FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid19 en Lima-2020.

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogada

AUTORAS:

Paredes Salazar, Edith Silvia (ORCID 0000-0003-1912-0451)

Silva Rueda, Elsa Milagros (ORCID 0000-0001-6470-913X)

ASESOR:

Dr. Santiesteban Llontop, Pedro Pablo (ORCID 0000-0003-0998-0538)

LÍNEA DE INVESTIGACIÓN:

Derecho de familia, derechos reales, contratos y responsabilidad civil contractual y extracontractual y resolución de conflictos.

Lima – Perú

2021

Dedicatoria

A Dios que fue nuestro principal pilar y nos brindo el apoyo espiritual, a nuestros padres quienes nos dieron la vida, educación sobre todo consejos para seguir siempre adelante sin cesar, a nuestras hermanas que son ejemplos de perseverancia y a todos los que nos motivaron y creyeron en nosotras en el trayecto de nuestra carrera universitaria.

Agradecimento

En primer lugar, al profesor asesor de tesis, el Dr. Pedro Pablo Santisteban Yontop, por su paciencia, sus conocimientos rigurosos y precisos, en segundo lugar, a nuestros entrevistados, a quienes les debemos que nos hayan ampliado sobre el tema de nuestra tesis, finalmente a nuestros padres que nos dieron su motivación incondicional.

Índice de contenido

Índice De Tablas

Índice de figuras

RESUMEN

En esta investigación surgió de la identificación de un problema que aqueja a la sociedad desde el inicio de la era cibernética, pero que han ido incrementándose en tiempos de pandemia, esto es el ausentismo de los bancos tras el fraude cibernético Phishing; por tal motivo, se planteó como objetivo analizar de qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phising en tiempos de covid 19 en Lima- 2020; a fin de arribar a respuestas que contribuyan a finiquitar estas situaciones.

Para ello, se tuvo como base el enfoque cualitativo, tipo básico, nivel descriptivo y el diseño de teoría fundamentada; permitiendo obtener como hallazgos diversas fuentes de análisis documental, reforzadas con la aplicación de guías de entrevistas a expertos en la materia; lo que permitió tener como resultado y conclusión: Se determinó que la responsabilidad civil de los bancos frente al delito de fraude informático phising en tiempos de covid 19 en Lima- 2020. Se debe ser aplicada de manera objetiva debido que los bancos son los principales entes que utilizan a las plataformas digitales, existiendo actualmente usuarios que prefieren acercarse a una entidad bancaria, pero lamentablemente con el tema de la pandemia ya se incorporaron nuevas acciones que solo se realizan por la banca por internet, dejando toda la responsabilidad a los usuarios frente a los delitos informáticos, creando una situación de desprotección.

Palabras claves: Phishing, fraude cibernético, responsabilidad objetiva, teoría del riesgo

ABSTRACT

This research arose from the identification of a problem that afflicts society since the beginning of the cybernetic era, but which has been increasing in times of pandemic, that is, the absenteeism of banks after the cybernetic fraud Phishing; For this reason, the objective was to analyze how the civil liability of banks should be applied against the crime of computer fraud phishing in times of covid 19 in Lima-2020; in order to arrive at answers that contribute to finalizing these situations.

For this, the qualitative approach, basic type, descriptive level and the grounded theory design were based; allowing different sources of documentary analysis to be obtained as findings, reinforced with the application of interview guides to experts in the field; which allowed to have as a result and conclusion: It was determined that the civil liability of banks against the crime of computer fraud phishing in times of covid 19 in Lima-2020. It must be applied objectively because banks are the main entities who use digital platforms, there are currently users who prefer to approach a bank, but unfortunately with the issue of the pandemic, new actions that are only carried out by internet banking have already been incorporated, leaving all the responsibility to the users against computer crimes, creating a situation of vulnerability.

Keywords: Phishing, cyber fraud, strict liability, risk theory

I. INTRODUCCIÓN. -En referencia a la aproximación temática, el presente informe de investigación abarco un hecho importante por registrar las etapas en donde se ha ido incrementando las transacciones cibernéticas técnica que ha facilitado las labores diarias de la sociedad, sin embargo, se convierte también en un instrumento del cual se vale para concretarse actos contrarios a fines beneficiosos por los cuales fueron creadas y de esta forma sacar dichos beneficios de forma ilícita de ello.

Por tanto, en el **ámbito internacional** en Colombia estos tipos de delitos de fraude informáticos se identificó una gran problemática probatoria dado que las redes sociales son un medio de obtener información de las víctimas por tanto es complicado finalmente poder determinar la existencia de la responsabilidad del autor del delito.

No obstante en **el ámbito nacional** dentro de las bondades que da este avanzado instrumento no está libre de vulneraciones creadas por personas inescrupulosas con el fin de apropiarse de forma ilícita del patrimonio ajeno mediante engaños, de esta forma se adueñan de los datos personales , claves y atacan a la parte más débil que es el usuario, debido a esto existen controversias ya que los usuarios alegan que se encuentra Responsabilidad civil objetiva por parte de los bancos , en el **ámbito local** en Lima se ve el incremento de esta modalidad de delito con gran fluidez debido a las escasas implementaciones de seguridad en las plataformas virtuales y de esta forma cometer el ilícito donde en la gran mayoría de los casos se libera de responsabilidad a la entidad financiera ; por tanto como **posible solución a este problema** sería que las entidades financieras que prestan estos servicios virtuales ante esta clase de delito deben responder por los daños producidos que deviene de las actividades que prestan y proteger al usuario.

Por lo que, respecto a la formulación del problema, se consideró como **problema general**, ¿de qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de covid 19 en Lima- 2020?; el **problema específico 1** planteado fue, ¿de qué manera se debe evitarel ánimo de lucro frente a la modalidad vishing en tiempos del covid-19 en

Lima -2020?, y como **problema específico 2**,¿cómo se debe reponer el daño patrimonial frente la modalidad de smishing en tiempos del Covid 19 en Lima – 2020?.

Tal cuestionamiento, surgió como consecuencia de la revisión de información referida al tema, y aunado al contexto de la realidad actual, que denota situaciones del aumento de esta modalidad de delitos en el ámbito cibernético y se reflexionó sobre los contratos de adhesión que presentan las entidades bancarias para eludir la responsabilidad que deviene de las consecuencias de estos servicios , las medidas de protección ineficientes para la protección de estas transacciones , ocasionó que repercutan de esta forma se libere a la entidad bancaria de responsabilidades y se perjudique al usuario.

Por otro lado, en razón a la **justificación de la investigación** se ha tenido a la **justificación teórica**, que consideró y desarrolló en la parte conceptual aquellos conceptos afines de responsabilidad civil de los bancos, lucro indebido, daño patrimonial, delitos de fraude informáticos, medidas de protección al usuario; las mismas destinadas a ampliar el panorama legal, sea para estudiantes, abogados y demás interesados. De igual forma, en lo concerniente a la **justificación en la esfera práctica**, la importancia radicó en que dio respuesta a una problemática común y con gran reincidencia encontrado en el contexto social que actualmente atraviesa el país, con la finalidad de determinar la responsabilidad que no es aplicada debidamente, lo cual conlleva a que se agudice el problema, en efecto ver alternativas que posiblemente contribuirán a efectivizar la normativa civil vigente; asimismo, mediante la **justificación metodológica**, se empleó y aplicó el método científico, así como, diversa normativa y técnicas, que permitieron elaborar de forma debida y correcta la presente investigación proba, por ende, el sustento fue la realización del análisis de libros, tesis, artículos de revistas indexadas nacionales e internacionales, jurisprudencia, doctrina, derecho comparado, entre otros.

Por lo tanto, el presente informe de investigación contribuyo a implantar criterios jurídicos que se deben valorar para determinar la responsabilidad de los bancos para proteger la tutela del usuario sobre todo evitar los delitos cibernéticos cometidos dentro de las plataformas virtuales de las entidades financieras, siendo relevante porque podría influir en la determinación de la aplicación de la

responsabilidad civil de las entidades financieras en los casos en los cuales el delito de fraude cibernético phishing es aplicado contra los usuarios en sus cuentas bancarias. Ello permitió establecer el siguiente **objetivo general**: analizar de qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phising en tiempos de covid 19 en Lima- 2020; como **objetivo específico 1**: analizar de qué manera se debe evitar el ánimo de lucro frente a la modalidad vishing en tiempos del covid19 en Lima -2020; y **objetivo específico 2**:analizar cómo se debe reponer el daño patrimonial ante la modalidad de smishing en tiempos del covid19 en Lima – 2020.

Así mismo establecemos el siguiente **supuesto general:** El delito fraude informático phishing crea una controversia generalizada ya que los bancos no asumen su responsabilidad frente a estos robos cibernéticos y al contrario se responsabiliza el usuario, sin embargo; el ente que tendrá que asumir las consecuencias es el banco, por ser quien ofrece una banca virtual, y está en el deber de brindar la información, las precauciones y medidas de seguridad frente a estos riesgos. Por consiguiente, el **primer supuesto específico** Los bancos afirman que uno de sus métodos de seguridad para proteger las cuentas del usuario son los llamados estándares de idoneidad que son los datos personales del usuario es el acceso a la cuenta es inmediato con esto se atribuyó que el usuario proporcionó bajo su voluntad estos datos a un tercero según el Contrato de adhesión celebrado ; pero debe prevalecer la circunstancia de que el usuario no le dio sus datos personales a un tercero , sino más bien crean que era el mismo ente lo cual no configura con lo que se le atribuyo al usuario y por ende debe prevalecer el Principio de Primacía de la Realidad; y por último el **segundo supuesto específico** que el banco debe probar para que no se le atribuya responsabilidad que este fraude informático ha sido un hecho extraordinario, irreversible e irresistible pero jamás se llega a probar ; es más en sentencias anteriores no se le pide dichos requisitos y pese a esto se le libera lo cual a nuestro criterio no es factible ya que el banco debe poner el total del daño patrimonial en la modalidad del delito de smishing.

II. MARCO TEÓRICO.- Para sustentar este informe de investigación debemos valorar y realizarlo en base a trabajos previos, de los cuales tenemos el ámbito nacional, citando a Campos (2018), en su investigación titulada "El deber civil de las entidades financieras por el peligro de *phishing"*. Esta investigación tuvo un enfoque cualitativo, asimismo se determinó como objetivo general establecer patrones de fraude, en razón al estudio estructurado de los datos históricos de las operaciones, los mismos que deberán incluirse al sistema que realiza el monitoreo de las operaciones o movimientos realizados. Se concluyó que existe la deficiencia de los bancos en la detección oportuna y verificación con los retiros, asimismo que las entidades bancarias tienen el deber de acreditar que sus sistemas de protección contienen valores prohibitorios los cuales imposibilitan la generación de los diversos modos de fraudes, dentro de los que se utilizan**.**

Por otro lado, Pardo (2017) en su tesis titulada "Procedimiento legal jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018". La tesis acotada tuvo su enfoque cualitativo y se logró obtener como objetivo general; Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018. Se concluyó que el procedimiento legal de los delitos informáticos contra los bienes no resulta efectivo, pues en este tipo penal se encuentra el fraude informático y todas sus modalidades, los cuales generan suspicacia al momento de revisar el marco normativo, puesto que el mismo no permite cumplir eficazmente el marco normativo.

Por otro lado, León (2018) en su tesis titulada "Agujeros jurídicos que no admiten el uso de castigos por delitos informáticos en la ley n° 30096 y modificatoria en el distrito cercado lima 2017". Esta investigación tuvo enfoque cualitativo y como objeto general, se obtuvo; señalar los agujeros jurídicos que no admiten el uso de castigos por delitos informáticos en la Ley N° 30096 Cercado Lima 2017. Se llegó a la conclusión que los delitos informáticos no deberían restringir al sujeto de proveer la tecnología, opuestamente, se debería reforzar las políticas de estado y la proporción de la información con fin de garantizar la seguridad, el control y integridad de la información, etc. en las instituciones.

Por otro lado, Mengoa (2015) en su investigación titulada “Punibilidad del comportamiento del phishermule en el delito de fraude informático en el Perú”. En la presente indagación se empleó el enfoque cualitativo se obtuvo como objeto general determinar cómo el comportamiento del phishermule incurre en los delitos informáticos a la luz del Derecho Penal Peruano. Se concluyó que en Perú carece de organismos públicos sólidos que tengan niveles y mecanismos adecuados para luchar contra los delitos informáticos.

Asimismo, Abanto (2020) en su investigación titulada “La clonación de tarjetas de crédito y la obligación civil de los bancos, olivos año 2020”. La indagación presento un enfoque cualitativo, asimismo se obtuvo como objeto general Analizar si los bancos tienen responsabilidad civil en la clonación de tarjetas de crédito en el distrito de Los Olivos, 2020. Se concluyó que en las entidades financieras si debe asumir la responsabilidad en el pago de los bienes de los que se obtuvo por la clonación, una vez comunicado y confirmado con la entidad las operaciones no reconocidas, siguiendo el protocolo de reclamo, se debe realizar el pago por el resarcimiento, pero se observa que en ocasiones la entidad asume su responsabilidad cuando el tarjetahabiente acude a otras vías como medio alternativo.

En el **ámbito internacional** el autor Martínez (2015) en su tesis titulada “El deber de los bancos ante a los delitos informáticos”. En esta investigación tuvo como enfoque cualitativo, además como objetivo general se obtuvo; determinar si es suficiente el mecanismo de responsabilidad bancaria frente a delitos informáticos establece la responsabilidad al banco. Concluyó que Las entidades bancarias al igual que los usuarios se ven perjudicados en la comisión de estos delitos, puesto que gran parte de ellos es cometido por terceros sin vinculo a la entidad financiera, pero cabe resaltar que éstas últimas se encuentran en el deber de brindar a sus clientes protección con tecnología adecuada para el ingreso a sus plataformas vía online.

Asimismo, Alarcón & Barrera (2017) en su tesis titulada “Empleo de internet y delitos informáticos en los alumnos del primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016”. La indagación presento un enfoque cuantitativo el cual logro como objeto establecer el

nexo del empleo del internet con los delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, seccional Sogamoso, 2016. Se concluyó que el empleo de tecnología y las plataformas digitales permiten la ocurrencia de los delitos de esta naturaleza, esto es debido al empleo de redes sociales y el internet.

Por otro lado, Ruiz (2016) en su tesis titulada “Estudio de los delitos informáticos y su transgresión a los derechos constitucionales de las personas”. En esta investigación tuvo como enfoque cualitativo, además, se obtuvo como objetivo general dar una visión clara sobre los delitos de fraude informático, especialmente de la violación que se perpetra hacia los derechos constitucionales de las personas, a mediante el empleo de nuevas tecnologías de comunicación y de la información, como son las redes sociales, los correos electrónicos, el comercio electrónico que actualmente es un boom a raíz de la situación crisis sanitaria que atraviesa el mundo; asimismo se analiza y conceptualiza la naturaleza de las Infracciones Informáticas y sus tipificaciones de acuerdo a sus características principales, además se plantean posibles alternativas de solución para castigar los ilícitos informáticos y evitar la perpetración de estos delitos que vulnera. Los derechos constitucionales del ciudadano. Concluyó que las redes sociales son un mecanismo para interactuar los sujetos, los cuales en algunos casos comparten intereses y ello conlleva al intercambio de información, lo cual es además el medio idóneo para la realización de actos delictivos a través de la internet.

Asimismo, Salas (2017) en su tesis titulada “Obligación civil de las entidades financieras ante los consumidores por delitos informáticos”. El enfoque de la citada tesis es cualitativo y se obtuvo como objeto general revisa la objetividad de la obligación civil de las empresas del sistema financiero, en el caso de que uno de sus consumidores es víctima de un delito informático. Concluyó que la responsabilidad civil objetiva como opinión de impugnación, la finalidad es reparar el daño causado por el delito informático que permanecía fuera de la esfera de responsabilidad civil subjetiva. Por ello se debe buscar la ampliación de protección legal para todas las situaciones en las que se genere afectación y deba ser reparada. Por tanto, Hidalgo (2018) en su tesis titulada “Los ilícitos informáticos y su repercusión en las riquezas legales”. tuvo como enfoque cualitativo se estudiar

las riquezas legales como un sacramento constitucional y social y su incurrencia en los delitos informáticos con la finalidad de otorgar relevancia a la indagación, y en la supuesta configuración de un delito. Concluyó que se visualiza la fenomenología en el aspecto penal, ya sea por el incremento indiscriminado de las acciones, lo cual conlleva va a los magistrados a la creación de nuevas normativas en las cuales encuadran estos nuevos tipos penales, pero de otro lado resultan algunas veces ineficientes y no llegan a salvaguardar la bien jurídica materia de discusión.

En relación a los enfoques conceptuales de la categoría **la responsabilidad de los bancos** nos dice que las entidades privadas en el rubro financiero en los casos de su responsabilidad subjetiva, están obligado a dar seguridad en las transiciones electrónicas con mayor grado de seguridad. Pero excluyen de esa responsabilidad subjetiva cuando al cliente se le verifica su responsabilidad por negligencia. (Rodríguez, 2014).

De acuerdo con el artículo 1969 del Código Civil nos dice que el que por dolo o culpa origina un menoscabó a otro se encuentra en la obligación de indemnizar.

Debemos tener en cuenta que se ha originado una constante discrepancia en el ámbito financiero y bancario frente a su responsabilidad objetiva con sus usuarios, ya que ambas partes se ven agraviadas por un tercero, el cual afecta la relación de estos, al ser un problema complejo en la legislación, por ende, el Estado debería proporcionar soluciones igualitarias a los involucrados, pero la realidad es diferente ya que existen vacíos legales. (Zabala, 2017).

Por otro lado, como subcategoría **es el ánimo de lucro** es entendible como acción del sujeto activo para realizar un hecho punible concretamente para la obtención de aprovechamiento económico en sí mismo. (Mayer & Oliver**,** 2020). Cabe resaltar que la realización de una actividad económica con mira a la obtención de un beneficio, el que podría o no ser repartido en cualquiera de sus miembros o cualquiera fuese una persona natural. (Iribarra, 2017).

Asimismo, como otra subcategoría es **el daño patrimonial** es toda afectación que se genere de un situación dolosa o culposa, por tanto, la indemnización se dará de forma secundaria; siempre y cuando los métodos empleados hayan sido ineficaces, y cumplan con la responsabilidad reparatoria. (Isler 2020)

En el contexto sobre otra categoría **delitos de fraudes informáticos** se relaciona con la puesta en marcha de operaciones bancarias, ya que la corroboración online es difícil de comprobarse debido a su fácil manipulación. (Mayer & Oliver 2020).

El fraude informativo son trasgresiones que se vincula al robar información de las personas que utilizan el internet para beneficios de ellos. Por tanto, nos mencionan que esos delitos de fraude de información son la violencia en contra de tu información personal y financiero de las personas para beneficios de un tercero. **(**Saltos, Robalino & Pazmiño2021).

Lamperti (2017) establece que un suceso de relevancia jurídica forma parte de un delito, lo que conlleva a señalar que cualquier suceso para ser delito debe estar establecido en la normativa penal; por ello se puede decir que la acción enmarca en un tipo penal, esto es conocido como principio de legalidad, y el juez está impedido de otorgar sanciones por acciones que no se encuentren en el tipo penal legalmente establecido.

El delito informático comprende acciones delincuenciales que diversos países han buscado enmarcar en tipos penales de origen común, como son: robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Cabe resaltar que el empleo de nuevas modalidades de tecnologías informáticas lo que da origen a una nueva probabilidad de utilización ilegal de computadoras lo que conlleva a necesitar un marco normativo en la esfera del derecho. (Imbaquingo, et. al, 2016).

Ley de delitos informáticos ley Nª 30096 en su Art. 8 Artículo modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente: nos dice que:

> El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa.

El phishing consiste en una acción de defraudación patrimonial que consiste utilizar un objeto o dispositivo llamado scanner para poder obtener información confidencial en el tema financiero en tanto lo beneficie al que realiza la acción delictiva. (Ortiz, 2019)

Por otro lado, Díaz, Angulo & Barboza en modalidad **vishing** nos dicen que:

> La forma para realizar este delito es el empleo el protocolo VoIP o mediante suplantación de los trabajadores bancarios en llamadas, las mismas que corroboran la visualización de transacciones inusuales con las tarjetas de crédito de la víctima con el propósito de la obtención minuciosa de como claves de usuario para posteriormente perpetrar delito. (2018, p.12)

Daño patrimonial es toda afectación que se genere de un situación dolosa o culposa, por tanto, la indemnización se dará de forma secundaria; siempre y cuando el mecanismo otorgado para evitar el daño no resulte eficaz, y debe cumplir el presupuesto de responsabilidad preparatoria. (Isler2020)

Por otro lado, Díaz, Angulo & Barboza en **modalidad smishing** nos dicen que:

> Esta modalidad de delito utiliza los teléfonos móviles de los usuarios financieros, los delincuentes pretenden suplantar la identidad, a menudo de personal bancario o establecimientos comerciales, gerentes o representantes de ventas con el fin de que las personas accedan mediante mensaje de texto o llamada a un link que le proporcionara al atacante información necesaria para hackear el teléfono de la víctima. (2018, p.31).

It is the pertinent disposition to obtain the information of the financial companies that opts for this technology of operations via internet; therefore, it is important to protect these operations from different threats, such as phishing, in order to avoid cybercrime against its users, which is why technicians in this area are vital. (Mushtaque, Ahsan & Umer2015).

Es la disposición pertinente de obtener la información de las financieras que opta por esta tecnología de operaciones vía internet; por tanto, es importante proteger estas operaciones de las diferentes amenazas como por ejemplo la modalidad de

phishing para poder evitar los ciberdelito en contra de sus usuarios, por ello son vitales los técnicos en esa materia. **(**Mushtaque, Ahsan & Umer2015).

The majority of users who despite suffering a cyberattack in the vishing mode or another type of computer fraud modality still claim to be affected by this computer crime, however, what they report are people whose amounts are too high. On the other hand, the other users only leave their claim in the financial institution as a suggestion to put more security in their electronic services. (Echeverría, Garaycoa & Tusev, 2020).

La mayoría de usuarios que a pesar de sufrir con un ciberataque en la modalidad vishing u otro tipo de modalidad de fraude informático han manifiesta todavía ser afectado por ese delito informático, sin embargo, que lo que denuncian son personas que los montos son demasiados altos. En cambio, los otros usurarios solo dejan su reclamo en la entidad financiera como sugerencia de poner más seguridad en sus servicios electrónicos. (Echeverría, Garaycoa & Tusev, 2020).

Respecto a los **enfoques conceptuales** los cuales nos permite profundizar en la presente investigación teniendo en cuenta como primera definición **la responsabilidad de los bancos** consiste en la afectación que se hace a otra persona y cuando de verifica el daño causado. Por tanto, se identifica la responsabilidad objetiva del daño causado. En tanto **los delitos de fraude informáticos** constituye acciones delincuenciales que diversos países han buscado enmarcar en tipos penales de origen común, como son: robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. En relación a la modalidad **phishing,** Se define como la acción que realiza un tercero de manera ilícita utilizando un dispositivo de scanner para apropiarse de patrimonio e información financiera de un individuo.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

La actual indagación presento un **enfoque cualitativo**, ya que explica y realiza el planteamiento de incógnitas en el desarrollo del estudio. Se caracteriza por la recolección de información (Sampieri y Collado, 2013, p.21).

Asimismo, presenta un enfoque cualitativo, puesto que emplea singularidades y características de las categorías, asimismo recopila datos sin medición numérica, ya que el fin es la recopilación de información no estructurada (Noruega, 2014, p. 49).

En ese sentido, se exploró y describió la fenomenología vista de diversos aspectos, estableciéndose la **aproximación temática**; por ello ha tenido como particularidad que no se probaron hipótesis, lo cual hace referencia a que, no se realizaron procedimientos estadísticos; pues los supuestos se generaron antes, y durante el transcurso de la indagación, se utilizó **Análisis de fuente documental.** De esta forma, la revisión de las técnicas de recopilación de información, tuvo carácter inductivo.

La investigación es de **tipo básica**, según Tam, Vera y Oliveros (2008), este tipo de indagación tiene como finalidad primordial recopilar información para ampliar un conocimiento o crear uno nuevo (p. 146). Por lo tanto, después de identificar la problemática actual de la sociedad, se empleó distintas fuentes para establecer el origen de los mismos, para que a través de un procedimiento informativo se encuentre posibles alternativas de solución ante la problemática encontrada.

Resulta imprescindible establecer que, al referirnos a una investigación del tipo básica, se buscó aumentar el entendimiento de las teorias, empleando el **nivel de investigación descriptivo** en razón que la descripción, del funcionamiento y como se está realizando la fenomenología a estudiar, por ello el indagador no puede intervenir en el funcionamiento.

Por ello, no se influencio en los datos recopilados de distintas fuentes, ni en el problema real de la indagación, puesto que, según señala el autor, se centró en la búsqueda de descripción del objeto de la indagación, según el desarrollo, sin modificarla.

Diseño de investigación: Al presentar un enfoque el cualitativo, según señala Hernández, Fernández y Baptista, el diseño dio respuesta a la **teoría fundamentada**, dado que resulto la más acorde al enfoque y objetivo de la actual indagación, dado que, es un diseño y un resultado del cual el indagador recopilara una aclaración, de la fenomenología analizada en un espacio establecido, de forma que, de la teoría generada derivada de la recolección de datos del campo. (2014, p. 472).

Por ello, a través de la teoría fundamentada se abordó de manera global los problemas analizados, de esa manera, se aportó recientes puntos de vista de la fenomenología analizada, a través de un procedimiento donde se empleó la interpretación. Esto a su vez, permitió que se crearan recientes teorías provenientes de la recolección de información en el campo indagado, la cual al ser procesadas y analizadas generaron una nueva teoría. Es de manifestar, que las aportaciones de derecho desarrollados en el ámbito teórico, contribuyeron en la formación de las teorías que responden al objetivo planteado por las investigadoras.

3.2 Categorías, Subcategorías y matriz de categorización

Noruega (2014) las categorías son cuestiones que se encuentran inmersos en la exploración y que posteriormente serán analizadas y trabajadas, como: La unidad temática se realiza en relación al tema de estudio.Por ello en esta investigación determino en la siguiente tabla las categorías y subcategorías de este artículo de revisión:

Tabla 1. *Tabla de Categorías y Subcategorías*

Categorías	Subcategorías
RESPONSABILIDAD CIVIL DE LOS BANCOS	**1. El ánimo de lucro**
	2. **Daño patrimonial**
DELITO DE FRAUDE INFORMATICO PHISING	**1. Vishing**
	2. Smishing

Fuente: elaboración propia.

3.3 Escenario de estudios.

Zúñiga (2007) señala que:" el escenario está conformado por un lugar determinado y físicamente apto para dar uso al instrumento, en este caso la entrevista" (p.24). En ese sentido el escenario se ubicó en Poder Judicial, La corte Superior de Justicia Zúñiga (2007) señala que: "el escenario está conformado por lugar determinado y físicamente apto para dar uso al instrumento, en este caso la entrevista" (p.24). En ese sentido el escenario se ubicó en el Poder Judicial, La Corte Superior de Justicia e Indecopi, se recogió información de especialistas tanto en material civil como penal.

3.4 Participantes.

Si bien es cierto los individuos participantes de la presente indagación deben cumplir con ciertas características, que son requeridas según el tipo de investigación. Es por ello que Balestrini (2012). establece que, a caracterización de los individuos, proporciona diferentes informaciones, siempre se solicita sujetos acordes a la investigación.

En ese contexto, los participantes de la presente tesis, son conocedoras y ejercedoras del derecho, por ende se le consideran expertos y el juicio u opinión emitidos por ellos es relevante respecto al tema abordado.

Por consiguiente, los participantes en el presente trabajo de investigación fueron **1 Juez** especializado en la materia Civil, **1 juez** especializado en la materia penal, **1 especialista** del área de infracciones de INDECOPI, **2 especialistas** del Poder Judicial, **3 abogados** especialistas en materia civil y **2 abogados** especialistas en materia penal, es importante señalar que los participantes en mención fueron elegidos en razón a nuestra conveniencia, puesto que se consideró el fácil acceso a sus instituciones, asimismo la disponibilidad de los expertos para la contribución de información.

Tabla 2. *Tabla de escenario de estudio y participantes*

ESCENARIO DE ESTUDIO	*PARTICIPANTES*
Juzgado Judicial de Lima Norte	2 Jueces (civil, penal)
Área de infracción, comisión de signos distintivos de INDECOPI	1 Especialista
Poder Judicial Lima Norte	2 especialistas del Poder Judicial
Estudio Jurídico de abogados especialistas en materia civil	3 abogados especialistas en materia civil
Estudio Jurídico de abogados especialistas en materia penal	2 abogados especialistas en materia penal
TOTAL:	10 participantes

FUENTE: elaboración propia.

3.5 Técnicas e instrumentos de recolección de datos.

Para la investigación cualitativa la **recopilación de datos** es fundamental para obtener la perspectiva de los entrevistados en base a la realidad problemática que se encuentra siendo materia de investigación.

Por ello, se utilizó en la presente tesis la entrevista como primera técnica y como segunda, el análisis de fuente documental, que permitieron responder al objetivo de la investigación, por lo que se encontraban directamente relacionadas tanto a las categorías, así como a las sub categorías. En ese sentido, la técnica de la entrevista, se define como una reunión acontecida entre el entrevistador y el entrevistado, en la cual se busca construir de manera conjunta significados relacionados a un tema en específico, conversando e intercambiando información (Hernández, Fernández y Baptista, 2014, p. 403).

Asimismo, el instrumento de la entrevista fue la guía de la entrevista, en la cual se plasmaron tres preguntas por cada objetivo de la investigación, es decir nueve preguntas entre el objetivo general y los objetivos específicos, estas fueron elaboradas de forma abierta, clara, y precisa, por ende el entrevistado fue capaz de dar respuesta a los objetivos planteados.

Por otro lado, se empleó la técnica de análisis documental, que es importante y aportante para la presente tesis, puesto que resulta de provechosa y ayuda al investigar temas que dejan registros tanto en escritos, medios digitales u otros (Tello, Verástegui y Rosales, 2016, p. 78).

Asimismo, debemos señalar que la técnica del análisis documental tuvo como instrumento: la guía de análisis de la ley, la guía de análisis de resoluciones administrativas. la guía de análisis de artículo informativo de página web, guía de analisis de informes, guia de analisis de publicación en los medios de comunicación visual, las mismas consistieron en la realización de fichas de análisis de fuentes documentales, que sirvieron de apoyo para realizar el análisis integral respecto a los temas de la investigación.

Cabe señalar que, los precitados instrumentos fueron aplicados en relación a las muestras por conveniencia, asimismo por expertos, puesto que los participantes fueron profesionales especialistas con dominio en el tema de investigación abordado, es decir, las preguntas y respuestas estaban directamente orientadas a responder ante el objetivo de la presente investigación; igualmente, las fuentes de información empleadas, fueron

aquellas que contribuían, aportando datos relevantes a fortalecer las teorías formuladas en el contexto de análisis, ambos instrumentos se encontraron debidamente validados en señal de conformidad, como figura a continuación.

En razón a lo señalado, se consolidó en la siguiente tabla el porcentaje calificado, tras la elaboración del instrumento de guía de entrevista, donde los tres docentes expertos metodólogos de la UCV consignaron el meriorio prcentaje de 95%.

Tabla 3. *Tabla de validación de la guía de instrumentos.*

VALIDACION DE INSTRUMENTOS (Guía de entrevista)		
Datos generales	**Cargo**	**Porcentaje**
Dr. Pedro Pablo Santisteban Llontop	Docentes de metodología de la investigación científica en la Universidad César Vallejo.	**95%**
Mgtr.Ángel Fernando La Torre G.		**95%**
Mgtr.Eliseo Segundo Wenzel Miranda		**95%**
PROMEDIO		**95%**

FUENTE: elaboración propia

Por otro lado, para la elaboración de la guía de análisis documental se asignó el 95% en señal de aprobación, lo cual fue un logro para su posterior aplicación en el resultado y discusión.

Tabla 4. *Tabla de validación de la guía de análisis documental*

VALIDACIÓN DE INSTRUMENTOS (Guía de entrevista)		
Datos generales	**Cargo**	**Porcentaje**
Dr. Pedro Pablo santiesteban Llontop	Docente de metodología de la investigación científica en la Universidad César Vallejo.	**95%**
PROMEDIO		**95%**

FUENTE: elaboración propia.

3.6 Procedimiento

Para Rodríguez, el empleo de diversas fases tales como: señalar la realidad, formulación de incógnitas, empleando los supuestos establecidos. Además, al realizar y determinar la técnica, posteriormente se realizó el tipo de estudio y el diseño de investigación, para concluir; sin embargo, las obtenidas con las recomendaciones correspondientes.

3.7 Rigor científico

El rigor científico es de carácter relevante e indispensable para lograr el desarrolllo de la tesis y otrogarle la confiabilidad y la validez correspondiente, para ello se seguirán los siguientes campos dentro de los cuales se encuentra la d**ependencia, la credibilidad, la triangulación y la transferencia,** estos son criterios relevantes puesto que aportan a construir una investigación de calidad respetando los parámetros de la ciencia, obteniendo como resultado el desarrollo de una investigación sólida, con argumentos válidos y encaminados a la obtención de un resultado legítimo.

3.8 Método de análisis de información

El instrumento a utilizarse es la entrevista, cuyo fin es obtener un estudio de la información recopilada eficazmente para la indagación y correcta interpretación. Este tipo de estudio es particular de las investigaciones cualitativas, pues desglosan minuciosamente el significado para determinar la esfera determinada.

a) Método Hermenéutico: Con este método se interpretó los datos recolectados, que permitió, darle el significado o aclaración a la información recabada, pudiendo convertirla en un aporte.

b) Método Sistemático: ha estado ligado al desarrollo del método científico. Sus usos más comunes son en la sistematización de información o datos y en la sistematización de experiencias. El primero se refiere al ordenamiento y la clasificación de datos e información y el segundo a procesos que se desarrollan en un periodo determinado, en un contexto económico-social y dentro de una institución dada.

c) Método Comparativo: La comparación que se realizó fue examinando toda la información recolectada a través de los instrumentos, en relación con las teorías y los antecedentes, ello permitió obtener resultados verídicos.

d) Método Exegético y Sintético: Permitió que en el desarrollo de la investigación el objeto de estudio sea descrito y desarrollado empleando normativa jurídica, de la que se encontró luego de un proceso de análisis el significado que le da el legislador. En el caso

del método sintético, contribuyó a sintetizar la información obtenida de modo que, se obtuvo la idea central más relevante.

e) Método analítico: Martínez (2016), precisa que el método se utilizó para analizar la documentación referente al tema de in- vestigación, lo cual permitió la extracción de los elementos más importantes que se encadenan con el objeto de estudio (p.45).

f) Método inductivo:Caduch(2014)señala que: “el método inductivo permite obtener conocimientos de peculiaridades globales, las mismas obtenidas de la comparación, y es así que se formulan las preposiciones, además estudia la doctrina, la normativa, etc. (p. 33).

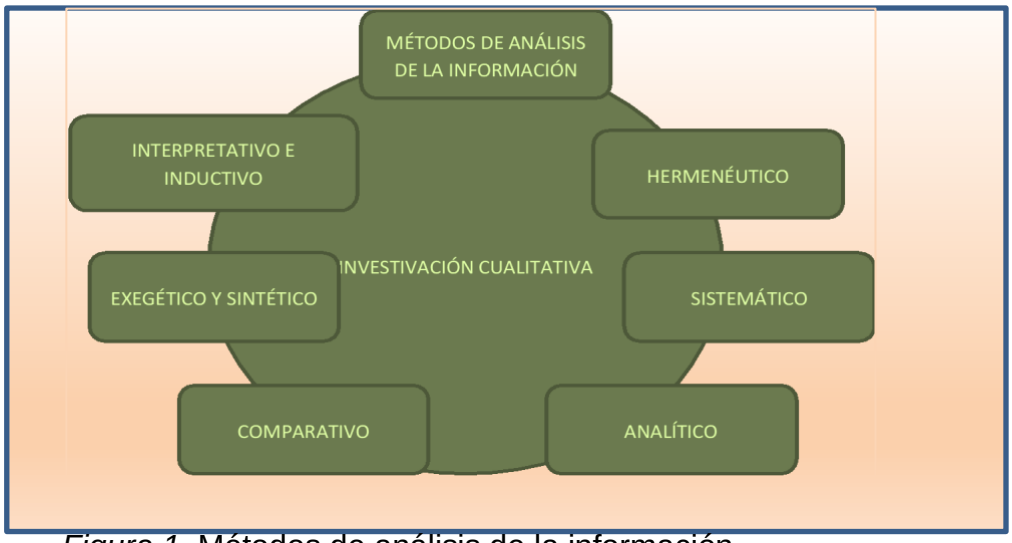


Figura 1. Métodos de análisis de la información.

3.9 Aspectos Éticos

El presente trabajo se encuentra realizado cumpliendo los lineamientos presentados por la Universidad Cesar Vallejo, respetando los derechos de los entrevistados y todos los sujetos que participen en la investigación, puesto que se encuentra enmarcado dentro de la ética. Asimismo, respeta las normas APA, respecto a las citas, fuentes, etc.

IV. RESULTADOS Y DISCUSIÓN

En relación los resultados, estos se basaron en la utilización de los instrumentos del enfoque cualitativo, los cuales fueron La guía de entrevista, asimismo la guía de análisis de fuente documental los cuales cumplen con los parámetros y criterios del rigor científico, otorgándole confiabilidad y credibilidad al presente trabajo, finalmente se contribuyó con los hallazgos plasmados en el marco teórico, confromados en el orden siguiente: por los antecedentes nacionales e internacionales, las revistas jurídicas indexadas y los enfoques y teorías conceptuales. Cabe señalar que todo lo mencionado, posteriormente se sometió a discusión.

En ese orden de ideas, para obtener los resultados de las **entrevistas** que aportaron con nuestro **objetivo general** que fue: Analizar de qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phising en tiempos de Covid 19, se plantearon 3 preguntas para recolectar información relevante, Por ello, se plantearon las preguntas presentadas a continuación:

1. ¿De qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid 19 en Lima- 2020?

Al respecto, el magistrado **Rodríguez y** el abogado civilista **Fernández(2021)** coincidieron en considerar que la entidad financiera debe asumir una responsabilidad civil objetiva y que el banco debe resarcir el daño al patrimonio del usuario quien confió en el banco, pero no se le otorgó las medidas correspondientes ante esta nueva modalidad de robo de información financiera, pero que esta entidad debe conocer su modalidad de perfección para contrarrestarla. Con lo que también concuerda **Tineo (2021),** pero a su vez agrega que debería implementarse medidas de seguridad en la detección de fraudes cibernéticos para que así ofrezcan una atención adecuada a los usuarios que se vieron perjudicados con el uso de las plataformas digitales.

En acotación a ello, **Gastiaburu (2021)**: precisa que los bancos hacen referencia el mal manejo de los usuarios de las plataformas tecnológicas, buscando así librarse de toda responsabilidad, por ello se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la seguridad financiera suficiente a sus usuarios.

Por su parte, **La Torre (2021)** precisó que: La responsabilidad civil de los bancos frente al delito de fraude informático phishing, debe ser tratada de forma radical y sancionadora, buscando que los bancos también asuman su responsabilidad por la exigencia que realizan del uso de plataformas digitales y como sabemos existen usuarios que no se llegan a familiarizar con estas plataformas, cayendo en algunos casos en error y es allí donde se ven envueltos en los delitos cibernéticos.

En ese orden de ideas, el magistrado **Chávez y Ponce (2021)** respondieron que: Se debe establecer una responsabilidad directa, ya que son los bancos los principales entes que utilizan a las plataformas digitales, existiendo actualmente usuarios que prefieren acercarse a una entidad bancaria, pero lamentablemente con el tema de la pandemia se incorporaron nuevas acciones que solo se realizan por la banca por internet, dejando toda la responsabilidad a los usuarios frente a los delitos informáticos, creando una situación de desprotección.

Aunado a ello, **Callirgos (2021)** nos manifiesta que el banco debe responsabilizarse en su totalidad del dinero robado de forma fraudulenta a los clientes de estas mismas ya que el phishing es una nueva modalidad de robo de información pero que esta entidad debe conocer su modalidad de perfección.

En contraposición **Melgarejo y Cadenillas (2021)** coincidieron en que se debería aplicar la Responsabilidad subjetiva, enfocado a una Reparación civil dependiendo el grado de su participación y en efecto ante las circunstancias en reintegrar el monto económico afectado del agraviado, debido a la relación contractual entre el banco y cliente, en calidad de consumidor.

2. ¿qué responsabilidad civil tienen los bancos cuando los datos personales y financieros se filtran de una persona?

Este periodo de crisis sanitaria se filtran en mayor porcentaje los datos personales y financieros de las personas, ello en razón al avance desmedido del uso de la tecnología y al respecto **Rodríguez, Chávez, Cadenillas, Tineo y Gastiaburu (2021)** consideraron que las entidades financieras tienen responsabilidad directa, pues se entiende como aquella que se manifiesta cuando los bancos hacen uso de los datos personales y financieros para ser filtrados, asimismo **Torre (2021)** coincide con lo manifestado, sin embargo en modo de complementación agrega que dichas entidades deben asumir las consecuencias de ello, de igual modo **Ponce (2021)**, se encuentra en el margen de quienes refirieron que tras la filtración de datos personales y financieros de los usuarios,

hacemos referencia a la responsabilidad directa, ya que el resguardo de estos datos es exclusivamente de la entidad bancaria.

De otro lado, **Melgarejo (2021)** indicó que los Bancos poseen una gran base de datos personales y financieros de cada cliente, por ende, están sujetos a una estricta conservación de los mismos, ante un filtro de ellos afectaría y vulneraria el patrimonio económico del cliente o consumidor, generando pérdidas al patrimonio, podemos recomendar denunciar ante INDECOPI por los daños al consumidor.

En tanto, **Callirgos (2021)** manifestó al respecto que los bancos al ser un servidor público y al ofrecer estas alternativas de uso de sus servicios debe procurar cuidar al cliente de estas modalidades de estafas por eso al caer en este delito el cliente la entidad debe responsabilizarse de forma objetiva.

Por su parte, **Fernandez (2021)** consideró al respecto que debe aplicarse el Art.1969 de C.C.P , puesto que hay daño generado por culpa del banco y en consecuencia, una responsabilidad total ya que este es experto en banca virtual y estos mismos no tienen seguridad propia para evitar los daños en perjuicio del patrimonio del usuario.

Finalmente, se planteó la tercera pregunta en relación al objetivo general:

3. ¿Qué medida recomendaría para que la responsabilidad Civil de los bancos sea aplicada dentro del contrato de adhesión en el tema de delito fraude informático?

Frente a esta interrogante, **Rodríguez (2021)** recomendó la implementación de medidas idóneas de seguridad como un filtro de información para que así no se pueda vulnerar el derecho a la información personal con facilidad, coincidiendo al con lo señalado el especialista Fernández **(2021).**

En tanto, **Gastiaburu, La Torre, Ponce Chávez y Tineo (2021)** precisaron que se deben establecer dentro del contrato disposiciones de cláusulas contractuales

que los resguarden frente a los delitos informáticos a fin de evitar la vulderación del derecho a la protección de datos personales y financieros.

Aunado a ello, **Melgarejo (2021)** recomendaron que: Los Bancos o entidades financieras, Ofrecen un servicio y obtienen un beneficio “contraprestación” bajo esa lógica deben responder conforme lo señalado por la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor “cliente” en ese sentido no se ha cumplido con el Contrato establecido entre partes, requiriendo una sanción por la inconducta contractual y las determinando el grado de participación en el delito Informático.

Otro punto relevante y mencionado repetitivamente por los participantes durante esta entrevista, fue la falta de coordinación de las partes, es decir tanto de la entidad financiera como de la parte contratante, puesto que los usuarios no leen los contratos antes de firmarlos y más aún si estos son los famosos contratos de adhesión a los que nos encontramos subordinados.

Por otro lado, **Callirgos (2021)** refirió que se debería aplicar otra clase de contrato donde haya también cláusulas que responsabilice al banco frente a estos delitos de la nueva era.

En controversia y difiriendo con lo expuesto por los demás especialistas, **Cadenillas (2021)** recomendó que dentro de las clausulas están especficas todo lo comprendido acerca de acudir a una banca por internet, por ende el usuario al firmar el contrato sabe a lo que se tiene que pegar.

En continuación con los resultados, se plantearon tres preguntas para recolectar información relevante para **el objetivo específico uno** que es: Analizar de qué manera se debe evitar el ánimo de lucro frente a la modalidad vishing en tiempos del covid-19 en Lima -2020. Las interrogantes son las siguientes:

4. ¿De qué manera se puede evitar el ánimo de lucro frente a la modalidad vishing en tiempos del Covid-19 en Lima -2020?

Ante la interrogante planteada, coincidieron los magistrados **Rodríguez y Chavez,** asimismo los especialistas **Ponce, Gastiaburu y Tineo (2021)** quienes indicaron que se evitaría el ánimo de lucro en tanto que se establezcan marcos normativos contractuales para resguardar a los usuarios frente a las prácticas abusivas realizadas por los bancos ente esta modalidad de delitos, en contribución a ello **Melgarejo y La Torre (2021)** precisaron que al momento de la firma de contratos con las financieras se debe estipular cuales son las plataformas digitales establecidas y verificar si el usuario desea hacer uso de las mismas.

Consolidando los resultados por los especialistas precitados, **Fernández (2021)** consideró que se evitaría ello, tras la inversión de las entidades financieras en las medidas de seguridad pertinentes que contrarresten la consumación de los delitos de fraude cibernético, además firmando un seguro gratuito, de modo tal que el usuario exija el cumplimiento de ello frente a estos casos.

En tanto, **Callirgos (2021)** manifestó que el impedimento de la consumación del ánimo de lucro como tal en cualquier delito en especial del vishing seria aplicando medidas más eficientes por parte de las entidades y por parte del Estado, es decir aplicando penas más severas para esta clase de delitos. Finalmente, **Cadenillas (2021)** consideró que el ánimo de lucro siempre existirá en delitos y también en la situación de reparaciones civiles.

5. ¿Qué criterios debe tener el juez en el tema del ánimo de lucro para responsabilizar objetivamente o subjetivamente a los bancos sobre la información filtrada de sus usuarios ocasionando la afectación del daño causado por la modalidad vishing?

Al respecto, **Rodríguez (2021)** nos indica que el Juez debe tener criterios de razonabilidad, imparcialidad, siendo firmes, claros analizando la situación en el que el fraude que se produjo. En tanto, **Gastiaburu (2021)** coincidió con el criterio de razonabilidad, pues señaló que dentro de los criterios más importantes que debe valorar el Juez, se encuentra el criterio de razonabilidad y proporcionalidad de la norma y el daño generado,

De otro lado, **Ponce (2021)** contribuyó al respecto considerando que el Juez debe verificar las leyes vigentes en el país sobre esta materia y apegarse a ello en la emisión de sus resoluciones, ya que se debe evitar la impunidad en casos relativos al fraude informático. Por su parte, **Melgarejo, Tineo y La Torre (2021)** manifestaron que el Juez debe poner en aplicación los acuerdos plenarios, casaciones, u otras, para subsanar los vacíos legales que subsisten en la norma. Asimismo, **Chávez (2021)** expresó que los Jueces deben basarse en las normativas y si estas presentan vacíos legales debe emplear otras fuentes del derecho para resguardar los derechos de los usuarios y evitar su transgresión.

En tanto, **Fernández (2021)** Consideró que el Juez debe resolver con el criterio de imparcialidad, sin embargo, para la valoración de las pruebas, el banco debe demostrar que el hecho no se puedo evitar de forma alguna.

Finalmente, y en contraposición a lo señalado por los demás expertos respecto a la interrogante planteada **Callirgos y Cadenillas (2021)** manifestaron que el juez debe tomar criterios para responsabilizar a los bancos si es que se prueba que el usuario brindó su información adrede o él mismo es parte de un grupo criminal e hizo todo el fraude a beneficio propio o de terceros conocidos de este.

6. ¿qué recomendaría para que el tema de seguridad en la información de los usuarios sea pertinente en el delito de fraude informático en la modalidad vishing?

Frente a esta pregunta, **Rodríguez (2021)** recomendó que se brinde información de forma oportuna sobre los riesgos que existen en la era digital para que los usuarios puedan tener una prevención adecuada. Siguiendo ese marco de ideas **Callirgos (2021)** señaló que debe ser la misma entidad quien brinde una información idónea y la prevención específica sobre esta modalidad de crímenes.

En tanto, **Gastiaburu (2021)** exhortó a los usuarios a evitar la recepción de mensajes o llamadas de dudosa procedencia, ya que los ciber-delincuentes emplean esto como fachada para delinquir. En relación a ello **Melgarejo y La Torre**

(2021) recomendaron al uso de plataformas respaldadas por las mismas entidades financieras. Asimismo, **Cadenillas, Tineo y Ponce (2021)** acotó con que los usuarios bajen aplicaciones donde te avisen de donde más o menos provienen esos mensajes y llamadas extrañas, pues estas ya se encuentran en las tiendas de apps virtuales.

De otro lado, es importante resaltar que en relación a la pregunta planteada coincidieron los expertos, y señalaron de forma repetitiva que los bancos tienen el deber de invertir en las medidas de seguridad de sus plataformas virtuales, y en mayor magnitud en la actualidad, puesto que dada la coyuntura que afrontamos, nos acercamos a una realidad de la era tecnológica. cometen los delitos.

Asimismo, **Chávez (2021)** manifestó que recomienda a las entidades financieras realicen mayores filtros al momento de realizar las contrataciones de su personal, ya que muchos de ellos son los que otorgan la información de los usuarios a terceras personas que consuman el delito.

Posteriormente, **Fernández (2021)** agregó que se debería crear una especie de programa especializado para ver estas modalidades de phishing, seguir de donde provienen a fin de contrarrestar y evitar el vishing.

En relación a los resultados relevantes para **el objetivo específico dos** que es analizar cómo se debe reponer el daño patrimonial ante la modalidad de smishing en tiempos del covid 19 en Lima – 2020. Por ello, se planteó la primera pregunta que es:

7. ¿Cómo se debería reponer el daño patrimonial, en su totalidad o en forma parcial ante la modalidad de smishing en tiempos del Covid 19 en Lima – 2020?

Ante ello**, Rodríguez y Chávez (2021)** señalaron conjuntamente que se debe reponer en forma total ya que la entidad es quien de forma indirecta puso en peligro al usuario al no informar, preparar y prevenir al cliente sobre estos delitos.

Al respecto **Gastiaburu (2021)** agregó que si el cliente es una persona de tercera edad que desconoce de los medios digitales la responsabilidad debe ser total acotada a esta posición.

Asimismo, **Tineo, Callirgos, Chávez (2021)** concordaron y recomendaron que se debe reponer en forma total ya que la entidad es quien de forma indirecta puso en peligro al usuario al no informar, preparar y prevenir al cliente sobre estos delitos y riesgos al acceder a estas plataformas.

Al respecto coincidieron **La Torre y Melgarejo (2021)** con que debe ser en base a los acuerdos y parámetros contractuales.

En contraposición **Cadenillas y Ponce (2021)** nos mencionaron que el daño patrimonial afectado se debería reponer en partes iguales por parte del banco y el usuario y la responsabilidad debe ser aplicada por igual.

8. ¿Cuál es el criterio que debe tener el juez para reponer el daño patrimonial de los clientes de los bancos por la modalidad smishing?

En tanto, **Cadenillas , Melgarejo , La Torre, Gastiaburu (2021)** nos atribuyeron que el Juez debe tener criterios objetivos para impartir el resarcimiento entre los sujetos de la relación contractual y verificar el daño ocasionado. Asimismo, se debe tomar en cuenta el grado de responsabilidad por parte del banco y ase dejar de vulneran los derechos del usuario.

Aunado **Callirgos , Ponce y Chavez (2021)** señalaron que el juez debe tener en cuenta que el cliente es totalmente inocente de este delito que accedió a dar información pensando que no era para el fin ilícito.

Por otra parte, **Rodríguez, Tineo y La Torre (2021)** mencionaron que se debe tomar en cuenta el grado de responsabilidad de las partes involucradas para poder aplicar la responsabilidad.

9. ¿Qué medidas jurídicas aportaría para que el daño patrimonial de los clientes de los bancos sea adecuado en el tema de delito de fraude informático en la modalidad de smishing?

Tras esta pregunta cinco de los diez entrevistados **Cadenillas, Melgarejo, La Torre, Gastiaburu y Ponce (2021**) coincidieron en que para que no haya perdidas tanto para la entidad como para el usuario se tendría que reforzar la seguridad virtual de las plataformas, llamadas y mensajes a nuestros dispositivos agregaron que se debe establecer un marco normativo de protección al usuario a su información personal para así evitar esta clase de delitos.

Por otro lado, **Callirgos, Chávez ,Tineo , Rodriguez y Chávez (2021)** atribuyeron que se aplicaría penas más efectivas para los ciberdelincuentes que hacen esta clase de delitos y crearía nuevas leyes que sean específicas para responsabilizar a las entidades en circunstancias como estas que es la pandemia y se accede de forma virtual por necesidad.

En relación a **los resultados del análisis de ficha de fuente documental del objetivo general** que es: Analizar de qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de covid 19 en Lima- 2020.

La Resolución S.B.S. N° 5570-2019 La Superintendenta de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones. Esta resolución nos dice que:

> Todo tipo de operaciones no reconocidas y rechazadas por el usuario(cliente) de la financiera. Por ello la empresa es responsable de evaluar y demostrar que las operaciones fueron auténticas y registradas. Para que la empresa sea responsable de estas operaciones perdidas por el cliente son los siguientes supuestos cuando las tarjetas ha sido clonadas, como también la manipulación de información sustraída tecnológicamente, pero lo relevante de este artículo es que la financiera tiene estas operaciones no reconocidas deben ser evaluadas y demostradas por misma financiera. por tanto, también lo importante es que

manifiesta esta resolución se produjera la perdida, robo o uso no autorizado de la tarjeta indica que la empresa es responsable de las operaciones posteriores a los sucesos.

Ley Nª 30096-Ley de delitos informáticos nos afirma que:

Es cuando una persona realiza un acto delictivo a través de las tecnologías de la información o comunicación para beneficiar para sí mismo o para otros en perjuicio de otra persona todo tipo de manipulación de información (diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático), con el uso de tecnología. Asimismo, los agravantes son cuando el acto delictivo es por pertenecer a una organización criminal, cuando abusas de la confianza de la información por tu cargo de función y cuando esa información afecta a las personas con fines asistenciales, la defensa, la seguridad y soberanía nacional.

En relación a los resultados de la ficha de análisis de fuente documental del **objetivo específico uno** que es: Analizar de qué manera se debe evitar el ánimo de lucro frente a la modalidad vishing en tiempos del covid19 en Lima -2020.

El convenio sobre la ciberdelincuencia Budapest, 23.xi.200. Ministerio de relaciones exteriores. por tanto, nos dice que:

Se puede extraer las medidas que debe adoptar nuestro ordenamiento jurídico en el tema de delitos informáticos, con ello este artículo del convenio nos hace entender que el Estado peruano debe establecer medidas de seguridad interna para erradicar el fraude informático y también este convenio tiene un tema de cooperación internacional con las entidades que salvaguardan este tipo de afectación a un tercero.

El informe Nº 00001 -2020-UIF-SBS nos menciona que:

Se puede analizar que el confinamiento del Covid 19 se apreciado el aumento de estas modalidades por el tema de que la mayoría de personas han estado utilizando todo tipo de acceso a internet para no tener contacto con otra persona y por ello las organizaciones delictivas han comenzado utilizar

> modalidades como phising, vishing y smishing para afectar a un tercero en su patrimonio en el tema financiero.

En relación a los resultados de ficha de análisis de fuente documental del **objetivo específico dos** que es: Analizar cómo se debe reponer el daño patrimonial ante la modalidad de smishing en tiempos del covid 19 en Lima – 2020.

Caso BCP reclamo nro. C04363889 de fraude informático:

Nos dice que se manifiesta que el usuario le clonaron su tarjeta, dado que lo montos realizados son continuos y el mismo cajero de pago por comisión e igual el banco no quiere reponer el daño patrimonial ante este fraude argumentado que no es una operación no reconocida establecida en el artículo 23 numeral 2. Cuando las tarjetas hayan sido objeto de clonación. (…) de la Resolución S.B.S. N° 5570-2019 La Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.

Nota de prensa TV Frecuencia latina nos indica que:

> Se análisis que este caso fue por una llamada por la modalidad de smishing, dado que el usuario tuvo la pérdida de 19 mil soles indican que el Lima se está incrementado este tipo de robo o fraude informático, pero como no está como tipificado como operaciones no reconocidas para que el banco te devuelva tu dinero por motivo de fraude, en cambio te pide que compres seguros en tu tarjeta para protegerte en cambio como está la otra modalidad de clonación de tarjetas que si está tipificado en el artículo 23 numeral 2. Cuando las tarjetas hayan sido objeto de clonación. (…) de la Resolución S.B.S. N° 5570-2019 La Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.

En relación a la **discusión** se procedió a realizar la teoría de la triangulación entre los mencionado por los especialistas, la información analizada de instrumento de análisis documental y las teorías de otros investigadores sobre nuestro estudio.

Por ello, para Hernández, Fernández y Baptista (2014), refirieron que dentro

de la investigación cualitativa la discusión comprende todas aquellas lecciones encontradas durante el estudio, en donde se confirma o no, los conocimientos anteriores a la investigación a través de los hallazgos, esto permite proponer acciones a tomar en cuenta como consecuencia de las conclusiones obtenidas, recomendaciones específicas para nuevas investigaciones, así como la implicancia teórica y práctica concomitantes a dicha investigación (p. 522). A partir de ello, situándose en los resultados obtenidos de las entrevistas y las fuentes de análisis documentales, estas han sido sometidas a discusión conjuntamente con los trabajos previos, y los enfoques y teorías conceptuales desarrollados en el marco teórico, esto es conocido como la triangulación de los hallazgos, los cuales han sido presentados considerando el orden de cada objetivo planteado, por ello, en cuanto al objetivo general:

Objetivo general
Analizar de qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phising en tiempos de covid 19 en Lima- 2020.
Supuesto general
El delito fraude informático phishing crea una controversia generalizada ya que los bancos no asumen su responsabilidad frente a estos robos cibernéticos y al contrario se responsabiliza el usuario, sin embargo; el ente que tendrá que asumir las consecuencias es el banco, por ser quien ofrece una banca virtual, y está en el deber de brindar la información, las precauciones y medidas de seguridad frente a estos riesgos.

Con respecto a los hallazgos sobre el objetivo general como se debe aplicar la responsabilidad civil de los bancos sobre los delitos informáticos la resolución **S.B.S. N° 5570-2019** nos indicó que es todo tipo de operaciones no reconocidas y rechazadas por el usuario (cliente) de la financiera. Por ello la empresa es responsable de evaluar y demostrar que las operaciones fueron auténticas y registradas. Para que la empresa sea responsable de estas operaciones perdidas por el cliente son los siguientes supuestos cuando las tarjetas ha sido clonadas, como también la manipulación de información sustraída tecnológicamente, pero lo

relevante de este artículo es que la financiera tiene estas operaciones no reconocidas deben ser evaluadas y demostradas por misma financiera. por tanto, también lo importante es que manifiesta esta resolución se produjera la perdida, robo o uso no autorizado de la tarjeta indica que la empresa es responsable de las operaciones posteriores a los sucesos.

Asimismo, los **expertos Rodríguez,** el abogado civilista **Fernández y** el Doctor **Tineo (2021)** nos afirmaron que la responsabilidad de los bancos frente a los delitos informáticos, hemos encontramos diversas disputas, ya que los bancos hacen referencia el mal manejo de los usuarios de las plataformas tecnológicas, buscando así librarse de toda responsabilidad, por ello se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la seguridad suficiente a sus usuarios. Asimismo, se debe establecer una responsabilidad directa, ya que son los bancos los principales entes que utilizan a las plataformas digitales, y no dan la debida información a los usuarios para prevenir esta clase de delito; existiendo actualmente usuarios que prefieren acercarse a una entidad bancaria, pero lamentablemente con el tema de la pandemia ya se incorporaron nuevas acciones que solo se realizan por la banca por internet, dejando toda la responsabilidad a los usuarios frente a los delitos informáticos, creando una situación de desprotección

Por lo tanto, según **Abanto (2020)** en su tesis titulada *"La clonación de tarjetas de crédito y la obligación civil de los bancos, olivos año 2020"* **citado en el marco teórico** en su conclusión nos expresó que las entidades financieras si debe asumir la responsabilidad en el pago de los bienes de los que se obtuvo por la clonación, una vez comunicado y confirmado con la entidad las operaciones no reconocidas, siguiendo el protocolo de reclamo, se debe realizar el pago por el resarcimiento, pero se observa que en ocasiones la entidad asume su responsabilidad cuando el tarjetahabiente acude a otras vías como medio alternativo.

Por otro lado, la **Ley Nº 30096-Ley de Delitos Informáticos** nos atribuyó que el delito informático es un acto delictivo a través de las tecnologías de la información o comunicación para beneficiar para sí mismo o para otros en perjuicio de otra persona todo tipo de manipulación de información (diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático), con el uso de

tecnología. Asimismo, los agravantes son cuando el acto delictivo es por pertenecer a una organización criminal, cuando abusas de la confianza de la información por tu cargo de función y cuando esa información afecta a las personas con fines asistenciales, la defensa, la seguridad y soberanía nacional.

Asimismo**, Hidalgo (2018)** en su tesis ***"****Los ilícitos informáticos y su repercusión en las riquezas legales"* citado en el **marco teórico** nos indicó que la fenomenología en el aspecto penal, ya sea por el incremento indiscriminado de las acciones, lo cual conlleva va a los magistrados a la creación de nuevas normativas en las cuales encuadran estos nuevos tipos penales, pero de otro lado resultan algunas veces ineficientes y no llegan a salvaguardar la bien jurídica materia de discusión.

Respecto a lo manifestado sobre la información obtenida en la **triangulación** se determinó que la responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de covid 19 en Lima- 2020. Debe ser aplicada de manera objetiva debido que los bancos son los principales entes que utilizan a las plataformas digitales, existiendo actualmente usuarios que prefieren acercarse a una entidad bancaria, pero lamentablemente con el tema de la pandemia ya se incorporaron nuevas acciones que solo se realizan por la banca por internet, dejando toda la responsabilidad a los usuarios frente a los delitos informáticos, creando una situación de desprotección.

Objetivo específico uno
Analizar de qué manera se debe evitar el ánimo de lucro frente a la modalidad vishing en tiempos del covid19 en Lima -2020
Supuesto específico uno
Los bancos afirman que uno de sus métodos de seguridad para proteger las cuentas del usuario son los llamados estándares de idoneidad que son los datos personales del usuario es el acceso a la cuenta es inmediato con esto se atribuyó que el usuario proporcionó bajo su voluntad estos datos a un tercero según el Contrato de adhesión celebrado ; pero debe prevalecer la circunstancia de que el usuario no le dio sus datos personales a un tercero , sino más bien crean que era el mismo ente lo cual no configura con lo que se le atribuyo al usuario y por ende debe prevalecer el Principio de Primacía de la Realidad.

Por tanto, las entidades financieras si debe asumir la responsabilidad en el pago de los bienes de los que se obtuvo por la clonación, una vez comunicado y confirmado con la entidad las operaciones no reconocidas, siguiendo el protocolo de reclamo, se debe realizar el pago por el resarcimiento, pero se observa que en ocasiones la entidad asume su responsabilidad cuando el tarjetahabiente acude a otras vías como medio alternativo.

En relación a los hallazgos del objetivo específico uno debemos entender que el ánimo de lucro en los delitos informáticos en la modalidad vishing podemos evitarlo con nuevos métodos para evitar la extracción de información de los bancos.

Para ello los **expertos Rodríguez y Chávez,** asimismo los especialistas **Ponce, Gastiaburu, Tineo, Melgarejo y La Torre (2021)** manifestaron que se establezcan formas contractuales para evitar filtrar la información de los usuarios, resguardarla en un privado financiero y como también al momento de la firma de contratos con las financieras se debe estipular cuales son las plataformas digitales establecidas y verificar si el usuario desea hacer uso de las mismas. Pero para ello el Estado debe aplicar penas más fuertes para esta modalidad de delitos informáticos. Por tanto, **el convenio sobre la ciberdelincuencia Budapest, 23.XI.200. Ministerio de relaciones exteriores** señaló que se puede extraer métodos que pueda adoptar nuestro ordenamiento jurídico en el tema de delitos informáticos, con ello este artículo del convenio nos hace entender que el Estado peruano debe establecer medidas de seguridad internas para erradicar el fraude informático y también este convenio tiene un tema de cooperación internacional con las entidades que salvaguardan este tipo de afectación a un tercero. Pero, **El Informe Nº 00001 -2020-UIF-SBS** nos mencionó que a consecuencia del confinamiento por el Covid 19 se apreció el aumento de estas modalidades por el tema de que la mayoría de personas han estado utilizando todo tipo de acceso a internet para no tener contacto con otra persona , por ello las organizaciones delictivas han comenzado a utilizar modalidades como phishing, vishing y smishing para afectar a un tercero en su patrimonio en el tema financiero.

Según **Mayer (2020) citado en el marco teórico** nos afirmó que por animo lucro se entiende a aquella acción realizada por el sujeto activo para un aprovechamiento

y actuación fuera del marco legal. Asimismo, **Díaz (2018) citado en el marco teórico** nos indica que el fraude electrónico se da por la suplantación mediante llamadas telefónicas, en las que las supuestas empresas bancarias observan transacciones sospechosas y así solicitar información confidencial de la víctima. En tanto, **Salas (2017)** en su tesis titulada *"Obligación civil de las entidades financieras ante los consumidores por delitos informáticos"*. **Citado en el marco teórico** en su conclusión nos mencionó que el fin de la responsabilidad civil objetiva es resarcir el daño que genera el delito informático, que se encuentra fuera de la esfera subjetiva, es por ende que se quiere generar mayor protección legal frente a estas situaciones.

Respecto a lo manifestado sobre la información obtenida en la triangulación se determinó que el ánimo de lucro se puede evitar de manera eficiente frente a la modalidad vishing en tiempos del covid19 en Lima -2020, estableciendo formas contractuales para evitar filtrar la información de los usuarios, resguardarla en un privado financiero y como también al momento de la firma de contratos con las financieras, de esta forma se debe estipular cuales son las plataformas digitales establecidas y verificar si el usuario desea hacer uso de las mismas.

Finalmente, del análisis y discusión realizada se obtuvo que el Estado peruano debe establecer medidas de seguridad internas para erradicar el fraude informático y también se debe aplicar nuevas formas de cooperación internacional con las entidades que salvaguardan este tipo de afectación por un tercero.

Objetivo específico dos
analizar cómo se debe reponer el daño patrimonial ante la modalidad de smishing en tiempos del covid 19 en Lima – 2020.
Supuesto especifico dos
El banco debe probar para que no se le atribuya responsabilidad que este fraude informático ha sido un hecho extraordinario, irreversible e irresistible pero jamás se llega a probar ; es más en sentencias anteriores no se le pide dichos requisitos y pese a esto se le libera lo cual a nuestro criterio no es factible ya que el banco debe poner el total del daño patrimonial en la modalidad del delito de smishing.

En relación a los hallazgos del objetivo específico dos el daño patrimonial se debe reponer de manera total en sus bienes patrimoniales para los usuarios de los bancos ante la modalidad de smishing en tiempos del covid 19 en Lima – 2020.

Asimismo, **los expertos Rodríguez , Gastiaburu , Melgarejo y La Torre (2021)** afirmaron que se debe reponer en forma total ya que la entidad es quien de forma indirecta puso en peligro al usuario al no informar, preparar y prevenir al cliente sobre estos delitos. En tanto si el cliente es una persona de tercera edad que desconoce de los medios digitales la responsabilidad debe ser total, dado que la información salió de la entidad bancaria.

En el Caso **BCP** reclamo nro. C04363889 de fraude informático se demostró que al usuario le clonaron su tarjeta, dado que lo montos realizados son continuos y el mismo cajero de pago por comisión e igual el banco no quiere reponer el daño patrimonial ante este fraude argumentado que no es una operación no reconocida establecida en **el artículo 23 numeral 2. Cuando las tarjetas hayan sido objeto de clonación. (…) de la Resolución S.B.S. N° 5570-2019 La Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.**

Asimismo, en la Nota de prensa TV latina nos indicó que este caso fue por una llamada por la modalidad de smishing, dado que el usuario tuvo la pérdida de 19 mil soles indican que el Lima se está incrementado este tipo de robo o fraude informático, pero como no está como tipificado como operaciones no reconocidas para que el banco te devuelva tu dinero por motivo de fraude, en cambio te pide que compres seguros en tu tarjeta para protegerte en cambio como está la otra modalidad de clonación de tarjetas que si está tipificado en el artículo 23 numeral 2. Cuando las tarjetas hayan sido objeto de clonación. **(…) de la Resolución S.B.S. N° 5570-2019 La Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.**

Por otro lado, Díaz (2018) **citado en el marco teórico** manifestó sobre **modalidad smishing** que esta modalidad de delito utiliza los teléfonos móviles de los usuarios financieros, los delincuentes pretenden suplantar la identidad, a

menudo de personal bancario o establecimientos comerciales, gerentes o representantes de ventas con el fin de que las personas accedan mediante mensaje de texto o llamada a un link que le proporcionara al atacante información necesaria para hackear el teléfono de la víctima.

Por tanto, sobre el daño patrimonial Isler (2020) **citado en el marco teórico** indica que es toda afectación que se genere de un situación dolosa o culposa, por tanto, la indemnización se dará de forma secundaria; siempre y cuando los métodos empleados hayan sido ineficaces, y cumplan con la responsabilidad reparatoria**.**

Respecto a lo manifestado sobre la información obtenida en la triangulación se determinó que el daño patrimonial se debe reponer de manera total ante la modalidad de smishing en tiempos del covid 19 en Lima – 2020, debido a que la entidad es quien de forma indirecta puso en peligro al usuario al no informar, preparar y prevenir al cliente sobre estos delitos.

Por ende, si el cliente es una persona de tercera edad que desconoce de los medios digitales la responsabilidad debe ser total, dado que la información salió de la entidad bancaria. Como también Si la responsabilidad es presentada por ambas partes, pues el daño patrimonial debe corresponder en partes iguales de usuario y entidad financiera.

V. CONCLUSIONES

PRIMERO. Se determinó que la responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de covid 19 en Lima- 2020 debe ser aplicada de manera objetiva y en su totalidad, toda vez que preexiste el riesgo de causar daño patrimonial al usuario aún sin actuar ilícitamente, debido a que los bancos son las entidades que administran y brindan sus servicios a través de las plataformas digitales, tales como las bancas por internet, los cajeros automáticos, así como la administración de la información que poseen en la base de datos financieros de los usuarios, entre otros, aunado a ello actualmente los usuarios que prefieren acercarse a una entidad bancaria, sin embargo lamentablemente no pueden hacerlo, ya que con la coyuntura sanitaria que se atraviesa a nivel mundial esto resulta imposible y en consecuencia se han incorporaron nuevas acciones que solo se realizan mediante la banca por internet, como las transacciones interbancarias, las recargas telefónicas, los pagos de servicios básicos, existiendo de por medio un contrato de adhesión que protege al banco y les faculta de ser ellos mismos quienes verifiquen, evalúen y demuestren si tales operaciones fueron fraudulentas, son dejando toda la responsabilidad a los usuarios frente a los delitos informáticos, creando una situación de desprotección y vulnerabilidad al cliente e Incumpliendo con lo dispuesto por el artículo 65 de la constitución Política del Estado que defiende el interés de los consumidores y usuarios.

SEGUNDO. Se analizó que el ánimo de lucro se puede evitar de manera eficiente frente a la modalidad vishing en tiempos del covid19 en Lima -2020 estableciendo formas contractuales para evitar filtrar la información de los usuarios, resguardarla en un privado financiero; como también al momento de la firma de contratos con las financieras se debe estipular, señalar y reiterar cuales son las plataformas digitales establecidas y verificar si el usuario desea hacer uso de las mismas. Asimismo el Estado peruano debe establecer medidas de seguridad interna para erradicar el fraude informático, velar por los intereses de los usuarios y exigir a las entidades financieras a que respeten sus derechos como tales, mediante una mayor inversión a las medidas de

seguridad de sus plataformas digitales, pues se debe considerar que al existir un riesgo inminente, estos deberían asumir las responsabilidades, a fin de sancionar el mal manejo y administración de sus sistemas, ante ello existen convenios que tienen un tema de cooperación internacional con las entidades que salvaguardan este tipo de afectación a un tercero.

TERCERO. Se analizó que el daño patrimonial se debe reponer de manera total ante la modalidad de smishing en tiempos del covid 19 en Lima – 2020, debido a que la entidad es quien de forma indirecta puso en peligro al usuario al no tener las medidas de seguridad adecuadas en sus sistemas, no informar, preparar o prevenir al cliente sobre estos delitos. Asimismo, es importante precisar que el daño patrimonial se ha generado debido a la infiltración en el sistema por parte de los ciber-delincuentes, quienes acceden sin peligro o grado de dificultad a las plataformas en perjuicio del usuario o víctima de este delito Cibernético, lo cual se podría impedir si el banco tomara las medidas necesarias para contrarrestar ello.

VI. RECOMENDACIONES

PRIMERO. Los Bancos o entidades financieras, ofrecen un servicio y obtienen un beneficio “contraprestación” bajo esa lógica deben responder conforme lo señala La Constitución Política del Perú en el artículo 64 donde indica que el Estado debe velar por el interés del usuario pero esto no se cumple , en ese sentido se recomienda al poder Legislativo crear e implementar un nuevo artículo en la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros que es la Ley Nº 26702 que proteja al usuario donde se especifique la responsabilidad de las entidades financieras en circunstancias ilícitas como estas sobre todo en pandemia ya que se accede a las plataformas virtuales financieras por necesidad y sin ninguna información idónea por parte del servidor público hacia el usuario y el cliente no sabe a los riesgos a los cuales se expone.

SEGUNDO. Los usuarios deben tener aplicaciones donde te avisen donde provienen esos mensajes y llamadas extrañas. Asimismo, se haga una información de forma oportuna sobre los riesgos que existen en la era digital para que los usuarios puedan tener una prevención adecuada. Con ello evitar el empleo de seudos agentes bancarios de dudosa procedencia, ya que algunos de ellos emplean esto como fachada para delinquir y afecta al patrimonio del usuario.

TERCERO. El banco debe establecer parámetros a base de lineamientos legales que garanticen el empleo correcto de la información personal de los usuarios, como también se tendría que reforzar la seguridad virtual de las plataformas, llamadas y mensajes a nuestros dispositivos y aplicar penas más efectivas para los ciber-delincuentes que hacen esta clase de delitos.

REFERENCIAS

Alarcón A. & Barrera J. (2017). *Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016*. (Tesis de Maestría, Universidad Privada Norbert Wiener). http://repositorio.uwiener.edu.pe/bitstream/handle/123456789/1630/MAESTRO%20%20%20Barrera%20Bar%C3%B3n%2C%20Javier%20Antonio.pdf?sequence=1&isAllowed=y

Aguilar, J. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. URVIO, Revista Latinoamericana de Estudios de Seguridad, (25),24-40. https://www.redalyc.org/articulo.oa?id=552661588002

Abanto, R. (2020). *La clonación de tarjetas de crédito y la responsabilidad civil de la entidad financiera los olivos año 2020.* (tesis para optar el título profesional de Abogado). Universidad Privada del Norte

Acosta, G. & Benavides, M. & García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. Revista Venezolana de Gerencia, 25(89),351-368. https://www.redalyc.org/articulo.oa?id=29062641023

Bolaños, F. & Gómez, C. (2015). Estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador. ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica, (3). https://www.redalyc.org/articulo.oa?id=512251503001

De La Haza, A. (2018). *Ni dejar hacer ni dejar pasar: el compromiso de las instituciones bancarias peruanas frente al lavado de activos a través de la implementación de una metodología por riesgo*. Derecho PUCP, (80), 281-331. https://dx.doi.org/10.18800/derechopucp.201801.008

Devia González, E.A. (2017). *El delito informático: Estafa informática del artículo 248.2 del código pena*l. (Tesis Doctoral Inédita). Universidad de Sevilla, Sevilla.

Díaz Jiménez, S. D., Angulo Cabrales, J. C. y Barboza Camelo, M. M. (2018). Análisis del delito de fraude electrónico: modalidad tarjeta de crédito (Tesis

de pregrado). Recuperado de: http://repository.ucc.edu.co/handle/ucc/8381

Díaz-Narváez VP, Calzadilla-Núñez A. *Artículos científicos, tipos de investigación y productividad científica en las ciencias de la salud*. Rev Cienc Salud. 2016;14(1): 115-121. doi:dx.doi.org/10.12804/revsalud14.01.2016.10

Dulley, I. & Sampaio, L. (2020). Accusation and Legitimacy in the Civil War in Angola1. VIBRANT - Vibrant Virtual Brazilian Anthropology, 17(). https://www.redalyc.org/articulo.oa?id=406964062018

Echeverría, M, & Garaycoa, M, & Tusev, Aleksandar (2020). *¿ARE ECUADORIAN MILLENNIALS PREPARED AGAINST A CYBERATTACK?* CHAKIÑAN, REVISTA DE CIENCIAS SOCIALES Y HUMANIDADES, (10),73-86. https://www.redalyc.org/articulo.oa?id=571763429005

Gauchi Risso, V. (2017). Estudio de los métodos de investigación y técnicas de recolección de datos utilizadas en bibliotecología y ciencia de la información. *Revista Española de Documentación Científica*, 40 (2): e175. doi: http://dx.doi.org/10.3989/redc.2017.2.1333

Geraci, M. (2020). Algorithmic Management: A liability-free method to manage workers' performance? Revista Facultad de Jurisprudencia, (7),269-294. https://www.redalyc.org/articulo.oa?id=600263428002

Gonetecki Oliveira, M, & Machado Toaldo, A. (2015). *NEW TIMES, NEW STRATEGIES: PROPOSAL FOR AN ADDITIONAL DIMENSION TO THE 4 P'S FOR E-COMMERCE DOT-COM*. JISTEM: Journal of Information Systems and Technology Management, 12(1),107-124. https://www.redalyc.org/articulo.oa?id=203238424006

Gonzales, J. et al (2019). *Análisis y revisión sobre delitos informáticos en el Ecuador.* Revista Semana de la Ciencia UTMACH, pp. 193-203. https://investigacion.utmachala.edu.ec/proceedings/index.php/utmach/article/view/367/312

Hausken, K. (2015). *A STRATEGIC ANALYSIS OF INFORMATION SHARING AMONG CYBER HACKERS. JISTEM*: Journal of Information Systems and Technology Management, 12(2),245-270. https://www.redalyc.org/articulo.oa?id=203242219004

Heredia Pazmiño, P, & Santacruz Mediavilla, A, & Zaldumbide Vaca, J. (2020).

Smart Regulation in times of COVID 19: An introspective preliminary analysis for its application in Ecuador. Revista Facultad de Jurisprudencia, 1(8),120-164. https://www.redalyc.org/articulo.oa?id=600263979003

Herbas,B & Rocha Gonzales, E. (2018). *Metodología científica para la realización de investigaciones de mercado e investigaciones sociales cuantitativas*. *Revista Perspectivas*, (42), 123-160. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1994-37332018000200006&lng=es&tlng=es.

Imbaquingo, H. et. al (2016). *Delitos Informáticos en la Provincia de Imbabura*. Universidad Técnica del Norte – Ecuador

Iribarra (2017). *El Lucro En Las Personas Jurídicas: Comentario A La Sentencia De La Excelentísima Corte Suprema, En Los Autos Caratulados*: Fundación Solidaridad Con Servicio De Impuestos Internos, ROL N ° 991-2015. Revista Chilena de Derecho, 44 (1), 305-316. https://www.redalyc.org/articulo.oa?id=177051304016

Isler Soto, E. (2020). *Seguridad: Principio en la adecuación de deberes preventivos y buenas prácticas en la atención remota y presencial al consumidor en el contexto de la pandemia COVID-19*. Derecho PUCP, (85), 203-244. https://dx.doi.org/10.18800/derechopucp.202002.007

Lamperti, S. B. (2017). Aspectos Legales. Los Delitos Informáticos. El rastro digital del delito: aspectos técnicos, legales y estratégicos de la Informática Forense. Mar de Plata: Universidad FASTA.

Lam Díaz, R. (2016). *La redacción de un artículo científico*. *Revista Cubana de Hematología, Inmunología y Hemoterapia*, *32*(1), 57-69. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-02892016000100006&lng=es&tlng=es.

León J. (2018). *Vacíos legales que impiden la aplicación de sanciones por delitos informáticos en la ley n° 30096 y modificatoria en el distrito cercado lima 2017*. (Tesis para obtener el título profesional de: abogado, Universidad Privada Telesup). https://repositorio.utelesup.edu.pe/bitstream/UTELESUP/812/1/LEON%20CORDOVA%20JOHNNY%20EFRAIN.PDF

Martínez M. (2015). *La responsabilidad bancaria frente a los delitos informáticos*. (Tesis de Maestría, Universidad Andina Simón Bolívar Sede Ecuador). file:///C:/Users/JL/Downloads/T1631-MDE-Martinez-La%20responsabilidad.pdf

Mengoa M. (2018). *Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú*. (Tesis para obtener el título profesional de: abogado). Universidad Cesar Vallejo Lima- Norte.

Mayer Lux, L. (2014). *El ánimo de lucro en los delitos contra intereses patrimoniales*. Revista de derecho (Valparaíso), (42), 285-319. https://dx.doi.org/10.4067/S0718-68512014000100009

Mayer Lux, L. & Oliver Calderón, G. (2020). *El delito de fraude informático: concepto y delimitación*. Revista chilena de derecho y tecnología, 9(1), 151-184. https://dx.doi.org/10.5354/0719-2584.2020.534477

Mushtaque, K. & Ahsan, K. & Umer, Ahmer (2015). *DIGITAL FORENSIC INVESTIGATION MODELS: AN EVOLUTION STUDY. JISTEM:* Journal of Information Systems and Technology Management, 12(2),233-243. https://www.redalyc.org/articulo.oa?id=203242219003

Ortiz, N. J. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. Revista Científica Hallazgos21, 4(1), 100- 111. http://revistas.pucese.edu.ec/hallazgos21/

Pardo A. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018*. (Tesis de Maestría, Universidad Privada Cesar Vallejo). https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_VA.pdf?sequence=1&isAllowed=y

Piedrahita, P. (2020). Local y global: el Estado frente al delito transnacional. Revista Derecho del Estado, (46),137-160. https://www.redalyc.org/articulo.oa?id=337664307006

Peci, Alketa, & Avellaneda, Claudia Nancy, & Suzuki, Kohei (2021). Governmental responses to COVID-19 Pandemic. Revista de Administração Pública - RAP, 55(1),1-11. https://www.redalyc.org/articulo.oa?id=241066211001

Roque Hernández, Ventura R., & Juárez Ibarra, C. (2018). *Concientización y*

capacitación para incrementar la seguridad informática en estudiantes universitarios. Paakat: Revista de Tecnología y Sociedad, (14). https://www.redalyc.org/articulo.oa?id=499063347005

Rojas, J. (2016*). Análisis de la penalización del cibercrimen en países de habla hispana.* Revista Logos, Ciencia & Tecnología, 8(1),220-231. https://www.redalyc.org/articulo.oa?id=517752176020

Rodriguez Zárate, A. (2014). *Análisis económico de la responsabilidad bancaria frente a los fraudes electrónicos: El riesgo provecho, el riesgo creado y el riesgo profesiona*l. Bogotá D.C.: Javeriana.

Ruiz C. (2016*). Análisis de los delitos informáticos y su violación de los derechos constitucionales de los ciudadanos*. (Tesis previo a la obtención del título de abogada, Universidad Nacional de Loja. https://dspace.unl.edu.ec/jspui/bitstream/123456789/17916/1/Tesis%20Lista%20Carolin.pdf

Saltos Salgado, M. F., Robalino Villafuerte, J. L., & Pazmiño Salazar, L. D. (2021). Análisis conceptual del delito informático en Ecuador. Revista Conrado, 17(78), 343-351.

Salas, D. (2017). *responsabilidad civil bancaria frente al cliente por delitos informáticos.* (tesis para obtener el grado de licenciatura en Derecho). Universidad de Costa Rica.

Serrano, E. (2020). *Responsabilidad civil, daños punitivos y propiedad intelectual. IUS*. Revista del Instituto de Ciencias Jurídicas de Puebla A.C., 14(46),129-142. https://www.redalyc.org/articulo.oa?id=293265423008

Zabala, (2017). *Responsabilidad Bancaria Frente Al Delito De Phishing En Colombia*. Bogotá D.C.: Javeriana. https://repository.ucatolica.edu.co/bitstream/10983/14943/1/Art%C3%ADculo%20Phishing%20-%20Alexander%20Zabala.pdf

ANEXO 1

DECLARATORIA DE AUTENTICIDAD

Nosotras Paredes Salazar, Edith Silvia y Silva Rueda, Elsa Milagros, alumnas de la Facultad de Derecho y Humanidades, Escuela Profesional de Derecho de la Universidad César Vallejo, filial Los Olivos, declaramos bajo juramento que todos los datos e información que acompañan al proyecto de investigación titulado "Responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid 19 en Lima-2020" son:

1. De nuestra autoría.
2. El presente proyecto de investigación no ha sido plagiado ni total, ni parcialmente.
3. El proyecto de investigación no ha sido publicado ni presentado anteriormente.
4. Los resultados presentados en el presente Artículo de revisión, 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 información aportada, por lo cual nos sometemos a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Los Olivos, 03 de junio del 2021

Paredes Salazar, Edith Silvia

DNI Nº 76326345

Silva Rueda, Elsa Milagros

DNI Nº 72298974

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 2

DECLARATORIA DE AUTENTICIDAD

Yo, Santisteban Llontop Pedro Pablo, docente de la Facultad de Derecho y Humanidades, Escuela Profesional de Derecho de la Universidad César Vallejo, filial Los Olivos, revisor del proyecto de investigación titulada ”Responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid 19 en Lima-2020”, de las estudiantes Paredes Salazar, Edith Silvia y Silva Rueda, Elsa Milagros, constato que la investigación tiene un índice de similitud de 19% verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyó que cada una de las coincidencias detectadas no constituyen plagio. 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.

Los Olivos, 20 de junio del 2021.

Dr. Santisteban Llontop Pedro Pablo

DNI Nº 09803311.

ANEXO Nº 3

MATRIZ DE CATEGORIZACION APRIORISTICA

NOMBRES DE LOS ESTUDIANTES: Paredes Salazar, Edith Silvia. Silva Rueda, Elsa Milagros.

FACULTAD/ESCUELA: DERECHO

ÁMBITO TEMATICO: RESPONSABILIDAD CIVIL

TÍTULO	
Responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid 19 en Lima-2020.	
PROBLEMAS	
Problema General	¿De qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de covid 19 en Lima- 2020?
Problema Específico 1	¿De qué manera se debe evitar el lucro indebido frente a la modalidad vishing en tiempos del covid-19 en Lima -2020?
Problema Específico 2	¿Cómo se debe reponer el daño patrimonial ante la modalidad de smishing frente en tiempos del Covid 19 en Lima – 2020?
OBJETIVOS	
Objetivo General	Determinar de qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de covid 19 en Lima- 2020.
Objetivo Específico 1	Analizar de qué manera se debe evitar el ánimo lucro frente a la modalidad vishing en tiempos del covid-19 en Lima -2020.
Objetivo Específico 2	Analizar cómo se debe reponer el daño patrimonial ante la modalidad de smishing en tiempos del covid 19 en Lima – 2020
SUPUESTOS JURÍDICOS	
Supuesto General	El delito fraude informático phishing crea una controversia generalizada ya que los bancos no asumirían su responsabilidad frente a estos robos cibernéticos y al contrario se responsabiliza el usuario, sin embargo; el ente que tendrá que asumir las consecuencias es el banco, por ser quien ofrece una banca virtual, y está en el deber de brindar la información, las precauciones y medidas de seguridad frente a estos riesgos.

Supuesto Específico 1	Los bancos afirman que uno de sus métodos de seguridad para proteger las cuentas del usuario son los llamados estándares de idoneidad que son los datos personales del usuario es el acceso a la cuenta es inmediato con esto se atribuyó que el usuario proporcionó bajo su voluntad estos datos a un tercero según el Contrato de adhesión celebrado ; pero debe prevalecer la circunstancia de que el usuario no le dio sus datos personales a un tercero , sino más bien crean que era el mismo ente lo cual no configura con lo que se le atribuyo al usuario y por ende debe prevalecer el Principio de Primacía de la Realidad
Supuesto Específico 2	El banco debe probar para que no se le atribuya responsabilidad que este fraude informático ha sido un hecho extraordinario ,irreversible e irresistible pero jamás se llega a probar ; es más en sentencias anteriores no se le pide dichos requisitos y pese a esto se le libera lo cual a nuestro criterio no es factible ya que el banco debe reponer el total del daño patrimonial en la modalidad del delito de smishing.
Categorización	**Categoría 1: Responsabilidad civil de los bancos.** subcategoría 1: ánimo de lucro subcategoría 2: daño patrimonial **Categoría 2: Delito de fraude informático phishing.** subcategoría 1: vishing subcategoría 2: smishing
METODOLOGÍA	
Tipos, diseño y nivel de investigación	**Enfoque:** Cualitativo **Diseño:** Teoría Fundamentada **Tipo de investigación**: Aplicada **Nivel de la investigación:** Descriptivo
Muestreo	

	Escenario de estudio: Corte superior de Lima, despachos de abogados. **Participantes:** 2 jueces en Derecho civil, 6 especialistas en Derecho Civil y 2 especialistas en Derecho Penal. **Muestra**: No probabilística **Muestra** No probabilística-Tipo: De experto. **Muestra Orientada: Por conveniencia.**
Técnica e instrumento de recolección de datos	**Técnica:** Entrevista análisis de documentos **Instrumento:** Guía de entrevista guía y ficha de análisis documental:(de jurisprudencia y derecho comparado).
Método de análisis de datos	Descriptivo, inductivo y hermenéutico.

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 4: INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

Título: **Responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid 19 en Lima-2020.**

Entrevistado/a:

Cargo/profesión/grado académico:

Normas básicas de la entrevista:

Objetivo general

Analizar de qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phising en tiempos de Covid 19

Premisa: Mucho se verifica que tanta responsabilidad tiene los bancos con el tema del delito de fraude informático para indemnizar a las personas que le roban su información personal como financiera, por ello,

1.- Desde su perspectiva ¿De qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid 19 en Lima- 2020?

……

……

……

2.- en su opinión ¿qué responsabilidad civil tiene los bancos cuando los datos personales y financieros se filtran de una persona?

……

……

……

3.- Desde su perspectiva. ¿Qué medida recomendaría para que la responsabilidad Civil de los bancos sea aplicada dentro del contrato de adhesión en el tema de delito fraude informático?

……..…

……..……...……...……..…

……

Objetivo específico 1

Analizar de qué manera se debe evitar el ánimo lucro frente a la modalidad vishing en tiempos del covid-19 en Lima -2020.

Premisa: Premisa: En el tema del ánimo de lucro que tienen los bancos para no asumir la responsabilidad de los daños causados por el delito de fraude informático, se observa que los usuarios se ven afectados con esta modalidad de fraude, por ello

4.- En su perspectiva ¿De qué manera se puede evitar el ánimo de lucro frente a la modalidad vishing en tiempos del Covid-19 en Lima -2020?

……..…

……..……...……...……..…

……

5- En su opinión ¿Qué criterios debe tener el juez en el tema del ánimo de lucro para responsabilizar objetivamente o subjetivamente a los bancos sobre la información filtrada de sus usuarios ocasionando la afectación del daño causado por la modalidad vishing?

……..……...……...……..…

……..…

……..……...……...……..…

6.- En el mismo contexto, ¿qué recomendaría para que el tema de seguridad en la información de los usuarios sea pertinente en el delito de fraude informático en la modalidad vishing?

……..…

……..……...……..……..…
……

Objetivo específico 2

Analizar cómo se debe reponer el daño patrimonial ante la modalidad de smishing en tiempos del covid 19 en Lima – 2020

Premisa: Es importante determinar el daño patrimonial emergente de los clientes de los bancos ante la modalidad de smishing. Por ello

7.- En ese escenario, ¿Cómo se debería reponer el daño patrimonial en su totalidad o en forma parcial ante la modalidad de smishing frente en tiempos del Covid 19 en Lima – 2020?

……..…
……..……...……..……..…
……..……
8.- ¿cuál es el criterio que debe tener el juez para reponer el daño patrimonial de los clientes de los bancos por la modalidad smishing?

……..…
……..……...……..……..…
……
9.- ¿qué medidas jurídicas aportaría para que el daño patrimonial de los clientes de los bancos sea adecuado en el tema de delito de fraude informático en la modalidad de smishing?

……..…
……..…
……..……...……..……..…
……..…

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 5:

VALIDACIÓN DE INSTRUMENTO:

I. DATOS GENERALES

1.1. Apellidos y Nombres: Dr. Santisteban Llontop, Pedro.

1.2. Cargo e institución donde labora: Docente UCV.

1.3. Nombre del instrumento motivo de evaluación: **GUIA DE ENTREVISTA**.

1.4. Autor(A) de Instrumento: Paredes Salazar, Edith.

Silva Rueda, Milagros.

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.												X	
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.												X	
4. ORGANIZACIÓN	Existe una organización lógica.												X	
5. SUFICIENCIA	Toma en cuanta los aspectos metodológicos esenciales												X	
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.												X	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												X	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos												X	
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.												X	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												X	

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación
- El Instrumento no cumple con Los requisitos para su aplicación

SI

IV. PROMEDIO DE VALORACIÓN:

95%

Lima, 29 de junio 2021

FIRMA DEL EXPERTO INFORMANTE
Dr. Santisteban Llontop Pedro
DNI No 09803311 Telf.: 983278657

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 5:

VALIDACIÓN DE INSTRUMENTO:

I. DATOS GENERALES

4.1. Apellidos y Nombres: Dr. Santisteban Llontop, Pedro.

4.2. Cargo e institución donde labora: Docente UCV.

4.3. Nombre del instrumento motivo de evaluación: **GUIA DE ENTREVISTA**.

4.4. Autor(A) de Instrumento: Paredes Salazar, Edith.
Silva Rueda, Milagros.

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	No cumple con suaplicación						Cumple en parte con su aplicación			Si cumple con su aplicación			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje apropiado.												✓	
2. OBJETIVIDAD	Se expresar la realidad como es, indica cualidad de objetivo y la adecuación al objeto investigado												✓	
3. ACTUALIDAD	Esta de acorde a los aportes recientes al derecho.												✓	
4. ORGANIZACIÓN	Existe una organización lógica.												✓	
5. SUFICIENCIA	Cumple con los aspectos metodológicos esenciales												✓	
6. INTENCIONALIDAD	Esta adecuado para valorar las Categorías.												✓	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												✓	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos y supuestos, basado en los aspectos teóricos y Científicos												✓	
9. METODOLOGÍA	El instrumento responde al objetivo de la Investigación: Tipo, diseño, categorías, escenario de estudios y participantes.												✓	
10. PERTINENCIA	El instrumento tiene sentido, enfrenta un problema crucial, está situado en una población en territorio, es interdisciplinaria, tiene relevancia global, y asume responsablemente las consecuencias de sus hallazgos.												✓	

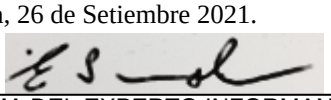
III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación — **SI**
- El Instrumento no cumple con Los requisitos para su aplicación

IV. PROMEDIO DE VALORACIÓN:

95%

Lima, 26 de Setiembre 2021.



FIRMA DEL EXPERTO INFORMANTE
Mag. Eliseo S. Wenzel Miranda.
DNI N° 09940210 Tel 992303480

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 5

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES:

1.1 Apellidos y Nombres: Mgtr. La Torre Guerrero. Ángel Fernando.
1.2 Cargo e institución donde labora: Docente de la UCV.
1.3 Nombre del instrumento motivo de evaluación: Guía de Entrevista.
1.4 Autor(A) de Instrumento: Paredes Salazar, Edith Silvia.
Silva Rueda, Elsa Milagros.

I. ASPECTOS DE VALIDACIÓN:

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. PRESENTACIÓN	Responde a la formalidad de la investigación.												X	
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Considera información actualizada, acorde a las necesidades reales de la investigación.												X	
4. INTENCIONALIDAD	Está adecuado para valorar las categorías.												X	
5. COHERENCIA	Existe coherencia entre los objetivos y supuestos jurídicos.												X	
6. METODOLOGÍA	La estrategia responde a una metodología y diseño aplicados para lograr verificar los supuestos.												X	
7. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												X	

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación
- El Instrumento no cumple con Los requisitos para su aplicación

SI

IV. PROMEDIO DE VALORACIÓN:

95%

Lima, 15 de Setiembre del 2020.

FIRMA DEL EXPERTO INFORMANTE
Mgtr. La Torre Guerrero. Ángel Fernando.
DNI N°: 09961844.- **TELF :**980758944

UNIVERSIDAD CÉSAR VALLEJO

GUÍA DE ENTREVISTA

Título: **Responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid 19 en Lima-2020.**

Entrevistado/a: Dr. Reyler Rodriguez Chavez.

Cargo/profesión/grado académico: Juez del Noveno Juzgado Penal de la Corte Superior de Justicia.

Objetivo general

Analizar de qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phising en tiempos de Covid 19.

Premisa: Mucho se verifica que tanta responsabilidad tiene los bancos con el tema del delito de fraude informático para indemnizar a las personas que le roban su información personal como financiera, por ello,

1.- Desde su perspectiva ¿De qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid 19 en Lima- 2020?

La entidad financiera debe asumir una responsabilidad objetiva ante esta nueva modalidad de robo de información pero que esta entidad debe conocer su modalidad de perfección.

2.- En su opinión ¿qué responsabilidad civil tiene los bancos cuando los datos personales y financieros se filtran de una persona?

Asumiria la responsabilidad de proteger los datos bancarios que tiene a su poder.

3.- Desde su perspectiva. ¿Qué medida recomendaría para que la responsabilidad Civil de los bancos sea aplicada dentro del contrato de adhesión en el tema de delito fraude informático?

Medidas idóneas de seguridad como un filtro de información para que asi no se

pueda llegar a esa información personal tan fácil del cliente.

Objetivo específico 1

Analizar de qué manera se debe evitar el ánimo de lucro frente a la modalidad vishing en tiempos del covid-19 en Lima -2020.

Premisa: En el tema del ánimo de lucro que tienen los bancos para no asumir la responsabilidad de los daños causados por el delito de fraude informático, se observa que los usuarios se ven afectados con esta modalidad de fraude, por ello

4.- En su perspectiva ¿De qué manera se puede evitar el ánimo de lucro frente a la modalidad vishing en tiempos del Covid-19 en Lima -2020?
Que se establezcan marcos normativos contractuales para resguardar a los usuarios.

5- En su opinión ¿Qué criterios debe tener el juez en el tema del ánimo de lucro de los bancos para no responsabilizarse objetivamente sobre la información filtrada de sus usuarios para la afectación del daño causado por el tema de vishing?
El juez debe tener criterios claros por parte imparcial y analizar la situación en el que el fraude que se produjo.

6.- En el mismo contexto, ¿qué recomendaría para que el tema de seguridad en la información de los usuarios sea pertinente en el delito de fraude informático en la modalidad vishing?
Que se informen de forma oportuna sobre los riesgos que existen en la era digital.

Objetivo específico 2

Analizar cómo se debe reponer el daño patrimonial ante la modalidad de smishing en tiempos del covid 19 en Lima – 2020

Premisa: Es importante determinar el daño patrimonial emergente de los clientes

de los bancos ante la modalidad de smishing. Por ello

7.- En ese escenario, ¿Cómo se debería reponer el daño patrimonial, en su totalidad o en forma parcial ante la modalidad de smishing en tiempos del Covid 19 en Lima – 2020?

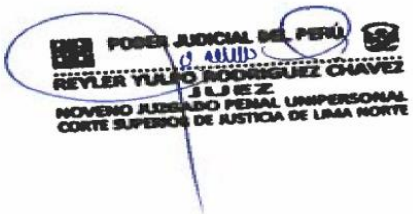
Reponer en forma total ya que la entidad es quien de forma indirecta puso en peligro al usuario al no informar, preparar y prevenir al cliente sobre estos delitos.

8.- ¿cuál es el criterio que debe tener el juez para reponer el daño patrimonial de los clientes de los bancos por la modalidad smishing?

Debe tomar en cuenta el grado de responsabilidad de las partes involucradas

9.- ¿qué medidas jurídicas aportaría para que el daño patrimonial de los clientes de los bancos sea adecuado en el tema de delito de fraude informático en la modalidad de smishing?

Establecer parámetros a base de lineamientos legales que garanticen el empleo correcto de la información personal de los usuarios.



UNIVERSIDAD CÉSAR VALLEJO

GUÍA DE ENTREVISTA

Título: **Responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid 19 en Lima-2020.**

Entrevistado/a:Dr. Robert Paul Cadenillas Silva.

Cargo/profesión/grado académico: Secretario de la Primera Sala Permanente de la Corte Superior de Justicia/Abogado/superior

\

Objetivo general

Analizar de qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phising en tiempos de Covid 19.

Premisa: Mucho se verifica que tanta responsabilidad tiene los bancos con el tema del delito de fraude informático para indemnizar a las personas que le roban su información personal como financiera, por ello,

1.- Desde su perspectiva ¿De qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid 19 en Lima- 2020?

La responsabilidad civil debe ser aplicada tanto como al banco, al delincuente y al usuario de la misma manera.

2.- En su opinión ¿qué responsabilidad civil tiene los bancos cuando los datos personales y financieros se filtran de una persona?

Tienen la responsabilidad de proteger los datos personales del cliente bajo esta responsabilidad se le contrata.

3.- Desde su perspectiva. ¿Qué medida recomendaría para que la responsabilidad Civil de los bancos sea aplicada dentro del contrato de adhesión en el tema de delito fraude informático?

Dentro de las clausulas están especificas todo lo comprendido acerca de acudir a una banca por internet el usuario al firmar el contrato sabe a lo que se tiene que pegar.

Objetivo específico 1

Analizar de qué manera se debe evitar el ánimo de lucro frente a la modalidad vishing en tiempos del covid-19 en Lima -2020.

Premisa: En el tema del ánimo de lucro que tienen los bancos para no asumir la responsabilidad de los daños causados por el delito de fraude informático, se observa que los usuarios se ven afectados con esta modalidad de fraude, por ello

4.- En su perspectiva ¿De qué manera se puede evitar el ánimo de lucro frente a la modalidad vishing en tiempos del Covid-19 en Lima -2020?
El animo de lucro siempre existirá en delitos y también en la situación de reparaciones civiles.

5- En su opinión ¿Qué criterios debe tener el juez en el tema del ánimo de lucro de los bancos para no responsabilizarse objetivamente sobre la información filtrada de sus usuarios para la afectación del daño causado por el tema de vishing?
La gente con tantas noticias de estas nuevas formas de fraudes debe estar mas atenta para no caer en manos de estos inescrupulosos.

6.- En el mismo contexto, ¿qué recomendaría para que el tema de seguridad en la información de los usuarios sea pertinente en el delito de fraude informático en la modalidad vishing?
Que los usuarios bajen aplicaciones donde te avisen de donde mas o menos provienen esos mensajes y llamadas extrañas.

Objetivo específico 2

Analizar cómo se debe reponer el daño patrimonial ante la modalidad de smishing en tiempos del covid 19 en Lima – 2020

Premisa: Es importante determinar el daño patrimonial emergente de los clientes de los bancos ante la modalidad de smishing. Por ello

7.- En ese escenario, ¿Cómo se debería reponer el daño patrimonial, en su totalidad o en forma parcial ante la modalidad de smishing en tiempos del Covid 19 en Lima – 2020?
El daño patrimonial afectado se debería reponer en partes iguales por parte del banco y el usuario.

8.- ¿cuál es el criterio que debe tener el juez para reponer el daño patrimonial de los clientes de los bancos por la modalidad smishing?
El juez debe tener criterios objetivos para impartir el resarcimiento entre los sujetos de la relación contractual.

9.- ¿qué medidas jurídicas aportaría para que el daño patrimonial de los clientes de los bancos sea adecuado en el tema de delito de fraude informático en la modalidad de smishing?

Para que no haya perdidas tanto para la entidad y el usuario se tendría que reforzar la seguridad virtual de las plataformas, llamadas y mensajes a nuestros dispositivos.

UNIVERSIDAD CÉSAR VALLEJO

GUÍA DE ENTREVISTA

Título: **Responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid 19 en Lima-2020.**

Entrevistado/a: Karen Liliana Gastiaburu Alania

Cargo/profesión/grado académico: Especialista1-Área de infracciones- Comisión de signos distintivos/ superior

Objetivo general

Analizar de qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phising en tiempos de Covid 19.

Premisa: Mucho se verifica que tanta responsabilidad tiene los bancos con el tema del delito de fraude informático para indemnizar a las personas que le roban su información personal como financiera, por ello,

1.- Desde su perspectiva ¿De qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid 19 en Lima- 2020?

Al referirnos a la responsabilidad de los bancos frente a los delitos informáticos, encontramos diversas disputas, ya que los bancos hacen referencia el mal manejo de los usuarios de las plataformas tecnológicas, buscando así librarse de toda responsabilidad, por ello se debe se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la seguridad suficiente a sus usuarios.

2.- En su opinión ¿qué responsabilidad civil tiene los bancos cuando los datos personales y financieros se filtran de una persona?

Según mi punto de vista, la responsabilidad directa es aquella que se manifiesta cuando los bancos hacen uso de los datos personales y financieros para ser filtrados.

3.- Desde su perspectiva. ¿Qué medida recomendaría para que la responsabilidad

Civil de los bancos sea aplicada dentro del contrato de adhesión en el tema de delito fraude informático?

Creo recomendable, la puesta a disposición de cláusulas contractuales frente a los delitos informáticos.

Objetivo específico 1

Analizar de qué manera se debe evitar el ánimo de lucro frente a la modalidad vishing en tiempos del covid-19 en Lima -2020.

Premisa: En el tema del ánimo de lucro que tienen los bancos para no asumir la responsabilidad de los daños causados por el delito de fraude informático, se observa que los usuarios se ven afectados con esta modalidad de fraude, por ello

4.- En su perspectiva ¿De qué manera se puede evitar el ánimo de lucro frente a la modalidad vishing en tiempos del Covid-19 en Lima -2020?

Que se establezcan disposiciones que enmarquen la responsabilidad de los bancos frente a la modalidad vishing.

5- En su opinión ¿Qué criterios debe tener el juez en el tema del ánimo de lucro de los bancos para no responsabilizarse objetivamente sobre la información filtrada de sus usuarios para la afectación del daño causado por el tema de vishing?

Uno de los criterios que debe emplear el juez es la de razonabilidad y proporcionablilidad de la norma y el daño generado.

6.- En el mismo contexto, ¿qué recomendaría para que el tema de seguridad en la información de los usuarios sea pertinente en el delito de fraude informático en la modalidad vishing?

Evitar el empleo de agentes bancarios de dudosa pocedencia, ya que algunos de ellos emplean esto como fachada para delinquir.

Objetivo específico 2

P s
d Analizar cómo se debe reponer el daño patrimonial ante la modalidad de smishing en tiempos del covid 19 en Lima – 2020

7.- En ese escenario, ¿Cómo se debería reponer el daño patrimonial, en su totalidad o en forma parcial ante la modalidad de smishing en tiempos del Covid 19 en Lima – 2020?

Si el cliente es una persona de tercera edad que desconoce de los medios digitales la responsabilidad debe ser total, dado que la información salió de la entidad bancaria.

Si la responsabilidad es presentada por ambas partes, pues el daño patrimonial debe corresponder en partes iguales de usuario y entidad financiera.

8.- ¿cuál es el criterio que debe tener el juez para reponer el daño patrimonial de los clientes de los bancos por la modalidad smishing?

Debe basarse en el daño ocasionado.

Debe tomar en cuenta el grado de responsabilidad de las partes involucradas.

Debe verificar los términos contractuales y verificar que los mismos no vulneren los derechos de los usuarios.

9.- ¿qué medidas jurídicas aportaría para que el daño patrimonial de los clientes de los bancos sea adecuado en el tema de delito de fraude informático en la modalidad de smishing?

Establecer un marco normativo de protección al usuario frente a la práctica abusiva de los bancos.

UNIVERSIDAD CÉSAR VALLEJO

GUÍA DE ENTREVISTA

Título: **Responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid 19 en Lima-2020.**

Entrevistado/a: Mgtr. La Torre Guerrero. Ángel Fernando

Cargo/profesión/grado académico: Docente/Abogado especializado en derecho civil/Magister.

Objetivo general

Analizar de qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phising en tiempos de Covid 19

Premisa: Mucho se verifica que tanta responsabilidad tiene los bancos con el tema del delito de fraude informático para indemnizar a las personas que le roban su información personal como financiera, por ello,

1.- Desde su perspectiva ¿De qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid 19 en Lima- 2020?

La responsabilidad civil de los bancos frente al delito de fraude informático phishing, debe ser tratada de forma radical y sancionadora, buscando que los bancos también asuman su responsabilidad por la exigencia que realizan del uso de plataformas digitales y como sabemos existen usuarios que no se llegan a familiarizar con estas plataformas, cayendo en algunos casos en error y es allí donde se ven envueltos en los delitos de ciberdelincuentes.

2.- en su opinión ¿qué responsabilidad civil tiene los bancos cuando los datos personales y financieros se filtran de una persona?

Los bancos cuando presentan filtración de los datos personales y financieros de un usuario, recaen en una responsabilidad civil directa y por ende deben asumir las

consecuencias de ello.

3.- Desde su perspectiva. ¿Qué medida recomendaría para que la responsabilidad Civil de los bancos sea aplicada dentro del contrato de adhesión en el tema de delito fraude informático?

La medida que recomendaría es establecer dentro del contrato explícitamente en un apartado la responsabilidad que tendría la entidad bancaria frente a los fraudes informáticos.

Objetivo específico 1

Analizar de qué manera se debe evitar el ánimo lucro frente a la modalidad vishing en tiempos del covid-19 en Lima -2020.

Premisa: En el tema del ánimo de lucro que tiene los bancos para no hacer responsable de los daños causado por el delito de fraude informático, por ello

4.- En su perspectiva ¿De qué manera se puede evitar el ánimo de lucro frente a la modalidad vishing en tiempos del Covid-19 en Lima -2020?
Al momento de la firma de contratos con las financieras se debe estipular cuales son las plataformas digitales establecidas y verifica si el usuario desea hacer uso de las mismas.

5- En su opinión ¿Qué criterios debe tener el juez en tema del ánimo de lucro de los bancos para no responsabilizarse objetivamente sobre la información filtrada de sus usuarios para la afectación del daño causado por el tema de vishing?
El juez debe poner en aplicación los acuerdos plenarios, casaciones , u otras para subsanar los vacíos legales de la norma.

6.- En el mismo contexto, ¿qué recomendaría para que el tema de seguridad en la información de los usuarios sea pertinente en el delito de fraude informático en la modalidad vishing?

Recomendaría el uso de plataformas respaldadas por las entidades financieras.

Objetivo específico 2

Analizar cómo se debe reponer el daño patrimonial ante la modalidad de smishing en tiempos del covid 19 en Lima – 2020

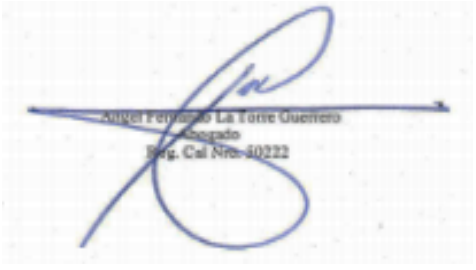
Premisa: Por ello es importante determinar el daño patrimonial emergente de los clientes de los bancos ante la modalidad de smishing. Por ello

7.- En ese escenario, ¿Cómo se debería reponer el daño patrimonial en su totalidad o en forma parcial ante la modalidad de smishing frente en tiempos del Covid 19 en Lima – 2020?
Debe ser en base a los acuerdos contractuales.

8.- ¿cuál es el criterio que debe tener el juez para reponer el daño patrimonial de los clientes de los bancos por la modalidad smishing?
Debe considerar si la responsabilidad recae sobre la entidad bancaria por filtración de información.

9.- ¿qué medidas jurídicas aportaría para que el daño patrimonial de los clientes de los bancos sea adecuado en el tema de delito de fraude informático en la modalidad de smishing?

Que los bancos garanticen el empleo de plataformas digitales respaldada por los mismos frente a los delitos cibernéticos. FECHA:



UNIVERSIDAD CÉSAR VALLEJO

GUÍA DE ENTREVISTA

Título: **Responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid 19 en Lima-2020.**

Entrevistado/a: Danilo Callirgos de la Cruz.

Cargo/profesión/grado académico: Especialista del NCPP de la Corte Superior de Justicia/ abogado/ superior

Objetivo general

Analizar de qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phising en tiempos de Covid 19.

Premisa: Mucho se verifica que tanta responsabilidad tiene los bancos con el tema del delito de fraude informático para indemnizar a las personas que le roban su información personal como financiera, por ello,

1.- Desde su perspectiva ¿De qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid 19 en Lima- 2020?

El banco en mi opinión debe responsabilizarse en su totalidad del dinero robado de forma fraudulenta a los clientes de estas mismas ya que el phishing es una nueva modalidad de robo de información pero que esta entidad debe conocer su modalidad de perfección.

2.- En su opinión ¿qué responsabilidad civil tiene los bancos cuando los datos personales y financieros se filtran de una persona?

Los bancos al ser un servidor público y al ofrecer estas alternativas de uso de sus servicios debe procurar cuidar al cliente de estas modalidades de estafas por eso al caer en este delito el cliente la entidad debe responsabilizarse de forma objetiva.

3.- Desde su perspectiva. ¿Qué medida recomendaría para que la responsabilidad

Civil de los bancos sea aplicada dentro del contrato de adhesión en el tema de delito fraude informático?
Desde el punto penal se debería aplicar otra clase de contrato donde haya también cláusulas que responsabilice al banco frente a estos delitos de la nueva era.

Objetivo específico 1

Analizar de qué manera se debe evitar el ánimo de lucro frente a la modalidad vishing en tiempos del covid-19 en Lima -2020.

Premisa: En el tema del ánimo de lucro que tienen los bancos para no asumir la responsabilidad de los daños causados por el delito de fraude informático, se observa que los usuarios se ven afectados con esta modalidad de fraude, por ello

4.- En su perspectiva ¿De qué manera se puede evitar el ánimo de lucro frente a la modalidad vishing en tiempos del Covid-19 en Lima -2020?
El ánimo de lucro en cualquier delito en especial del vishing seria aplicando medidas mas eficientes por parte de las entidades y por parte del Estado aplicando penas mas fuertes para esta clase de delitos.

5- En su opinión ¿Qué criterios debe tener el juez en el tema del ánimo de lucro de los bancos para no responsabilizarse objetivamente sobre la información filtrada de sus usuarios para la afectación del daño causado por el tema de vishing?
El juez debe tomar criterios para responsabilizar a los bancos si es que se prueba que el usuario dio su información adrede o el mismo es parte de un grupo criminal e hizo todo el fraude a beneficio propio o de terceros conocidos de este.

6.- En el mismo contexto, ¿qué recomendaría para que el tema de seguridad en la información de los usuarios sea pertinente en el delito de fraude informático en la modalidad vishing?
Yo recomendaría que la gente que accede a esta clase de servicios virtuales se informen sobre esta modalidad de crímenes y que sea la misma entidad quien de una información idónea y prevención especifica.

Objetivo específico 2

Analizar cómo se debe reponer el daño patrimonial ante la modalidad de smishing en tiempos del covid 19 en Lima – 2020

Premisa: Es importante determinar el daño patrimonial emergente de los clientes de los bancos ante la modalidad de smishing. Por ello

7.- En ese escenario, ¿Cómo se debería reponer el daño patrimonial, en su totalidad o en forma parcial ante la modalidad de smishing en tiempos del Covid 19 en Lima – 2020?

Se debe reponer en forma total ya que la entidad es quien de forma indirecta puso en peligro al usuario al no informar, preparar y prevenir al cliente sobre estos delitos.

8.- ¿cuál es el criterio que debe tener el juez para reponer el daño patrimonial de los clientes de los bancos por la modalidad smishing?

El juez debe tener en cuenta que el cliente es totalmente inocente de este delito que accedió a dar información pensando que no era para el fin ilícito.

9.- ¿qué medidas jurídicas aportaría para que el daño patrimonial de los clientes de los bancos sea adecuado en el tema de delito de fraude informático en la modalidad de smishing?

Aplicaría penas mas efectivas para los ciberdelincuentes que hacen esta clase de delitos y crearía nuevas leyes que sean específicas para responsabilizar a las entidades en circunstancias como estas que es la pandemia y se accede de forma virtual por necesidad.

ANEXO 7:

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1 Apellidos y Nombres: Santisteban Llontop, Pedro

1.2 Cargo e institución donde labora: UCV

1.3 Nombre del instrumento motivo de evaluación: **Ficha análisis de fuente documental**

1.4 Autoras de Instrumento: Paredes Salazar, Edith Silvia y Silva Rueda, Elsa Milagros

II. ASPECTOS DE VALIDACIÓN:

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. PRESENTACIÓN	Responde a la formalidad de la investigación.												X	
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Considera información actualizada, acorde a las necesidades reales de la investigación.												X	
4. INTENCIONALIDAD	Está adecuado para valorar las categorías.												X	
5. COHERENCIA	Existe coherencia entre los objetivos y supuestos jurídicos.												X	
6. METODOLOGÍA	La estrategia responde a una metodología y diseño aplicados para lograr verificar los supuestos.												X	
7. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												X	

III. OPINIÓN DE APLICABILIDAD

- El instrumento cumple con los requisitos para su aplicación
- El instrumento no cumple con Los requisitos para su aplicación

SI

IV. PROMEDIO DE VALORACIÓN:

Lima, 05 de octubre del 2021

FIRMA DEL EXPERTO INFORMANTE
Dr. Santisteban Llontop Pedro
DNI No 09803311 Telf.: 983278657

ANEXO 6

GUIA DE ANALISIS DE FUENTE DOCUMENTAL

Título de la investigación: Responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid19 en Lima-2020.

Autores:

Paredes Salazar, Edith Silvia (ORCID 0000-0003-1912-0451)

Silva Rueda, Elsa Milagros (ORCID 0000-0001-6470-913)

<table>
<tr><td colspan="2">Guía de análisis de fuente documental – resolución</td></tr>
<tr><td colspan="2">Objetivo general
Analizar de qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phising en tiempos de covid 19 en Lima- 2020</td></tr>
<tr><td colspan="2">Identificación de la fuente
Resolución S.B.S. N° 5570-2019 La Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones</td></tr>
<tr><td>Contenido</td><td>Análisis del contenido</td></tr>
<tr><td>Artículo 23.- Responsabilidad por operaciones no reconocidas
Ante el rechazo de una transacción o el reclamo por parte del usuario de que esta fue ejecutada incorrectamente, la empresa es responsable de realizar la evaluación correspondiente y de demostrar que las operaciones fueron autenticadas y registradas. La empresa es responsable de las pérdidas por las operaciones realizadas en los siguientes
casos:
1. Por incumplimiento de lo dispuesto en el artículo 21 del Reglamento.
2. Cuando las tarjetas hayan sido objeto de clonación. (…)
En caso no se cumpla con ninguno de los supuestos anteriores; y de producirse el extravío, sustracción, robo, hurto o uso no autorizado de la tarjeta, o de la información que contiene, la empresa es responsable de las operaciones realizadas con posterioridad a la comunicación efectuada a la</td><td>En contexto de esta resolución de SBS en su artículo 23 se analizó que todo tipo de operaciones no reconocidas y rechazadas por el usuario(cliente) de la financiera. Por ello la empresa es responsable de evaluar y demostrar que las operaciones fueron auténticas y registradas. Para que la empresa sea responsable de estas operaciones perdidas por el cliente son los siguientes supuestos cuando las tarjetas ha sido clonadas, como también la manipulación de información sustraída tecnológicamente, pero lo relevante de este artículo es que la financiera tiene estas operaciones no reconocidas deben ser evaluadas y demostradas por misma financiera. por tanto también lo importante es que manifiesta esta resolución se produjera la perdida, robo o uso no autorizado de la tarjeta indica que la empresa es responsable de las operaciones posteriores a los sucesos.</td></tr>
</table>

empresa por parte del usuario para informar tales hechos.	

Ponderamiento

En el Artículo 23 Resolución S.B.S. N° 5570-2019 La Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones se determinó que todo tipo de operaciones no reconocidas y rechazadas por el cliente de la financiera la empresa responsable tiene que evaluar y demostrar que las operaciones fueron auténticas y registradas para que esta sea responsable de estas operaciones perdidas por el cliente son los siguientes supuestos cuando las tarjetas ha sido clonadas, como también la manipulación de información sustraída tecnológicamente, por tanto también lo importante que esta resolución menciona que si se produjera la perdida, robo o uso no autorizado de la tarjeta indica que la empresa es responsable de las operaciones posteriores a los sucesos.

Guía de análisis de fuente documental – Ley

Objetivo general

Analizar de qué manera debe ser aplicada la responsabilidad civil de los bancos frente al delito de fraude informático phising en tiempos de covid 19 en Lima- 2020

Identificación de la fuente

LEY Nº 30096-LEY DE DELITOS INFORMÁTICOS

Contenido	**Análisis del contenido**
Artículo 8. Fraude informático **El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.** **Artículo 11. Agravantes**	En relación este artículo de la ley de delitos informáticos se analiza que una persona realiza un acto delictivo a través de las tecnologías de la información o comunicación para beneficiar para sí mismo o para otros en perjuicio de otra persona todo tipo de manipulación de información (diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático), con el uso de tecnología. Asimismo, los agravantes son cuando el acto delictivo es por pertenecer a una organización criminal, cuando abusas de la confianza de la información por tu cargo de función y cuando esa información afecta a las personas con fines

El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando: **1. El agente comete el delito en calidad de integrante de una organización criminal.2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.** **3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.** **4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales**	asistenciales, la defensa, la seguridad y soberanía nacional.

Ponderamiento

En el artículo 8 y sus agravantes Art.9 de la Ley Nº 30096-Ley de Delitos Informáticos se concluyó que una persona realiza un acto delictivo a través de las tecnologías de la información o comunicación para beneficiarse para sí mismo o para otros en perjuicio de otra persona todo tipo de manipulación de información, pero también la agravante de este delito es cuando utiliza esa información en un grupo criminal, y afecta fines asistenciales, defensa, seguridad; y soberanía nacional.

ANEXO 6

GUIA DE ANALISIS DE FUENTE DOCUMENTAL -

Título de la investigación: Responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid19 en Lima-2020.

Autores:

Paredes Salazar, Edith Silvia (ORCID 0000-0003-1912-0451)

Silva Rueda, Elsa Milagros (ORCID 0000-0001-6470-913)

<table>
<tr><td colspan="2">Guía de análisis de fuente documental – Revista</td></tr>
<tr><td colspan="2">Objetivo específico 1
Analizar de qué manera se debe evitar el ánimo de lucro frente a la modalidad vishing en tiempos del covid19 en Lima -2020</td></tr>
<tr><td colspan="2">Identificación de la fuente
CONVENIO SOBRE LA CIBERDELINCUENCIA Budapest, 23.XI.200. MINISTERIO DE RELACIONES EXTERIORES.
http://dataonline.gacetajuridica.com.pe/gaceta/admin/elperuano/2292019/22-09-2019_CONVENIO.pdf</td></tr>
<tr><td>Contenido</td><td>Análisis del contenido</td></tr>
<tr><td>Artículo 8 – Fraude informático
Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

a. la introducción, alteración, borrado o supresión de datos informáticos;
b. cualquier interferencia en el funcionamiento de un sistema informático, con la intención,</td><td>En relación sobre este convenio internacional de ciberdelincuencia lo más relevante que se puede extraer son las medidas que se debe adoptar en nuestro ordenamiento jurídico en el tema de delitos informáticos, con ello este artículo del convenio nos hace entender que el Estado peruano debe establecer medidas de seguridad interna para erradicar el fraude informático y también este convenio tiene un tema de cooperación internacional con las entidades que salvaguardan este tipo de afectación a un tercero.</td></tr>
</table>

dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.	

Ponderamiento

En el Convenio sobre la ciberdelincuencia Budapest, 23.XI.200. Ministerio de relaciones exteriores se determinó que este Convenio de colaboración internacional la ciberdelincuencia los países deben adoptar medidas pertinentes para proteger la información personal financiera de las personas para evitar el delito de fraude informático en contra de su patrimonio.

Guía de análisis de fuente documental – Informe

Objetivo específico 1

Analizar de qué manera se debe evitar el ánimo de lucro frente a la modalidad vhishing en tiempos del covid19 en Lima -2020

Identificación de la fuente

Informe Nº 00001 -2020-UIF-SBS

Asunto: Acciones, resultados y proyecciones de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS) con relación a la Unidad de Inteligencia Financiera del Perú (UIF), al primer semestre de 2020.

Contenido	**Análisis del contenido**
Aumento de fraudes y estafas asociados a planes de ayuda financiera, lanzados por el gobierno; robo de datos para acceder a las cuentas de bancos, por medio de llamadas telefónicas y sitios web falsos; y, fraudes	En este informe de SBS se puede analizar que el confinamiento a la cual somete el Covid19 se apreciado el aumento de estas modalidades por el tema de que la mayoría de personas han estado utilizando todo tipo de acceso a internet para no tener contacto con otra persona y por ello las organizaciones delictivas han

y delitos cibernéticos, debido al aumento de operaciones financieras remotas o no presenciales.	comenzado utilizar modalidades como phishing, vhishing y smishing para afectar a un tercero en su patrimonio financiero.
Ponderamiento	
En el Informe Nº 00001 -2020-UIF-SBS se determinó que el Estado debe poner medidas de seguridad a favor de las personas en el tema de fraude informático como también un tema de resarcimiento y reparación para las personas afectadas en el contexto de confinamiento, dado que lo indica el convenio internacional de ciberdelincuencia donde los Estados deben establecer medidas preventivas, correctivas y de reparación para los perjudicados que son los usurios.	

ANEXO 6

GUIA DE ANALISIS DE FUENTE DOCUMENTAL -

Título de la investigación: Responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid19 en Lima-2020.

Autores:

Paredes Salazar, Edith Silvia (ORCID 0000-0003-1912-0451)

Silva Rueda, Elsa Milagros (ORCID 0000-0001-6470-913)

Guía de análisis de fuente documental – caso concreto	
Objetivo específico 2 Analizar cómo se debe reponer el daño patrimonial ante la modalidad de smishing en tiempos del Covid 19 en Lima – 2020	
Identificación de la fuente Caso bcp reclamo nro. C04363889 de fraude informático	
Contenido solicitud No Favorable: Operaciones no reconocidas N° C04363889 Recibidos Servicio Post Venta - BCP <bcp.atencioncliente@bcp.com.pe> 13 sep. 2021 22:24	**Análisis del contenido** Analizando este caso se manifiesta que el usuario le clonaron su tarjeta, dado que lo montos realizados son continuos y en el mismo cajero de pago por comisión e igual el banco

para mí Hola Roberto, Te saluda Victoria del BCP y es un placer comunicarme contigo. Gracias por contactarnos y permitirme ayudarte en este proceso. Te informo que luego de haber revisado y analizado tu solicitud nro. C04363889 por las operaciones no reconocidas registradas en tu Cuenta de Ahorro nro. 193-96067878-0-58, he concluido que el resultado es no favorable ya que he validado que las operaciones fueron realizadas con tu tarjeta Credimás nro. 4557-88**-****-8474, con lectura de chip y tu clave secreta de 4 dígitos. En el siguiente cuadro podrás ver el detalle de las operaciones cuestionadas (*): FECHA HORA DETALLE IMPORTE MONEDA 30/08/2021 08:39:00 RETIRO CAJERO OTRO BANCO - BANCO INTERBANK - AV HUANDOY MZ J LT 16 S/ 400.00 SOLES 30/08/2021 08:40:00 Retiro cajero otro banco - banco Interbank - av Huandoy mz j lt 16 S/ 400.00 SOLES 30/08/2021	no quiere reponer el daño patrimonial ante este fraude el tipo de argumento que se usaría es que es una operación no reconocida establecida en el artículo 23 numeral 2. Cuando las tarjetas hayan sido objeto de clonación. (…) de la Resolución S.B.S. N° 5570-2019 La Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.

08:41:00 Retiro cajero otro banco - banco interbank - av Huandoy mz j lt 16 S/ 400.00 SOLES (*) Según nuestro reporte de sistemas. Entiendo lo que te ha sucedido y lamento por lo que estás pasando. Sin embargo, te comento que la operación no reconocida mencionada en tu solicitud no está relacionada a un evento de fraude. Por ello, los cobros de S/15.00 soles por la comisión por uso de cajero de otro banco por cada operación son conformes. De no encontrarse conforme con nuestra respuesta, puede solicitar una reconsideración a través de nuestra Banca por Teléfono al 311-9898. O dirigirse al Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), o a través de la Superintendencia de Banca, Seguros y AFP´s (SBS). Pd. Este Buzón es de envío automático, por favor no responder.	

Ponderamiento

En el Caso bcp reclamo nro. C04363889 de fraude informático se determinó que la responsabilidad de la financiera no se está dando adecuadamente para la reposición del patrimonio afectado por parte de la financiera, ellos sabe que esto es un proceso de doble instancia y se excusan en ellas para que los usuarios vayan ha Indecopi o SBS y basarse en los artículos mencionados en el análisis de caso concreto, por tanto el usuario tiene que esperar que otra instancia le favorezca en su reclamo con ello quiere decir que la resolución de la SBS no se aplica en primera instancia por parte de la financiera.

<table>
<tr><td colspan="2">Guía de análisis de fuente documental – caso concreto</td></tr>
<tr><td colspan="2">Objetivo específico 2
Analizar cómo se debe reponer el daño patrimonial ante la modalidad de smishing en tiempos del covid 19 en Lima – 2020</td></tr>
<tr><td colspan="2">Identificación de la fuente
Nota de prensa TV Frecuencia latina</td></tr>
<tr><td>Contenido
Un joven ingeniero es una nueva víctima de los delincuentes cibernéticos. Daniel Barriga denuncia que todo comenzó con una llamada aparentemente de la entidad bancaria, alertando a la víctima por una compra en Amazon, para confirmar sus datos y realizar diversas transferencias de su cuenta bancaria.</td><td>Análisis del contenido
Se análisis que este caso fue por una llamada por la modalidad de smishing, dado que el usuario tuvo la pérdida de 19 mil soles indican que el Lima se está incrementado este tipo de robo o fraude informático, pero como no está como tipificado como operaciones no reconocidas para que el banco te devuelva tu dinero por motivo de fraude, en cambio te pide que compres seguros en tu tarjeta para protegerte en cambio como está la otra modalidad de clonación de tarjetas que si está tipificado en el artículo 23 numeral 2. Cuando las tarjetas hayan sido objeto de clonación. (…)
de la Resolución S.B.S. N° 5570-2019 La Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Ponderamiento</td></tr>
<tr><td colspan="2">En la Nota de prensa TV latina en conclusión, en esta modalidad nuestro ordenamiento jurídico no lo pone como operación no reconocida a favor del cliente para la devolución del patrimonio financiero. Por ello se tiene que regular dado que en</td></tr>
</table>

el contexto del confinamiento se incrementado estos tipos de modalidades de fraudes informáticos para poder resarcir al usuario.