Universidad César Vallejo

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

La responsabilidad civil de las entidades financieras y de los usuarios afectados por phishing y sim swapping en el Perú

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogado

AUTORES:

Ferro Huayllacayan, Josue David (orcid.org/0000-0002-3294-030X)

Vega Orcon, Moises Alfredo (orcid.org/0000-0002-1270-8327)

ASESOR:

Mg. Guerra Campos, Jefferson Williams (orcid.org/0000-0003-0158-7248)

LÍNEA DE INVESTIGACIÓN:

Derecho de Familia, Derechos Reales, Contratos y Responsabilidad Civil Contractual y Extracontractual y Resolución de Conflictos

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía

LIMA - PERÚ

2023

Dedicatoria

A mi madre Gladys por motivarme a estudiar constantemente y no rendirme durante estos 11 años, especialmente a mis abuelos Filomeno y Fernandina que con ansias esperan mis logros en la eternidad, a mi hijo Joshua que le sirva de ejemplo que no hay límites para los sueños, a su madre Beatriz por tolerarme, comprenderme y ayudarme durante estos años. - Moisés Alfredo Vega Orcón

El presente trabajo va dedicado a nuestros padres, los cuales nos han brindado un total apoyo a lo largo del desarrollo de mi carrera tanto moralmente como económicamente, sin esta ayuda no podríamos ser quienes somos hoy en día. - Josué David Ferro Huayllacayan

Agradecimiento

A mi familia y seres queridos, compañeros de trabajo, amigos, profesores y familiares que a la luz de este trabajo esperan ya algunos en la eternidad y el apoyo incondicional de nuestros docentes de la Universidad César Vallejo- Lima este que nos inculcaron a lo largo de este tiempo, Es preciso mencionar nuestra institución mater la Universidad César Vallejo que nos permitió formarnos como profesionales

A los docentes que nos han brindado conocimiento a través de una ardua enseñanza, preocupándose por el futuro de su alumnado, además por su paciencia y comprensión que tuvieron con nosotros en diversas ocasiones, gracias a su guía en este tiempo en el cual se viene desarrollando mis estudios universitaria

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Autenticidad del Asesor

Yo, GUERRA CAMPOS JEFFERSON WILLIAMS, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, asesor de Tesis Completa titulada: "La responsabilidad civil de las entidades financieras y de los usuarios afectados por phishing y sim swapping en el Perú", cuyos autores son FERRO HUAYLLACAYAN JOSUE DAVID, VEGA ORCON MOISES ALFREDO, constato que la investigación tiene un índice de similitud de 11.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis Completa cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 08 de Julio del 2023

Apellidos y Nombres del Asesor:	**Firma**
GUERRA CAMPOS JEFFERSON WILLIAMS **DNI:** 71012547 **ORCID:** 0000-0003-0158-7248	Firmado electrónicamente por: JGUERRACA el 17-07-2023 18:44:17

Código documento Trilce: TRI - 0580669

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Originalidad de los Autores

Nosotros, FERRO HUAYLLACAYAN JOSUE DAVID, VEGA ORCON MOISES ALFREDO estudiantes de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, declaramos bajo juramento que todos los datos e información que acompañan la Tesis titulada: "La responsabilidad civil de las entidades financieras y de los usuarios afectados por phishing y sim swapping en el Perú", es de nuestra autoría, por lo tanto, declaramos que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. Hemos mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de la información aportada, por lo cual nos sometemos a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Nombres y Apellidos	**Firma**
FERRO HUAYLLACAYAN JOSUE DAVID **DNI:** 76670859 **ORCID:** 0000-0002-3294-030X	Firmado electrónicamente por: JFERROH7 el 02-08-2023 11:09:21
VEGA ORCON MOISES ALFREDO **DNI:** 47818719 **ORCID:** 0000-0002-1270-8327	Firmado electrónicamente por: MVEGAOR el 26-07-2023 18:48:20

Código documento Trilce: INV - 1335928

Índice de contenidos

Índice de tablas

Resumen

La concepción de esta investigación surgió a raíz de la crearon de plataformas virtuales y móviles por parte de las entidades financieras, para la atención de usuarios, quienes posteriormente fueron víctimas de los ciberdelitos denominados como *phishing* y *sim swapping,* que en la mayoría de casos no se determinó la responsabilidad por parte de las entidades.

Es de esta manera la presente investigación tuvo como objetivo general desarrollar la responsabilidad de las entidades financieras y los usuarios a través de los canales digitales en el Perú, es así que se desarrolló bajo el tipo básico, a su vez se tomó el tipo de enfoque cualitativo, por tal motivo el diseño que demandó fue el fenomenológico, la técnica aplicada fue la entrevista profunda en la que participaron 6 personas entre abogados, trabajadores activos y policía, la cual se reforzó con la aplicación de la guía entrevistas.

El cual concluyó determinando que existe una responsabilidad civil acreditada por parte de las entidades financieras al no tomar los protocolos de autenticación adecuados y no realizar un estudio periódico para la actualización de futuros ciberataques los no fueron regulados expresamente por la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.

Palabras clave: phishing, SIM swapping, seguridad, ciberataques, entidades financieras.

Abstract

The conception of this investigation arose as a result of the creation of virtual and mobile platforms by financial institutions, for the attention of users, who later became victims of cybercrimes known as phishing and sim swapping, which in most cases do not the responsibility of the entities was determined.

In this way, the present investigation had the general objective of developing the responsibility of financial entities and users through digital channels in Peru, so it was developed under the basic type, in turn the type of approach was taken qualitative, for this reason the design that I demand was the phenomenological one, the technique applied was the deep interview in which 6 people participated between lawyers, active workers and police, which was reinforced with the application of the interview guide.

Which concluded by determining that there is an accredited civil liability on the part of the financial entities for not taking the appropriate authentication protocols and not carrying out a periodic study to update future cyberattacks, which were not expressly regulated by the Superintendency of Banking, Insurance and Administrators. Private Pension Funds.

Keywords: phishing, SIM swapping, security, cyberattacks, financial entities.

I. INTRODUCCIÓN

El desarrollo tecnológico avanza a pasos agigantados a través del tiempo, desde la aparición de los ordenadores, qué se convirtieron en factor importante para mejorar aspectos cotidianos de la población; al inicio tenían como objetivo facilitar la correcta transmisión de información, actualmente siendo necesarios para el desarrollo del trabajo del ser humano, así como su interacción con otras personas; los cuales almacenan gran cantidad de información en memorias físicas y nubes virtuales. Tal es así que han sobrepasado la barrera de los ordenadores a los equipos móviles.

Es así como al avance de la tecnología y el uso habitual de las personas forzó a las entidades como los bancos, a buscar tener una llegada más cercana y común con sus clientes, es de esta forma que las personas realizaron sus operaciones bancarias por plataformas virtuales y aplicativos móviles y/o web, por ser estos los más fáciles de realizar sin moverte de tu domicilio, y así contrarrestar los asaltos y/o secuestros de los delincuentes.

Al presentarse dicha situación, ha provocado que los delincuentes adopten otras modalidades con respecto a cometer su actuar delictivo, en estos casos, valiéndose de diversos engaños o argucias, con el uso de programas inescrupulosos.

Es así que estos métodos delictivos cometidos, a través de internet, se consideran parte de los delitos informáticos, siendo una de estas modalidades del *phishing* (suplantación de identidad) y *sim swapping* (intercambio de tarjeta SIM en inglés). En la actualidad, se ha podido denotar el aumento de casos por estas modalidades, los cuales ha afectado a los clientes de entidades bancarias que denuncian estos hechos ante las entidades que velan por el resguardo de sus intereses, casos como el de mensajes engañosos con enlaces web simulando por una entidad financiera, cometen el error de ingresar datos y también la pérdida de señal de sus equipos móviles que posteriormente, observan reflejado en sus aplicativos el vaciado de sus cuentas. En el Perú, desde inicios del año y hasta julio, la Policía Nacional del Perú (PNP) recibió 1117 denuncias relacionadas al fraude informático, las cuales 974 fueron por transferencias electrónicas no autorizadas y 142 por compras fraudulentas (El Comercio, S.F.).

Pese a que el *phishing* es cada vez más recurrente en elactuar delincuencial al cometer estos delitos a través de aplicativos de banca móvil, en el ordenamiento jurídico peruano, se entendería que al momento de que se cometa este actuar delictivo mediante servicios de banca móvil o internet, con el cual presta servicio a su cliente, el banco debería responder de alguna forma ante el daño ocasionado debido a qué es mediante su servicio de banca móvil o internet qué fue vulnerada a través de una suplantación de identidad causándole un perjuicio hacia su cliente por lo que se tendrá que responder de alguna forma.

Mediante esta investigación, se identificará a qué nivel de respuesta tendrá que asumir el banco por los delitos cibernéticos cometidos mediante servicios de banca móvil o web. Asumiendo el problema general es el siguiente: ¿Cuál es la responsabilidad de las entidades financieras y los usuarios a través de los canales digitales en Perú en casos de phishing y sim swapping? Como problemas específicos se tiene: (a) ¿Cómo se relaciona la responsabilidad extracontractual de las entidades financieras en los casos de operaciones no reconocidas por usuarios a través de sus canales digitales y móviles?, y (b) ¿Cuáles son los niveles de seguridad que las entidades financieras utilizan para reconocer las operaciones fraudulentas o “no conocidas” por el usuario en sus canales digitales y móviles?

Por lo mismo, es evidente que la investigación es de interés académico, que busca dar un acercamiento teórico a las nuevas modalidades de ciberdelincuencia qué se viene desarrollando a través de las nuevas tecnologías que vienen siendo implementadas al uso cotidiano de los potenciales clientes, también denominados usuarios, los cuales convierten a dichas herramientas, potenciales blancos de ciberataques.

Por lo que, el enfoque teórico de la investigación, para un mayor reconocimiento y que aportará información sobre la identificación de las modalidades de ciberdelincuencia *phishing* y *sim swapping* y la implicancia de las entidades financieras ante el cometimiento de estás modalidades de ciberdelincuencia mediante sus servicios digitales, identificando si existe una responsabilidad por parte de las entidades financieras, ya que, como bien se sabe,

sus servicios digitales o banca móvil son los más usados al momento de cometer el hecho ilícito que es subsiguiente al acto de *phishing* y *sim swapping.*

Entre tanto, el punto de vista metodológico, es de enfoque cualitativo, por lo que la investigación se realizó mediante la realidad dinámica, la cual implica diversos contextos, por lo que se prima una indagación proporcional y juicioso de las categorías de la presente investigación, bajo un tipo de investigación básica, lo cual indica una problemática ya existente, además cuenta con un diseño de investigación fenomenológico, por lo que es primordial en el estudio de las experiencias de vida, respecto de un suceso controversiales, desde la representación, forma y disposición con las que observa el sujeto.

Según Husserl (1998), se usa de referencia para poder esclarecer la concepción de las cosas, la esencia y la veracidad de acontecimiento extraordinario. Lo cual sirve como objetivo para entender la experiencia vivida; siendo esta la forma de búsqueda para poder tomar conciencia y todo aquello que facilite la compresión del torno del fenómeno.

Siendo considerable para poder dar inicio a una investigación de este tipo de enfoque, es importante saber la concepción y los principios de la fenomenología, así como el método para abordar un campo de estudio y mecanismos para la búsqueda de significados.

Asu vez, el aspecto práctico de la investigación brindó resultados los cuales, aportaron en la obtención de información respecto a cuanta responsabilidad derivada tendrá estas entidades financieras sobre sus usuarios afectados por los ciberdelitos de *phishing* y *sim swapping,* Usuarios que en su mayoría desconocen cómo se desarrollan estas modalidades, además de ser susceptibles por su ineficaz nivel de seguridad que tienen las entidades financieras en sus servicios digitales que perjudican a ellos, haciendo mención de cómo se desarrolla la realización de esta modalidad. Por lo que, la investigación trata de presentar los aspectos de mayor relevancia, para que así, los usuarios de las entidades financieras que usen sus servicios digitales reconozcan y no sean víctimas de estas nuevas modalidades.

Es de esta forma, cómo objetivo general se planteó: desarrollar la responsabilidad de las entidades financieras y los usuarios a través de los canales

digitales en Perú. A esto se señalaron como objetivos específicos (a) identificar la relación de la responsabilidad de las entidades financieras en los casos de operaciones no reconocidas por usuario y entidades financieras, través de sus canales digitales y (b) identificar los niveles de seguridad que las entidades financieras utilizan para reconocer las operaciones fraudulentas o “no conocidas” por el usuario en sus canales digitales.

II. MARCO TEÓRICO

En la presente investigación se tomó en consideración diversos trabajos previos, de los cuales se seleccionaron tres trabajos de nivel internacional y tres trabajos de nivel nacional, que tuvieran mayor relación con la problemática y objetivos de la investigación.

En el ámbito internacional, Fernández (2020) en su ensayo planteó como objetivo general: Definir que responsabilidad tiene la entidad bancaria ante fraudes electrónicos para proponer estrategias que sirvan a la par del trabajo del auditor, en la identificación inmediata de aquellas fallas en las controversias surgidas por fraude electrónico, en las que se implican el compromiso de la entidad. Para el cual, aplicó la metodología cualitativa. Concluyó, que estas entidades deben asumir las pérdidas por los fraudes que se realizan en sus plataformas y restituirles por el daño económico perpetrado a sus clientes, por la ineficiencia de su servicio.

Por tanto, Hidalgo (2018) planteó como objetivo general: Estudiar las 7 riquezas legales como tema de fondo constitucional y social, su incidencia en los delitos informáticos con la finalidad de determinar su importancia a la indagación, y en la conjetura de la conformación de un delito. Para lo cual aplicó la metodología cualitativa. Obtuvo como resultado lo siguiente: resultando ocasionalmente ineficiente y no llegando a custodiar el bien jurídico del que se infiere de esta discusión. Por tal motivo, concluyó que observar la fenomenología de envergadura penal, ya sea, aumento desmesurado de estos hechos, lo cual implica a que los magistrados enmarquen nuevas normativas en las cuales se contextualizan los nuevos hechos fraudulentos de índole penal.

Salas (2017) planteó como objetivo general: Revisar la objetividad nacida de la responsabilidad de la obligación civil acarreada de las entidades que forman parte de la Superintendencia de Banca, Seguros y AFP, en la situación en que uno de sus consumidores sea atacado fruto de un delito informático. Para lo cual aplicó la metodología cualitativa. Concluyó que la responsabilidad civil objetiva, el cual tiene por finalidad reparar el daño que como efecto del delito informático permanezca alejada de la esfera de responsabilidad civil subjetiva. De esta forma deberá encontrar el completo amparo legal para todos los escenarios que generen afectación y deban ser restablecidas.

De la Cruz (2021) planteó cómo objetivo general el siguiente: Establecer que aquellas transacciones financieras realizadas mediante el canal wed articulan con la responsabilidad civil de diversas entidades financieras en la ciudad de Huaura - Huacho del año 2018. En esta investigación se aplicó el enfoque mixto. Concluyendo la investigación lo siguiente, el dilema sobre la responsabilidad de la entidad financiera, respecto al usuario, por delitos informáticos es un tema peculiar para nuestra doctrina y la jurisprudencia nacional, siendo inevitable el analizar en conjunto diversas ramas del derecho que tienen relación, de modo que, rodea el conflicto, muestra datos sobre el banco o el sistema financiero el cual en la actualidad no brinda las garantías correspondientes a favor de sus usuarios.

Por otro lado, Vigo y Zavala (2021) plantearon como objetivo general: Examinar el fruto que produce inoperancia de la administración legal en relación a la protección a los sujetos pasivos afectados por phishing en las entidades financieras en Lima en año 2020. En la cual se aplicó el enfoque el cualitativo. Concluyendo en que existe una vulneración al resguardo de los afectados por *phishing* en las entidades financieras junto a una escasa normatividad, todo esto debido a que el proceder sobre el ilícito de *phishing* afecta a la masa económica de la víctima, quien es aquella que adolece debido al agravio económico cometido por el delito informático, el cual ocasiona el *Phisher* mediante su actuar malicioso generando cuantiosas pérdidas económicas mediante el uso de su saber tecnológico, por lo que, la víctima sufre una victimización al no tener conocimiento tecnológico para poder así señalar aquellos portales webs maliciosos, lo que a su vez crea una necesidad de reconocer los tipos de afectados para realizar una investigación eficiente.

A esto, el Estado es quien debe ofrecer resguardo jurídico sobre las víctimas, a través de sus operadores que administran justicia, con lo cual brinda soporte a las víctimas sin vulnerar su derecho a la obtención de justicia, sin embargo, en muchas ocasiones existen diversas limitaciones en la investigación lo cual obstruyen en lograr una sanción efectiva, quedando el ilícito impune.

Zambrano (2021) planteó como objetivo general: Precisar si el uso de banca móvil fomenta y a su vez crea vulnerabilidad ante los delitos informáticos que a la par afectaron el patrimonio en la ciudad de Arequipa. En ese sentido,

aplicó la metodología cualitativa. Concluyó al ser los aplicativos móviles de fácil acceso, ocasiona que los ciberdelincuentes se aprovechen y obtengan información personal sobre el acceso a la banca móvil de los usuarios financieros, inclusive en momentos donde no contaban con el aplicativo móvil instalado en sus dispositivos, siendo estos afiliados sin su consentimiento y, claro está, con aprobación de quienes administran estas aplicaciones móviles, además de las entidades financieras que poseen su información bancaria de sus usuarios.

En consecuencia, respecto a los enfoques conceptuales presentados, permitió tener mayor información respecto a los delitos informáticos cometidos, a través de los medios digitales de las entidades financieras, los que vulneran actualmente con mayor ocurrencia al momento de sustracción de la información personal y financiera, cuyas víctimas son personas con poco conocimiento de las modalidades de ilícitos informáticos. De ahí, se entiende la responsabilidad administrativa en que se le relaciona a las entidades financieras cómo aquellas que demuestran poco interés hacia sus usuarios, ya que, le es más factible el seguir ofreciendo servicios cuando son afectados por esta modalidad ocasionándole un perjuicio económico una vez identificado el daño.

Teniendo en cuenta los antecedentes mencionados, se deberán conceptualizar las siguientes categorías: La responsabilidad civil, entidades financieras, usuarios y modalidades *phishing* y *sim swapping.*

En relación a la categoría de la responsabilidad civil, se define estando sujeto a la obligación, siendo esta, como efecto: el responder, resarcir, reparar o recuperar lo que sea dañado a su estado inicial.

Según León (2017), la responsabilidad civil es definida como aquella situación en la que el sujeto afrontará consecuencias perjudiciales a raíz de sus acciones.

También, Ayala (2017) en su tesis, definió que la responsabilidad civil es aquella obligación de resarcir un daño ocasionado de una acción que necesariamente tendrá que ser de índole patrimonial o extrapatrimonial.

Teniendo en cuenta que la responsabilidad se encuentra normada en el Código Civil peruano del año 1984 en sus artículos 1969 y 1970 en el que se definen como se configuran de manera subjetiva y objetiva.

De esta manera, Zabala (2017) indicó que el Estado en caso del sistema financiero y bancario se enfrenta a una responsabilidad objetiva, la cual, tendrá que proporcionar soluciones equitativas a los involucrados.

Es de esta manera, que la resolución Nº 3412-2018/SPCINDECOPI en la que se resolvió que la falta de comunicación de la entidad financiera, por servicios brindados, correspondían a la falta de medidas de seguridad y prevención ante cualquier siniestro, tal es así que ordenó al banco responder por dicha falta con un resarcimiento de la pérdida económica y la medida correctiva para su mejora normativa.

A su vez la subcategoría de entidades financieras, se conceptualiza según la Superintendencia de Banca, Seguros y AFP, la cual determina que son entidades que recibe el dinero de muchas personas y lo presta para negocios o proyectos personales.

Es así que, las entidades financieras son reguladas bajo la Ley nº 26702 titulada como Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, la cual regula a las siguientes entidades:

- Superintendencia de Banca, Seguros y AFP (SBS)
- El Banco Central de Reserva del Perú (BCRP)
- La Superintendencia del Mercado de Valores (SMV)

Es así que, la tercera categoría denominada usuarios, se define según Pablo Elías Maza quien es funcionario del Ministerio de economía y finanzas que a la par forma parte de la Contaduría Pública de la Nación, formando parte como catedrático Asociado en la Universidad Nacional Federico Villarreal, “… es el ciudadano de a pie, los electores y sus representantes …”

A su vez, los usuarios se encuentran protegidos por la Defensoría del Cliente Financiero (DCF) la cual está relacionada con la Asociación de Bancos del Perú Asbanc, además que, esta es parte del Instituto Nacional de Defensa de la

Competencia y de la Protección de la Propiedad Intelectual, quien lo define como consumidor financiero.

Asi mismo, se tiene una cuarta categoría denominada *PHISHING* y *SIM SWAPPING*, ambas son modalidades ilícitas, de las cuales, los ciberdelincuentes obtienen la información de los usuarios de entidades financieras para subsecuentemente cometer el delito con estos datos receptados en perjuicio de estos.

Sobre esto, Rosero (2021) mencionó sobre el *phishing* como secuela de un ataque de ingeniería social, que tiene como objetivo obtener atribuciones consecuencia de las debilidades que figuran en las etapas del sistema y que están fomentados por los consumidores del sistema.

Entonces, para que el *Phishing* pueda dar efectos tiene que haber intervención del usuario de la entidad financiera brindando sus datos, esto mediante astucia y engaño es inducido a consignarlos sin conocimiento del para qué van a ser utilizados.

Siguiendo con la cuarta categoría, según Albors (2020) concluyó, el *SIM swapping* es una modalidad de defraudación que permite a los criminales suplantar tu identidad por medio de la apropiación del número de teléfono al conseguir una reproducción de la tarjeta *SIM*.

A su vez, la subcategoría de las modalidades antes mencionadas *Phishing* y *Sim Swapping*, se tomó en cuenta su evolución en el tiempo, lo cual según Romaña (2022) indicó lo siguiente:

> Este problema actualmente es uno de los más preocupantes y críticos por los que confrontan al sistema regulatorio ya que si no se establecen las medidas de prevención y bloqueo respectivas estamos hablando que este tipo de actividad criminal se incrementara y vulnerara la seguridad de información de miles de usuarios, es por ello la razón de grado de importancia de normar este tipo de conductas y establecer sus medios de defensa frente a estas conductas (p. 51).

En lo que respecta al ordenamiento normativo peruano, correspondiente a estas modalidades de delitos informáticos o ciber delitos, no están regulando de

forma objetiva teniendo un artículo específico, pero están inmersos en las definiciones qué tiene la Ley n° 30096 en la cual, el artículo 2° establece lo siguiente:

> El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado (p. 3).

Entonces sobre la jurisprudencia en los casos de modalidades de ciberdelitos *Phishing* y *Swim Swapping;* Hidalgo (2021) mencionó que existe una ausencia sobre jurisprudencia en delitos informáticos, ya qué, la Ley nº30096 no es específica, más bien, toma un entorno general dificultando la labor de los operadores del derecho del Perú al impartir justicia.

Ante esto, existe una gran falta de jurisprudencia respecto a estas modalidades de ciberdelitos, todo esto que, a su vez no existe una tipificación objetiva en la ley, que corresponde a los delitos informáticos, sobre las modalidades antes mencionadas denotando una clara inexactitud sobre las sanciones de estos delitos.

.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

Este trabajo fue desarrollado basándose al tipo de investigación básica, siendo esta que se aplicó el tipo de enfoque cualitativo, por lo que la naturaleza de este demandará el diseño que es fenomenológico.

3.1.1. Tipo de investigación

Siendo así, se determinó que el tipo de investigación tendría que ser básica, Tam et al. (2008) mencionaron que los resultados de la investigación arribarán conceptos nuevos a nuestra realidad, que no necesariamente serán aplicados de manera inmediata.

Navarro (2016) resaltó que el aporte de teorías innovadoras, podrán mejorar la modificación de las normas actuales enriqueciéndose con la experiencia de otras legislaciones relacionadas con la misma problemática, que es de interés para esta investigación.

En cuanto al enfoque que se trabajo es el cualitativo, para lo cual, Flick (2015) enfatizó, que, en el proceso de investigación, los investigadores desde su experiencia personal a la vez de sus vivencias de campo y reflexividad que aportan a partir de la función que desempeñan, son de suma importancia en su investigación.

Según Hernández y Mendoza (2018), al momento en el que se realizó la búsqueda de información y datos que aporten a la solución de la problemática discutida, mediante un proceso de inducción, el cual, constituye el aporte de conocimiento, opiniones y argumentos de especialistas en la materia, se sabe que se está trabajando con un enfoque cualitativo.

3.1.2. Diseño de investigación

Es así que, al enfocarse cualitativamente, la problemática de este trabajo, amerita que su diseño sea fenomenológico, es así que, Palacios y Corral (2010) manifestaron que es muy importante mantener la congruencia entre la orientación cualitativa, es así que es relevante el posicionamiento que el investigador fije al iniciar, frente al fenómeno que se estudia, de tal manera que su forma de pensar o criterio no afecte el desarrollo.

Así, también Hernández, et al. (2014) expresaron, como los diversos acontecimientos son de estudio infinito, por lo que se puede obtener todo tipo de emociones, experiencias, razonamientos o percepciones, es decir, puede vincularse en el estudio de aspectos del día a día como también en fenómenos poco usuales.

3.2 Categorías, subcategorías y matriz de categorización

Tabla 1

Matriz de categorias

CATEGORÍA	SUBCATEGORÍA	CRITERIO 1	CRITERIO 2
La responsabilidad civil de las entidades financieras	*Responsabilidad civil*	*Normativa civil*	*Jurisprudencia*
	Entidades financieras	*Normativa*	*Entidades reguladoras*
Los usuarios afectados por phishing y sim swapping	*Usuarios*	*Entidades protectoras*	
	Phishing y sim swapping	*Evolución*	*Normativa penal*

3.3 Escenario de estudio

Siendo esta investigación una problemática actual y controversial, que surgió con mayor énfasis a partir de la implementación de canales digitales para un mejor acceso, dado que, en estos momentos se está regresando de una normalidad post pandemia, ésta se desarrolla en ámbito nacional, el Perú, ya que este es uno de los países que tienen escasa regulación normativa, aumento de casos a nivel nacional y el desconocimiento de gran parte de la población en relación a esta problemática.

3.4 Participantes

Los individuos a formar parte de esta investigación serán 6 personas de nacionalidad peruana que cumplan el siguiente perfil:

- Personas que se encuentren laborando en entidades bancarias
- Personas que hayan formado parte del área de seguridad cibernética o afines

- Personas con título de abogado con conocimientos en materia civil o procesos Indecopi y Osiptel.

Tabla 2

Tabla de participantes

PARTICIPANTES	CENTRO DE LABORES	PROFESIÓN	CARGO
P.C.M.	*CAJA LOS ANDES*	*ADMINISTRADORA*	*GERENTE DE AGENCIA*
E.Q.R.	*FINANCIERA COMPARTAMOS*	*ADMINISTRADORA*	*GERENTE DE AGENCIA*
G.S.V.	*TAILOY*	*POLICIA (RETIRO)*	*JEFE DE SEGURIDAD*
L.M.L.	*CMAC PIURA SAC.*	*ABOGADO*	*ASESOR LEGAL*
L.F.F.	*UNIVERSIDAD CESAR VALLEJO*	*ABOGADO*	*DOCENTE*
L.M.V.	*UNIVERSIDAD CESAR VALLEJO*	*ABOGADO*	*DOCENTE*

3.5 Técnicas e instrumentos de recolección de datos

La técnica utilizada fue el de la entrevista profunda, ya que, el tema de materia de investigación lo exigió por el tipo de problemática que se discutió.

Es así que, Arias (2016) afirmó que es una de las formas de comunicación interpersonal, su objetivo es proporcionar o decepcionar datos de suma importancia, los cuales serán discutibles al momento de decidir.

Además, Sullivan (1977) expresó, que la entrevista es la comunicación vocal de 2 personas a más, que participan voluntariamente, para de esta manera obtener la experiencia de vida del sujeto, de las cuales servirán para obtener de información valiosa y de relevancia para obtener un beneficio.

La guía de entrevista fue el instrumento el cual fue de uso en esta investigación, en ese sentido Hernández y Mendoza (2018) definieron como el conjunto de recursos (items) que serán de utilidad para los investigadores, con las que obtendrán información.

3.6 Procedimientos

La presente investigación dio como resultado necesario la utilización de la Entrevista como técnica a proceder, es de esta forma que Trujillo et al., (2019) señalaron que la preparación de la ficha es anticipada, estructurando este por medio de preguntas fijas y ordenadas que permiten la consolidación de todos los criterios.

Es así que al hacer uso de la técnica de entrevista, los investigadores harán uso de un documento, el cual será brindado a los entrevistados qué con previo comunicación se les dará una idea sobre su contenido y se pedirá su previo consentimiento, en los cuales deberán responder sobre sus conocimientos del tema.

Además de esto, se le indicó en todo momento que se desarrolla la entrevista que la información que se recopila será específicamente usada para temas académicos.

3.7 Rigor científico

Reedificando los acontecimientos de estudio como objeto para el resultado, siendo este resguardado para la ejecución de las normas y reglas científicas para que el resultado sea fiel a la realidad en lo posible. (Espinoza y Toscano, 2015)

El presente trabajo se realizó con rigor científico, todo esto debido a que contiene fuentes de información recopiladas de diversas revistas científicas, artículos científicos. Siendo que todo esto va realizarse mediante etapas que constan a un procedimiento, a lo que Espinoza (2020) definió como una contribución hacia la garantía de la calidad de los datos, su representatividad, fiabilidad y validez; lo cual demanda del investigador el dominio de cada uno de los diferentes métodos, técnicas y procedimientos existentes para el registro, procesamiento y análisis de los datos de las diversas metodologías empleadas en los procesos investigativos cualitativos.

3.8 Método de análisis de la información

Vera (2010) menciono sobre el análisis lo siguiente Todo el análisis y elaboración de la información de los datos obtenidos, son la llave en una investigación cualitativa, en la cual se puede hablar de un proceso cíclico inserido en todas las

etapas de investigación, y que tiene com objetivo, contestar, triangular y validar todo el estudio obtenido para establecer en referencias los objetivos de la investigación.

La presente investigación se realizo con los siguientes métodos aplicados según su naturaleza:

Según Ramos (2018) el método sociológico; es aquel que se entendió a partir del comportamiento de la sociedad en su entorno de como se ha desarrollado a través de lo largo de su historia, lo cual da múltiples posibilidades al investigador de observar desde primera línea las vivencias, lo cual le permite dejar de lado tecnología para poder evidenciarlo desde primera persona.

Según Ramos (2018) el método de la *ratio legis* el cual permite dar un punto de vista desde la realidad lo cual permite relacionarla con la convivencia social para el mejor desarrollo de la interpretación de los sucesos con la normativa actual y poder relacionarla con los acontecimientos.

3.9 Aspectos éticos

El presente trabajo de indagación se rige a los siguientes principios éticos:

El principio de beneficencia se entiende como el deber de no afectar a terceros, buscar la minimización del daño y maximización de beneficios, a lo cual exige un análisis minucioso de riesgos y de aquello que beneficie a los sujetos participantes de la investigación. (Campi, 2019)

El principio de no maleficencia se refiere a la responsabilidad de prevenir que se concrete el daño a otros, es un principio esencial de la ética médica y forma parte del juramento hipocrático. (Sánchez, 2009).

El principio de autonomía se refiere a la ética que representa el respeto a la autonomía de los sujetos que puedan ser incluidos y afectados por su participación directa en un estudio o intervención de carácter científico. (Valdés, 2011).

El principio de justicia esta referida a la distribución de los participantes en esta investigación, siendo de esta forma que permita que las cargas y los beneficios estén compartidos en forma equitativa. (Nuñez, 2012).

Es de vital importancia, manifestar que también se consideró en este trabajo el Código de ética en la investigación de la Universidad César Vallejo, en

sus artículos 15 “sobre la política antiplagio”, 16” sobre derechos de autor”, y 17 “sobre del investigador principal y personal investigador”, así mismo el uso del software TURNITIN y el manual APA vigente.

IV. RESULTADOS Y DISCUSIÓN

RESULTADOS

1. Desde su realidad, ¿En algún momento ha recibido información sobre el phishing y sim swapping de manera física por parte de los bancos? Comente.

Tabla 3

Pregunta n.° 1: respuestas

Entrevistado	Respuesta de la pregunta n.° 1
P.C.M.	Si, correcto en efecto he recibido información por el área de seguridad de la información.
E.Q.R.	Si, en distintas capacitaciones de manera trimestral.
G.S.V.	No, nunca he recibido esa información de manera física, tengo conocimiento de estos delitos por los medios de comunicación de señal abierta y por internet.
L.M.L.	Como colaboradora de una institución financiera, recibimos capacitación respecto a los delitos informáticos que se originan en la banca.
L.F.F.	No, el banco lo que hace es mandar por correo información con respeto que debemos mantener nuestras cuentas con códigos y cada cierto tiempo cambiar nuestras claves, o en su defecto informar que jamás por correo o vía telefónica nos pedirían claves.
L.M.V.	No. La única información que he recibido es que puedo adquirir un seguro en caso de robos.

Tabla 4

Pregunta n.° 1: análisis

Convergencia	Divergencia	Interpretación
Es correcto afirmar que en algún momento se recibió información, siendo esta en forma, trimestral o mediante capacitación por el área de seguridad de la información siendo esta referente al tema de delitos informáticos, siendo los beneficiados aquellos que se encuentra relacionado al ámbito del sistema financiero.	De la misma forma, se debe entender que no todos recibieron la información de manera directa siendo esta por correos electrónicos los cuales no son de lectura inmediata o de poca relevancia, hasta en algunos casos esta fue brindada por otros medios que no están relacionados al sistema financiero.	Es así que se afirma que la información brindada acerca del phishing y swapping fue dada de manera exclusiva, periódica y mediante capacitación a aquellos que se encuentran laborando en entidades financieras. Siendo lo contrario que aquellos que no laboran en entidades bancarias, no fueron concientizados de manera inmediata, exclusiva, personalísima y en algunos casos de manera indirecta acerca del phishing y swapping.

2. ¿Conoce usted que es un canal de atención digital, phishing y sim swapping? Fundamente su respuesta.

Tabla 5

Pregunta n.° 2: respuestas

Entrevistado	Respuesta de la pregunta n.° 2
P.C.M.	Si, claro un canal digital es la banca por internet o una aplicación de banca móvil.
E.Q.R.	Son tipos de métodos que se están utilizando para realizar fraudes.
G.S.V.	Pienso que el canal de atención digital del banco para atender estos casos, son los del aplicativo o telefónico, desconozco si hay un canal exclusivo para atender estos casos.
L.M.L.	En la actualidad, las empresas del sistema financiero han implementado canales electrónicos para la atención de requerimientos de los usuarios o consumidores cuando sufren algún delito electrónico sobre sus cuentas.

L.F.F.	Por mi carrera conozco los términos, para canales de atención digital por lo general los encuentro en la banca por internet y por ahí me informo sobre ello
L.M.V.	No, la única información que tengo es que hay un número para enviar reclamos o sugerencias al banco, pero no sobre problemas de phishing o swapping.

Tabla 6

Pregunta n.° 2: análisis

Convergencia	Divergencia	Interpretación
Es claramente entendible el concepto básico de lo que se conoce como canal digital, como un elemento virtual de atención al público y que a su vez se relaciona con los aplicativos móviles, y que estos son a la vez medios de solución en casos de delitos informáticos.	Siendo deducible que no se tiene un concepto exclusivo para poder determinar que es el phishing y sim swapping, que algunos tienen conocimientos generales de lo que significan los cuales fueron obtenidos por otros medios que no están relacionados directamente por una campaña de concientización eficaz de alguna entidad financiera.	Los conceptos como canal digital, phishing y sim swapping no son del todo conocidos. Claramente el concepto de canales digitales se conoce como medios virtuales de atención al usuario y que también son presentados como aplicativos móviles. En cambio, los conceptos como phishing y sim swapping no son reconocidos de manera explícita, no se conoce su procedencia, ni tampoco su forma actuar, siendo este el concepto que tienen de estos son solamente fraudes. Es de esta manera que la información acerca de canales digitales, phishing y sim swapping no son proporcionados directamente por una campaña de concientización de alguna entidad financiera, sino también por los medios de comunicación.

3. Según su criterio, ¿Qué responsabilidad tienen los bancos al obligar el uso de un determinado canal de atención para un servicio en relación casos de phishing y sim swapping?

Tabla 7

Pregunta n.° 3: respuestas

Entrevistado	Respuesta de la pregunta n.° 3
P.C.M.	Considero que no es una obligación, si no una facilidad para facilitar las operaciones.
E.Q.R.	Los bancos no pueden obligar a tener algún servicio que no sea necesario para el cliente.
G.S.V.	Según mi criterio debería haber diferentes canales mediante los cuales se puedan denunciar estos hechos y no un canal exclusivo, ya que cuanto más rápido se pueda denunciar un delito de esta índole es mejor para poder bloquear las cuentas y adoptar medidas.
L.M.L.	En este caso, no considero que las empresas del sistema financiero tengan alguna responsabilidad sobre el procedimiento que establecen para que un consumidor informe sobre algún delito informático. En la Actualidad, las empresas del sistema financiero establecen procedimientos para que los consumidores presenten un reclamo o se comuniquen a través de las centrales de atención a fin de informar los hechos delictivos y también se encargan de informar a sus consumidores los protocolos de seguridad que utilizan para estos casos.
L.F.F.	Los bancos tienen responsabilidad porque son ellos quienes deben cuidar nuestra información y tener software adecuados de protección y evitar ser hackeadas.
L.M.V.	Es obligatorio que los bancos cuenten con un canal para este tipo de casos; con personas especializadas en esta clase de problemas, y puedan ser capaces de brindarle una solución a los clientes.

Tabla 8

Pregunta n.° 3: análisis

Convergencia	Divergencia	Interpretación
Los bancos no son responsables del uso de sus canales de atención por parte de los usuarios, ya que no obligan a estos a utilizarlos, actualmente, las empresas del sistema financiero establecen procedimientos para que los consumidores presenten un reclamo o se comuniquen a través de las centrales de atención a fin de informar los hechos delictivos y también se encargan de informar a sus consumidores los protocolos de seguridad que utilizan para estos casos.	Si, hay responsabilidad porque deben de brindar la protección adecuada para el uso de su canal de atención ya que estos vuelven vulnerable a los usuarios ante casos de phishing y sim swapping, a la vez debería de haber diferentes canales mediante los cuales se puedan denunciar estos hechos y no un canal exclusivo, ya que cuanto más rápido se pueda denunciar un delito y de esta forma poder adoptar medidas más eficaces.	Los canales de atención son medios implementados por los bancos para facilitar diversas operaciones, los cuales no obligan a los usuarios a su uso, desde ese punto de vista no presentan una obligación, pero al no presentar los criterios de seguridad adecuaos son vulnerables a cualquier ataque. Actualmente hay procedimientos para que los consumidores presenten un reclamo o comuniquen de estos hechos delictivos para tomar las acciones del caso, lo cual representa que hay canales de atención inmediatos y de uso exclusivo que deberían atender las 24 horas y no ser maquinas automatizadas porque cada caso es particular y no igual.

4. En su opinión, ¿Qué tanta responsabilidad tiene los usuarios, al usar canales de atención digitales que los vuelven vulnerables ante los casos de phishing y sim swapping?

Tabla 9

Pregunta n.°4: respuestas

Entrevistado	Respuesta de la pregunta n.° 4
P.C.M.	La responsabilidad es compartida tanto el banco como el cliente, el banco brinda las medidas de seguridad y el cliente no debe compartir sus claves.
E.Q.R.	Los usuarios deben tener cuidado con las tdo, correos y aplicaciones, ya que colocar contraseñas básicas hace que sea vulnerables,

G.S.V. La responsabilidad del usuario es mínima ya que está sujeta a que tanto sabe de la comisión de estos delitos y el banco debe ser responsable ya que es el que brinda un servicio a sus usuarios.

L.M.L. En este caso, considero que los consumidores deben estar muy atentos con la información que comparten a través de los teléfonos móviles ya que la mayoría de casos que se han reportado sobre este delito ha sido por el uso del teléfono móvil del consumidor.

L.F.F. Considero que los usuarios no deberían tener responsabilidad pues en muchos casos se paga seguros para evitar estas situaciones y además se confía en la seguridad que debe tener el banco.

L.M.V. Tienen responsabilidad muy grande, pues actualmente los delitos informáticos están a la orden del día y siempre se ve en las noticias información sobre eso. Es por eso que deben entender que realizar compras por internet en sitios web de dudosa reputación, puede provocar robos sistemáticos a sus cuentas bancarias.

Tabla 10

Pregunta n.° 4: análisis

Convergencia	Divergencia	Interpretación
Los usuarios son responsables por su navegación en los canales de atención ya que no toman las medidas de seguridad adecuadas para su uso, a la vez estos se vuelven vulnerables ya que proporcionan información de manera muy indiscriminada a cualquier aplicación o mensaje que los persuada.	La responsabilidad debe ser mínima ya que los usuarios, tienden a tener plena confianza con los canales de atención que brindan los bancos y con los mecanismos de seguridad que estos ofrecen en los aplicativos, y también en la seguridad de sus seguros de paga que algunos usuarios solicitan para la protección de su dinero.	Los usuarios son responsables de las acciones que realicen y a la vez son conscientes de proporcionar información secreta para su autentificación. La gran mayoría se siente seguro en la navegación en estas paginas web y aplicativos móviles, por lo tanto, las medidas de seguridad no son plenamente seguras si no en todo caso vulnerables a ciber ataques, lo que demuestra que el uso de autentificación mediante datos personales que utiliza los bancos no es seguro si no vulnerable.

5. Según su experiencia, ¿Qué tipo de responsabilidad tienen los bancos al no brindar un informe detallado de sus movimientos de los usuarios de manera inmediata, cuando suceden casos de operaciones no reconocidas en sus canales digitales?

Tabla 11

Pregunta n.° 5: respuestas

Entrevistado	Respuesta de la pregunta n.° 1
P.C.M.	Actualmente si se genera una alerta después de cada operación, considero que todos los bancos deben implementar esta acción,
E.Q.R.	A mi experiencia siempre se ha detallado las solicitudes de los clientes es decir si solicita su EECC. (estado de cuenta) siempre se le da la información.
G.S.V.	La responsabilidad de la entidad bancaria es absoluta y para ello INDECOPI debe de velar por el consumidor (cliente), lamentablemente se debe aprobar un procedimiento simple y único que sea inmediato, sin tanta burocracia.
L.M.L.	Considero que las instituciones financieras si tienen un deber de informar a los consumidores sobre las operaciones inusuales o en caso que el consumidor lo requiera de atender a la brevedad los requerimientos de información sobre las operaciones que se realicen sobre sus cuentas, a fin de no generar perjuicio a sus clientes.
L.F.F.	Toda la responsabilidad, pues actualmente los bancos informan mediante correo ante cualquier movimiento, si esto no sucedería pues genero los hurtos informáticos.
L.M.V.	Tiene responsabilidad total, ya que muchas veces se malentiende como que el banco no se quiere hacer responsable de los problemas de estas operaciones y es por ello la vista tan negativa sobre los bancos.

Tabla 12

Pregunta n.° 5: análisis

Convergencia	Divergencia	Interpretación
Las entidades financieras tienen responsabilidad por no brindar los elementos necesarios, inmediatos y simples para que se pueden evitar perjuicios de gran pérdida económica del cliente y a su vez con el apoyo de INDECOPI para la defensa del consumidor.	La medida de seguridad optada por las entidades financieras en algunos casos en brindar una alerta después de cada movimiento de dinero en sus cuentas, y claramente estas brindan EE.CC. (estado de cuenta) el cual es detalla todos los movimientos realizados desde esa cuenta de manera física y digital, es claro determinar que las entidades financieras informan de forma automática y a pedido del cliente para evitar perjuicio alguno que afecte su economía.	La responsabilidad de los bancos es inminente al no brindar información de manera inmediata ya que no todas las entidades practican el método de seguridad como alerta mediante un mensaje demostrando de esa manera que estas no son obligadas por norma específica, de esta forma también debemos reconocer al usuario como un consumidor y por ende hay un código del consumidor que exige la protección por el servicio brindado. Por ende, los bancos son responsables y las medidas de seguridad optadas no son eficientes en todos los casos, solamente son un mecanismo de protección ante una inminente responsabilidad acarreada hacia los bancos.

6. En su opinión, ¿Cree que los bancos tienen responsabilidad por el uso de sus canales digitales, en los casos de operaciones no reconocidas? Fundamente su respuesta.

Tabla 13

Pregunta n.° 6: respuestas

Entrevistado	Respuesta de la pregunta n.° 1
P.C.M.	Si tienen responsabilidad cuando los controles no son suficientes para evitar este tipo de operaciones no reconocidas.
E.Q.R.	Creo que todos los bancos deben reforzar sus medidas de seguridad tecnológica.
G.S.V.	Pienso que la responsabilidad siempre debe ser del banco ya que como cualquier negocio o de servicios, el cliente debe tener todas las facilidades para poder agilizar y recuperar su dinero por ser víctima de este tipo de delitos.

L.M.L.	En este caso, considero que el Banco tiene responsabilidad siempre que no cumpla con informar al consumidor sobre las operaciones que se realicen en sus cuentas y siempre que esta información sea atendida en el plazo legal que establece el Código de Protección al Consumidor.
L.F.F.	Lo que sucede que estas personas copian todo el formato del banco, por eso es importante que los bancos busquen siempre actualizar sus canales digitales y si encuentran o ven movimientos inusuales, a monederos digitales con transferencias altas retener el movimiento.
L.M.V.	Lo que sucede, es que en algunas ocasiones algunas operaciones demoran en aparecer en sistema, entonces es problemático porque al no aparecer en el momento, no hay facilidad para poder denunciar apropiadamente el hurto, hasta 2 o 3 días después.

Tabla 14

Pregunta n.° 6: análisis

Convergencia	Divergencia	Interpretación
Se reconoce que los bancos son responsables por el uso de sus canales de atención digitales tanto como en los canales móviles ya que un mucho hecho suscitado se ve el pobre nivel de seguridad que estos brindan para la protección, ya que en la mayoría de casos se observa la poca inversión de nuevos sistemas de seguridad como hardware sofisticados para la protección e identificación de los usuarios.	Los controles de seguridad deben de ser los mas eficientes para poder evitar posibles e inminentes ciber ataques y operaciones no reconocidas por los usuarios.	Es determinante reconocer que los bancos son responsables en el uso de sus canales digitales en los casos de operaciones no reconocidas, de esta manera es deducible que no hay una norma que especifique el cambio periódico de sistemas de seguridad digital, de la misma manera no implementación ni inversión de parte de estos en defensa y protección de sus consumidores que en futuro siempre creara desprotección de estos usuarios siendo afectados económicamente que a la par crearan mas procesos legales y problemas para las entidades financieras.

7. Según su criterio, ¿Por qué los usuarios en general son blanco de las operaciones no reconocidas a través de los canales digitales de los bancos?

Tabla 15

Pregunta n.° 7: respuestas

Entrevistado	Respuesta de la pregunta n.° 1
P.C.M.	Por falta de capacitaciones o por desconocimiento del phishing y swapping,
E.Q.R.	Falta de un buen sistema de seguridad.
G.S.V.	Porque el usuario no tiene el verdadero respaldo de las autoridades y además se debe tener en cuenta que tanto el banco como el cliente obtienen ganancias, pero en este caso el banco brinda un servicio y por lo tanto debe de hacerse responsable y asumir las pérdidas previa denuncia del resultado de una investigación.
L.M.L.	En este caso, considero que toda persona puede ser vulnerable para la delincuencia digital independientemente de los canales electrónicos que usen los bancos, quizá un elemento importante es que el consumidor sepa cuales son los protocolos que usan los bancos, de esta manera cuando se les requiera información sensible, no la entregaran dado que saben cuáles son los procedimientos del Banco.
L.F.F.	Porque en ocasiones no leemos o los mismos bancos se demoran en informar todos los movimientos deben existir campañas a través de los canales (medios de comunicación) de las evoluciones de estas estafas digitales.
L.M.V.	Porque actualmente los medios de seguridad no son suficientemente fuertes para prevenir o anular los posibles ataques de hackers externos, es por ello que deben mejorar su servicio y que este sea óptimo para sus usuarios.

Tabla 16

Pregunta n.° 7: análisis

Convergencia	Divergencia	Interpretación
El desconocimiento y la poca atención que los usuarios dan a la información brindada, sumada a la poca campaña de concientización pobre ofrecida por estas entidades provoca que estos se al vulnerables y potenciales víctimas de estos ciberdelitos.	En su mayoría no tienen respaldo de las autoridades, ya que la información no es brindada apropiadamente y los protocolos de seguridad son exclusivamente información confidencial de las entidades financieras.	La poca información brindada por campañas pobres de concientización, el poco interés por estos incidentes, la indiferencia de los usuarios por conocer los procedimientos o protocolos de seguridad para la protección de sus datos e

	información de sus cuentas para prevenir posibles incidentes a futuro a la vez que la información no es difundida de manera preventivas a los usuarios da como resultado la vulnerabilidad constante al momento de utilizar los medios digitales.

8. En su opinión, ¿Cree que, el uso de la identificación por número de celular o código por sms son eficaces ante las operaciones fraudulentas realizadas en canales digitales? Fundamente su respuesta

Tabla 17

Pregunta n.° 8: respuestas

Entrevistado	Respuesta de la pregunta n.° 1
P.C.M.	Si, correcto es un mecanismo que ayuda mucho a evitar este tipo de operaciones.
E.Q.R.	Si, siempre y cuando el usuario no entregue datos a otras personas y que al banco otorgue preguntas secretas.
G.S.V.	Son medidas que se adoptan, pero no son totalmente eficaces, ya que se evidencia con el incremento de estos delitos, para los cuales la delincuencia innova permanentemente.
L.M.L.	En este caso se debe entender que actualmente los bancos han informado a sus clientes que ellos no solicitan información de sus cuentas por ningún medio electrónicos de los que se menciona. Solo para la confirmación de ciertas operaciones si requiera la autorización del consumidor para algunas operaciones de tarjetas.
L.F.F.	No, considero que la manera mas segura es aparte de mandar mensajes es por el correo personal porque en muchas ocasiones lo hacen luego de un robo al celular y el mensaje de acceso le puede llegar al mismo delincuente.
L.M.V.	No son eficaces, porque actualmente se puede clonar o intervenir celulares; por tanto, acceder a su información. Es por ello que el nivel de seguridad del celular debería ser alto.

Tabla 18

Pregunta n.° 8: análisis

Convergencia	Divergencia	Interpretación
Estos medios de autentificación son eficaces ya que en su mayoría comparten patrones accesibles para el consumidor o cliente, claramente si es que ellos no brindan información personal como numero de celular o compañía telefónica de manera indiscriminada. Estos medios cumplirán con las expectativas brindadas, ya que el usuario ya fue informado por algún medio para su prevención.	El uso de estos medios de autentificación no es considerado de manera eficaz ya que en su mayoría ya han sido violentados y la mayoría de información de los usuarios ya esta a la venta en un mercado negro.	Los mecanismos de autenticación deben ser de fácil interpretación de los usuarios, estos deben ser concientizados en la difusión de sus datos móviles como número de celular y compañía telefónica ya que fueron informados en algún momento por parte de la entidad financiera. Pero para el cumplimiento de esto tenemos que referirnos a que se encuentren actualizados a nuevos métodos de robo de información que después derivaría en una afectación económica del usuario. De esta manera el protocolo de autentificación no cumple en su totalidad su función protectora.

9. En su opinión, ¿Cree que la identificación por llenado de datos personales como: "nombres de padres, lugar de nacimiento, edad, DNI, número de Ubigeo o lugar de nacimiento de padres" son los adecuados ante la identificación de operaciones fraudulentas realizadas en canales digitales? Fundamente su respuesta

Tabla 19

Pregunta n.° 9: respuestas

Entrevistado	Respuesta de la pregunta n.° 1
P.C.M.	Considero que sí, ya que esta información lo maneja solo el titular de la cuenta y la información y es confidencial.
E.Q.R.	No, ahora se tiene la información que RENIEC también ha sido saqueado y por ello se debe realizar otras preguntas más eficaces.
G.S.V.	Ayudan, pero no son suficientes, ya que muchas veces la delincuencia tiene esos datos ya que saben el procedimiento y cuentan con toda la información.

L.M.L.	Considero que la razón de ser de pedir esta información es porque es muy poco conocida por los delincuentes y que solo el consumidor lo sabe, pero definitivamente hay mucha inseguridad en el ciberespacio y quizá el sistema debería mejorar en cuanto a sus controles de seguridad para identificar operaciones inusuales de los usuarios.
L.F.F.	Considero que los además de ello se debe pedir clave secreta, reconocimiento detectar se debe actualizar mecanismos más idóneos, pues los datos personales son de fácil acceso.
L.M.V.	Estos datos son datos confidenciales que pide el banco para poder crear su cuenta. Si en algunas páginas los piden, la persona puede ser víctima de un robo sistemático, pues está dando información confidencial. Sin embargo, el banco debe proveer esta información de forma constante a sus afiliados, para que estos eviten seguir con este problema.

Tabla 20

Pregunta n.° 9: análisis

Convergencia	Divergencia	Interpretación
Es de suma importancia este método ya que los datos personales como: “nombres de padres, lugar de nacimiento, edad, DNI, número de Ubigeo o lugar de nacimiento de padres” son los adecuados porque esta información es manejada solamente por el usuario y ayuda en gran parte a su identificación.	En la actualidad este método de identificación mediante datos personales como: “nombres de padres, lugar de nacimiento, edad, DNI, número de Ubigeo o lugar de nacimiento de padres” no son los más adecuados; ya que esta información puede ser conseguidas en un mercado negro ya existente, en su mayoría obtener este tipo de datos prácticamente ya es información pública, por lo cual se tendría que buscar otros métodos aparte de este para evitar vulnerabilidades en su sistema de seguridad.	Se entiende que la identificación por datos personales como: “nombres de padres, lugar de nacimiento, edad, DNI, número de Ubigeo o lugar de nacimiento de padres” ya no son los adecuados por ya han sido vandalizados, por ciber delincuentes que ya difundieron esta información que tiene el RENIEC, es claro determinar que este método de autentificación ya no brinda la seguridad adecuada, por ende este tendría que formar parte de otro método de seguridad para poder ser validada para poder ser eficaz.

10. Desde su punto de vista, ¿Cuáles deberían de ser las medidas de seguridad que los bancos deberían de optar para poder reconocer las operaciones fraudulentas y si están sucedieran deberían de informar al usuario de inmediata?

Tabla 21

Pregunta n.° 10: respuestas

Entrevistado	Respuesta de la pregunta n.° 1
P.C.M.	Como medida de seguridad seria realizar capacitaciones o envió de información respecto a este tipo de operaciones a los clientes, y en efecto después de cada operación se debe alertar al cliente.
E.Q.R.	Siempre deben enviar un sms o correo indicando el moviente que se realizó en sus cuentas.
G.S.V.	Si se debería de informar en forma inmediata al usuario, por lo que entre las medidas adoptarse debería pagarse un seguro mínimo (1 o 2 soles) obligatoriamente en forma mensual, un pago extra por operación a partir de ciertos horarios, una comunicación directa con el usuario y mejorar los sistemas tecnológicos anti hacker.
L.M.L.	Considero que deben existir procedimientos claros que se informen a los clientes para que sepan que los bancos no piden información sobre números de cuenta, claves de seguridad entre otros. Asimismo, mejorar su sistema de seguridad a fin de no tener intromisiones con terceros.
L.F.F.	Ante cualquier movimiento no reconocido a paginas de desconfianza como los monederos digitales debería bloquear se la tarjeta e inmediatamente remitir un correo para que no se siga cometiendo los movimientos la mayoría de delincuente primero verifican si pueden hacerlo, para ello realizar movimientos de S/.1.00 sol y luego hacen el movimiento grande.
L.M.V.	Debería hacer un reconocimiento de huella digital, ya que es algo un poco más complicado de clonar. Adicional a ello, crear aplicaciones para detectar actividades anómalas e informar al usuario.

Tabla 22

Pregunta n.° 10: análisis

Convergencia	Divergencia	Interpretación
Las medidas de seguridad optadas o protocolares de parte de las entidades financieras son eficientes hasta cierto grado, debemos de reconocer que el avance tecnológico es constante y por ende los mecanismos de seguridad anteriores ya se vuelve obsoletos y se crean vulnerabilidades a cibernéticas, por eso de implementarse tecnologías actuales que mejoraran su funcionalidad a par de las anteriores.	Las medidas de seguridad actuales son casi obsoletas por ende se debe implementar: Campañas de concientización atractivas al público e informativos para la prevención de ilícitos y hurtos. Alertas continuas por todo movimiento de dinero en las cuentas de forma inmediata. Seguros de paga que salvaguarden las cuentas ante posibles siniestros económicos digitales. Comunicación inmediata y no automatizada al servicio del cliente los 365 días del año, las 24 horas. El reconocimiento de huellas dactilares en todo movimiento de dinero sin escatimar el monto.	La implementación de nuevos métodos de seguridad para la prevención debe de estar regulado de manera explícita especificando los mecanismos a realizarse y a su vez especificar las actualizaciones constantes e innovadoras que deben de ser contempladas de manera constante. Algunas de estas opciones a aportar serian: Campañas de concientización atractivas al público e informativos para la prevención de ilícitos y hurtos. Alertas continuas por todo movimiento de dinero en las cuentas de forma inmediata. Seguros de paga que salvaguarden las cuentas ante posibles siniestros económicos digitales. Comunicación inmediata y no automatizada al servicio del cliente los 365 días del año, las 24 horas. El reconocimiento de huellas dactilares en todo movimiento de dinero sin escatimar el monto. Siendo estas medidas de seguridad que mejoraran los protocolos de seguridad y la mejor protección económica de los usuarios.

DISCUSIÓN

OBJETIVO GENERAL

Desarrollar la responsabilidad de las entidades financieras y los usuarios a través de los canales digitales en Perú

La responsabilidad se puede identificar como aquel deber en los que incurren las entidades financieras cuyo alcance a sus usuarios para realizar actividades son los medios digitales mediante los cuales han sido perjudicados.

Es así que se afirma que la información brindada acerca del phishing y swapping fue dada de manera exclusiva, periódica y mediante capacitación a aquellos que se encuentran laborando en entidades financieras. Siendo lo contrario que aquellos que no laboran en entidades bancarias, no fueron concientizados de manera inmediata, exclusiva, personalísima y en algunos casos de manera indirecta acerca del phishing y swapping.

Además, según León (2017), la responsabilidad civil es definida como aquella situación en la que el sujeto afrontará consecuencias perjudiciales a raíz de sus acciones. Esto es, Esto debido a un incumplimiento contractual, en la cual el fundamento de este tipo de responsabilidad se basa en el hecho de que las entidades financieras, brindan diversos servicios hacia sus usuarios a través de sus medios digitales, tales como el resguardo de su patrimonio en cuentas que ofrecen, por lo qué se deberá verificar en todo momento qué este patrimonio resguardado se encuentre protegido correctamente y qué si el usuario lo requiere pueda realizar transferencias de su patrimonio libremente con toda las medidas que garantizasen una seguridad qué únicamente son ellos los que autoricen los movimientos que se realicen con su patrimonio.

A si mismo, se puede ocasionar mediante un hecho que ocasione un prejuicio al usuario el cual no se encontraba con vinculo contractual, quiere decir previo a lo que llamamos responsabilidad extra contractual, lo cual genera a la entidad financiera una obligación de resarcir este prejuicio cometido contra el

usuario, lo qué en la mayoría de casos se denomina al pago de una indemnización por daños y perjuicios.

Por otro lado, L.M.L Y P.C.M (2023), mencionan que las entidades financieras no están obligadas a responder mediante una responsabilidad sobre sobre los procedimientos mediante operaciones por canales digitales de las entidades financieras, todo esto a qué según indican las entidades financieras que brindan servicios mediante canales digitales a sus usuarios cuentan con procedimientos de puesta en conocimiento sí se ha visto perjudicado su patrimonio custodiado, brindando facilidades.

Finalmente, se debe mencionar que es fundamental que las entidades financieras se encuentran obligadas con sus usuarios con el fin de proteger su patrimonio custodiado a través de sus servicios digitales, siendo que las modalidades de Phishing y SIM swapping son modalidades de obtención de datos mediante la falsa figura de ser el usuario, las entidades financieras están obligadas a capacitar a sus usuarios.

Objetivo especifico 1: Identificar la relación de la responsabilidad de las entidades financieras en los casos de operaciones no reconocidas por usuarios y entidades financieras, a través de sus canales digitales.

Las operaciones no reconocidas por usuarios, se identifican como aquellas operaciones o transacciones realizadas mediante un canal digital brindado como servicio por las entidades financieras en las cuales el usuario titular de dicho servicio no ha realizado, ni realizó la aprobación correspondiente.

Siento que La responsabilidad de los bancos es inminente al no brindar información de manera inmediata ya que no todas las entidades practican el método de seguridad como alerta mediante un mensaje demostrando de esa manera que estas no son obligadas por norma específica, de esta forma también debemos reconocer al usuario como un consumidor y por ende hay un código del consumidor que exige la protección por el servicio brindado. Por ende, los bancos son responsables y las medidas de seguridad optadas no son eficientes en todos

los casos, solamente son un mecanismo de protección ante una inminente responsabilidad acarreada hacia los bancos

A su vez, según Zambrano(2021) en su investigación concluyó qué al ser los aplicativos móviles de fácil acceso, ocasiona que los ciberdelincuentes se aprovechen y obtengan información personal sobre el acceso a la banca móvil de los usuarios financieros, inclusive en momentos donde no contaban con el aplicativo móvil instalado en sus dispositivos, siendo estos afiliados sin su consentimiento y, claro está, con aprobación de quienes administran estas aplicaciones móviles, además de las entidades financieras que poseen su información bancaria de sus usuarios.

En la actualidad se identifica una respuesta por parte de los bancos al momento de que se realizan operaciones no reconocidas por el usuario a través de sus medios digitales de forma lenta, puesto a qué al ser la modalidad de Phishing y SIM Swapping aquellas que simulan ser el usuario que utiliza estos canales digitales para resguardar su patrimonio, se indica que el Banco tiene responsabilidad siempre que no cumpla con informar al consumidor sobre las operaciones que se realicen en sus cuentas y siempre que esta información sea atendida en el plazo legal que establece el Código de Protección al Consumidor (L.M.L, 6)

Por lo qué, se considera que por parte de las entidades financiera existe una responsabilidad debido al constante uso que realizan sus usuarios a través de sus canales digitales, en los casos de operaciones no reconocidas, por lo qué es deducible que hasta la fecha no existe una regulación adecuada que especifique el periodo de actualización de sistemas de seguridad digital para la protección de sus usuarios que incurren en caer en las modalidades de Phishing y SIM Swapping que se utiliza en perjuicio de su patrimonio.

Objetivo específico 2

Identificar los niveles de seguridad que las entidades financieras utilizan para reconocer las operaciones fraudulentas o "no conocidas" por los usuarios en sus canales digitales

Las entidades financieras al brindar servicios mediante canales digitales hacia sus

usuarios adquieren la obligación de proveerse de las medidas suficientes que garanticen al usuario una seguridad al realizar operaciones con el patrimonio resguardado por esta, siendo qué al vulnerarse estos canales digitales mediante Phishing o SIM Swapping son las entidades financieras aquellas que deberán asumir las consecuencias que ocasionaron un perjuicio al usuario que utilizaba sus canales digitales.

La implementación de nuevos métodos de seguridad para la prevención debe de estar regulado de manera explícita especificando los mecanismos a realizarse y a su vez especificar las actualizaciones constantes e innovadoras que deben de ser contempladas de manera constante. Algunas de estas opciones a aportar serian: Campañas de concientización atractivas al publico e informativos para la prevención de ilícitos y hurtos. Alertas continuas por todo movimiento de dinero en las cuentas que de forma inmediata. Seguros de paga que salvaguarden la cuentas ante posibles siniestros económicos digitales. Comunicación inmediata y no automatizada al servicio del cliente los 365 días del año, las 24 horas. El reconocimiento de huellas dactilares en todo movimiento de dinero sin escatimar el monto. Siendo estas medidas de seguridad que mejoraran los protocolos de seguridad y la mejor protección económica de los usuarios.

Es de esta manera, que la resolución Nº 3412-2018/SPCINDECOPI en la que se resolvió que la falta de comunicación de la entidad financiera, por servicios brindados, corresponden a la falta de medidas de seguridad y prevención ante cualquier siniestro, tal es así que ordenó al banco responder por dicha falta con un resarcimiento de la pérdida económica y la medida correctiva para su mejora normativa.

Entonces, sí a la entidad financiera que presta servicios mediante sus canales digitales a sus usuarios se deberá reconocer Ante cualquier movimiento no reconocido a páginas de desconfianza como los monederos digitales debería bloquearse la tarjeta e inmediatamente remitir un correo para que no se siga cometiendo los movimientos la mayoría de delincuente primero verifica si pueden hacerlo, para ello realizar movimientos de S/.1.00 sol y luego hacen el movimiento grande. (L.F.F 21)

IV. CONCLUSIONES

.

1. La ciberdelincuencia haciendo uso de diversos actos de manipulación mediante medios informáticos o modalidades de engaño mediante redes, cómo lo son el *Phishing* y el *SIM Swapping*, simulan tener la imagen del usuario que cuenta con su patrimonio depositado en una entidad financiera, suplantando su identidad y así obtener de los usuarios de canales digitales datos personales determinados para el uso de los canales digitales que ofrecen como servicio las entidades financieras, de esta forma logran acceder a las cuentas de los usuarios. De esta forma sustraen el patrimonio para así ocasionar un perjuicio.

   Cabe señalar que, estos servicios mediante canales digitales que ofrecen las entidades financieras se piensan como seguros y eficaz para un correcto resguardo del patrimonio de sus usuarios, no obstante, modalidades como el Phishing y el SIM Swapping han puesto al descubierto la ineficacia de estos servicios mediante canales digitales que ofrecen las entidades financieras a la hora de realizar una correcta detección de que son los usuarios los que realizaron los movimientos del patrimonio custodiado por las entidades financieras.

2. La responsabilidad asumida por las entidades bancarías tiene como punto de partida la existencia de un vínculo, siendo esto la contratación del usuario al servicio de canal digital ofrecido por las entidades financieras, los cuales han sido vulnerados en su ciberseguridad generando un perjuicio al patrimonio custodiado del usuario, el cual es deber de la entidad financiera el indemnizar o resarcir el daño ocasionado al patrimonio del usuario, debido a qué el ilícito se cometido en sus canales digitales.

   Sin embargo, en los casos que los usuarios denuncian haber sido victimas de estas modalidades Phishing y SIM Swapping en perjuicio de su patrimonio, lo que habitualmente realizan las entidades financieras es señalar que la negligencia fue cometida por el propio usuario, el cual permitió que se le engañara facilitando sus datos a los ciber delincuentes, haciéndolo recurrir a

vías judiciales como único medio de resarcir este ilícito cometido, cuyo fin tiene el recuperar lo sustraído.

3. Las entidades financieras que brinden servicios mediante canales digitales, se encuentran sujetas de optimizar sus medidas de ciber seguridad en atención a una correcta custodia del patrimonio del usuario, por lo que en caso de qué se cometiese una sustracción mediante operaciones no reconocidas, es la entidad financiera quien deberá asumir la consecuencia derivada del fallo de su ciber seguridad implementada en su servicio digital, no atribuyéndole la responsabilidad al usuario víctima del ilícito.

   Se presume que los servicios que ofrecen las entidades financieras mediante canales digitales son confiables y eficaces en la protección del patrimonio del usuario, sin embargo, con el avance de la tecnología, avanza a su vez la ciber delincuencia, siendo el *phishing* y el *sim swapping* una de las modalidades que quebrantan la ciberseguridad de los servicios digitales, los cuales en perjuicio del patrimonio del usuario se realizan operaciones no reconocidas.

V. RECOMENDACIONES

Se sabe que en estos últimos años han aumentado los casos de *phishing* y *sim swapping*, que el uso de las redes digitales, canales de atención y aplicativos móviles se han vuelto una necesidad por ende la protección debe ser una prioridad de los bancos es así que se debe regular plazos exactos para renovar los protocolos de seguridad, los programas de seguridad y que estos sean evaluados por especialistas en ciberseguridad, por todo lo antes mencionado la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones debe establecer plazos mensuales para la actualización de programas de protección y anti- hacking, los cuales deben ser supervisados periódicamente.

Es también importante darle la opción al usuario de poder retirar toda su información personal una vez terminado su vínculo con alguna entidad financiera, apara que esta no sea utilizada sin su consentimiento por ende la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones debe de regular de manera expresa el retiro de la información del usuario a pedido de este y el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual apoyar en la regulación de esta ya que son los usuarios los que son afectados por un producto.

Las entidades financieras deberían de ofrecer un producto de protección y seguridad un seguro de operaciones de alto riesgo que sirva para poder resguardar el patrimonio económico, que sea accesible para cualquier usuario y a la vez un seguro de protección gratuito ha sabiendas que sus protocolos de no cumplen con la totalidad de seguridad, el cual deberá de ser regulado Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones y el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual

Se recomienda a la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones encargada de regular a las entidades financieras modificar en su el artículo 17.1 de índice “d”, de la resolución 504-2021 del sub capítulo de título autentificación, en el cual crea un proceso ineficaz de autentificación por no restringir el número de intentos fallidos, dando cabida libre a programas que generan diversas respuestas para acceder a la información , ya que el principal ciberataque se configura con los ciberdelitos denominados *phishing* y

sim swapping que su propósito es la suplantación de identidad con la finalidad de sacar un provecho económico.

REFERENCIAS

Albors, J (2020). SIM Swapping: Qué es y como funciona este fraude. Welivesecutirty. 30 de Marzo de 2020. https://www.welivesecurity.com/la-es/2020/03/30/que-es-sim-swapping-como-funciona/

Aramburu, M. (2007) responsabilidad civil contractual por fraudes con tarjeta de crédito en Colombia (Tesis de titulo de abogado, Medellin, Colombia) https://repository.eafit.edu.co/bitstream/handle/10784/457/JoseSantiago_RendonVera_2007.pdf?sequence=1&isAllowed=y

Campi, N.(2019) Ética de los ensayos clínicos adaptativos (Master's thesis, Buenos Aires).

Cabrera, C. (2020) "Criterios para resolver casos de operaciones no reconocidas efectuadas mediante el uso de tarjetas de crédito o débito [trabajo Académico para optar el título de Segunda Especialidad en Derecho de Protección al Consumidor, Pontificia Universidad Catolica de Perú]. https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/19164

Enriquez Caro, R. (19 de Agosto de 2019). " Digitalización de la Banca Peruana. ". t.ly/gswi

Escudero, C, Cortez, L (2017), Técnicas y métodos cualitativos para la investigación científica. UTMACH.

Espinoza, E., & Toscano, D. (2015). Metodología de Investigación Educativa y Técnica. Ediciones Utmach.

Espinoza, E. (2020). La investigación cualitativa, una herramienta etica en el ambito pedagogico.Scielo.http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1990-86442020000400103#B6

González, G. F. L., & García, V. M. D. P. (2021) Retos de la investigación jurídica en las aulas universitarias hacia el 2021.“cómo hacer una tesis y no envejecer en el intento”. in actas del v congreso investigación, desarrollo e

innovación de la universidad internacional de ciencia y tecnología. 1(1) (401). https://doi.org/10.47300/978-9962-5599-8-6-23

Guzman, V. (2021) El método cualitativo y su aporte a la investigación en las ciencias sociales. https://revistagestionar.com/index.php/rg/article/view/17

Herrera J, Jara M, Jerez M. (2005) "Los Bancos y las Nuevas Tecnologías". https://repositorio.uchile.cl/bitstream/handle/2250/111497/Herrera%2c%20Juan%20S..pdf?sequence=1&isAllowed=y

Interbank. (2021). Interbank entre los bancos más innovadores del país. t.ly/MG63

Lauphan, W. (2006). El dato científico y la matriz de datos. Universidad Nacional de Entre Ríos. Facultad de Ciencias Agropecuarias. Argentina, 1.

Nuñez, J. E. (2012). Islas Malvinas: entre soberanía compartida y justicia distributiva. In VI Congreso de Relaciones Internacionales (La Plata, 2012).

Pareja Palomino, J. Informe jurídico sobre la Resolución Nº 3412- 2018/SPCINDECOPI.

Pardo A (2018). Perú Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018 [Tesis de titulo de magister, Lima, Perú] https://repositorio.ucv.edu.pe/handle/20.500.12692/20372

Romaña, G (2022) análisis del sistema regulatorio en los servicios de telefonía e internet fija y móvil y su necesidad de permanente revisión y cambio, perú 2021. (Tesis de Maestria, Arequipa, Perú) http://repositorio.sfx.edu.pe/handle/SFX/76

Ramos, C. (2018). Cómo hacer una tesis de derecho y no envejecer en el intento. Marzo de 2018. https://virtual.legis.pe/wp-content/uploads/2019/01/Como-hacer-una-tesis.pdf

Ramos-Galarza, C., y Caycho-Rodríguez, T. (2019). El título de una investigación: De la catársis a la técnica. CienciAmérica, 8(2), 1-10. Obtenido de http://cienciamerica.uti.edu.ec/openjournal/index.php/uti/article/view/227

Rosero, L (2021). El phishing como riesgo informático, técnicas y prevención en los canales electrónicos: un mapeo sistemático.

Sánchez, P. I. G. (2009). Principios básicos de bioética. Revista Peruana de Ginecología y Obstetricia, 55(4), 1-12.

Vargas, J. (2019). Perú: el sistema financiero deja cinco mil afectados al día. 28 de octubre de 2019. https://ojo-publico.com/1431/peru-el-sistema-financiero- deja-cincomil-afecta dos-al-dia

Valdés, E. (2011). El principio de autonomía en la doctrina del bioderecho. La lámpara de Diógenes, 22(12), 113-128.

Villavicencio, F (2014). "Delitos informáticos". Revista ius et veritas 1 (1), 284-304 https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630/14253

ZavalaJ, Luz V. (2021) Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020. (Tesis de doctorado, Universidad Cesar Vallejo, Lima, Perú) Repositorio Universidad
Cesar Vallejo. https://repositorio.ucv.edu.pe/handle/20.500.12692/83325

ANEXOS

Anexo A

Tabla de categorización

Categoría de estudio	Definición conceptual	Categoría	Subcategoría	Códigos
Responsabilidad civil de las entidades financieras	Fernández (2020) Concluyo que las entidades financieras deben de asumir la responsabilidad por el uso de sus plataformas virtuales Salas (2017) concluyo quela responsabilidad es objetiva y esta tiene por finalidad la reparacion del daño a efecto de este delito Hidalgo (2018) Concluyo que la fenomenología es de envergadura penal y que a futuro se deberán de crear nuevas normas en hechos fraudulentos	Responsabilidad civil de las entidades financieras	Entidades Financieras	Entidades bancarias Fraudes electrónicos consumidores
			Responsabilidad Civil	Responsabilidad Objetiva Responsabilidad Subjetiva Daño Reparación Fenomenología Penal
			Usuarios	Hechos fraudulentos Bien jurídico
Los usuarios afectados por phishing y sim swapping	Zambrano (2021) concluyo que los aplicativos móviles y plataformas virtuales son de fácil acceso y ocasionan los principales a taques cibernéticos	Los usuarios afectados por phishing y sim swapping		Delito informativo Banca móvil Consentimiento
			Phishing y Sim Swapping	Aplicativos móviles Ciber delincuencia Información

Anexo B

INSTRUMENTO DE RECOLECCIÓN DE DATOS

TÍTULO: La responsabilidad civil de las entidades financieras y de los usuarios afectados por phishing y sim swapping en el Perú

GUÍA DE ENTREVISTA

INDICACIONES: El presente instrumento tiene como propósito recaudar su opinión respecto la responsabilidad civil de las entidades financieras y de los usuarios afectados por phishing y sim swapping en el Perú; motivo por el cual, se le pide responder las siguientes preguntas con la mayor seriedad y compromiso.

Entrevistado/a:

Cargo :

Institución :

OBJETIVO GENERAL

Desarrollar la responsabilidad de las entidades financieras y los usuarios a través de los canales digitales en el Perú en casos al phishing y swapping

Preguntas:

1. Desde su realidad, ¿en algún momento ha recibido información sobre el phishing y swapping de manera física por parte de los bancos? Comente.

2. ¿Conoce usted que es un canal de atención digital, phishing y swapping? Fundamente su respuesta

3. Según su criterio, ¿qué responsabilidad tienen los bancos al obligar el uso de un determinado canal de atención para un servicio en relación casos de phishing y swapping?

4. En su opinión, ¿qué tanta responsabilidad tiene los usuarios, al usar canales de atención digitales que los vuelven vulnerables ante los casos de phishing y swapping?

OBJETIVO ESPECÍFICO 1

Identificar la relación de la responsabilidad de las entidades financieras en los casos de operaciones no reconocidas por usuarios y bancos, a través de sus canales digitales.

Preguntas:

5. Según su experiencia, ¿qué tipo de responsabilidad tienen los bancos al no brindar un informe detallado de sus movimientos de los usuarios de manera inmediata, cuando suceden casos de operaciones no reconocidas en sus canales digitales?

6. En su opinión, ¿cree que los bancos tienen responsabilidad por el uso de sus canales digitales, en los casos de operaciones no reconocidas? Fundamente su respuesta.

7. Siete Según su criterio, ¿por qué los usuarios en general son blanco de las operaciones no reconocidas a través de los canales digitales de los bancos?

OBJETIVO ESPECÍFICO 2

Identificar los niveles de seguridad que las entidades financieras utilizan para reconocer las operaciones fraudulentas o "no conocidas" por los usuarios en sus canales digitales.

Preguntas:

8. En su opinión, ¿cree que, el uso de la identificación por número de celular o código por sms son eficaces ante las operaciones fraudulentas realizadas en canales digitales? Fundamente su respuesta

9. En su opinión, ¿cree que la identificación por llenado de datos personales como: "nombres de padres, lugar de nacimiento, edad, DNI, número de Ubigeo o lugar de nacimiento de padres" son los adecuados ante la identificación de operaciones fraudulentas realizadas en canales digitales? Fundamente su respuesta

10. Desde su punto de vista, ¿cuáles deberían de ser las medidas de seguridad que los bancos deberían de optar para poder reconocer las operaciones fraudulentas y si están sucedieran deberían de informar al usuario de inmediata?

SELLO	FIRMA

Anexo B

FICHA PARA REGISTRAR LA OPINIÓN DE UN EXPERTO ACERCA DE UN INSTRUMENTO DE RECOPILACIÓN DE INFORMACIÓN EN UNA INVESTIGACIÓN

I. DATOS DEL INSTRUMENTO DE RECOPILACIÓN DE INFORMACIÓN

Título de la investigación	La responsabilidad civil de las entidades financieras y de los usuarios afectados por phishing y sim swapping en el Perú
Nombre del instrumento	Guía de entrevistas
Autor(es) del instrumento	Ferro Huayllacayan, Josue David Vega Orcón, Moisés Alfredo

II. DATOS DEL EXPERTO

Apellidos y nombres	CRUZ RODRIGUEZ MIGUEL ANGEL
Código ORCID	
Grados y títulos	MAGISTER EN DERECHO EMPRESARIAL
Centro de trabajo	UNIVERSIDAD CÉSAR VALLEJO
Cargo que ocupa	CODENTE A TIEMPO PARCIAL
Teléfono	989979354

III. VALORACIÓN DE LOS ÍTEMS DEL INSTRUMENTO

A continuación, se presenta cada uno de los ítems del instrumento a evaluar. Por favor lea cada uno de ellos y registre con un aspa (x) su valoración: (3) logrado, (2) en proceso y (1) en inicio. Cuando la valoración de un ítem es (2) o (1) se debe redactar en la columna de sugerencias el ítem como considera que debe presentarse o una recomendación concreta. Muchas gracias por su valioso aporte.

N.° de Ítem	Ítems del instrumento	Valoración				Sugerencias
		3	2	1	0	
OBJETIVO GENERAL: **Desarrollar la responsabilidad de las entidades financieras y los usuarios a través de los canales digitales en el Perú en casos al phishing y swapping**						
1	Desde su realidad ¿En algún momento ha recibido información sobre el phishing y swapping de manera física por parte de los bancos? comente.	X				

N.° de Ítem	Ítems del instrumento	Valoración				Sugerencias
		3	2	1	0	
2	¿Conoce usted que es un canal de atención digital, phishing y swapping? Fundamente su respuesta	X				
3	Según su criterio ¿Qué responsabilidad tienen los bancos al obligar el uso de un determinado canal de atención para un servicio en relación casos de phishing y swapping?	X				
4	Según su opinión ¿Qué tanta responsabilidad tienen los usuarios, al usar canales de atención digitales que los vuelven vulnerables ante los casos de phishing y swapping?	X				
OBJETIVO ESPECÍFICO 1: **Identificar la relación de la responsabilidad de las entidades financieras en los casos de operaciones no reconocidas por usuarios y entidades financieras, a través de sus canales digitales.**						
5	Según su experiencia ¿Qué tipo de responsabilidad tienen los bancos al no brindar un informe detallado de sus movimientos de manera inmediata, cuando suceden casos de operaciones no reconocidas en sus canales digitales?	X				
6	Según su opinión ¿cree usted que los bancos tienen responsabilidad por el uso de sus canales digitales, en los casos de operaciones no reconocidas? Fundamente su respuesta.	X				
7	Según su criterio ¿Por qué los usuarios son blanco de las operaciones no reconocidas a través de los canales digitales de los bancos?	X				
OBJETIVO ESPECÍFICO 2: Identificar los niveles de seguridad que las entidades financieras utilizan para reconocer las operaciones fraudulentas o “no conocidas” por los usuarios en sus canales digitales.						

N.° de Ítem	Ítems del instrumento	Valoración				Sugerencias
		3	2	1	0	
8	En su opinión ¿cree usted que el uso de la identificación por número de celular o código por sms, son eficaces ante las operaciones fraudulentas realizadas en canales digitales? Fundamente su respuesta	X				
9	En su opinión ¿cree usted que la identificación por llenado de datos personales como "nombres de padres, lugar de nacimiento, edad, DNI, número de Ubigeo o lugar de nacimiento de padres" son los adecuados ante la identificación de operaciones fraudulentas realizadas en canales digitales? Fundamente su respuesta	X				
10	A su punto de vista ¿Cuáles deberían de ser las medidas de seguridad que los bancos deberían de optar para poder reconocer las operaciones fraudulentas y si están sucedieran deberían de informar al usuario de inmediato?	X				

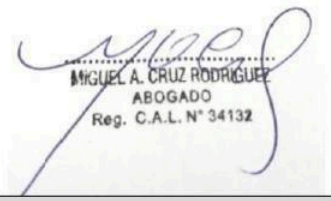
IV. CALIFICACIÓN Y OPINIÓN DE APLICACIÓN

Calificación	Aplicable	Aplicable después de corregir	No aplicable
	X		

V. LUGAR Y FECHA:

Lugar	Fecha
Lima	28-04-2023

VI. FIRMA Y POSTFIRMA DEL EXPERTO:



Nombre:MIGUEL ANGEL CRUZ RODRIGUEZ

DNI: 09980023

FICHA PARA REGISTRAR LA OPINIÓN DE UN EXPERTO ACERCA DE UN INSTRUMENTO DE RECOPILACIÓN DE INFORMACIÓN EN UNA INVESTIGACIÓN

I. DATOS DEL INSTRUMENTO DE RECOPILACIÓN DE INFORMACIÓN

Título de la investigación	La responsabilidad civil de las entidades financieras y de los usuarios afectados por phishing y sim swapping en el Perú
Nombre del instrumento	Guía de entrevistas
Autor(es) del instrumento	Ferro Huayllacayan, Josue David Vega Orcón, Moisés Alfredo

II. DATOS DEL EXPERTO

Apellidos y nombres	Romero Saavedra Erick Enrique
Código ORCID	ORCID: 0000-0003-3969-9210
Grados y títulos	Abogado, con estudios de Postgrado en Derecho Civil y Comercial en la UNMSM, y Maestro en Gestión Pública
Centro de trabajo	Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres - CENEPRED
Cargo que ocupa	Especialista Legal
Teléfono	--------

III. VALORACIÓN DE LOS ÍTEMS DEL INSTRUMENTO

A continuación, se presenta cada uno de los ítems del instrumento a evaluar. Por favor lea cada uno de ellos y registre con un aspa (x) su valoración: (3) logrado, (2) en proceso y (1) en inicio. Cuando la valoración de un ítem es (2) o (1) se debe redactar en la columna de sugerencias el ítem como considera que debe presentarse o una recomendación concreta. Muchas gracias por su valioso aporte.

N.° de Ítem	Ítems del instrumento	Valoración				Sugerencias
		3	2	1	0	
OBJETIVO GENERAL: **Desarrollar la responsabilidad de las entidades financieras y los usuarios a través de los canales digitales en el Perú en casos al phishing y swapping**						
1	Desde su realidad, ¿en algún momento ha recibido información sobre el phishing y swapping de manera física por parte de los bancos? Comente.		x			La responsabilidad de las entidades financieras por el uso imperfecto de los canales digitales, en el Perú, se aborda desde una perspectiva administrativa, Derecho de Consumidor.

N.° de Ítem	Ítems del instrumento	Valoración				Sugerencias
		3	2	1	0	
2	¿Conoce usted que es un canal de atención digital, phishing y swapping? Fundamente su respuesta			x		Podría poner en riesgo las contraseñas de usuarios, se prefiere canales digitales
3	Según su criterio, ¿qué responsabilidad tienen los bancos al obligar el uso de un determinado canal de atención para un servicio en relación casos de phishing y swapping?		x			Actualmente, responsabilidad administrativa.
4	En su opinión, ¿qué tanta responsabilidad tienen los usuarios, al usar canales de atención digitales que los vuelven vulnerables ante los casos de phishing y swapping?	x				
OBJETIVO ESPECÍFICO 1: **Identificar la relación de la responsabilidad de las entidades financieras en los casos de operaciones no reconocidas por usuarios y entidades financieras, a través de sus canales digitales.**						
5	Según su experiencia, ¿qué tipo de responsabilidad tienen los bancos al no brindar un informe detallado de sus movimientos de manera inmediata, cuando suceden casos de operaciones no reconocidas en sus canales digitales?	x				
6	En su opinión, ¿cree que los bancos tienen responsabilidad por el uso de sus canales digitales, en los casos de operaciones no reconocidas? Fundamente su respuesta.	x				
7	Según su criterio, ¿por qué los usuarios son blanco de las operaciones no reconocidas a través de los canales digitales de los bancos?			x		Los usuarios en general
OBJETIVO ESPECÍFICO 2: Identificar los niveles de seguridad que las entidades financieras utilizan para reconocer las operaciones fraudulentas o "no conocidas" por los usuarios en sus canales digitales.						
8	En su opinión, ¿cree que, el uso de la identificación por número de celular o código por sms son eficaces ante las operaciones fraudulentas realizadas en canales digitales? Fundamente su respuesta	x				

Erick E. Romero Saavedra
REG CAL N° 59589

N.° de Ítem	Ítems del instrumento	Valoración				Sugerencias
		3	2	1	0	
9	En su opinión, ¿cree que la identificación por llenado de datos personales como: "nombres de padres, lugar de nacimiento, edad, DNI, número de Ubigeo o lugar de nacimiento de padres" son los adecuados ante la identificación de operaciones fraudulentas realizadas en canales digitales? Fundamente su respuesta	x				
10	Desde su punto de vista, ¿cuáles deberían de ser las medidas de seguridad que los bancos deberían de optar para poder reconocer las operaciones fraudulentas y si están sucedieran deberían de informar al usuario de inmediata?	x				

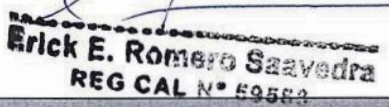
IV. CALIFICACIÓN Y OPINIÓN DE APLICACIÓN

Calificación	Aplicable	Aplicable después de corregir	No aplicable
75 %		Si, pero para pauta de entrevista. Aplicando la técnica de entrevista.	

V. LUGAR Y FECHA:

Lugar	Fecha
San Isidro	04 de mayo de 2023

VI. FIRMA Y POSTFIRMA DEL EXPERTO:



Romero Saavedra Erick Enrique

40151899