financieras y los organismos reguladores a efectos de que no se continue vulnerando el principio constitucional de protección al consumidor,

- Se concluye de las resoluciones, que los artículos vulnerados y que establecen las sanciones impuestas a las entidades financieras, tienen su base, mayoritariamente, en los artículos 18 y 19 del Código de Protección y Defensa del Consumidor referentes a la idoneidad y a la obligación de los proveedores. El primero, hace alusión a la relación que existe entre las expectativas de lo que se va a consumir y lo que se recibe, al mismo tiempo contempla las características, así como la naturaleza del producto o servicio que se ofrece, también se considera el precio, entre otros elementos. Y, en el segundo, se menciona la obligación que tienen los proveedores de dar respuesta por la excelencia de los productos y servicios ofrecidos, igualmente se toman en consideración la autenticidad del producto o servicio, así como la falta de aceptación a razón de la discordancia entre lo prometido por la publicidad y lo recibido.

- Del mismo modo, del análisis, se descubrió que la entidad bancaria con mayor incidencia en casos de phishing en el 2024 es el Banco de la Nación, el cual pertenece al Estado y por tanto debería ser el más actualizado y precavido,

teniendo en cuenta las normativas antes descritas. Sin embargo, en la actualidad se demuestra que no adopta las medidas de seguridad necesarias para evitar que sus usuarios sean víctimas de phishing, ni reconoce la falta de idoneidad en su servicio, pues no se allano al proceso en ninguna de las resoluciones analizadas.

- Se llega a la conclusión que, la autoridad administrativa viene sancionando a las entidades financieras de manera severa, pues no solo impone multas económicas calculadas en base a la unidad impositiva tributaria – UIT, sino también ordena la devolución del monto materia de phishing y registra a las empresas en el “Registro de infracciones y sanciones del INDECOPI”, el mismo que se encuentra de manera abierta y pública y permite que los usuarios y consumidores se informen respecto a sus decisiones financieras.

RECOMENDACIONES

Por todo lo expuesto y analizado, se recomienda que las entidades financieras refuercen los protocolos de seguridad establecidos, como la autenticación biométrica, el uso de tokens y el monitoreo continuo de actividades sospechosas con la finalidad de garantizar la protección de los consumidores. Además, las instituciones deben adoptar procedimientos más rigurosos y transparentes en la gestión de riesgos digitales, con el fin de fortalecer la confianza de los usuarios y cumplir con sus responsabilidades en cuanto a la idoneidad y seguridad de los servicios ofrecidos. Adicionalmente, es crucial que las entidades financieras sigan perfeccionando sus mecanismos de autenticación y monitorización para detectar de manera proactiva cualquier transacción sospechosa, asegurando así una experiencia más segura para el usuario. La colaboración entre las entidades financieras y los consumidores es esencial para reducir los riesgos de fraude y garantizar la integridad del sistema financiero.

De igual forma, es recomendable que las entidades financieras implementen, de manera interna, simulaciones de ataques de phishing de manera regular como parte de sus programas de formación en ciberseguridad. Estos ejercicios controlados permitirán evaluar la resistencia de los usuarios frente a amenazas reales, proporcionándoles una experiencia práctica para identificar vulnerabilidades y áreas de mejora. Además, es fundamental que tras cada simulacro se realicen sesiones informativas en las que se discutan los aciertos y errores, lo que fortalecerá el aprendizaje y ayudará a mejorar la capacidad de respuesta ante futuros intentos de fraude. Además, las entidades deben cumplir con las normativas nacionales e internacionales en materia de

ciberseguridad, asegurando que sus infraestructuras tecnológicas estén actualizadas y sean resilientes ante posibles ataques.

Asimismo, se recomienda a la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS) que promueva, normativas claras y actualizadas que regulen la protección del consumidor financiero en casos de phishing, para lo cual deberán de colaborar con expertos en derecho informático, para garantizar que las normativas sean claras y aplicables en la actualidad. De igual forma, se deben establecer mecanismos de supervisión y cumplimiento para garantizar su aplicación efectiva como parte fundamental de la responsabilidad de toda entidad dedicada al rubro financiero.

Se recomienda a la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS) que capacite a entidades financieras públicas y privadas sobre el marco legal vigente e informe sobre las mejores prácticas a aplicarse, respecto a la protección de los datos informáticos y la forma en la que se viene sancionando a las empresas por no actuar de manera idónea, de tal forma que se busque fortalecer las políticas públicas que fomenten el cumplimiento normativo en este ámbito. Asimismo, sería recomendable que se promuevan auditorías por parte de la SBS a todas las empresas financieras, de tal forma que se corrobore que vienen actualizando constantemente sus servicios de ciberseguridad y que fomentan la capacitación frecuente de sus usuarios respecto a las nuevas modalidades de fraudes informáticos, concientizando del procedimiento interno a seguir y de las normas aplicables fuera de la entidad.

Aunado a ello, la SBS puede instar a las entidades financieras la implementación de un enfoque integral de comunicación para informar de manera clara y oportuna a los usuarios sobre los riesgos asociados al phishing y las medidas de protección de sus datos personales. De igual forma, implementar programas informativos y de formación para que los usuarios comprendan mejor los riesgos asociados con el uso de servicios digitales y cómo evitar ser víctimas de phishing.

Con respecto al INDECOPI, como autoridad administrativa, es recomendable que establezca incentivos para la adopción de medidas alineadas con los principios legales en la materia, campañas de concientización y capacitación sobre las implicancias legales sobre las sanciones que deben asumir las entidades financieras en casos de phishing; lo que impulsara a las entidades a la colaboración con expertos en derecho para garantizar que apliquen de manera correcta las normativas en la práctica, de tal forma que impulse la creación de jurisprudencia que respalde las sanciones en caso de phishing. De igual manera, dichas campañas de concientización, deberán de implementarse para los consumidores, a efecto que tomen conocimiento de las nuevas modalidades de ciberdelitos de las que pueden ser víctimas y se informen respecto a los procedimientos sancionadores que aplican las autoridades administrativas a las entidades financieras, frente a estos casos.

Por último, se recomienda a los usuarios estar constantemente alerta frente a posibles intentos de phishing y adoptar prácticas preventivas para evitarlo. Es fundamental que no compartan información sensible a través de correos electrónicos o mensajes de fuentes no verificadas, y que verifiquen siempre la autenticidad de los sitios web antes de realizar cualquier transacción.

Referencias

Aedo, M., y Huamanciza , W. (2023). *La responsabilidad civil solidaria de las entidades bancarias frente al delito de phishing en la Ley N° 30096 en el Perú.* [Tesis de pregado, Universidad Cesar Vallejo], Lima. Obtenido de https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/122525/Aedo_PMF-Huamanciza_FWMF-SD.pdf?sequence=1&isAllowed=y.

Alva, N., Quintero, J., y Díaz, M. (2022). La protección al consumidor financiero en Colombia, estado de cosas. *Artículos de investigación científica y tecnológica, 2*(1), 1-26. doi:10.15765/rndd.v2i1.4085.

Arméstar, G., y Toche , F. (2024). El tratamiento del fraude informático: un estudio del derecho comparado entre Perú y Estados Unidos. *Revista De Derecho De La UARM, 4*, 139-156. doi:https://doi.org/10.53870/lvj.390.

Ayuhandika, N., Putri, R., y Rahma, I. (2023). Bank Responsibility and Legal Protection of Customers Damaged Due to Phishing Crime. *International Journal of Multicultural and Multireligious Understanding, 10*(3), 261-267. doi:10.18415/ijmmu.v10i3.4509.

Barahona, V. (2023). *La tipificación del phishing en nuestro sistema penal peruano, y la prevención de ciberdelincuencia, Lima Norte 2022.* [tesis de licenciatura, Universidad César Vallejo]. Obtenido de https://repositorio.ucv.edu.pe/handle/20.500.12692/134504.

Bermúdez, M., y Flores, L. (2024). *La protección de los datos personales, frente a la vulneración al derecho a la intimidad, en el sistema financiero-bancario de Lima-Perú, 2023.* [Tesis de grado, Universida Tecnológica del

Perú]. Repositorio Institucional de la UTP. Obtenido de https://hdl.handle.net/20.500.12867/9842.

Blume, I. (2021). Las nuevas tecnologías y la protección de datos en el entorno laboral: retos y perspectivas legales. *THEMIS Revista De Derecho* (79), 435-449. doi:https://doi.org/10.18800/themis.202101.025.

Calvo, M. (2023). La responsabilidad civil de los bancos en los delitos de estafa por "phishing". *Actualidad Jurídica Iberoamericana*(18), 1788-1809. Obtenido de https://revista-aji.com/articulos/2023/18/AJI18_64.pdf.

Carranza, C., y Alcántara, O. (2022). Consumer Protection in Peru: Origins, Evolution, and Main Regulatory Influences. *Journal of Consumer Policy, 45*. Obtenido de https://link.springer.com/article/10.1007/s10603-022-09506-7.

Carril, M. (2022). Responsabilidad de las entidades bancarias ante estafas electrónicas. El deber de seguridad y prevención en el marco del contrato de consumo. *Revista Jurídica De La Universidad De San Andrés*(13), 52-66. Obtenido de https://revistasdigitales.udesa.edu.ar/index.php/revistajuridica/article/view/143.

Castillo, A., Pérez, A., y Contreras, L. (2021). Consideraciones sobre el derecho a la protección de los datos personales respecto de las cuentas bancarias de las personas naturales en Cuba. *Revista de Derecho Cesumar - Maestría, 21*(2), 623–636. doi:10.17765/2176-9184.2021v21n2p623-636.

Chávez, R. (2023). Las medidas correctivas en la ley 29571 ¿Garantizan el derecho de información de los consumidores en el etiquetado de los

alimentos y bebidas industrializados? *Ecno Humanismo, 3*(4), 1-24. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=9862402.

Chawla, N., y Kumar, B. (2021). E-Commerce and Consumer Protection in India: The Emerging Trend. *Journal of Business Ethics, 180*. Obtenido de https://link.springer.com/article/10.1007/s10551-021-04884-3.

Código de Protección y Defensa del Consumidor [CPDC]. (2023). Ley 29571 de 2023. Perú. Obtenido de https://cdn.www.gob.pe/uploads/document/file/1351847/LEY%2029571.pdf.pdf?v=1602084982.

Congreso de la República. (2024). Ley de transparencia y acceso a la información pública. Obtenido de https://www.minedu.gob.pe/normatividad/leyes/Ley27806.php.

Constitución Política del Perú. (1993). Obtenido de Artículo 77 [Titulo III] (Edición Especial). Congreso de la República. https://www.congreso.gob.pe/Docs/constitucion/constitucion/Constitucion-Agosto-2023.pdf.

Convenio de Budapest. (2001). *Convenio sobre la Ciberdelincuencia - Budapest.* Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.

Cumbicos, H., Señalin, L., y Tapia, N. (2023). La importancia del control interno contable en la gestión efectiva de las empresas. *Ciencia Latina Revista Científica Multidisciplinar,* 7(4), 1635-1647. doi:10.37811/cl_rcm.v7i4.6981.

Dalgo, H. (2022). *Protección de datos en el comercio electrónico.* Editorial Ebooks. Obtenido de https://books.google.co.ve/books?id=fnxXEAAAQBAJ&newbks=1&newbks_redir=0&dq=delito+inform%C3%A1tico&source=gbs_navlinks_s.

Decreto Supremo N.° 010-2019-RE del 2019 [Ministerio de Relaciones Exteriores]. Por medio del cual se ratifica el "Convenio sobre la Ciberdelincuencia" adoptado el 23 de noviembre de 2001 en la ciudad de Budapest. 12 de febrero de 2019. (2019). Obtenido de https://transparencia.rree.gob.pe/index.php/datos-generales-11/13-normas-emitidas-por-la-entidad/133-decretos-supremos-ds/ano-2019-7/13496-ds-n-010-re-2019/file.

Diaz, A., y Goitia, S. (2024). *El delito de phishing en las entidades financieras del perú.* Tesis de pregrado, Universidad Autónoma del Perú.

Diaz, I., Bodero, M., Ulloa, L., y Mora, D. (2022). Análisis jurídico de la responsabilidad bancaria frente a delitos informáticos. *Iustitia Socialis: Revista Arbitrada de Ciencias Jurídicas y Criminalísticas, 7*(2).

Durand, J. (2019). Aproximación a una teoría de los derechos humanos del consumidor en el mercado global y su tratamiento en el derecho constitucional peruano. *Prolegómenos,* *22*(44), 117-142. doi:10.18359/prole.3960.

El Peruano. (2024). Ley N° 29733. *Ley de Protección de datos personales*. Obtenido de https://cdn.www.gob.pe/uploads/document/file/272360/Ley%20N%C2%BA%2029733.pdf.pdf.

Espinoza, S. (2023). Responsabilidad civil objetiva de la actividad bancaria frente al fraude informático (phishing). *Derecho en Sociedad, 16*(2), 28-52. Obtenido de https://revistas.ulacit.ac.cr/index.php/derecho-en-sociedad/article/view/37.

Estancona, A. (2023). Responsabilidad de las entidades financieras ante el hackeo de cuentas bancarias. En particular, casos de "phising". *Actualidad Jurídica Iberoamericana*(18), 1590-1617. Obtenido de https://repositorio.unican.es/xmlui/bitstream/handle/10902/30168/ResponsabilidadEntidadesFinancieras.pdf?sequence=3&isAllowed=y.

Flores, M. (2023). *El sector financiero es el más usado en los ataques de phishing*. Obtenido de https://www.elperuano.pe/noticia/221669-el-sector-financiero-es-el-mas-usado-en-los-ataques-de-phishing#:~:text=En%20Per%C3%BA%2C%20en%20el%20%C3%BAltimo,la%20compa%C3%B1%C3%ADa%20de%20ciberseguridad%20Kaspersky.

Flores, C. (2023). *La responsabilidad de las entidades financieras ante la comisión de delitos informáticos.* [tesis de maestría, Pontifica Universidad Católica del Perú]. Obtenido de https://tesis.pucp.edu.pe/items/c9662514-c03e-4502-9e50-341f5e0709aa.

Flores, L., Carrión, K., y Rivera, J. (2024). Fundamentos jurídicos para la inclusión del delito de phishing en el código penal ecuatoriano. *Revista Dilemas Contemporáneos: Educación, Política y Valores, 1*(113), 1-26. doi:10.46377/dilemas.v12i.4515.

Flores-Álava, S., y Mena-Hernández, L. (2023). Propuesta de Buenas Prácticas para Mitigar Ciberataques en Usuarios de Entidades Financieras. *593 Digital Publisher CEIT,* *8*(4), 159-173. doi:https://doi.org/10.33386/593dp.2023.4.1652.

Grimes, R. (2024). *Fighting Phishing: Everything You Can Do to Fight Social Engineering and Phishing.* [Cómo combatir el phishing: todo lo que puede hacer para combatir la ingeniería social y el phishing]. John Wiley & Sons. Obtenido de https://books.google.co.ve/books?id=SpPvEAAAQBAJ&newbks=1&newbks_redir=0&dq=phishing&source=gbs_navlinks_s.

Hadi, M., Martel, C., Huayta, F., Rojas, C., y Arias, J. (2023). *Metodología de la investigación. Guía para el proyecto de tesis.* Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú S.A.C.

Hernández, G. (2020). *Marco legal del Banco de la República Banco central de Colombia* (La Imprenta Editores S. A. ed.). Obtenido de https://repositorio.banrep.gov.co/server/api/core/bitstreams/df8c7332-bf86-40f7-b1a4-fc43da9f5e7b/content.

Hernández, J. (2020). *La responsabilidad de las entidades financieras por fraudes electrónicos.* [Tesis de maestría, Universidad Pontificia Bolivariana], Medellin. Obtenido de https://repository.upb.edu.co/bitstream/handle/20.500.11912/6161/La%20responsabilidad%20de%20las%20entidades%20financieras%20por%20fraudes%20electr%C3%B3nicos.pdf?sequence=1.

Hernández, R., y Mendoza, C. (2018). *Metodología de la investigación, las rutas cuantitativa, cualitativa y mixta.* Ciudad de México: McGRAW-HILL INTERAMERICANA EDITORES.

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual [INDECOPI]. (2024). Obtenido de Sistema Nacional Integrado de Protección al Consumidor: https://www.gob.pe/27595-instituto-nacional-de-defensa-de-la-competencia-y-de-la-proteccion-de-la-propiedad-intelectual-sistema-nacional-integrado-de-proteccion-al-consumidor.

Kaspersky. (2024) Amenazas financieras móviles crecen 32% a nivel mundial, revela Kaspersky. Obtenido de: https://latam.kaspersky.com/about/press-releases/amenazas-financieras-moviles-crecen-32-a-nivel-mundial-revela-kaspersky?srsltid=AfmBOoooT4UZnKWs991avtVZxHQb9Z7-dYsobIBN4ZRFLJx3tqj1jVwL.

La Superintendencia de Banca,Seguros y AFP. (2022). Resolución SBS 02286 de 2024. *La Superintendencia de Banca,Seguros y AFP, 1*(214), 1-22. Obtenido de Por medio de la cual se modifica el el Reglamento de Tarjetas de Crédito y Débito, aprobado por Resolución SBS N° 6523-2013. 26 de junio de 2024: https://busquedas.elperuano.pe/cuadernillo/NL/20240628.

Ley 30171 de 2014. Por la cual se modifica la Ley 30096, Ley de los delitos informáticos. 10 de marzo de 2014. D.O. No. 518568. (2014). Obtenido de https://cdn.www.gob.pe/uploads/document/file/200326/197055_Ley30171.pdf20180926-32492-1l0lzim.pdf?v=1594241856.

Ley N° 27444. (2001). *Ley del Procedimiento Administrativo General.*

Ley Nº 30096. (2023). *Ley de Delitos Informáticos.* Obtenido de https://cdn.www.gob.pe/uploads/document/file/1671764/1678028-ley-n-30096-ley-de-delitos-informaticos-vigente-pdf.pdf?v=1708709859.

Machuca, J. (2021). *Manual del consumidor financiero peruano.* doi:10.19083/978-612-318-323-3.

Mayer, L., y Calderón, G. (2020). El delito de fraude informático: concepto y delimitación. *Revista chilena de derecho y tecnología, 9*(1). Obtenido de https://www.scielo.cl/scielo.php?pid=S0719-25842020000100151&script=sci_arttext.

Melgar, C. (2023). *Modifican el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad aprobado por la Resolución SBS N° 504-2021 y la Circular Nº S-661-2016, Productos de seguros sujetos al régimen simplificado de debida diligencia en el conocimie.* Retrieved from https://busquedas.elperuano.pe/dispositivo/NL/2235205-1.

Mendoza, A., Bolaños, F., y Cedeño, C. (2020). La importancia de la autenticación multifactor para el usuario final en un entorno financiero. *Informática y Sistemas, 4*(1), 42-51. doi:10.33936/isrtic.v4i1.2347.

Ministerio de Justicia y Derechos Humanos. (2021). *Ley N° 27444 - Ley del Procedimiento Administrativo general* (Segunda Edición ed.). Obtenido de https://www.minedu.gob.pe/transparencia/2021/pdf/TUO_27444-PROCED_ADMINISTRA-Final.pdf.

Ministerio Público Fiscalía de la Nación [MPFN]. (2024). *¿Qué es la seguridad de la información?* Obtenido de https://www.gob.pe/23391-que-es-la-seguridad-de-la-informacion.

Niño, D. (2022). Los datos personales y sus riesgos jurídicos a partir de la transformación digital en el comercio electrónico. *CES Derecho, 13*(1), 70-89. doi:10.21615/cesder.6386.

Ñaupas, H., Valdivia, M., Palacios, J., y Romero, H. (2018). *Metodología de la investigación cuantitativa - cualitativa y redacción de la tesis.* Bogotá: Ediciones de la U.

Palomino, F. (2023). *Protección al consumidor financiero: ¿Las controversias sobre atención de reclamos se deben resolver de manera conjunta entre SBS e Indecopi a través de grupos de trabajo para brindar una respuesta integral y especializada?* [Tesis de grado, Pontificia Universidad Católica del Perú]. Repositorio PUCP. Obtenido de http://hdl.handle.net/20.500.12404/24585.

Paragua, M., Bustamante, N., Norberto, L., Paragua, M., y Paragua, C. (2022). *Investigación científica. Formulación de Proyectos de Investigación y Tesis.* (M. PARAGUA MORALES, Ed.).

Paredes, E., y Silva, E. (2021). *Responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid19 en Lima-2020.* [Tesis de pregrado, Universidad Cesar Vallejo], Universidad Cesar Vallejo, Lima. Obtenido de https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/82463/Paredes_SES-Silva_REM-SD.pdf?sequence=1&isAllowed=y

Pérez, M. (2021). Ciberdelitos y responsabilidad civil de las entidades financieras a la luz de la jurisprudencia. *Revista de derecho del mercado de*

valores(29). Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=8263990.

Previti, L. (2023). A colaboración entre sector público e privado no sistema de seguridade cibernética: reflexións a partir da estratexia europea e italiana. *Regap, 65*(1), 105-123. doi:10.36402/regap.v1i65.5094.

Quiroga, J. (2021). Ciberseguridad y protección de datos personales en el Perú. *Advocatus*(39), 15-21. doi: https://doi.org/10.26439/advocatus2021.n39.5114.

Ramírez, J. (2023). *Modificación código penal sobre responsabilidad de terceros involucrados en ciberdelitos en entidades financieras - Corte Superior de Justicia - Piura - Periodo 2022.* [Tesis de grado, Universidad César Vallejo]. Obtenido de https://hdl.handle.net/20.500.12692/145157.

Raygada, M. (2023). Las garantías preferidas en la regulación bancaria. *Giuristi: Revista De Derecho Corporativo, 4*(8), 116-138. doi:https://doi.org/10.46631/Giuristi.2023.v4n8.06.

Resolución S.B.S 504 de 2021 [Superintendenta de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones]. (s.f.). Obtenido de Por la cual se aprueba el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad. 19 de febrero de 2021: https://intranet2.sbs.gob.pe/dv_int_cn/2046/v2.0/Adjuntos/504-2021.R.pdf.

Resolución SBS N° 02286-2024. (2024). *Modifican el Reglamento de Tarjetas de Crédito y Débito, el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, el Reglamento de Gestión de Conducta*

de Mercado del Sistema Financiero y el Reglamento de Reclamos y Requerimient.

Revilla, D., Rodriguez, D., y Mendoza, A. (2024). Importancia de la implementación de ciberseguridad en la gestión de riesgos financieros: Clave para garantizar la confianza del cliente. *Revista Científica Ciencias Ingenieriles, 4*(2), 74-82. doi:10.54943/ricci.v4i2.516.

Richards, N., y Hartzog, W. (2021). A Duty of Loyalty for Privacy Law. *Washington University Law Review, 961*. Obtenido de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217.

Rincón, F. (2023). *Delitos informáticos.* Ecoe Ediciones. Obtenido de https://books.google.co.ve/books?id=XujnEAAAQBAJ&newbks=1&newbks_redir=0&dq=delito+inform%C3%A1tico&source=gbs_navlinks_s.

Rodríguez, H., y Moreno, C. (2024). Seguridad de la información y ciberseguridad: su importancia para los Estados, empresas y las personas, una revisión sistemática. *Revista Científica y Académica, 4*(1), 159–178. doi:10.61384/r.c.a..v4i1.90.

Rosero, L. (2021). *El Phishing como riesgo informático, técnicas y prevención en los canales electrónicos: Un mapeo sistemático.* [trabajo de grado, Universidad Politécnica Salesiana]. Retrieved from https://dspace.ups.edu.ec/handle/123456789/21699.

Saenz, M. (2023). *Tres casos de phishing se detectaron en la primera semana del 2023*. Obtenido de https://rpp.pe/economia/economia/cuantos-casos-de-pishing-se-detectaron-el-2023-noticia-1458903.

Serrano, I. (2024). *Responsabilidad del banco en caso de phishing y medidas preventivas*. Obtenido de https://sellolegal.com/blog/responsabilidad-del-banco-en-caso-de-phishing-y-medidas-preventivas/.

Sihui, R., y Unchupaico, A. (2024). *Análisis jurídicode la incorporación de la responsabilidad penal de las entidades delsistema financiero frenteal fraude informático.* [Tesis de grado, Universidad Tecnológica del Perú]. Repositorio Institucional de la UTP. Obtenido de https://hdl.handle.net/20.500.12867/9406.

Silvestre, I., y Huamán, C. (2019). *Pasos para elaborar la investigación y la redacción de la tesis universitaria.* Lima: San Marco.

Superintendencia de Banca , Seguros y AFP. (2023). *Resolución SBS n° 02250-2023.* Retrieved from https://www.sbs.gob.pe/Portals/0/jer/RES_ADMIN/GPO/2023/02250-2023.pdf.

Tenorio, I. (2021). Aplicaciones de la Inteligencia Artificial en la Detección y Prevención de Amenazas Cibernéticas. *Technology Rain Journal, 1*(1), 1-11. Obtenido de https://www.researchgate.net/publication/380031301_Articulo_de_Investigacion_Original_Aplicaciones_de_la_Inteligencia_Artificial_en_la_Deteccion_y_Prevencion_de_Amenazas_Ciberneticas_Applications_of_Artificial_Intelligence_in_the_Detection_and_Prevent.

Tomalá, J. (2024). *Análisis de phishing y técnicas de ingeniería social: estrategias de concientización y prevención de ataques.* [tesis de

maestría, Universidad Estatal Península de Santa Elena]. Obtenido de https://repositorio.upse.edu.ec/handle/46000/12538.

Torres, A. (2023). *Responsabilidad administrativa de los bancos en los casos de phishing a propósito de las resoluciones brindadas por Indecopi.* Obtenido de http://hdl.handle.net/20.500.12423/6488.

Tribunal Constitucional. (2020). *Pleno. Sentencia 1100/2020.* Obtenido de https://tc.gob.pe/jurisprudencia/2020/01189-2019-HC.pdf.

Vargas, C. (2023). *Finanzas digitales: notas para la transformación digital en la industria bancaria y financiera.* CygnaP Ediciones de Negocios. Obtenido de https://books.google.co.ve/books?id=jzKxEAAAQBAJ&newbks=1&newbks_redir=0&dq=ciberdelito++phishing&source=gbs_navlinks_s.

Vazquez, A. (2021). Sistema para determinar si un mensaje corresponde a un ataque "phishing" o es "spam". Obtenido de https://oa.upm.es/68507/.

Vélez, S., y Reyes, M. (2023). La protección de los derechos de los consumidores en el Derecho Civil Ecuatoriano: Un análisis de su evolución y desafíos actuales. *MQRInvestigar,* *7*(4), 849–862. doi:10.56048/MQR20225.7.4.2023.849-862.

Viteri, J., Loachamín, S., Campaña, R., y Galarza, C. (2024). La apelación en procesos de defensa al consumidor y el derecho a recurrir. *Revista Ciencia UNEMI, 17*(44), 137 - 148. doi:10.29076/issn.2528-7737vol17iss44.2024pp137-148p.

Zhang, Y., Shao, Y., y Zhang, J. (2023). Challenges to Sustainable Development in China's Banking Industry: A Structural Equipment Modeling Approach for Fighting Phishing in China. *Public Organization Review*, 1-22. doi:10.1007/s11115-023-00713-5.