UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

“La responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing”

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogado

AUTORES:

Coarite Espinoza, Betsabe Celeste (ORCID: : 0000-0001-5115-928X)

Ramos Flores, Daniel Andres (ORCID: 0000-0002-9463-7525)

ASESORA:

Dra. Zevallos Loyaga, Maria Eugenia (ORCID: 0000-0002-2083-3718)

LÍNEA DE INVESTIGACIÓN:

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

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

TRUJILLO - PERÚ

2022

Dedicatoria

A mis padres Gerardo RAMOS ALE, y Natividad FLORES VELA, quienes fueron las primeras personas que me motivaron, y que en estos últimos meses fallecieron y están a lado de Dios, y en reconocimiento sé que lograré obtener el título de abogado, para de esta manera honrar sus nombres.

Agradecimiento

En primer lugar, agradezco, el apoyo de mi asesora de tesis la Dra. María Eugenia Zevallos Loyaga, quien es la que corrige y encamina mi tesis y con su conocimiento enfoca lo que quiero contribuir en mi presente investigación con la finalidad de poder aportar en el tema y de esta manera conseguir alternativas de solución al presente problema enfocado.

Índice de contenidos

Índice de tablas

Resumen

Esta investigación se inició a raíz de la identificación de un problema que ha afectado a la sociedad desde hace varios años y que va en constante incremento, y es que el fraude informático es una amenaza a la estabilidad financiera, ya que, en estos tiempos, a través de las redes, se pueden realizar muchas transacciones como transferencias, pago de sueldos, banca por internet, entre otros.

Por consiguiente, la investigación, es elementalmente de **tipo** básica, con un nivel descriptivo, con **diseño** no experimental y transversal, de enfoque **cualitativo**; 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 que , el phishing es el método más usado por los cyberdelincuentes para captar a usuarios y poder despojarlos de su patrimonio económico, mediante el uso de la tecnología.

La investigación concluyó que, la responsabilidad civil de las entidades financieras es asumir la restitución del daño patrimonial de los usuarios que fueron víctimas de la comisión del fraude informático a través del phishing.

Se propone, que las entidades financieras incluyan en su procedimiento de seguridad el uso de reconocimiento facial y biométrico.

Palabras clave: Daño patrimonial, responsabilidad civil, fraude informático, phishing, entidades financieras.

Abstract

This investigation was initiated as a result of the identification of a problem that has affected society for several years and that is constantly increasing, and that is that computer fraud is a threat to financial stability, since, in these times, Through the networks, many transactions can be carried out such as transfers, payment of salaries, internet banking, among others.

Therefore, the research is basically of a basic type, with a descriptive level, with a non-experimental and cross-sectional design, with a qualitative approach; allowing various 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 that phishing is the method most used by cybercriminals to capture users and be able to strip them of their economic assets, through the use of technology.

The investigation concluded that the civil responsibility of financial entities is to assume the restitution of the patrimonial damage of the users who were victims of the commission of computer fraud through phishing.

It is proposed that financial entities include the use of facial and biometric recognition in their security procedure.

Keywords: Property damage, civil liability, computer fraud, phishing, financial entities.

I. INTRODUCCIÓN

Actualmente, el avance y progreso de la tecnología informática ha proporcionado a la colectividad una cantidad cada vez mayor de información tecnológica de todo tipo. Esta creación, transferencia e intercambio de información ha hecho una importante contribución a la transformación de la sociedad, la organización económica y gubernamental, el comercio en red, entre otras transacciones.

Este avance tecnológico también implica una gran fragilidad en todos los niveles sociales de cualquier estado, puesto que ha dado paso a la formación de hechos delictivos cada vez más sofisticados como el denominado por Aboso y Zapata (2006) el “Ciberdelito” o delitos informáticos, los cuales en los últimos tiempos han representado una gran amenaza para las organizaciones financieras, incluyendo las economías de los países, debido a que se incrementan día a día, incluso más rápido que la misma creación de leyes o códigos penales que puedan reconocerlos.

Las infracciones cibernéticas o delitos informáticos han aumentado significativamente a nivel mundial, y el Perú no es la excepción, es el sector financiero el sector más vulnerable. En el tiempo trascurrido, las instituciones financieras lidian contra los delitos informáticos que sufren a diario, sea contra la entidad financiera, o bien, dirigidos a sus usuarios. El daño económico de este tipo de delito informático es cada vez más alto. Una investigación publicada el 26.09.2017 por la revista Gestión indica que el líder mundial, Boston Consulting Group, Stefan Deustcher, en un evento denominado “Ciberseguridad: más allá de bits y bytes” ejecutado en Lima el mismo año, afirmó que el cibercrimen cuesta al mundo $575 mil millones por año y el costo promedio por ciberataque $11 millones y el 72% de las infracciones se deben a errores humanos. Lo que significa que diversas entidades, incluidas las financieras, se han visto obligadas a invertir en sistemas de respaldo informático para prevenir estos delitos; realizando

cambios en sus sistemas operativos y métodos comerciales para evitar robos, duplicaciones y fraudes.

En referencia a lo anterior, Bermúdez (2018) afirmó que los bancos enfrentan tres riesgos informáticos principales: (i) duplicación de tarjetas (ii) usurpación de identidad al realizar compras directas no autorizadas (iii) “fraude”.

Señala que, según la 19ª Encuesta Mundial de Seguridad de la Información (Ernst and Young), el phishing es una amenaza de mayor crecimiento, pasando del 39% en el 2014 y 44 % en el 2015 a 51 % en el 2016. Este tipo de fraude digital ha crecido mucho en Latinoamérica y Perú.

Por otro lado, el Perú suscribió un importante acuerdo sobre ciberdelincuencia, el acuerdo de Budapest (2004), el cual fue aceptado, con la correspondiente aprobación contenida en la R.L. N°30912, del 13.02.2019. Este acuerdo, pionero en casos de esta materia, tiene como finalidad convertirse en un instrumento normativo internacional para la erradicación de los nuevos delitos en red o los denominados delitos informáticos mediante la adopción de normas internas de búsqueda efectiva legal y la cooperación internacional para su erradicación.

El uso de “políticas penales comunes” aparece desde el primer momento, sentando las bases para la lucha contra el ciberdelito. Cuatro años de trabajo en el acuerdo, en colaboración con varios expertos internacionales, dieron como resultado una lista de delitos que los estados, como parte de su compromiso, deben incluir en sus ordenamientos jurídicos de su país. Además de lo anterior, los estados contratantes también se han visto comprometidos a cooperar en cuanto a la investigación y procedimientos necesarios para obtener datos que constituyan un delito de esta naturaleza. Tal es el caso de prevención de delitos informáticos ejecutado por la Superintendencia de Banca y Seguros AFP en 2018, que emitió reglamentos

de tarjetas de débito y crédito para combatir los delitos informáticos relacionado al uso de tarjetas de sus clientes.

Nuestro sistema jurídico, relacionado a delitos informáticos, se encuentra en el Art. 186 código penal donde se tipifica como agravante el “hurto electrónico”. Nuevamente reformado por la ley 27309 del 17.07.2009, que transforma el título V, 2do libro del Código Penal, implantando un nuevo capítulo. Mediante ese nombre se introducirán los siguientes delitos: (Art. 207-A) fraude informático y estafa; (Art.207-B) sabotaje informático; (Art. 207-C) circunstancias agravantes y (Art. 207-D) tráfico ilegal de información. Los delitos mencionados, son amonestaciones penales para quienes accedieron ilegalmente a una información por sistema o red informática, con la finalidad de causar daños, como consecuencia de un cambio, modificación o robo de información.

Por lo anterior, se promulgó la Ley N°30096, la misma que fue reformada por la Ley N°30171, “Ley de delitos informáticos”. Donde se incorporó nuevas legislaciones a nuestro sistema penal para ajustar el ordenamiento jurídico local a las medidas internacionales establecidas por la "Convención de Budapest". Como tal, se ha tipificado: acceso ilegal, invasión a información informática, invasión a un sistema informático que dañe a infantes y adolescentes con desenlaces sexuales por medio de un sistema o red tecnológico, incluido el robo de información, fraude informático y de identidad, robo ilegal de dispositivos informáticos, representado en varios países europeos como Alemania, España y Francia, estados latinos como Argentina, Chile, Ecuador y Estados Unidos.

Como ha señalado Arbulú (2002), “el delito informático es cualquier acto típico, ilegal y pecaminoso realizado mediante un delito o hurto automático de la información, sistemas de información que siempre provoca en perjuicio de una persona física o de la ley. Los delitos informáticos presentan características altamente ofensivas ya que pueden ser contra el patrimonio, privacidad, seguridad pública, seguridad tecnológica, esta última puede

considerarse una nueva tipología de participación jurídica que requiere ser amparada como un delito ley.

Por otro lado, esta situación en nuestro país y ciudad, se ha acrecentado a consecuencia de la aparición de la pandemia por COVID-19, puesto que para ayudar al ciudadano en época de confinamiento, el Estado apoyó a sus ciudadanos con bonos y beneficios económicos; el mismo que fue encargado a las entidades financieras para su distribución, lo que ha provocado un masivo movimiento ciudadano a las entidades financieras de forma directa y virtual, provocando acoso de estafadores, fraudes informáticos como duplicación de tarjetas de crédito, phishing, transferencias electrónicas de dinero fraudulentas, sansomware, hurto, robo de identidad entre otros.

Debido a la gran cantidad de transacciones virtuales que se realizan sin la presencia del titular de la tarjeta, el banco trata de evitar responsabilidades y solo en casos excepcionales reconoce transacciones fraudulentas para los clientes, generalmente aquellos con seguro, el haber depositado dinero en un banco no será suficiente para garantizar que los fondos están seguros y por lo tanto el banco trata de no ser responsable de los delitos informáticos u otras actividades de red que ocurren en las cuentas de sus clientes.

Una obligación civil es el cumplimiento de una obligación con el fin de recuperar un crédito inverso resultante de un evento adverso, en cuyo caso los delitos bancarios por Internet, aunque reales, no fueron cometidos por la banca por Internet, pero indirectamente si, al no buscar métodos, estrategias que brinden seguridad a sus clientes. Asimismo, la responsabilidad civil de la entidad bancaria frente a sus clientes debería intervenir tanto en el ámbito "contractual" como "fuera del contrato" o “extracontractual” de la obligación vinculante, no del contrato, donde se creyó erróneamente.

Por otro lado, el régimen de riesgo bancario que constituye un pasivo es parte de la distinción de las entidades financieras, por lo que debe

incorporarse al pasivo del banco y debe incorporarse a las políticas voluntarias de buenas prácticas, ya que no está legalmente incorporado, depende de las financieras. El descubrimiento de su incumplimiento o incumplimiento en el cumplimiento, que es la base de la responsabilidad civil, no es una imposición objetiva, sino una actuación pericial, con criterio fuerte, con capacidad y espíritu de acción para buscar una adecuada sanción a la entidad financiera.

Una propuesta del estudio para las instituciones financieras cuyos fondos se les confían en forma de ahorros, transacciones o de cualquier otro modo, es que estén enteramente sujetas a las consecuencias de los delitos informáticos bancarios, se entiende a la responsabilidad civil, aquella responsabilidad derivada de acuerdos, bajo el respaldo legal de los que nace una obligación, de pagar o restituir cierta cantidad que debe ser indemnizada a favor del cliente perjudicado o del ahorrador.

Ante esta coyuntura, se ha identificado el siguiente **problema de investigación** ¿Cuál es la responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing?

La realización de la presente investigación denominada “La responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing”, se justifica desde un **enfoque teórico**, ya que el tema se ha pronunciado más desde la coyuntura del COVID 19, y se ha visto que la ley que protege el sistema financiero no ampara a la mayoría de los usuarios, en cuanto a que, no ha existido resarcimiento económico en la mayoría de los casos. Por tal motivo se logrará establecer la responsabilidad civil de las entidades financieras frente a la comisión de delitos informáticos, profundizando en los delitos de suplantación de identidad.

Por otro lado, desde el **enfoque metodológico**, la investigación se sustentará bajo un fundamento legal, puesto que los "delitos informáticos"

son un fenómeno reciente con impacto global, los ataques no son diferenciados en todas las disciplinas y en todos los niveles, todavía no hay suficiente investigación académica sobre este fenómeno y su impacto permitirá ver el lado legal real de la responsabilidad civil de las instituciones financieras derivada de la comisión de los delitos financieros ocurridas en la ciudad de Tacna.

Por último, desde el **enfoque práctico** resulta ser que existe una necesidad por parte de los usuarios de las entidades financieras, de clarificar la legislación que protege a los usuarios frente a la comisión de los delitos informáticos, puesto que, en los casos existentes, hasta la actualidad no han sido resarcidos económicamente en su mayoría y por lo tanto la presente investigación propondrá una probable solución a la problemática planteada.

Finalmente, el **objetivo general** de la investigación será: Determinar la responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

Considerando para nuestra investigación los siguientes **objetivos específicos** son: (i) Examinar la legislación comparada derivada de la comisión del fraude informático a través del phishing; (ii) Identificar los fundamentos para imputar responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing; (iii) Determinar los métodos más frecuentes derivada de la comisión del fraude informático inmersos en las entidades financieras; y (iv) Proponer alternativas de solución en beneficio de los usuarios de las entidades financieras inmersos en la comisión del fraude informático a través del phishing.

Asimismo, se consigna como hipótesis, la siguiente: Existe responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

II. MARCO TEÓRICO

En el presente capítulo se tratarán investigaciones relevantes en el contexto nacional e internacional para el tema de investigación, se seleccionan investigaciones similares según el criterio de las categorías de la investigación. Por lo que describimos los antecedentes a **nivel internacional**: La investigación titulada “La responsabilidad bancaria frente a los delitos informáticos” de Martínez (2015) de Ecuador, concluye: Que la SB y FG han emitido resolución en el año 2011, según la cual se requieren instituciones bancarias para restituir a sus usuarios que han sufrido las secuelas de los delitos informáticos. En la promulgación de las resoluciones se utilizaron los argumentos de ley; en el entorno legislativo, se señala que las instituciones financieras prestan ayuda en diversos sectores, en referencia a una obligación objetiva. Pero, todavía hay muchas dudas sobre la legalidad, así como si las entidades bancarias realmente están brindando ayuda pública o es el trato bancario donde el cliente puede aplicarse la responsabilidad estricta. Los delitos más comunes a nivel nacional son los productos pharming y el phishing.

La responsabilidad civil de las entidades bancarias frente a sus clientes por delitos informáticos se deriva de las obligaciones contractuales de la banca en línea. Las entidades financieras deben aplicar sistemas tecnológicos apropiados para utilizar los servicios informáticos. En el entorno nacional, en el COIP no precede responsabilidad penal a las instituciones financieras por delitos informáticos sufridos por los clientes.

La Tesis titulada “Responsabilidad bancaria frente al phishing” de Rodríguez (2015) de Colombia, concluye que el derecho constitucional dicta que, en el interés público, el Estado debe intervenir en la actividad financiera principal; garantizar la seguridad de los clientes que utilizan el mercado de la red bancaria; en caso contrario, teniendo en cuenta la responsabilidad civil o penal por los delitos. El Estado y las entidades responsables deben sumarse al esfuerzo y determinar quiénes son los responsables de los riesgos

asociados al uso de los medios electrónicos a través de una legislación clara.

La investigación titulada “Responsabilidad civil bancaria frente al cliente por delitos informáticos” de Salas (2010) de Costa Rica, concluye que es necesario analizar las diferentes ramas del derecho para reducir aún más la controversia relacionada con este tema; en el estado costarricense no existe una ley determinada que regularice este tipo de delitos en la banca en línea, también consideran que el riesgo que se puede presentar al apoyar la banca en línea es responsabilidad objetiva de los bancos, especialmente verificar la autenticidad de los clientes y el daño que causará. Asimismo, resulta que los acuerdos de membresía establecidos por las instituciones bancarias deben revisarse para descartar disposiciones abusivas que perjudiquen a los consumidores y establezcan abusos de poder.

La investigación titulada “Fraude al sistema financiero y a sus clientes” de Núñez (2013) de ecuador, Concluye que: las entidades financieras manejan diferentes métodos para minimizar los riesgos que existen para sus usuarios, la inversión en sistemas tecnológicos es alta; Los pagos electrónicos utilizan la tecnología SSL (Secure Socket Layers), este sistema garantiza que la información en tránsito no sea descifrada por un tercero. Los clientes son informados continuamente para que puedan tomar acciones preventivas.

Relacionado a los **antecedentes nacionales**, tenemos la investigación titulada “La responsabilidad civil de los bancos por la indebida gestión de sus riesgos en la operación económica de compra financiada de un inmueble en planos” de Campos (2016) de Lima, concluye que: El riesgo bancario es un pasivo que ha sido incorporada al juicio profesional. La verificación del incumplimiento o de su cumplimiento incompleto, pudiendo encontrar un registro de responsabilidad civil, no es un criterio objetivo a imponer, pero en el marco de un juicio sobre su actividad profesional, una condena infaliblemente tiene más autoridad, capacidad para obligar a actuar y obtener una sentencia de responsabilidad frente a la entidad financiera. En este

aspecto, la responsabilidad civil de las entidades financieras debe tener en cuenta el compromiso de administrar el riesgo en sus operaciones bancarias.

La tesis titulada “Diseño de herramientas de control y medidas de prevención para evitar ser víctimas de Delitos Informáticos” de Fernández, Cabezudo, Arenas, Herrera, y Gastelu (2010), concluye que: La falta de tipificación de delitos cometidos por un sistema informático, permite a delincuentes seguir delinquiendo con nuevas estrategias. Los delitos informáticos son un gran vacío en el derecho penal, existe una gama de delitos no contemplados en el Código Penal y necesitan ser analizados por investigadores en la materia, abogados penalistas, especialistas jurídicos; el sistema de justicia, precisamente la Ley 27309, del 26.06.2000, incluye la numeración “Delitos Informáticos” en el Código Penal, en sus artículos 207A - Manipular, acceder o copiar ilegalmente el contenido de la base de datos, art. 207B - Vandalismo informático, Art. 207C - Gravedad de las publicaciones anteriores. La clasificación es incompleta, con términos técnicos muy poco entendidos; El derecho debe ir más allá de la tecnología.

La tesis de “Legislación del secreto bancario y su relación con el delito de hurto informático de dinero mediante la violación de claves secretas, Iquitos-2010” de Tenorio y Tuesta (2012), concluye que: Lo estipulado en la ley por secreto bancario es incompatible con el desarrollo tecnológico ante el aumento de los delitos cibernéticos, además indica que el secreto bancario es un impedimento en la indagación de delitos de robo informático, puesto que la confidencialidad bancaria es levantado en su totalidad por orden judicial en procesos específicos, afectando la declaración de autores de robo de dinero informático, además, existen estadísticas de clientes de entidades financieras sobre robo de fondos de sus cuentas, en la modalidad de brecha criptográfica.

La investigación titulada “La clonación de tarjetas de crédito y la responsabilidad civil de la entidad financiera, los olivos año 2020” de Abanto

(2020), llego a la conclusión que: existe un alto nivel de responsabilidad civil de las entidades financieras por el uso de tarjetas de crédito, en materia derivada del fraude, mediante la replicación, la norma nacional como el código civil, los procedimientos de uso de tarjetas, los procesos llevados en materia de protección de información, aplicados al uso de tarjetas de pago (crédito o débito), tienen la obligación de buscar estrategias preventivas de apoyo al usuario.

En cuanto a los **antecedentes locales,** cabe señalar que no existen fuentes de investigación sobre la comisión del delito en la modalidad de los delitos informáticos, por lo que se presentan estudios relacionados al problema de seguridad de la información y delitos informáticos de manera directa.

En cuanto a las teorías relacionadas a la problemática que servirá como sustento **teórico de investigación**; a continuación, se presentarán teorías necesarias para comprender los delitos informáticos. Desde el lado filosófico podemos manifestar que, la investigación presenta dos corrientes: el empirismo y el positivismo, porque su fundamento se basa en la experiencia y fuentes basados en las ciencias y la tecnología. Desde el entorno jurídico penal, presenta un método doctrinario, dogmático, jurisprudencial, teórico y normativo basado en delitos informáticos, con las modalidades de fraude, sabotaje, estafa, robo en el aspecto informático, asimismo, el procedimiento legal se basa en tratamiento procesal y legislativo.

Para Rodríguez (2013), el procedimiento legal de delitos informáticos en la modalidad de estafa, fraude, vandalismo y hurto informático se refiere a ocuparse de los aspectos procesales legales de contención. En este sentido, existe un problema muy grave debido a la especial naturaleza de este tipo de delitos, es decir, el acto de delitos informáticos puede llevarse a cabo sin tener en cuenta las limitaciones espaciales.

Rodríguez (2013), describe que el tratamiento normativo debe tener en cuenta diversas reglas, relacionadas con las infracciones informáticas o

delitos, en el ámbito nacional o internacional. A nivel nacional, la legislación de delitos informáticos y sus modificaciones están contemplados en el código penal, a nivel internacional, existen normativas de otros países, pero el acuerdo de alcance internacional, aplicable a los países signatarios, es el Convenio de Budapest sobre Ciberdelincuencia. Sin embargo, dado que el mencionado acuerdo data de 2001, el contenido debe ser revisado y sometido a actualización de acuerdo a los hechos de los países en la actualidad.

Chaparro (2014) sobre el derecho penal informático, expresa que surgió como una formación de derecho penal, para sancionar actividades informáticas ilegales que afecten capitales humanos y corporativos, sin embargo, el progreso tecnológico y de actos ilegales, se ha ampliado al ámbito del derecho penal informático a actos en el sistema informático, para que no afecten bienes personales y/o corporativos, sino que incluyen bienes penalmente tutelados, derechos jurídicos a la integridad humana, datos, el propio sistema, público confianza, seguridad y otros factores de similar importancia.

Por otro lado, desde el lado de conceptos legislativos, tenemos que decir que la **responsabilidad civil** merece ser examinada, para comprender su importancia en la investigación, como señala León (2016), la responsabilidad de reparar los daños y perjuicios impuestos a cualquier persona definida como una "responsabilidad civil", ya sea establecida por reglamento o mediante un "juicio", es la autoridad judicial en virtud de la ley quien establece.

Por otro lado, Belaunde, fuentes y Bermúdez (2007) afirman que la responsabilidad civil surge de los actos o contratos, realizados dentro del marco legal del que surge el compromiso u obligación, de pagar o indemnizar determinadamente a quien se beneficia o cae en desventaja. Así, la obligación civil es el cumplimiento de una obligación de restablecer los tratos alterados por un evento desfavorable, puede ser una obligación

"contractual" o "extracontractual".

La responsabilidad civil de las entidades financieras, según Barbier (2002), manifiesta que es la defensa de los clientes, generalmente asegurando su crédito, merece ser considerada desde una perspectiva proteccionista, indemnizada, como contribución a la protección preventiva y coactiva, para que la tutela más frágil sea adecuadamente asimilada, no en términos de indemnización sino para evitar que se debilite. La indemnización es el último recurso para restablecer el patrimonio, ya que conduce al traslado de las partes al justo momento que podrían haber encontrado si no hubieran sufrido la pérdida. Las entidades financieras son los garantes de sus clientes por los contratos que celebran con ellos, por lo que alegan haber incumplido o realizado inadecuadamente las actividades a que están expuestos; También, actúan como garante con sus usuarios por las acciones realizadas de sus beneficiarios.

Bustamante (1993), establece que la responsabilidad civil, es un compromiso de un sujeto de derecho, es, según normas objetivas o subjetivas, el compromiso de reparar el daño causado a otras personas como consecuencia del incumplimiento de un bien jurídico u obligación contractual, como consecuencia del propio evento. La responsabilidad es de dos tipos, *contractual:* la responsabilidad se define como la falta de cumplimiento del contrato u obligación; *extracontractual:* causa un daño ajeno a cualquier relación ordinaria. La Responsabilidad civil contractual en un compromiso, hay dos grandes categorías. El primer incumplimiento de las obligaciones procedentes del contrato y las normas aplicables del código civil, es caso de falta de compromiso según el art. 1314. (Código civil, 2012).

Taboada (2013) por su parte determina que el perjuicio es producto del incumplimiento de compromisos voluntarios, que deriva del incumplimiento de las obligaciones según la doctrina de la responsabilidad contractual establecido en la legislación civil peruana.

Leysser (2004) describe que es el medio por la cual el deudor asume en caso de incumplimiento, se le atribuye la obligación, es decir, en caso de incumplimiento ya sea en parte o en ejecución cumplimiento tardío del servicio prometido.

Según, Leysser (2004) se puede apreciar que este es el daño causado tras el fallo de una obligación voluntaria, dado bajo un trato o pacto.
De la Puente y Lavalle (2001), con respecto a la naturaleza contractual de la responsabilidad, señala que ésta no se originó por la naturaleza de la obligación a no cumplirse sino por un fallo que, conforme a lo previsto en el contrato sucesorio, produjo consecuencias jurídicas.

Por Responsabilidad civil extracontractual, conocida como aquiliana, comprende la obligación del autor de un hecho, de subsanar el daño que el hecho ha producido a un sujeto. En el Código Civil se regula por lo siguiente: Art. 1984°: indemnización por perjuicio mental teniendo en cuenta la dimensión del perjuicio causado a la víctima o familiar de la víctima (Código civil, 2012).

Art. 1985°: la compensación alcanza las secuelas de los actos u omisiones que causen un daño, incluido el daño personal, moral y lucro cesante y debe coexistir una relación de causalidad entre la realidad y el daño causado. La indemnización tiene interés legítimo desde la fecha del daño (Código civil, 2012).

Para la OECD (Organización para la Cooperación y Desarrollo Económico) del 2014, los delitos informáticos, es cualquier acto antijurídico, antiético o no considerado, que involucre sistema informático o base de datos y/o transmisores de datos.

En la pirámide de Kelsen, según la Carta magna del Perú (1993) existe una serie de derechos esenciales que son vulnerados directa o indirectamente por los delincuentes informáticos sin ningún impedimento, sobre todo si

tenemos la libertad al derecho de la información, autonomía de creencias, expresión, etc.

Internamente, contamos con una normativa penal en materia de investigación desde 1991 con la promulgación del Código Penal (que entró en vigencia), pero se enfoca en el tema de puntos de vista patrimonial, introducen nuevos actos de los ciberdelincuentes, considerándose oportuno incluirlo en los métodos descritos por el artículo 186 del Código , más penal precisamente en el apartado 3 del segundo párrafo, que dice que el robo también se configura “mediante el uso de medios de transferencia electrónica de dinero, telecomunicaciones en general, o violaciones al uso de códigos secretos”.

Posteriormente, encontrando que sólo se atacaban ciertos hechos y otros quedaban en la impunidad, se incluyó en el Código Penal el capítulo X, con las siguientes especificaciones: Obstrucción, acceso o copia ilícita contenida en una plataforma de información o base de información (Art. 207°A); Variación, daño o destrucción de base de información (Art. 207°B); circunstancias calificantes agravantes (Art. 207°C); tráfico ilegal de datos (Art. 207°D), y algunas especificaciones penales especiales.

Por otro lado, la ley N° 30096 promulgada en el Diario Oficial de El Peruano el 22.10.2013, sobre Ley de Delitos Informáticos, en su Art. 1° describe que la ley tiene el objeto de prevenir y sancionar los actos ilícitos que afecten a los sistemas informáticos, datos y demás bienes jurídicos de carácter delictivo, realizados mediante el uso de las tecnologías de la información, la información o las comunicaciones, para garantizar una lucha eficaz contra la ciberdelincuencia.

Las modificaciones de la Ley N° 30171 por la Ley N°30096 promulgada en el Diario Oficial El Peruano el 10.03.2014 sobre Ley de Delitos Informáticos, se buscó adecuar normativas según el Convenio de Budapest sobre ciberdelincuencia, mediante la integración de diversos artículos (2, 3, 4, 7, 8

y 10). A la vez, también sufrió algunas modificaciones con la aparición de la Ley Nº 30171, las mismas que son:

- Art. 1°: Modifica artículos de la Ley N°30096 sobre Delitos Informáticos (2°, 3°, 4°, 5°, 7°, 8° y 10°).
- Art. 2°: Reforma a las disposiciones finales adicionales de la Ley N° 30096 “Ley de Delitos Informáticos” (3ra, 4ta y 11ma disposiciones complementarias finales).
- Art. 3°: Se incorpora a la Ley N° 30096 “Ley de Delitos Informáticos” el artículo 12°.
- Art. 4°: Reforma del Código Penal los siguientes art. 158°, 162° y 323°.
- Art. 5°: Se Incorpora en el Código Penal los art. 154°A y 183°B. Asimismo, se deroga el art. 6° de la Ley N° 30096 “Ley de Delitos Informáticos”.

Barrios (2017) describe que el delincuente informático personifica acciones con características delictivas, utilizando un sistema tecnológico o quebrantando los derechos del usuario de un medio informático (hardware o software). El delito informático se refiere a cualquier conducta de naturaleza ilegal, sin ética, que involucre el procesamiento y/o transferencia de información sin permiso.

Lamperti (2017) afirma que un acto constituye un delito cuando tiene relevancia jurídica, lo que implica que todo lo que se considere delito debe ser regulado penalmente; entonces podemos decir que las circunstancias son delictivas, esto se llama estado de derecho, y el juez tiene terminantemente prohibido sancionar otros actos que no estén claramente definidos por la ley penal.

Villavicencio (2014) afirma que se entiende por delito informático los actos destinados a romper los sistemas de los equipos de seguridad, es decir, infiltrarse en las computadoras, correos electrónicos o sistemas de datos a través de códigos de acceso; los comportamientos típicos solo pueden lograrse mediante la tecnología.

Laredo y Ramírez (2013) reafirma el delito informático se da desde cualquier sistema informático con el fin de cometer un delito.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

La investigación, es elementalmente de **tipo** básica, con un nivel descriptivo, con **diseño** no experimental y transversal, de enfoque **cualitativo**. Tratándose de una investigación *Básica*, Navarro (2016) enfatiza que el objetivo es aplicar nuevas teorías o modificar las establecidas, con el fin de enriquecer el conocimiento legislativo actual de los delitos informáticos, con teorías actuales que influyan en la modificación de leyes de países donde el ciberdelito ha aumentado considerablemente; con ello, los ejecutivos judiciales podrán responder ante las amenazas de los ciberdelincuentes porque conocerán y percibirán el alcance de estos delitos.

Cuando hablamos de un diseño de investigación no experimental, se entiende como el análisis e interpretación de los medios de información antes mencionadas; como base del estudio, no se deben considerar variables, se manipulan los estudios y se analizan en su contexto natural. No se ha establecido un escenario de causa y efecto para evaluar su impacto. Los participantes, pertenecen a la unidad de análisis estudiada. Hernández et al. (2003), aclara que una investigación cuando es no experimental, se realiza sin manejo intencional de categorías. Es decir, es un estudio donde no se vulneran las variables independientes, solo se observa cambios o efectos tal como ocurren en su entorno para luego analizar.

Asimismo, el estudio presenta un enfoque **cualitativo**, recogiendo cada vez información que pueda probar la hipótesis planteada. En cuanto a Hernández (2003) manifiesta que: un trabajo cualitativo argumenta que las bases que sustentan la construcción del conocimiento, brindan pautas generales para planificar la investigación.

3.2 Categorías, Subcategorías y matriz de categorización

Se determinó las categorías y subcategorías empleadas en esta investigación, siendo la primera categoría: “La responsabilidad civil de las entidades financieras” y sus sub categorías son: “fundamentos de imputación” y “propuesta de incorporación” y la segunda categoría “fraude informático” y sus sub categorías son: “legislación nacional y comparada” y “métodos más frecuentes en el fraude informático”.

Según Straus y Corbin (2005) “La categorización radica en la en conceptos de nivel abstracto, las categorías asumen un poder conceptual debido a que poseen la capacidad de juntar grupos de conceptos o subcategorías.

Anexo 01: Matriz de Categorización
Fuente: Elaboración propia

3.3 Escenario de estudio

El principal escenario de esta investigación es la comisión de delitos informáticos de usuarios y la responsabilidad civil de las entidades financieras del distrito judicial y fiscal de Tacna, por lo que se solicita información fidedigna, ya que se iniciará un diálogo con especialistas de la materia en tiempo real, de igual manera, todos estos se sustentan en las afirmaciones realizadas, las cuales contribuyen al conocimiento del problema identificado en la investigación.

3.4 Participantes

Los participantes en esta investigación están supeditados a 07 especialistas que estén involucrados en casos de delitos informáticos, como la Policía Nacional del Perú, fiscales a cargo de investigación de delitos informáticos, agentes especializados de instituciones financieras que tienen experiencia en el seguimiento de delitos informáticos; de igual forma, se tomará como unidad de análisis las encuestas y entrevistas. El número de entrevistados

será de 03 efectivos policiales, 02 fiscales, y 2 agentes pertenecientes a entidades financieras.

3.5 Técnicas e instrumentos de recolección de datos

La **técnica** utilizada será la entrevista y análisis documental, la entrevista es un diálogo directo, serio y con un fin determinado, entre dos individuos (Benjamín, 1980), los **instrumentos** que se utilizarán: El cuestionario de entrevista y la guía del análisis de documentos, considerando las categorías, sub categorías, las unidades de análisis y el análisis e interpretación del fenómeno objeto de estudio, obteniendo los datos necesarios para la investigación

3.6 Procedimiento

El proceso de recolección se ejecutará considerando lo siguiente: En la entrevista se considerará un número reducido de personas, equilibrando los datos sin retroceder. Realizaremos entrevistas a 07 especialistas conocedores de la problemática, luego recogeremos los resultados de las entrevistas, analizaremos y realizaremos discusiones, conclusiones y recomendaciones sobre la temática.

Cada instrumento de documentación o análisis de documentos descrito incluirá sus respectivas categorías, subcategorías y análisis e interpretación. Según Hernández (2018), la información recopilada se traducirá en forma de tabulación de tablas y gráficos estadísticos, se discutirán los mismos, hasta arribar a las conclusiones y recomendaciones pertinentes.

3.7 Rigor científico

Los datos cualitativos que se obtendrán en la presente investigación serán de fuentes confiables y válidas, lo cual será validado por 3 especialistas en

la materia, quienes darán su conformidad, así también se someterá el instrumento de investigación a juicio de expertos.

Por consiguiente, para el uso de la misma se seguirán los métodos necesarios para lograr el resultado que se pretende.

3.8 Métodos de análisis de datos

Los métodos y técnicas relacionados a la investigación cualitativa será el método comparativo, al extraer información de distintas fuentes nacionales e internacionales, método hermenéutico jurídica, pues se explica el sentido concreto de la norma y por último el método inductivo requerido para la revisión de normas nacionales e internacionales.

3.9 Aspectos éticos

La presente investigación cumple con todos los principios éticos con la finalidad de realizar la misma con mayor calidad y probidad establecidas por la Universidad Cesar Vallejo, siendo responsables al momento de valorar la información de fuente no propia y haciendo las menciones correspondientes conforme dictan las normas APA última edición.

IV. RESULTADOS Y DISCUSIÓN

Resultados

Para el desarrollo del presente trabajo de investigación, se realizó a través del análisis documentario con el objetivo específico Nro. 01, que se refiere examinar la legislación comparada referida de la comisión del fraude informático a través del phishing.

También se llevó a cabo la recolección de la información en un cuestionario de entrevista con la finalidad de cumplir el objetivo Nro. 3, a los especialistas en la materia de investigación, siendo los entrevistados 1, 2 y 3 funcionarios trabajadores de las entidades financieras.

Con la finalidad de cumplir los objetivos Nros. 2 y 4, siendo los entrevistados el 4 y 5, dos efectivos policiales que laboran en la División de Investigación Criminal PNP Tacna y finalmente los entrevistados 6 y 7, son fiscales pertenecientes de la fiscalía Provincial Penal Corporativa de Tacna, todo esto con el propósito de dar cumplimiento y fortalecimiento a los objetivos específicos de la investigación, donde posteriormente se procederá con las siguientes tablas:

Con respecto al **objetivo específico N°01, se buscó examinar la legislación comparada derivada de la comisión del fraude informático a través del phishing.**

Tabla 1 **:** Legislación Comparada sobre Fraude Informático.

País	**Dispositivo jurídico**	**Fecha de emisión**	**Análisis del contenido**
Perú	Resolución SBS Nº 6523-2013 Art.23	Año 2013-	Son las entidades bancarias los responsables de demostrar, que cada operación realizada por el usuario sea legítimas y registradas, frente al reclamo del usuario tras una operación o transacción mal ejecutada.
España	Ley 16/2009 Art. 31 LSP	Año 2009	En caso se ejecute una operación no autorizada y se confirme, la entidad bancaria deberá restituir el importe económico afectado a la cuenta del usuario, tal y como estaba originalmente antes de haberse ejecutado la operación no autorizada.
Chile	Ley 21 234		La nueva legislación, atribuye la responsabilidad de un fraude al emisor, y permite legítimamente que el emisor pueda accionar contra quien sea el autor del delito, o ante la existencia de un dolo o culpa graves que hubiere facilitado la comisión del ilícito, pero también lo

			restringe, eficazmente, a la posible litigación temeraria, que dilate o impida la determinación de su responsabilidad, para con el usuario, ya que cada día que transcurre le significaría un incremento al monto a desembolsar por medio del máximo interés convencional del monto en cuestión, en caso de no lograr acreditar el dolo o culpa grave, con lo cual, el emisor deberá evaluar seriamente el accionar en contra del usuario, y de los medios de prueba que tenga para demostrar su pretensión, ya que la ley empodera al usuario, ante el gran desequilibrio e inequidad existente, que es que el emisor tiene dentro de su equipo a decenas de letrados para su defensa, por costos ya asociados a su operación, cosa que no ocurre con el usuario
Colombia	Sentencia SC18614	19-12-2016	Los bancos deberán responder y reparar económicamente por aquellas defraudaciones realizadas en las plataformas digitales, en perjuicio del usuario donde existe daños económicos, puesto que es un riesgo inherente a las actividades financieras.

INTERPRETACIÓN: De los resultados obtenidos se pudo determinar que en la legislación Peruana no es muy explícita en cuanto a la responsabilidad bancaria en delitos de fraudes informáticos se refiere, no hay un apartado claro en donde se especifique en qué casos las entidades bancarias tendrían responsabilidad en caso se suscite el delito de fraude informático, comparado con la legislación internacional, podemos apreciar que la legislación Española es la más clara, puesto que señala explícitamente que en caso de que se ejecute una operación de pago no autorizada, la entidad bancaria le devolverá de inmediato el importe de la operación al usuario víctima de este suceso, por su parte la legislación Chilena atribuye la responsabilidad de un fraude al emisor, y permite legítimamente que el emisor pueda accionar contra quien sea el autor del delito, finalmente la legislación de Colombia indica que las entidades financieras deben de reparar perjuicios producidos por fraudes electrónicos, la ley indica que las entidades financieras deben asumir la responsabilidad por la defraudación sufrida por sus usuarios a través de transacciones electrónicas y reparar los prejuicios sufridos por estos actos.

Fuente: Elaboración propia de los autores

Con respecto al **objetivo específico N°02, se buscó Identificar los fundamentos para imputar responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.**

De las entrevistas realizadas se llegó a los siguientes resultados

Tabla 2 : Opinión acerca del cumplimiento de los bancos en la comprobación de la legitimidad de las transacciones virtuales

Pregunta N°01: ¿Considera Ud. que los bancos no cumplen correctamente la comprobación de legitimidad para las transacciones virtuales? Justifique su respuesta.			
Especialista N°01	**Especialista N°02**	**Especialista N°03**	**Especialista N°04**
Si cumple, porque cada operación bancaria te envía un mensaje para verificar si está de acuerdo o no con dicha transacción.	Si, para la perpetración del delito informático conocido como phishing, los datos de acceso a una operación bancaria que han sido obtenidos ilegalmente (número de cuenta, nombre, contraseña, fecha o CCV), son los mismo que se requieren para una operación legal ya que el protocolo de las operaciones son espontáneos	Si, en razón que no se advierte un sistema de seguridad confiable que permita a los usuarios de las entidades financieras, poder acceder en forma segura a realizar diversas operaciones o transacciones virtuales, generando más bien el incremento de fraudes o hurtos informáticos.	Considero que ante el avance de la tecnología y la aparición de nuevas formas de criminalidad “ciberdelincuencia”, las entidades bancarias en general deben fortalecer sus mecanismos de seguridad, atendiendo como entidades del sistema financiero administran los fondos de sus clientes.

	y sin saber si son legales o ilegales, en todo caso se debiera incrementar otro tipo de requerimientos para estas operaciones virtuales, lo cual no es de conveniencia a la entidad bancaria ya que en todo momento buscan simplificar las operaciones y en la simplificación se encuentran los peligros utilizados por la cyber delincuencia	
Interpretación:	De los resultados obtenidos con respecto a la comprobación de legitimidad para las transacciones virtuales, se puede apreciar que los 03 primeros entrevistados coinciden que los bancos no cumplen correctamente con la comprobación de legitimidad para las transacciones virtuales, por su parte el entrevistado 04 menciona que las entidades bancarias en general deben fortalecer sus mecanismos de seguridad puesto que administran los fondos de sus clientes.	

Fuente: Entrevista a los especialistas.

Tabla 3 **:** Opinión acerca de la responsabilidad civil de los bancos frente a daños patrimoniales ocasionados por el fraude frente en sus diferentes modalidades

Pregunta N°02: ¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños patrimoniales, ocasionados por el fraude informático en sus diferentes modalidades? Explique.			
Especialista N°01	**Especialista N°02**	**Especialista N°03**	**Especialista N°04**
Si, ya que deberían hacerse cargo de los daños económicos como informáticos sustraídos a las entidades bancarias de la información bajo su cuidado.	Si, únicamente que los mecanismos jurídicos frente a la responsabilidad civil no están claros al respecto, la responsabilidad de las entidades bancarias frente a este delito es que siendo que los bancos reciben el dinero de las personas en calidad de DEPOSITOS, la salida de los activos sean físicos o de forma virtual, es responsabilidad del que posee el bien, en tal sentido los	Si, considero que, al carecer las entidades financieras de un sistema de seguridad confiable y seguro, permite que se ocasionen perjuicios económicos en sus usuarios, lo cual conlleva y genera una responsabilidad civil por parte de la entidad bancaria, más aún que como se advierte en la actualidad, estos delitos son realizados por personas especializadas en informática y tecnología, ante lo cual no existe	En la medida que las entidades bancarias no cuenten con una adecuada seguridad, ella podría generar una responsabilidad civil, dado que como administradores de los fondos de sus clientes deben adoptar las medidas necesarias para evitar el fraude informático.

	bancos deberían preocuparse más en asegurar las operaciones que en simplificarlas, así como implementar no solo la seguridad en las operaciones, sino en el uso de sus dominios ya que es de esa forma en la cual los ciber delincuentes obtienen ilegalmente los datos que utilizaran para las operaciones.	la información necesaria hacia los usuarios de las entidades financieras. .
Interpretación:	De los resultados obtenidos con respecto a la responsabilidad civil que tienen los bancos frente a los daños, se puede apreciar que los 03 primeros entrevistados refieren que los bancos si tendrían responsabilidad civil frente a los daños patrimoniales, siendo que el entrevistado 01 considera que el banco tendría que hacerse cargo de los daños económicos, el entrevistado 2 refiere que los mecanismos jurídicos frente a la responsabilidad civil no están claros al respecto, el entrevistado 3 refiere que sí tendría responsabilidad ya que carecen de un sistema de seguridad confiable y seguro permitiendo que ocasionen perjuicios económicos en sus usuarios, por último el entrevistado 4 menciona que en la medida que las entidades bancarias no cuenten con una adecuada seguridad, ella podría generar una responsabilidad civil.	

Fuente: Entrevista a los especialistas.

Tabla 4 **:** Opinión acerca de la responsabilidad civil de los bancos frente a los daños de naturaleza extra patrimoniales, en la afectación psicológica del agraviado, ocasionados por el fraude informático en sus diferentes modalidades.

Pregunta N°03: ¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños de naturaleza extra patrimoniales, como por ejemplo la afectación psicológica del agraviado, ocasionados por el fraude informático en sus diferentes modalidades? Explique.			
Especialista N°01	**Especialista N°02**	**Especialista N°03**	**Especialista N°04**
Si, deberían hacerse cargo de los gastos ocasionados por los clientes afectados por dichos fraudes.	Si, los daños ocasionados no solamente se centran en lo patrimonial, también afectan a la persona agraviada psicológicamente, incluso sin tener contacto con ellas, y en el caso del phishing los agraviados se ven afectados emocionalmente por la pérdida del dinero, ya que en un gran porcentaje saben que no volverán a recuperarlo, por otro lado el banco sin ser el	Si, también consideramos que si el problema se inicia por sistemas de las entidades financieras, inseguros, porque pueden ser clonados, copiados, a través de páginas web, correos electrónicos, llamadas telefónicas y mensajes de textos, con creaciones de links u otros, que permiten que los delincuentes hurten el patrimonio de los usuarios, ello en definitiva va afectar psicológicamente a los	Es posible que concurran daños extra patrimoniales, según cada caso en concreto en la medida que en las entidades financieras hayan actuado con dolo o culpa y se encuentren presente los demás elementos de la responsabilidad civil.

	autor de los hechos, por ser un delito informático viene siendo víctima al vulnerarse sus sistemas de seguridad, pero por su posición frente al patrimonio de las victimas debiera asumir responsabilidad al menos en lo civil.	agraviados; debiendo tener en cuenta que el en estos delitos, se realizan en su mayoría las sustracciones del total de fondos de las cuentas bancarias.
Interpretación:	De acuerdo con nuestros entrevistados todos concluyen que los bancos tendrían responsabilidad civil frente a los daños de naturaleza extra patrimoniales, el entrevistado 1 afirma que los bancos deberían asumir los gastos que esto acarrearía, por su parte el entrevistado 2 reconoce que los bancos también serían victimas del cyberdelito pero por su posición frente a estos delitos les correspondería asumir por lo menos responsabilidad civil, el entrevistado 3 por su parte, indica que en definitiva las víctimas de estos fraudes electrónicos, sufren daños psicológicos ya que en la mayoría de casos pierden todos sus fondos, por último el entrevistado 4 refiere que es posible que concurran daños extra patrimoniales, según cada caso en concreto en la medida que en las entidades financieras hayan actuado con dolo o culpa.	

Fuente: Entrevista al especialista

Tabla 5: Opinión acerca de la responsabilidad civil de los bancos cuando se utilizan sus canales digitales de atención para la comisión del fraude informático en sus diferentes modalidades.

Pregunta N°04: ¿Considera Ud. que los bancos tienen responsabilidad civil, cuando se utilizan sus canales digitales de atención para la comisión del fraude informático en sus diferentes modalidades? Explique.			
Especialista N°01	**Especialista N°02**	**Especialista N°03**	**Especialista N°04**
Si, ya que deberían cuidar celosamente dicha información que podría ser utilizada maliciosamente por algún delincuente informático.	Si, como explique en la respuesta número “1” la atención de las operaciones virtuales se hacen sin el conocimiento de que sean ilegales, ya que al tener los requisitos para la operación es factible llevarla a cabo, por otro lado las investigaciones no debieran centrarse en la operación sino en la obtención de los datos para la posterior perpetración de la operación ilegal, para lo cual la ciber	Si, en razón de que, si un usuario ingresa a través de un medio o canal digital de una entidad bancaria para realizar una transacción y operación financiera, lo realiza en la confianza de seguridad que debe tener este tipo de medio ofrecido por la entidad.	Debemos de partir que se genera responsabilidad civil, cuando concurren determinados aspectos, como el daño, la antijuricidad, el nexo causal, factor de atribución, de ahí que en la medida que las entidades bancarias no otorguen las debidas seguridades en la atención de sus canales digitales, según el caso concreto puede generar responsabilidad civil.

	delincuencia no utiliza las plataformas de los bancos, sino que construye plataformas virtuales similares o idénticas con el fin de que los usuarios ingresen sus datos y ellos poder utilizarlos en las plataformas verdaderas.	
Interpretación:	De acuerdo con nuestros entrevistados, los tres primeros concluyen que los bancos tendrían responsabilidad civil cuando se utiliza sus canales digitales de atención o plataformas bancarios, ya que los usuarios ingresarían de buena fe para realizar sus operaciones, mientras que el entrevistado 04 refiere que se genera responsabilidad civil, cuando concurren determinados aspectos, como el daño, la antijuricidad, el nexo causal, factor de atribución, de ahí que en la medida que las entidades bancarias no otorguen las debidas seguridades en la atención de sus canales digitales.	

Fuente: Entrevista a los especialistas

Tabla 6: Opinión acerca de la responsabilidad civil de los bancos, ante el daño causado por las operaciones no reconocidas de sus clientes, ocasionados por el fraude informático en sus diferentes modalidades.

Pregunta N°05: ¿Considera Ud. que los bancos tienen responsabilidad civil, cuando se utilizan sus canales digitales de atención para la comisión del fraude informático en sus diferentes modalidades? Explique.			
Especialista N°01	**Especialista N°02**	**Especialista N°03**	**Especialista N°04**
Si tienen responsabilidad y deberían hacerse cargo de las sustracciones del dinero de las cuentas de los clientes, así como de su información.	Sería muy arbitrario responsabilizar a la entidad bancaria por operaciones únicamente NO REONOCIDAS, las cuales debiera reunir una serie de requisitos para generar sospecha y determinar la ilegitimidad de la operación virtuales similares o idénticas con el fin de que los usuarios ingresen sus datos y ellos poder utilizarlos en las plataformas verdaderas.	Sí, siempre y cuando se haya llegado a determinar la manera en que los usuarios fueron víctimas de fraudes informáticos, y si es evidente que el usuario a pesar de aplicar un deber de cuidado de sus bienes, no pudo advertir el engaño o fraude en que fui inducido a incurrir.	En tanto, puede establecerse que las operaciones en efecto, no han sido realizadas por sus clientes, y en tanto aparezcan los elementos de la responsabilidad civil, daño, la antijuricidad, el nexo causal, factor de atribución.

Interpretación:	De acuerdo con nuestros entrevistados 01 y 03 concluyen que los bancos tienen responsabilidad civil, ante el daño causado por las operaciones no reconocidas de sus clientes, ocasionados por el delito de fraude informático en sus diferentes modalidades, por su parte el entrevistado 2 manifiesta que sería muy arbitrario responsabilizar al banco por estas operaciones no reconocidas, por último el entrevistado 04 refiere que en tanto si tendrían responsabilidad civil en tanto se demuestre que las operaciones no fueron realizadas por los clientes.

Fuente: Entrevista a los especialistas

Tabla 7 **:** Opinión de la ejecución eficiente de los bancos, en los estándares de idoneidad respecto a los métodos de seguridad para proteger las cuentas del usuario.

Pregunta N°06: ¿Considera usted que los bancos ejecutan eficientemente los estándares de idoneidad respecto a los métodos de seguridad para proteger las cuentas del usuario? Explique			
Especialista N°01	**Especialista N°02**	**Especialista N°03**	**Especialista N°04**
Sí, pero les falta mayor celo en el cuidado del dinero, así como de la información de los clientes, deberían tener lo último de seguridad informática en sus agencias.	No, en mi opinión, los bancos no están centrados en brindar seguridad en las operaciones, sino en simplificarlas, ya que por su naturaleza una operación bancaria suele verse como tediosa y complicada y las entidades bancarias quieren hacerlas más simples para que sean utilizadas por mayor cantidad de personas y es allí donde se aprovecha	No, ya como se ha señalado precedentemente, las estadísticas de criminalidad, llegan a determinar que los sistemas de seguridad utilizados por las entidades financieras, no son confiables, es decir son inseguras, conllevando al aumento de incidencia de los delitos informáticos.	Entiendo que cada banco tienen sus propios mecanismos de seguridad que, para poder arribar a referida conclusión, habría que tener conocimiento de los mismos; sin embargo, consideramos que esos mecanismos de seguridad deben ser eficaces y eficientes.

	para la perpetración de los diferentes delitos informáticos. Mi opinión es incrementar los medios de seguridad y no solo buscar su simplificación.	
Interpretación:	De acuerdo con nuestros entrevistados , el entrevistado 1 concluye que los bancos deberían de invertir en tecnología avanzada para la seguridad de los fondos de los usuarios, por su parte el entrevistado 2 y 3 concluyen que el banco no ejecutan eficientemente los estándares de idoneidad respecto a los métodos de seguridad para proteger las cuentas del usuario, el entrevistado 2 indica que los bancos se enfocarían más en la simplificación de sus transacciones más que en la seguridad de sus usuarios, por su parte el entrevistado 3 señala que según estadísticas y el incremento de fraudes informáticos , estos indicarían que los métodos no serían confiables, por último el entrevistado 04 refiere que esos mecanismos de seguridad deberían de ser eficaces y confiables.	

Fuente: Entrevista a los especialistas.

Con respecto al **objetivo específico N°03, se buscó determinar los métodos más frecuentes derivada de la comisión del fraude informático inmersos en las entidades financieras**.

Tabla 8 : Opinión respecto al phishing, como método frecuente del fraude informático.

Pregunta N°01: ¿Considera usted que el phishing es un método frecuente del fraude informático? Explique		
Trabajador bancario N°01	**Trabajador bancario N°02**	**Trabajador bancario N°03**
Sí, nuestros clientes reciben correos electrónicos falsos que los dirigen a una página web que simula ser del BCP donde los estafadores les solicitan "actualizar tus datos" donde buscan obtener sus claves secretas, número de tarjeta, fecha de vencimiento, código de seguridad y clave token. Nuestros clientes ingresan al enlace y llenan sus datos creyendo que es de nuestro banco y nosotros jamás pedimos esta información a través de un mail.	Sí, el phishing como tal es una de las modalidades más utilizadas en los últimos tiempos utilizando información confidencial, generando pérdidas económicas a los usuarios de diversas entidades financieras.	Sí, porque el estafador o delincuente hace que el cliente divulgue su información personal haciéndolo vulnerable; por ejemplo: número de tarjeta, clave, cvv2, fecha de caducidad del plástico, DNI. Información que se requiere para vaciar los fondos del cliente.

Interpretación:	De acuerdo con nuestros entrevistados trabajadores del banco, todos concluyen que efectivamente el phishing es un método frecuente de fraude informático, puesto que es de los más utilizados actualmente, el entrevistado 01 afirma que los clientes entran a enlaces falsos o a páginas que simulan ser del BCP , cuando ellos jamás solicitan este tipo de información, por otro lado el entrevistado 02 indica que es un método muy utilizado en los últimos tiempos, por último el entrevistado 03 menciona que los usuarios son vulnerables puesto que brindan información confidencial y los estafadores muchas veces logran vaciar los fondos del cliente.

Fuente: Entrevista a los trabajadores bancarios

Tabla 9 : Opinión respecto al pharming, como método frecuente del fraude informático.

Pregunta N°02: ¿Considera usted que el pharming es un método frecuente del fraude informático? Explique		
Trabajador bancario N°01	**Trabajador bancario N°02**	**Trabajador bancario N°03**
Sí, hoy en día he sabido de algunos casos en mi entidad financiera.	Sí, este método de delito desvía a los clientes a páginas fraudulentas generando así pérdidas económicas por la malversación de información, este delito de fraude informático viene operando día a día con mayor énfasis.	Sí, porque este fraude informático es a través de páginas fraudulentas las que no están autorizadas por los Bancos; siendo toda responsabilidad del tarjetahabiente por ingresar a páginas a través de buscadores.
Interpretación:	De acuerdo con nuestros entrevistados, el entrevistado 1 concluye que efectivamente se ha suscitado algunos casos de pharming en su agencia bancaria, mientras que el entrevistado 02 menciona que este método se viene dando día a día, generando pérdidas económicas a los usuarios, finalmente el entrevistado 03 refiere que si sería el pharming un método frecuentes llevadas a cabo mediante paginas falsas en donde considera que la responsabilidad es del tarjetahabiente.	

Fuente: Entrevista a los trabajadores bancarios

Tabla 10 : Opinión respecto al smishing, como método frecuente del fraude informático.

Pregunta N°03: ¿Considera usted que el smishing es un método frecuente del fraude informático? Explique		
Trabajador bancario N°01	**Trabajador bancario N°02**	**Trabajador bancario N°03**
Sí, los estafadores envían sms falsos a nuestros clientes haciéndose pasar por nosotros indicando que tienen transferencias retenidas o solicitando la actualización de datos inmediata para evitar el bloqueo de sus tarjetas. Nuestros clientes se alarman e ingresan rápidamente al enlace que está en esos sms, cayendo en esta modalidad de fraude.	Sí, ya que comúnmente recibimos publicidad o anuncios de las entidades financieras mediante los equipos móviles y con la practicidad de esto muchas veces optamos por acceder, siendo estas no siempre las legítimas emitidas por las entidades financieras.	Sí, es fraude a través de los dispositivos móviles donde el cliente de igual forma brinda toda su información vulnerando así sus datos personales para que puedan ingresar a sus cuentas.
Interpretación:	De acuerdo con nuestros entrevistados, el entrevistado 1 concluye que efectivamente se ha suscitado algunos casos de pharming en su agencia bancaria, mientras que el entrevistado 02 menciona que este método se viene dando día a día, generando pérdidas económicas a los usuarios, finalmente el entrevistado 03 refiere que si sería el pharming un método frecuentes llevadas a cabo mediante paginas falsas en donde considera que la responsabilidad es del tarjetahabiente.	

Fuente: Entrevista a los trabajadores bancarios

Tabla 11 : Opinión respecto a otros métodos, frecuentes para la comisión de fraude informático.

Pregunta N°04: ¿Qué otros métodos conocen Ud. que sean frecuentes para la comisión del fraude informático?		
Trabajador bancario N°01	**Trabajador bancario N°02**	**Trabajador bancario N°03**
El vishing, nuestros clientes reciben llamadas telefónicas de los estafadores haciéndose pasar por colaboradores de nuestro banco donde les solicitan datos confidenciales y ellos brindan esa información, es allí donde son víctimas de esta modalidad de fraude.	También son conocidos los fraudes por redes sociales, las instalaciones de software malintencionados y el vishing.	No, los que vemos constantemente en el Banco son los anteriormente mencionados.
Interpretación:	De acuerdo con nuestros entrevistados, el entrevistado 1 hace referencia al vishing, que se realiza mediante llamadas telefónicas a los usuarios, para acceder a sus claves, por consiguiente, acceder a sus cuentas bancarias, el entrevistado 02 por su parte indica que el vishing también es conocido como fraude realizado por redes sociales, por su parte el ultimo entrevistado señala que este método no es muy visto en su entidad bancaria, siendo más frecuentes el pharming y el smishing.	

Fuente: Entrevista a los trabajadores bancarios

Con respecto al **objetivo específico N°04, se buscó proponer alternativas de solución en beneficio de los usuarios de las entidades financieras inmersos en la comisión del fraude informático a través del phishing.**

Tabla 12 : Opinión respecto a la aplicación de políticas de responsabilidad que sancionen a los bancos por no otorgar la información y seguridad suficiente a sus usuarios frente a los riesgos existentes en la red.

Pregunta N°07: En su opinión ¿Se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la información y seguridad suficiente a sus usuarios frente a los riesgos existentes en la red?			
Especialista N°01	**Especialista N°02**	**Especialista N°03**	**Especialista N°04**
Sí, deben asumir el total de la sustracción del capital de las cuentas bajo cuidado de las agencias bancarias.	Sí, de hecho, la información respecto a una operación sospechosa o ilegal, es algo que los propios dueños de las cuentas no logran obtener de forma idónea y eso debe ser sancionado, asimismo el no brindar la seguridad al patrimonio de los usuarios es su	Sí, definitivamente, teniendo en cuenta el avance de la tecnología digital actual y la modernidad en el uso de los sistemas, aplicativos, app y otros, utilizados por las entidades financieras, estas entidades están en la obligación de brindar y proporcionar toda esta información a través entre otros	Sí, en la medida que los bancos prestan un servicio a sus clientes, están obligados a adoptar adecuados mecanismos de seguridad, máxime si en una relación de consumo quien presta un servicio debe realizarlo con idoneidad.

	responsabilidad.	de los medios de comunicación (televisión, radio, prensa escrita, redes sociales y otros), sin embargo, no se advierten estas políticas de información en forma idónea por parte de las entidades.
Interpretación:	De acuerdo con nuestros entrevistados todos concluyen que se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la información y seguridad suficiente a sus usuarios frente a los riesgos existentes en la red, el entrevisto 1 concluye que la entidad financiera debería asumir el total de la sustracción monetaria, por su parte el entrevistado 2 afirman que los bancos deberían recibir una sanción por no brindar la información adecuada a sus usuarios, el entrevistado 3 refiere que no se advierten políticas de información para los usuarios en el uso de sus plataformas digitales, finalmente el entrevistado 04 señala que en la medida que los bancos prestan un servicio a sus clientes, están obligados a adoptar adecuados mecanismos de seguridad.	

Fuente: Entrevista a los especialistas.

Tabla 13 **:** Opinión respecto a la consideración de un apartado dentro del contrato, referente a la responsabilidad que tendría la entidad bancaria frente a los fraudes informáticos.

Pregunta N°08: Considera Ud. ¿Que se debería establecer explícitamente dentro del contrato un apartado de la responsabilidad que tendría la entidad bancaria frente a los fraudes informáticos? Explique			
Especialista N°01	**Especialista N°02**	**Especialista N°03**	**Especialista N°04**
Sí, debería registrarse clausulas en los contratos de uso de las cuentas bancarias a favor de los clientes y que estas sean claras para que ellos tomen la decisión de poner su capital o no en dicha entidad bancaria.	Sí, debiera ser parte de todo contrato que un usuario acepta frente a una entidad bancaria para establecer correctamente los límites de la responsabilidad del usuario y la del banco frente al patrimonio y no únicamente ofrecer los famosos seguros anti robo, que al final el usuario viene pagando.	Sí, porque ello serviría para delimitar las responsabilidades de los usuarios y de las entidades financieras, en forma expresa.	Considero que si resultaría factible, sería necesario realizar una propuesta legislativa en ese sentido, para obligatoriedad de cláusulas específicas en los contratos bancarios; ello también generaría un mayor compromiso de las entidades financieras.

Interpretación:	De acuerdo con nuestros entrevistados todos concluyen que si se debería establecer explícitamente dentro del contrato un apartado de la responsabilidad que tendría la entidad bancaria frente a los delitos de fraude informático, donde el entrevistado 1 menciono que sería de suma importancia para que el usuario pueda elegir en que entidad bancaria depositara su dinero, por su parte el entrevistado 2 considero que sería de vital importancia para la seguridad de los usuarios y no solo se basen en seguros, por su parte el entrevistado 3 concluyo que sería necesario para delimitar responsabilidades de ambas partes, por último el entrevistado 04 considera que sería necesario presentar una propuesta legislativa para que sea obligatorio en los contratos bancarios.

Fuente: Entrevista a los especialistas.

Tabla 14 : Opinión respecto sobre la implementación de la seguridad de las transacciones virtuales mediante un reconocimiento facial o biométrico.

Pregunta N° 09: Considera Ud. ¿Qué se debería implementar la seguridad de las transacciones virtuales mediante un reconocimiento facial o biométrico? Explique			
Especialista N°01	**Especialista N°02**	**Especialista N°03**	**Especialista N°04**
Sí, eso sería lo ideal y de esta manera se evitaría los delitos de fraude informáticos, ya que existiría mayor control y habría mayor seguridad para el usuario.	Sí, mi punto en todas las respuestas ha sido incrementar los medios de seguridad y no simplificarlos, la incrementación del reconocimiento biométrico faciales y dactilares es algo que ya se utiliza en gran porcentaje de los teléfonos celulares de la población, por lo tanto, hacer de eso un paso más para realizar una operación sería útil y	Sí, porque son métodos de seguridad que deben adoptar las entidades financieras en beneficio y salvaguarda de sus usuarios; lo cual impediría las suplantaciones de identidad, y otras formas de fraude informático.	Es una alternativa, que puede ser utilizada, debemos tener presente que la tecnología en estos tiempos ha sido de gravital importancia para la realización de diferentes tramites de los ciudadanos, como de hacer diferentes transacciones civiles, comerciales, tributarias, etc.; en ese sentido, la utilización de la tecnología para fortalecer la seguridad de las transacciones bancarias, así como otras medidas que pueden tomarse

	reduciría la perpetración de gran parte de los delitos informáticos.	para dotar de mayor seguridad.
Interpretación:	De acuerdo con nuestros entrevistados todos concluyen que si se debería implementar el reconocimiento facial y biométrico para mayor seguridad en las transacciones virtuales, los tres coinciden en que esto reduciría los delitos de fraude informático, puesto que se evitaría las suplantaciones, finalmente el entrevistado 04 señala que la tecnología en estos tiempos es de vital importancia y es una alternativa que debería tenerse en cuenta.	

Fuente: Entrevista a los especialistas.

Discusión

En relación al objetivo general de la investigación cabe precisar que, el fin que la motivó fue determinar la responsabilidad civil de las entidades financieras frente al fraude informático – phishing. Ante ello, **Rodríguez y Chávez (2021)** coinciden en que las entidades bancarias deberán responder en su totalidad por las actividades fraudulentas realizadas por las plataformas digitales, ya que son los bancos los que indirectamente han puesto en peligro al usuario al no informar y prevenir sobre los riesgos informáticos que existen en la red.
Asimismo, **Tineo, Callirgos, Chávez (2021)** concordaron que a los bancos les corresponde restituir en forma total a los usuarios que fueron víctimas de fraudes informáticos, puesto que son los bancos los responsables de informar y prevenir sobre los riesgos existente en las plataformas digitales, la cual se alcanzó a través de los siguientes objetivos específicos:

En cuanto al ***primer objetivo específico***, concerniente a examinar la legislación comparada derivada de la comisión del fraude informático a través del phishing; en lo que respecta al análisis documental **(Véase Tabla 1),** de las normas de países tales como: España, Colombia, Chile y Perú; se observa que la legislación peruana no es muy explícita en cuanto a la responsabilidad bancaria en delitos de fraudes informáticos, comparado con las legislaciones internacionales. Tal es el caso de la legislación española, en donde se señala explícitamente que en caso de que se ejecute una operación de pago no autorizada, la entidad bancaria le devolverá de inmediato el importe de la operación al usuario que fue víctima de este suceso. Por su parte la legislación chilena, atribuye la responsabilidad de un fraude al emisor, y pueda accionar contra quien sea el autor del delito, finalmente la legislación de Colombia indica que las entidades financieras deben de reparar perjuicios producidos por fraudes electrónicos, por lo que podemos decir en conclusión que existe vacíos en las normas peruanas respecto al delito de fraude informático en relación a la responsabilidad civil de las entidades financieras. Con relación a lo anteriormente expuesto, se encontró un apoyo en lo

manifestado en la tesis de **Ananías (2020)**, la misma que concluyó que en España el Real Decreto-ley 19/2018, contiene similitudes con la normativa de otros países de la comunidad europea, donde conforme a su artículo 46 hace responsable al emisor de todas las operaciones no autorizadas por el tarjetahabiente, y lo obliga a restituir los montos defraudados al usuario.

Al respecto, el magistrado **Rodríguez y el abogado civilista Fernández (2021),** coincidieron en considerar que son las entidades financieras tienen responsabilidad civil objetiva, frente a los daños causados al usuario que han sido víctimas de actos fraudulentos a través del uso de las plataformas bancarias digitales, puesto que los usuarios confían en su entidad bancaria, por consecuencia les corresponde a los bancos resarcir los daños económicos afectados.

Con lo que respecta al ***segundo objetivo específico*** referida a Identificar los fundamentos para imputar responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing; en lo que respecta la entrevista realizada a los especialistas **(Véase Tabla 2, 3, 4. 5, 6 y 7)**, mediante la cual se puso en evidencia sobre el no cumplimiento de los bancos en la comprobación de la legitimidad de las transacciones virtuales, en razón que no se advierte un sistema de seguridad confiable que permita a los usuarios de las entidades financieras, de esta manera ocasionan daños patrimoniales, extra patrimoniales cuando se utilizan sus canales digitales, por las operaciones no reconocidas de sus clientes y de esta manera ejecutan deficientemente los estándares de idoneidad respecto a los métodos de seguridad para proteger las cuentas del usuario. Todo lo antes señalado constituye los fundamentos por los cuales se tendría que imputar a las entidades bancarias.

En acotación a ello, **Gastiaburu (2021)**, precisa que las entidades bancarias se deslindan de toda responsabilidad aludiendo que el usuario hace un mal manejo de las plataformas digitales, por consiguiente, se debe emplear

políticas de responsabilidad que protejan al usuario y sancionen a los bancos, por no brindar la seguridad financiera conveniente a sus usuarios.

En tanto, **Callirgos (2021)** manifestó que las entidades bancarias, al ser servidores públicos les corresponde cuidar al usuario de fraudes informáticos existentes en las plataformas digitales, en consecuencia, les corresponde a los bancos responder por este tipo de delitos de manera objetiva.

En cuanto al ***tercer objetivo específico*** referida a determinar los métodos más frecuentes derivada de la comisión del fraude informático inmersos en las entidades financieras; en lo que respecta la entrevista realizada a los trabajadores bancarios **(Véase Tabla 8, 9,10 y 11)**, mediante la cual se puso en evidencia que los métodos más frecuentes para cometer fraude informático son: phishing, pharming, y smishing, , siendo el phishing, el más usado por los ciberdelincuentes, el cual es a través de una página web, muy similar a la página de una entidad financiera, donde los estafadores les solicitan "actualizar los datos" de los usuarios y de esta manera logran obtener sus claves secretas, número de tarjeta, fecha de vencimiento, código de seguridad y clave token, los usuarios ingresan al enlace y llenan sus datos creyendo que es la entidad financiera correcta, todo esto se produce por la falta de información por parte del banco sobre el uso de la plataforma virtuales a sus clientes. Con relación a lo anteriormente expuesto, se encontró un apoyo en la tesis **Paredes (2021)**, donde evidencia que el phishing es el delito de fraude informático más usado por los cyberdelincuentes.

Asimismo, según **Zevallos (2020)**, es importante que la población conozca las modalidades de fraude informático a fin de que pueda evitar ser víctima de este tipo de ilícitos, dentro de estas están, el phishing, la clonación de tarjetas de crédito, el smishing, el vishing y el ransomware.

Con lo que respecta al ***cuarto objetivo específico*** referida a proponer alternativas de solución en beneficio de los usuarios de las entidades

financieras inmersos en la comisión del fraude informático a través del phishing; en lo que concierne en las entrevistas realizadas a los especialistas **(Véase Tabla 12, 13 y 14)**, mediante la cual se evidenció sobre la aplicación de políticas de responsabilidad que sancionen a los bancos por no otorgar la información y seguridad suficiente a los usuarios frente a los riesgos existentes en la red, con relación del apartado dentro del contrato, se busca clausulas a favor de los clientes y que estas sean claras para que ellos tomen la decisión de depositar su capital o no en dicha entidad bancaria, y respecto a la implementación de la seguridad de las transacciones virtuales mediante un reconocimiento facial o biométrico, infieren que serían sistemas de seguridad que los bancos deben de implementar un sus plataformas digitales para tener la asertividad que se trata del mismo usuario.

Asimismo, según **Salcedo (2010)**, otra serie de medidas protectoras ante ataques del phishing están ligadas a las legislaciones nacionales e internacionales que reglamentan el uso del internet, al instaurar leyes que contemplen multas y condenas a los delincuentes informáticos que se hacen pasar por entidades debidamente constituidas ante la ley, al establecer mecanismos legales que ayuden a confirmar la identidad de quien establece un sitio web, se aumentaría la complejidad para llevar a cabo un ataque de phishing.

De las discusiones antes señaladas, se ha logrado contrastar la **hipótesis** planteada al inicio de la presente investigación, en el sentido que: La responsabilidad civil de las entidades financieras, está referida a asumir la restitución del daño patrimonial de manera parcial o total, de los usuarios que fueron víctimas en la comisión del fraude informático a través del phishing, con la finalidad de que estos no estén desamparados, en razón que, las entidades financieras estarían asumiendo dicha responsabilidad, por ser tercero civil responsable.

V. CONCLUSIONES

PRIMERO

La responsabilidad civil de las entidades financieras, estaría a asumir la restitución del daño patrimonial de manera parcial o total, de sus usuarios (clientes), que fueron víctimas en la comisión del fraude informático a través del phishing, con la finalidad de que sus usuarios no estén desamparados, en razón que, las entidades financieras estarían asumiendo dicha responsabilidad, por ser tercero civil responsable.

SEGUNDO

Se logró examinar la legislación comparada derivada de la comisión del fraude informático a través del phishing, mediante la cual se pudo determinar que en la legislación peruana no es muy explícita en cuánto a la responsabilidad bancaria en los fraudes informáticos se refiere, no hay un apartado claro en donde se especifique en qué casos las entidades bancarias tendrían responsabilidad en caso se suscite el delito de fraude informático, comparado con la legislación internacional, se puede apreciar que la legislación Española es la más clara, puesto que señala explícitamente que en caso de que se ejecute una operación de pago no autorizada, la entidad bancaria le devolverá de inmediato el importe de la operación al usuario víctima de este suceso.

TERCERO

Los fundamentos para imputar responsabilidad civil a las entidades financieras ante la comisión de los fraudes informáticos a través del phishing, son: el daño patrimonial, el daño extra patrimonial y la omisión del deber de protección.

CUARTO

Los métodos más frecuentes en el fraude informático son: el phishing, el pharming y el smishing, siendo el phishing el más usado por los

cyberdelincuentes, pues es el más recurrente en las entidades financieras según lo manifiestan los trabajadores bancarios entrevistados.

QUINTO

Se propone como alternativa de solución, en beneficio de los usuarios de las entidades financieras, el uso de reconocimiento facial y biométrico para garantizar efectivamente la seguridad de los usuarios que utilizan dichas plataformas digitales.

VI. RECOMENDACIONES

PRIMERO

El estado debe de velar por el interés del usuario, pero no siempre se cumple, por tal motivo se recomienda que el poder legislativo incorpore un nuevo artículo en la ley, donde se detalle la responsabilidad de las entidades bancarias cuando se presente un escenario ilícito al acceder a las plataformas digitales bancarias, puesto que el usuario hace uso de estas por necesidad y lamentablemente sin un asesoramiento por parte del servidor público y muchas veces el usuario esta desinformado de los riesgos existentes en estas plataformas virtuales.

SEGUNDO

Las entidades bancarias deberían de crear aplicaciones que te alerten de donde provienen los mensajes y llamadas extrañas, así también, se brinde información oportuna sobre los riesgos que existen en las plataformas digitales para que los usuarios puedan tener la prevención adecuada.

TERCERO

Las entidades financieras deben incluir dentro de su protocolo de seguridad, que sus agentes bancarios otorguen información oportuna y precisa, en el momento que el usuario adquiere alguno de sus productos, para informar y prevenir sobre los riesgos existentes en sus plataformas digitales.

VII. PROPUESTA

Para poder prevenir el fraude informático a través del phishing se propone, mediante un proyecto de ley, que las entidades financieras incluyan en el procedimiento de la seguridad de las transacciones bancarias virtuales, el uso de reconocimiento facial y biométrico en sus plataformas digitales, con la finalidad de comprobar la identidad de sus usuarios, y garantizar la seguridad de sus transacciones virtuales, de esta forma se reduciría los fraudes informáticos.

REFERENCIAS

Abanto R (2020). *La Clonación de tarjetas de crédito y la responsabilidad civil de la entidad financiera los olivos año 2020*. [Tesis de Pregrado, Universidad Privada del Norte]. Recuperado de: https://repositorio.upn.edu.pe/handle/11537/25054

Aboso, G.E. y Zapata, M. F. (2006). *Cibercriminalidad y Derecho Penal.* Julio César Faira Editor. Buenos Aires. Buenos Aires. Editorial IB de f. de Montevideo

Arbulu, V. (2002). *Delitos informáticos, contratación electrónica, protección jurídica de programas informáticos*. Editorial: CEPREDIM – UNMSM. Lima - Perú.

Barrios, Moisés A. (2017). *Ciberdelitos Amenazas Criminales del Ciberespacio*. Madrid, editorial: REUS.

Bustamante, J. (1993). *Teoría General de la Responsabilidad Civil*. Buenos aires: Abeledo Perrot. Código civil. (2012). Jurisprudencia civil. Lima: Grijley.

Barbier, E. A. (2002). *Consumidores y usuarios - Contratación Bancaria. II Edic.* Buenos Aires, Argentina: Editorial Astrea.

Belaunde, G., Fuentes, F. A., Bermúdez, M. A. (2007). *Diccionario Jurídico*. Lima, Perú: Editorial San Marcos.

Campos, J. A. (2016). *La responsabilidad civil de los bancos por la indebida gestión de sus riesgos en la operación económica de compra financiada de un inmueble en planos*. [Tesis de Magíster Derecho Civil, Pontificia Universidad Católica del Perú]. Lima – Perú. Recuperado de: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/9212/Campos_Berm%c3%badez_Responsabilidad_civil_bancos.pdf?sequence=1&isAllowed=y

Chaparro, M. F. (2014). *Legislación informática y protección de datos en Colombia, comparada con otros países.* INVENTUM, 9(17), 32-37.

Código civil. (2012). *Jurisprudencia civil.* Lima, editorial: Grijley.

De la Puente y Lavalle, J. (2001). *El contrato general, comentarios a la sección primera del libro VII del código civil*. Lima, editorial: Palestra Editores.

Hernández, R.; Fernández, C. y Baptista, P. (2003). *Metodología de la investigación.* 3ra Edición. México. 265-270 pp. Editorial: Mc Graw Hill Educación.

Hernández, R.; Fernández, C. y Baptista, P. (2014). *Metodología de la investigación.* Editorial: Mc Graw Hill Education. Recuperado de: https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Fernández, L., Cabezudo, J., Arenas, M., Herrera, R., & Gastelu, J. (2010). *Diseño de herramientas de control y medidas de prevención para evitar ser víctimas de Delitos Informáticos*. Perú: Policía Nacional del Perú. Recuperado de: http://www.buenastareas.com/ensayos/Dise%C3%B1o-De-Herramientas-De-Control-Inform%C3%A1tico/1245461.html

León, L. (2016). *Responsabilidad civil contractual y extracontractual.* Lima - Perú, editorial: Academia de la Magistratura

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. Editorial: Universidad FASTA.

Leysser, L. (2004). *La responsabilidad civil. Líneas fundamentales y nuevas perspectivas.* Lima, editorial: Normas legales.

Martínez, M. P. (2015). *La responsabilidad bancaria frente a los delitos informáticos.* [Tesis de maestría Derecho Financiero, Bursátil y de Seguros, Universidad Andina Simón Bolívar]. Quito - Ecuador: Recuperado de: http://hdl.handle.net/10644/4506

Núñez Ávila, R. F. (2013). *Fraude al sistema financiero y a sus clientes*. (Tesis de Licenciatura), Quito, Ecuador.

Noreña, A., Alcaraz-Moreno, N., Rojas, J., & Rebolledo-Malpica, D. (2012). *Aplicabilidad de los criterios de rigor y éticos en la investigación cualitativa.* 263-274 pp. Editorial: Aquichan,

Organización para la Cooperación y el Desarrollo Económico [OCDE] (2014), *Recomendación del Consejo de la OCDE relativa a la Cooperación Internacional en el marco de investigaciones y procedimientos en materia de competencia*. Aprobada por el Consejo el 16.9.2014, México.

OAS. (2019). Convenio sobre la Ciberdelincuencia. Tratados europeos Nº185. Budapest, 23.XI.2001. Recuperado de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Rodríguez, F. (2013). *Derecho informático. El derecho en la era digital. La sociedad de información y el sistema jurídico.* Contratos informáticos. Protección jurídica de los programas de computación. Delitos informáticos. La tutela jurídica del sistema informático. UNC y FCEFyN.

Rodríguez, M. (2015). *Responsabilidad bancaria frente al phishing*. [Tesis de Maestría en Derecho, Universidad Nacional de Colombia]. Bogotá - Colombia: Recuperado de: https://repositorio.unal.edu.co/bitstream/handle/unal/57088/marcosrodriguezpuentes.2015.pdf?sequence=1&isAllowed=y

Salas, D. (2010). *Responsabilidad civil bancaria frente al cliente por delitos informáticos.* [Tesis licenciatura en derecho. Universidad de Costa Rica]. San José de Costa Rica. Recuperado de: http://repositorio.sibdi.ucr.ac.cr:8080/jspui/bitstream/123456789/4492/1/31126.pdf

Tamayo y Tamayo (2005), *El proceso de la Investigación Científica*, México, Cuarta Edición. Editorial: Limusa

Tenorio, J. y Tuesta, M. (2012). *Legislación del secreto bancario y su relación con el delito de hurto informático de dinero mediante la violación de claves secretas, Iquitos- 2010*. [Tesis de Maestría, Universidad Nacional de la Amazonía Peruana]. Iquitos- Perú. Recuperado de: https://repositorio.unapiquitos.edu.pe/handle/20.500.12737/2193

Taboada, L. (2013). *Elementos de la responsabilidad civil.* Lima. Editora jurídica grijley.

Villavicencio, F. (2014). *Delitos informáticos*. Articulo Universidad Nacional Mayor de san Marcos. 24(49), 284-304. Editorial: Ius Et Veritas, Recuperado de: https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

ANEXOS

Anexo Nº01. Matriz de categorización

ÁMBITO TEMÁTICO	PROBLEMA DE INVESTIGACIÓN	PREGUNTAS DE INVESTIGACIÓN	OBJETIVO GENERAL	OBJETIVOS ESPECIFICOS	CATEGORÍAS	SUBCATEGORÍAS
Responsabilidad Civil de las entidades financiaras	La responsabilidad civil de las entidades financieras ¿Cuál es la responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing?	¿Cuál es la responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing?	Determinar la responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.	Examinar la legislación comparada derivada de la comisión del fraude informático a través del phishing	La responsabilidad Civil de las entidades financiaras	- Propuesta de incorporación
				Identificar los fundamentos para imputar responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing		- Fundamentos de imputación.
				Determinar los métodos más frecuentes derivada de la comisión del fraude informático inmersos en las entidades financieras.	Fraude informático	- Fraude informático más frecuentes
				Proponer alternativas de solución en beneficio de los usuarios de las entidades financieras inmersos en la comisión del fraude informático a través del phishing		- Propuestas

ANEXO 02

VALIDACIÓN DE INSTRUMENTO

CARTA DE INVITACIÓN N°01

Trujillo, 05 de marzo del 2022

Dra. Zevallos Loyaga María Eugenia

Asunto: **Participación en juicio de expertos para validar instrumento de investigación cualitativa**

Me es grato dirigirme a Ud., para expresarle mi respeto y cordial saludo; respecto al asunto hacerle conocer que estoy realizando el trabajo de investigación cualitativo titulado: **LA RESPONSABILIDAD CIVIL DE LAS ENTIDADES FINANCIERAS DERIVADA DE LA COMISIÓN DEL FRAUDE INFORMÁTICO A TRAVÉS DEL PHISHING.**

Con el fin de obtener el título profesional de Abogado.

La presente investigación tiene por finalidad investigar si la conformación de la mayoría de un grupo político en el congreso afecta este poder del estado, por lo que se deben realizar entrevistas cuyas preguntas conforman el instrumento de evaluación de investigación cualitativa, que deben ser validadas por expertos, como lo es en el caso de su persona, por lo que **lo invitamos a colaborar con nuestra investigación, validando en calidad de experto dicho instrumento de evaluación.**

Seguras de su participación en calidad de experto para la validación del instrumento de evaluación mencionado, se le alcanza dicho instrumento motivo de evaluación con el formato que servirá para que usted pueda hacerme llegar sus apreciaciones para cada ítem del instrumento de investigación

Conocedoras de su alto espíritu altruista, agradezco por adelantado su colaboración.

Atentamente:

Br. COARITE ESPINOZA Betsabe Celeste
DNI. N° 46482035

Br. RAMOS FLORES, Daniel A.
DNI. N°43063318

VALIDEZ DE TEST: JUICIO DE EXPERTOS

INSTRUCTIVO PARA LOS TRABAJADORES DEL BANCO

Indicación: Señor especialista se le pide su colaboración para que luego de un riguroso análisis de los ítems del **Cuestionario de Entrevista**, el mismo que le mostramos a continuación, indique de acuerdo con su criterio y su experiencia profesional el puntaje de acuerdo a si la pregunta permite capturar las variables de investigación del trabajo.

En la evaluación de cada ítem, utilice la siguiente escala:

RANGO	SIGNIFICADO
1	**Descriptor no adecuado y debe ser eliminado**
2	**Descriptor adecuado, pero debe ser modificado**
3	**Descriptor adecuado**

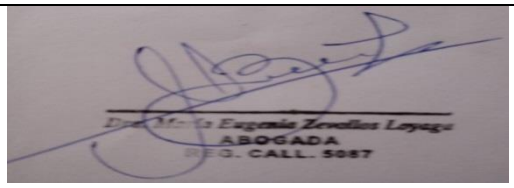
Los rangos de la escala propuesta deben ser utilizados teniendo en consideración los siguientes criterios:

- Vocabulario adecuado al nivel académico de los entrevistados.
- Claridad en la redacción.
- Consistencia Lógica y Metodológica.

Recomendaciones:

……
……
……

Gracias, por su generosa colaboración

Apellidos y nombres	ZEVALLOS LOYAGA MARÍA EUGENIA
Grado Académico	DOCTORA
Mención	DERECHO
Firma	

ÍTEM	CALIFICACIÓN DEL JUEZ			OBSERVACIÓN
	1	2	3	
1. ¿Considera usted que el phishing es un método frecuente del fraude informático? explique			X	
2. ¿Considera usted que el pharming es un método frecuente del fraude informático? explique			X	
3. ¿Considera usted que el smishing es un método frecuente del fraude informático? explique			X	
4. ¿Qué otros métodos conoce usted que sean frecuentes para la comisión del fraude informático? explique			x	

ANEXO 3

ENTREVISTA

TÍTULO: LA RESPONSABILIDAD CIVIL DE LAS ENTIDADES FINANCIERAS DERIVADA DE LA COMISION DEL FRAUDE INFORMATICO A TRAVES DEL PHISHING.

DATOS GENERALES DEL ENTREVISTADO (A):

FECHA: ..... HORA: …….....

LUGAR: .....

ENTREVISTADORES:.....

ENTREVISTADO: .....

PUESTO: .....

INSTRUCCIONES:

Leer detenidamente cada interrogante de la presente entrevista y responder desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

OBJETIVO ESPECíFICO 3: Determinar los métodos más frecuentes derivada de la comisión del fraude informático inmersos en las entidades financieras.

MATRIZ DE CATEGORIZACIÓN DE ENTREVISTA				
CATEGORÍA	**SUB CATEGORIA**	**INDICADORES**	**ÍTEMS**	**INSTRUMENTO**
Fraude informático	Métodos más frecuentes	Phishing	¿Considera usted que el phishing es un método frecuente del fraude informático? explique	Guía de entrevista
		Pharming	¿Considera usted que el pharming es un método frecuente del fraude informático? explique	
		Smishing	¿Considera usted que el smishing es un método frecuente del fraude informático? explique	
		Otros métodos	¿Qué otros métodos conoce ud. que sean frecuentes para la comisión del fraude informático?	

ANEXO 4

Entrevista

Título: LA RESPONSABILIDAD CIVIL DE LAS ENTIDADES FINANCIERAS DERIVADA DE LA COMISIÓN DEL FRAUDE INFORMÁTICO A TRAVÉS DEL PHISHING.

I. Datos generales de los investigadores entrevistado (a):

Fecha: ..... Hora: .....

Lugar: .....

Entrevistadores: .....

Entrevistado: ….....

Edad: ..... Género: .....

Puesto: .....

II. Instrucciones:

Leer detenidamente cada interrogante de la presente entrevista y responda desde su experiencia, conocimiento, opinión con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para corroborar nuestros objetivos.

OBJETIVO ESPECIFICO 3:

Determinar los métodos más frecuentes derivada de la comisión del fraude informático inmersos en las entidades financieras.

1. **¿ Considera usted que el phishing es un método frecuente del fraude informático? explique**

   _____

   _____

   _____

   _____

2. **¿ Considera usted que el pharming es un método frecuente del fraude informático? explique**

   _____

   _____

   _____

   _____

3. **¿Considera usted que el smishing es un método frecuente del fraude informático? explique**

_____
_____
_____
_____

4. **¿Qué otros métodos conoce usted que sean frecuentes para la comisión del fraude informático?**

_____
_____
_____
_____

ANEXO 05

VALIDACIÓN DE INSTRUMENTO

CARTA DE INVITACIÓN N°01

Trujillo, de 05 marzo del 2022

Dra. Zevallos Loyaga María Eugenia

Asunto: **Participación en juicio de expertos para validar instrumento de investigación cualitativa**

Me es grato dirigirme a Ud., para expresarle mi respeto y cordial saludo; respecto al asunto hacerle conocer que estoy realizando el trabajo de investigación cualitativo titulado: **LA RESPONSABILIDAD CIVIL DE LAS ENTIDADES FINANCIERAS DERIVADA DE LA COMISIÓN DEL FRAUDE INFORMÁTICO A TRAVÉS DEL PHISHING.**

Con el fin de obtener el título profesional de Abogado.

La presente investigación tiene por finalidad investigar si la conformación de la mayoría de un grupo político en el congreso afecta este poder del estado, por lo que se deben realizar entrevistas cuyas preguntas conforman el instrumento de evaluación de investigación cualitativa, que deben ser validadas por expertos, como lo es en el caso de su persona, por lo que **lo invitamos a colaborar con nuestra investigación, validando en calidad de experto dicho instrumento de evaluación.**

Seguras de su participación en calidad de experto para la validación del instrumento de evaluación mencionado, se le alcanza dicho instrumento motivo de evaluación con el formato que servirá para que usted pueda hacerme llegar sus apreciaciones para cada ítem del instrumento de investigación

Conocedoras de su alto espíritu altruista, agradezco por adelantado su colaboración.

Atentamente:

Br. COARITE ESPINOZA Betsabe Celeste
DNI. N° 46482035

Br. RAMOS FLORES, Daniel A.
DNI. N°43063318

VALIDEZ DE TEST: JUICIO DE EXPERTOS

INSTRUCTIVO PARA LOS JUECES Y ABOGADOS

Indicación: Señor especialista se le pide su colaboración para que luego de un riguroso análisis de los ítems del **Cuestionario de Entrevista**, el mismo que le mostramos a continuación, indique de acuerdo con su criterio y su experiencia profesional el puntaje de acuerdo a si la pregunta permite capturar las variables de investigación del trabajo.

En la evaluación de cada ítem, utilice la siguiente escala:

RANGO	SIGNIFICADO
1	**Descriptor no adecuado y debe ser eliminado**
2	**Descriptor adecuado, pero debe ser modificado**
3	**Descriptor adecuado**

Los rangos de la escala propuesta deben ser utilizados teniendo en consideración los siguientes criterios:

- Vocabulario adecuado al nivel académico de los entrevistados.
- Claridad en la redacción.
- Consistencia Lógica y Metodológica.

Recomendaciones:
……
……
……

Gracias, por su generosa colaboración

Apellidos y nombres	Zevallos Loyaga, María Eugenia
Grado Académico	DOCTORA
Mención	DERECHO
Firma	

ÍTEM	CALIFICACIÓN DEL JUEZ			OBSERVACIÓN
	1	2	4	
1. ¿Considera Ud. que los bancos no cumplen correctamente la comprobación de legitimidad para las transacciones virtuales? Justifique su respuesta.			X	
2. ¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños patrimoniales, ocasionados por el fraude informático en sus diferentes modalidades? Explique.			X	
3. ¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños de naturaleza extra patrimoniales, como por ejemplo la afectación psicológica del agraviado, ocasionados por el fraude informático en sus diferentes modalidades? Explique.			X	
4. ¿Considera Ud. que los bancos tienen responsabilidad civil, cuando se utilizan sus canales digitales de atención para la comisión del fraude informático en sus diferentes modalidades? Explique.			X	
5. ¿Considera Ud. que los bancos tienen responsabilidad civil, ante el daño causado por las operaciones no reconocidas de sus clientes, ocasionados por el fraude informático en sus diferentes modalidades? Explique.			X	
6. ¿Considera usted que los bancos ejecutan eficientemente los estándares de idoneidad respecto a los métodos de seguridad para proteger las cuentas del usuario? Explique			X	
7. En su opinión ¿Se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la información y seguridad suficiente a sus usuarios frente a los riesgos existentes en la red? ¿Por qué?			X	
8. Considera Ud. ¿Que se debería establecer explícitamente dentro del contrato un apartado de la responsabilidad que tendría la entidad bancaria frente al fraude informático? Explique			X	
9. Considera Ud. ¿Qué se debería implementar la seguridad de las transacciones virtuales mediante un reconocimiento facial o biométrico? Explique			X	

ANEXO 06

ENTREVISTA

TíTULO: LA RESPONSABILIDAD CIVIL DE LAS ENTIDADES FINANCIERAS DERIVADA DE LA COMISION DEL FRAUDE INFORMATICO A TRAVÉS DEL PHISHING.

DATOS GENERALES DEL ENTREVISTADO (A):

FECHA: ..... HORA: …….....

LUGAR: .....

ENTREVISTADORES:.....

ENTREVISTADO: .....

PUESTO: .....

INSTRUCCIONES:

Leer detenidamente cada interrogante de la presente entrevista y responder desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

OBJETIVO ESPECíFICO 2: Identificar los fundamentos para imputar responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

CATEGORÍA	SUB CATEGORIA	INDICADORES	ÍTEMS	INSTRUMENTO
La responsabilidad civil de las entidades financieras	Fundamentos de imputación	legitimidad	¿Considera Ud. que los bancos no cumplen correctamente la comprobación de legitimidad para las transacciones virtuales? Justifique su respuesta.	Guía de entrevista
		Daño patrimonial	¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños patrimoniales, ocasionados por el fraude informático en sus diferentes modalidades? Explique.	
		Daño extra patrimonial	¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños de naturaleza extra patrimoniales, como por ejemplo la afectación psicológica del agraviado, ocasionados por el fraude informático en sus diferentes modalidades? Explique.	

		Canales de atención	¿Considera Ud. que los bancos tienen responsabilidad civil, cuando se utilizan sus canales digitales de atención para la comisión del fraude informático en sus diferentes modalidades? Explique.	
		Operaciones no reconocidas	¿Considera Ud. que los bancos tienen responsabilidad civil, ante el daño causado por las operaciones no reconocidas de sus clientes, ocasionados por el fraude informático en sus diferentes modalidades? Explique.	
		Omisión de deber de protección	¿Considera usted que los bancos ejecutan eficientemente los estándares de idoneidad respecto a los métodos de seguridad para proteger las cuentas del usuario? Explique	

OBJETIVO ESPECíFICO 4: Proponer alternativas de solución en beneficio de los usuarios de las entidades financieras inmersos en la comisión del fraude informático a través del phishing.

MATRIZ DE CATEGORIZACIÓN DE ENTREVISTA				
CATEGORÍA	**SUB CATEGORÍA**	**INDICADORES**	**ÍTEMS**	**INSTRUMENTO**
Fraude informático	Propuesta	Políticas de responsabilidad	En su opinión ¿Se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la información y seguridad suficiente a sus usuarios frente a los riesgos existentes en la red? ¿Por qué?	Guía de entrevista
		Alternativas de solución	Considera Ud. ¿Que se debería establecer explícitamente dentro del contrato un apartado de la responsabilidad que tendría la entidad bancaria frente al fraude informático? Explique	
		Reconocimiento facial o biométrico	Considera Ud. ¿Qué se debería implementar la seguridad de las transacciones virtuales mediante un reconocimiento facial o biométrico? explique	

ANEXO 07

Entrevista

Título: La responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

I. Datos generales de los investigadores entrevistado (a):

Fecha: ..... Hora: .....

Lugar: .....

Entrevistadores: .....

Entrevistado: ….....

Edad: ..... Género: .....

Puesto: .....

II. Instrucciones:

Leer detenidamente cada interrogante de la presente entrevista y responda desde su experiencia, conocimiento, opinión con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para corroborar nuestros objetivos.

OBJETIVO ESPECíFICO 2:

Identificar los fundamentos para imputar responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

1. **¿Considera Ud. que los bancos no cumplen correctamente la comprobación de legitimidad para las transacciones virtuales? Justifique su respuesta.**

   _____

   _____

   _____

   _____

2. **¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños patrimoniales, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**

   _____

   _____

   _____

   _____

3. **¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños de naturaleza extra patrimoniales, como por ejemplo la afectación psicológica del agraviado, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**

_____

_____

_____

_____

4. **¿Considera Ud. que los bancos tienen responsabilidad civil, cuando se utilizan sus canales digitales de atención para la comisión del fraude informático en sus diferentes modalidades? Explique.**

_____

_____

_____

_____

5. **¿Considera Ud. que los bancos tienen responsabilidad civil, ante el daño causado por las operaciones no reconocidas de sus clientes, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**

_____

_____

_____

_____

6. **¿Considera usted que los bancos ejecutan eficientemente los estándares de idoneidad respecto a los métodos de seguridad para proteger las cuentas del usuario? Explique**

_____

_____

_____

_____

OBJETIVO ESPECíFICO 4:

Proponer alternativas de solución en beneficio de los usuarios de las entidades financieras inmersos en la comisión del fraude informático a través del phishing.

7. **En su opinión ¿Se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la información y seguridad suficiente a sus usuarios frente a los riesgos existentes en la red?**

   _____
   _____
   _____
   _____

8. **Considera Ud. ¿Que se debería establecer explícitamente dentro del contrato un apartado de la responsabilidad que tendría la entidad bancaria frente a la comisión del fraude informático? Explique**

   _____
   _____
   _____
   _____

9. **Considera Ud. ¿Qué se debería implementar la seguridad de las transacciones virtuales mediante un reconocimiento facial o biométrico? explique**

   _____
   _____
   _____
   _____

ANEXO 08

VALIDACIÓN DE INSTRUMENTO

CARTA DE INVITACIÓN N°01

Trujillo, 05 de marzo del 2022

Dr. Henry Eduardo Salinas Ruíz

Asunto: **Participación en juicio de expertos para validar instrumento de investigación cualitativa**

Me es grato dirigirme a Ud., para expresarle mi respeto y cordial saludo; respecto al asunto hacerle conocer que estoy realizando el trabajo de investigación cualitativo titulado: **LA RESPONSABILIDAD CIVIL DE LAS ENTIDADES FINANCIERAS DERIVADA DE LA COMISIÓN DEL FRAUDE INFORMÁTICO A TRAVÉS DEL PHISHING.**

Con el fin de obtener el título profesional de Abogado.

La presente investigación tiene por finalidad investigar si la conformación de la mayoría de un grupo político en el congreso afecta este poder del estado, por lo que se deben realizar entrevistas cuyas preguntas conforman el instrumento de evaluación de investigación cualitativa, que deben ser validadas por expertos, como lo es en el caso de su persona, por lo que **lo invitamos a colaborar con nuestra investigación, validando en calidad de experto dicho instrumento de evaluación.**

Seguras de su participación en calidad de experto para la validación del instrumento de evaluación mencionado, se le alcanza dicho instrumento motivo de evaluación con el formato que servirá para que usted pueda hacerme llegar sus apreciaciones para cada ítem del instrumento de investigación

Conocedoras de su alto espíritu altruista, agradezco por adelantado su colaboración.

Atentamente:

Br. COARITE ESPINOZA Betsabe Celeste
DNI. N° 46482035

Br. RAMOS FLORES, Daniel A.
DNI. N°43063318

VALIDEZ DE TEST: JUICIO DE EXPERTOS

INSTRUCTIVO PARA LOS TRABAJADORES DEL BANCO

Indicación: Señor especialista se le pide su colaboración para que luego de un riguroso análisis de los ítems del **Cuestionario de Entrevista**, el mismo que le mostramos a continuación, indique de acuerdo con su criterio y su experiencia profesional el puntaje de acuerdo a si la pregunta permite capturar las variables de investigación del trabajo.

En la evaluación de cada ítem, utilice la siguiente escala:

RANGO	SIGNIFICADO
1	**Descriptor no adecuado y debe ser eliminado**
2	**Descriptor adecuado, pero debe ser modificado**
3	**Descriptor adecuado**

Los rangos de la escala propuesta deben ser utilizados teniendo en consideración los siguientes criterios:

- Vocabulario adecuado al nivel académico de los entrevistados.
- Claridad en la redacción.
- Consistencia Lógica y Metodológica.

Recomendaciones:

……
……
……

Gracias, por su generosa colaboración

Apellidos y nombres	Salinas Ruiz Henry Eduardo
Grado Académico	Doctor
Mención	Gestión Pública y Gobernabilidad
Firma	

ÍTEM	CALIFICACIÓN DEL JUEZ			OBSERVACIÓN
	1	**2**	III.	
1. ¿Considera usted que el phishing es un método frecuente del fraude informático? Explique su respuesta.			X	
2. ¿Considera usted que el pharming es un método frecuente del fraude informático? Explique su respuesta.			X	
3. ¿Considera usted que el smishing es un método frecuente del fraude informático? Explique su respuesta.			X	
4. ¿Qué otros métodos conoce Ud. que sean frecuentes para la comisión del fraude informático? Explique su respuesta.			X	

ANEXO 09

ENTREVISTA

TíTULO: LA RESPONSABILIDAD CIVIL DE LAS ENTIDADES FINANCIERAS DERIVADA DE LA COMISIóN DEL FRAUDE INFORMATICO A TRAVÉS DEL PHISHING.

DATOS GENERALES DEL ENTREVISTADO (A):

FECHA: ..... HORA: …….....

LUGAR: .....

ENTREVISTADORES:.....

ENTREVISTADO: .....

PUESTO: .....

INSTRUCCIONES:

Leer detenidamente cada interrogante de la presente entrevista y responder desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

OBJETIVO ESPECíFICO 3: Determinar los métodos más frecuentes derivada de la comisión del fraude informático inmersos en las entidades financieras.

MATRIZ DE CATEGORIZACIÓN DE ENTREVISTA				
CATEGORÍA	**SUB CATEGORIA**	**INDICADORES**	**ÍTEMS**	**INSTRUMENTO**
Fraude informático	Métodos más frecuentes	Phishing	¿Considera usted que el phishing es un método frecuente del fraude informático? explique	Guía de entrevista
		Pharming	¿Considera usted que el pharming es un método frecuente del fraude informático? explique	
		Smishing	¿Considera usted que el smishing es un método frecuente del fraude informático? explique	
		Otros métodos	¿Qué otros métodos conoce usted que sean frecuentes para la comisión del fraude informático?	

ANEXO 10

Entrevista

Título: LA RESPONSABILIDAD CIVIL DE LAS ENTIDADES FINANCIERAS DERIVADA DE LA COMISION DEL FRAUDE INFORMATICO A TRAVÉS DEL PHISHING.

I. Datos generales de los investigadores entrevistado (a):

Fecha: ..... Hora: .....

Lugar: .....

Entrevistadores: .....

Entrevistado: ….....

Edad: ..... Género: .....

Puesto: .....

II. Instrucciones:

Leer detenidamente cada interrogante de la presente entrevista y responda desde su experiencia, conocimiento, opinión con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para corroborar nuestros objetivos.

OBJETIVO ESPECIFICO 3:

Determinar los métodos más frecuentes derivada de la comisión del fraude informático inmersos en las entidades financieras.

1. **¿Considera usted que el phishing es un método frecuente del fraude informático? explique**

   _____

   _____

   _____

   _____

2. **¿Considera usted que el pharming es un método frecuente del fraude informático? explique**

   _____

   _____

_____

_____

3. **¿Considera usted que el smishing es un método frecuente del fraude informático? explique**

_____

_____

_____

_____

4. **¿Qué otros métodos conocen Ud. que sean frecuentes para la comisión del fraude informático?**

_____

_____

_____

_____

ANEXO 11

VALIDACIÓN DE INSTRUMENTO

CARTA DE INVITACIÓN N°01

Trujillo, de 05 marzo del 2022

Dr. Henry Eduardo Salinas Ruíz

Asunto: **Participación en juicio de expertos para validar instrumento de investigación cualitativa**

Me es grato dirigirme a Ud., para expresarle mi respeto y cordial saludo; respecto al asunto hacerle conocer que estoy realizando el trabajo de investigación cualitativo titulado: **LA RESPONSABILIDAD CIVIL DE LAS ENTIDADES FINANCIERAS DERIVADA DE LA COMISION DEL FRAUDE INFORMATICO A TRAVÉS DEL PHISHING.**

Con el fin de obtener el título profesional de Abogado.

La presente investigación tiene por finalidad investigar si la conformación de la mayoría de un grupo político en el congreso afecta este poder del estado, por lo que se deben realizar entrevistas cuyas preguntas conforman el instrumento de evaluación de investigación cualitativa, que deben ser validadas por expertos, como lo es en el caso de su persona, por lo que **lo invitamos a colaborar con nuestra investigación, validando en calidad de experto dicho instrumento de evaluación.**

Seguras de su participación en calidad de experto para la validación del instrumento de evaluación mencionado, se le alcanza dicho instrumento motivo de evaluación con el formato que servirá para que usted pueda hacerme llegar sus apreciaciones para cada ítem del instrumento de investigación

Conocedoras de su alto espíritu altruista, agradezco por adelantado su colaboración.

Atentamente:

Br. COARITE ESPINOZA Betsabe Celeste	Br. RAMOS FLORES, Daniel Andrés
DNI. N° 46482035	DNI. N°43063318

VALIDEZ DE TEST: JUICIO DE EXPERTOS

INSTRUCTIVO PARA LOS JUECES Y ABOGADOS

Indicación: Señor especialista se le pide su colaboración para que luego de un riguroso análisis de los ítems del **Cuestionario de Entrevista**, el mismo que le mostramos a continuación, indique de acuerdo con su criterio y su experiencia profesional el puntaje de acuerdo a si la pregunta permite capturar las variables de investigación del trabajo.

En la evaluación de cada ítem, utilice la siguiente escala:

RANGO	SIGNIFICADO
1	**Descriptor no adecuado y debe ser eliminado**
2	**Descriptor adecuado, pero debe ser modificado**
3	**Descriptor adecuado**

Los rangos de la escala propuesta deben ser utilizados teniendo en consideración los siguientes criterios:

- Vocabulario adecuado al nivel académico de los entrevistados.
- Claridad en la redacción.
- Consistencia Lógica y Metodológica.

Recomendaciones:

……
……
……

Gracias, por su generosa colaboración

Apellidos y nombres	Salinas Ruiz Henry Eduardo
Grado Académico	Doctor
Mención	Gestión Pública y Gobernabilidad
Firma	

ÍTEM	CALIFICACIÓN DEL JUEZ			OBSERVACIÓN
	1	2	3	
1. ¿Considera Ud. que los bancos no cumplen correctamente la comprobación de legitimidad para las transacciones virtuales? Explique su respuesta.			X	
2. ¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños patrimoniales, ocasionados por el fraude informático en sus diferentes modalidades? Explique su respuesta.			X	
3. ¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños de naturaleza extra patrimoniales, como por ejemplo la afectación psicológica del agraviado, ocasionados por el fraude informático en sus diferentes modalidades? Explique su respuesta.			X	
4. ¿Considera Ud. que los bancos tienen responsabilidad civil, cuando se utilizan sus canales digitales de atención para la comisión del fraude informático en sus diferentes modalidades? Explique su respuesta.			X	
5. ¿Considera Ud. que los bancos tienen responsabilidad civil, ante el daño causado por las operaciones no reconocidas de sus clientes, ocasionados por el delito de fraude informático en sus diferentes modalidades? Explique su respuesta.			X	
6. ¿Considera usted que los bancos ejecutan eficientemente los estándares de idoneidad respecto a los métodos de seguridad para proteger las cuentas del usuario? Explique su respuesta.			X	
7. En su opinión ¿Se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la información y seguridad suficiente a sus usuarios frente a los riesgos existentes en la red? Explique su respuesta.			X	
8. Considera Ud. ¿Que se debería establecer explícitamente dentro del contrato un apartado de la responsabilidad que tendría la entidad bancaria frente a la comisión de fraude informático? Explique su respuesta.			X	
9. Considera Ud. ¿Qué se debería implementar la seguridad de las transacciones virtuales mediante un reconocimiento facial o biométrico? Explique su respuesta.			X	

ANEXO 12

ENTREVISTA

TíTULO: LA RESPONSABILIDAD CIVIL DE LAS ENTIDADES FINANCIERAS DERIVADA DE LA COMISION DEL FRAUDE INFORMATICO A TRAVÉS DEL PHISHING.

DATOS GENERALES DEL ENTREVISTADO (A):

FECHA: ..... HORA: …….....

LUGAR: .....

ENTREVISTADORES:.....

ENTREVISTADO: .....

PUESTO: .....

INSTRUCCIONES:

Leer detenidamente cada interrogante de la presente entrevista y responder desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

OBJETIVO ESPECíFICO 2: Identificar los fundamentos para imputar responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

CATEGORÍA	SUB CATEGORIA	INDICADORES	ÍTEMS	INSTRUMENTO
La responsabilidad civil de las entidades financieras	Fundamentos de imputación	legitimidad	¿Considera Ud. que los bancos no cumplen correctamente la comprobación de legitimidad para las transacciones virtuales? Justifique su respuesta.	Guía de entrevista
		Daño patrimonial	¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños patrimoniales, ocasionados por el fraude informático en sus diferentes modalidades? Explique.	
		Daño extra patrimonial	¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños de naturaleza extra patrimoniales, como por ejemplo la afectación psicológica del agraviado, ocasionados por el fraude informático en sus diferentes modalidades? Explique.	

		Canales de atención	¿Considera Ud. que los bancos tienen responsabilidad civil, cuando se utilizan sus canales digitales de atención para la comisión del fraude informático en sus diferentes modalidades? Explique.	
		Operaciones no reconocidas	¿Considera Ud. que los bancos tienen responsabilidad civil, ante el daño causado por las operaciones no reconocidas de sus clientes, ocasionados por el fraude informático en sus diferentes modalidades? Explique.	
		Omisión de deber de protección	¿Considera usted que los bancos ejecutan eficientemente los estándares de idoneidad respecto a los métodos de seguridad para proteger las cuentas del usuario? Explique	

OBJETIVO ESPECíFICO 4: Proponer alternativas de solución en beneficio de los usuarios de las entidades financieras inmersos en la comisión del fraude informático a través del phishing.

MATRIZ DE CATEGORIZACIÓN DE ENTREVISTA				
CATEGORÍA	**SUB CATEGORÍA**	**INDICADORES**	**ÍTEMS**	**INSTRUMENTO**
Fraude informático	Propuesta	Políticas de responsabilidad	En su opinión ¿Se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la información y seguridad suficiente a sus usuarios frente a los riesgos existentes en la red? ¿Por qué?	Guía de entrevista
		Alternativas de solución	Considera Ud. ¿Que se debería establecer explícitamente dentro del contrato un apartado de la responsabilidad que tendría la entidad bancaria frente a la comisión del fraude informático? Explique	
		Reconocimiento facial o biométrico	Considera Ud. ¿Qué se debería implementar la seguridad de las transacciones virtuales mediante un reconocimiento facial o biométrico? explique	

ANEXO 13

Entrevista

Título: LA RESPONSABILIDAD CIVIL DE LAS ENTIDADES FINANCIERAS DERIVADA DE LA COMISION DEL FRAUDE INFORMATICO A TRAVÉS DEL PHISHING.

I. Datos generales de los investigadores entrevistado (a):

Fecha: ..... Hora: .....

Lugar: .....

Entrevistadores: .....

Entrevistado: …..

Edad: ..... Género: .....

Puesto: .....

II. Instrucciones:

Leer detenidamente cada interrogante de la presente entrevista y responda desde su experiencia, conocimiento, opinión con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para corroborar nuestros objetivos.

OBJETIVO ESPECIFICO 2:

Identificar los fundamentos para imputar responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

1. **¿Considera Ud. que los bancos no cumplen correctamente la comprobación de legitimidad para las transacciones virtuales? Justifique su respuesta.**

   _____

   _____

   _____

   _____

2. **¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños patrimoniales, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**

   _____

   _____

   _____

3. **¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños de naturaleza extra patrimoniales, como por ejemplo la afectación psicológica del agraviado, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**

4. **¿Considera Ud. que los bancos tienen responsabilidad civil, cuando se utilizan sus canales digitales de atención para la comisión del fraude informático en sus diferentes modalidades? Explique.**

5. **¿Considera Ud. que los bancos tienen responsabilidad civil, ante el daño causado por las operaciones no reconocidas de sus clientes, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**

6. **¿Considera usted que los bancos ejecutan eficientemente los estándares de idoneidad respecto a los métodos de seguridad para proteger las cuentas del usuario? Explique**

OBJETIVO ESPECIFICO 4:

Proponer alternativas de solución en beneficio de los usuarios de las entidades financieras inmersos en la comisión del fraude informático a través del phishing.

7. **En su opinión ¿Se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la información y seguridad suficiente a sus usuarios frente a los riesgos existentes en la red?**

   _____
   _____
   _____
   _____

8. **Considera Ud. ¿Que se debería establecer explícitamente dentro del contrato un apartado de la responsabilidad que tendría la entidad bancaria frente al fraude informático? Explique**

   _____
   _____
   _____
   _____

9. **Considera Ud. ¿Qué se debería implementar la seguridad de las transacciones virtuales mediante un reconocimiento facial o biométrico? explique**

   _____
   _____
   _____
   _____

ANEXO 14

VALIDACIÓN DE INSTRUMENTO

CARTA DE INVITACIÓN N°01

Tacna, 07 de marzo del 2022

Dr. Edgar Damián Choque

Asunto: **Participación en juicio de expertos para validar instrumento de investigación cualitativa**

Me es grato dirigirme a Ud., para expresarle mi respeto y cordial saludo; respecto al asunto hacerle conocer que estoy realizando el trabajo de investigación cualitativo titulado: **LA RESPONSABILIDAD CIVIL DE LAS ENTIDADES FINANCIERAS DERIVADA DE LA COMISIÓN DEL FRAUDE INFORMÁTICO A TRAVÉS DEL PHISHING.**

Con el fin de obtener el título profesional de Abogado.

La presente investigación tiene por finalidad investigar si la conformación de la mayoría de un grupo político en el congreso afecta este poder del estado, por lo que se deben realizar entrevistas cuyas preguntas conforman el instrumento de evaluación de investigación cualitativa, que deben ser validadas por expertos, como lo es en el caso de su persona, por lo que **lo invitamos a colaborar con nuestra investigación, validando en calidad de experto dicho instrumento de evaluación.**

Seguras de su participación en calidad de experto para la validación del instrumento de evaluación mencionado, se le alcanza dicho instrumento motivo de evaluación con el formato que servirá para que usted pueda hacerme llegar sus apreciaciones para cada ítem del instrumento de investigación

Conocedoras de su alto espíritu altruista, agradezco por adelantado su colaboración.

Atentamente:

Br. COARITE ESPINOZA Betsabe Celeste
DNI. N° 46482035

Br. RAMOS FLORES, Daniel A.
DNI. N°43063318

VALIDEZ DE TEST: JUICIO DE EXPERTOS

INSTRUCTIVO PARA LOS TRABAJADORES DEL BANCO

Indicación: Señor especialista se le pide su colaboración para que luego de un riguroso análisis de los ítems del **Cuestionario de Entrevista**, el mismo que le mostramos a continuación, indique de acuerdo con su criterio y su experiencia profesional el puntaje de acuerdo a si la pregunta permite capturar las variables de investigación del trabajo.

En la evaluación de cada ítem, utilice la siguiente escala:

RANGO	SIGNIFICADO
1	**Descriptor no adecuado y debe ser eliminado**
2	**Descriptor adecuado, pero debe ser modificado**
3	**Descriptor adecuado**

Los rangos de la escala propuesta deben ser utilizados teniendo en consideración los siguientes criterios:

- Vocabulario adecuado al nivel académico de los entrevistados.
- Claridad en la redacción.
- Consistencia Lógica y Metodológica.

Recomendaciones:
……
……
……

Gracias, por su generosa colaboración

Apellidos y nombres	Damián Choque, Edgar
Grado Académico	Maestro en Derecho Penal
Mención	Derecho
Firma	

ÍTEM	CALIFICACIÓN DEL JUEZ			OBSERVACIÓN
	1	2	10.	
1. ¿Considera usted que el phishing es un método frecuente del fraude informático? Explique su respuesta.			X	
2. ¿Considera usted que el pharming es un método frecuente del fraude informático? Explique su respuesta.			X	
3. ¿Considera usted que el smishing es un método frecuente del fraude informático? Explique su respuesta.			X	
4. ¿Qué otros métodos conoce Ud. que sean frecuentes para la comisión del de fraude informático? Explique su respuesta.			X	

ANEXO 15

ENTREVISTA

TITULO: LA RESPONSABILIDAD CIVIL DE LAS ENTIDADES FINANCIERAS DERIVADA DE LA COMISION DEL FRAUDE INFORMATICO A TRAVÉS DEL PHISHING.

DATOS GENERALES DEL ENTREVISTADO (A):

FECHA: ..... HORA: …….....

LUGAR: .....

ENTREVISTADORES:.....

ENTREVISTADO: .....

PUESTO: .....

INSTRUCCIONES:

Leer detenidamente cada interrogante de la presente entrevista y responder desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

OBJETIVO ESPECIFICO 3: Determinar los métodos más frecuentes derivada de la comisión del fraude informático inmersos en las entidades financieras.

MATRIZ DE CATEGORIZACIÓN DE ENTREVISTA				
CATEGORÍA	**SUB CATEGORIA**	**INDICADORES**	**ÍTEMS**	**INSTRUMENTO**
Fraude informático	Métodos más frecuentes	Phishing	¿Considera usted que el phishing es un método frecuente del fraude informático? explique	Guía de entrevista
		Pharming	¿Considera usted que el pharming es un método frecuente del fraude informático? explique	
		Smishing	¿Considera usted que el smishing es un método frecuente del fraude informático? explique	
		Otros métodos	¿Qué otros métodos conoce usted que sean frecuentes para la comisión del fraude informático?	

ANEXO 16

Entrevista

Título: LA RESPONSABILIDAD CIVIL DE LAS ENTIDADES FINANCIERAS DERIVADA DE LA COMISIÓN DEL FRAUDE INFORMÁTICO A TRAVÉS DEL PHISHING.

I. Datos generales de los investigadores entrevistado (a):

Fecha: ..... Hora: .....

Lugar: .....

Entrevistadores: .....

Entrevistado: ….....

Edad: ..... Género: .....….

Puesto: .....

II. Instrucciones:

Leer detenidamente cada interrogante de la presente entrevista y responda desde su experiencia, conocimiento, opinión con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para corroborar nuestros objetivos.

OBJETIVO ESPECIFICO 3:

Determinar los métodos más frecuentes derivada de la comisión del fraude informático inmersos en las entidades financieras.

1. **¿Considera usted que el phishing es un método frecuente del fraude informático? explique**

   _____
   _____
   _____
   _____

2. **¿Considera usted que el pharming es un método frecuente del delito de fraude informático? explique**

   _____
   _____
   _____
   _____

3. **¿Considera usted que el smishing es un método frecuente del fraude informático? explique**

   _____
   _____
   _____
   _____

4. **¿Qué otros métodos conocen usted que sean frecuentes para la comisión del fraude informático?**

   _____
   _____
   _____
   _____

ANEXO 17

VALIDACIÓN DE INSTRUMENTO

CARTA DE INVITACIÓN N°01

Tacna, de 07 marzo del 2022

Dra. Edgar Damián Choque

Asunto: **Participación en juicio de expertos para validar instrumento de investigación cualitativa**

Me es grato dirigirme a Ud., para expresarle mi respeto y cordial saludo; respecto al asunto hacerle conocer que estoy realizando el trabajo de investigación cualitativo titulado: **LA RESPONSABILIDAD CIVIL DE LAS ENTIDADES FINANCIERAS DERIVADA DE LA COMISIÓN DEL FRAUDE INFORMÁTICO A TRAVÉS DEL PHISHING.**

Con el fin de obtener el título profesional de Abogado.

La presente investigación tiene por finalidad investigar si la conformación de la mayoría de un grupo político en el congreso afecta este poder del estado, por lo que se deben realizar entrevistas cuyas preguntas conforman el instrumento de evaluación de investigación cualitativa, que deben ser validadas por expertos, como lo es en el caso de su persona, por lo que **lo invitamos a colaborar con nuestra investigación, validando en calidad de experto dicho instrumento de evaluación.**

Seguras de su participación en calidad de experto para la validación del instrumento de evaluación mencionado, se le alcanza dicho instrumento motivo de evaluación con el formato que servirá para que usted pueda hacerme llegar sus apreciaciones para cada ítem del instrumento de investigación

Conocedoras de su alto espíritu altruista, agradezco por adelantado su colaboración.

Atentamente:

Br. COARITE ESPINOZA Betsabe Celeste
DNI. N° 46482035

Br. RAMOS FLORES, Daniel A.
DNI. N°43063318

VALIDEZ DE TEST: JUICIO DE EXPERTOS

INSTRUCTIVO PARA LOS JUECES Y ABOGADOS

Indicación: Señor especialista se le pide su colaboración para que luego de un riguroso análisis de los ítems del **Cuestionario de Entrevista**, el mismo que le mostramos a continuación, indique de acuerdo con su criterio y su experiencia profesional el puntaje de acuerdo a si la pregunta permite capturar las variables de investigación del trabajo.

En la evaluación de cada ítem, utilice la siguiente escala:

RANGO	SIGNIFICADO
1	**Descriptor no adecuado y debe ser eliminado**
2	**Descriptor adecuado, pero debe ser modificado**
3	**Descriptor adecuado**

Los rangos de la escala propuesta deben ser utilizados teniendo en consideración los siguientes criterios:

- Vocabulario adecuado al nivel académico de los entrevistados.
- Claridad en la redacción.
- Consistencia Lógica y Metodológica.

Recomendaciones:

……
……
……

Gracias, por su generosa colaboración

Apellidos y nombres	Damián Choque, Edgar
Grado Académico	Maestro en Derecho Penal
Mención	Derecho
Firma	

ÍTEM		CALIFICACIÓN DEL JUEZ			OBSERVACIÓN
		1	2	III.	
1.	¿Considera Ud. que los bancos no cumplen correctamente la comprobación de legitimidad para las transacciones virtuales? Justifique su respuesta.			X	
2.	¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños patrimoniales, ocasionados por el fraude informático en sus diferentes modalidades? Explique.			X	
3.	¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños de naturaleza extra patrimoniales, como por ejemplo la afectación psicológica del agraviado, ocasionados por el fraude informático en sus diferentes modalidades? Explique.			X	
4.	¿Considera Ud. que los bancos tienen responsabilidad civil, cuando se utilizan sus canales digitales de atención para la comisión del fraude informático en sus diferentes modalidades? Explique.			X	
5.	¿Considera Ud. que los bancos tienen responsabilidad civil, ante el daño causado por las operaciones no reconocidas de sus clientes, ocasionados por el fraude informático en sus diferentes modalidades? Explique.			X	
6.	¿Considera usted que los bancos ejecutan eficientemente los estándares de idoneidad respecto a los métodos de seguridad para proteger las cuentas del usuario? Explique			X	
7.	En su opinión ¿Se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la información y seguridad suficiente a sus usuarios frente a los riesgos existentes en la red? ¿Por qué?			X	
8.	Considera Ud. ¿Que se debería establecer explícitamente dentro del contrato un apartado de la responsabilidad que tendría la entidad bancaria frente a los fraudes informáticos? Explique			X	
9.	Considera Ud. ¿Qué se debería implementar la seguridad de las transacciones virtuales mediante un reconocimiento facial o biométrico? Explique			X	

ANEXO 18

ENTREVISTA

TITULO: LA RESPONSABILIDAD CIVIL DE LAS ENTIDADES FINANCIERAS DERIVADA DE LA COMISION DEL FRAUDE INFORMATICO A TRAVÉS DEL PHISHING.

DATOS GENERALES DEL ENTREVISTADO (A):

FECHA: ..... HORA: …….....

LUGAR: .....

ENTREVISTADORES:.....

ENTREVISTADO: .....

PUESTO: .....

INSTRUCCIONES:

Leer detenidamente cada interrogante de la presente entrevista y responder desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

OBJETIVO ESPECIFICO 2: Identificar los fundamentos para imputar responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

CATEGORÍA	SUB CATEGORIA	INDICADORES	ÍTEMS	INSTRUMENTO
La responsabilidad civil de las entidades financieras	Fundamentos de imputación	legitimidad	¿Considera Ud. que los bancos no cumplen correctamente la comprobación de legitimidad para las transacciones virtuales? Justifique su respuesta.	Guía de entrevista
		Daño patrimonial	¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños patrimoniales, ocasionados por el fraude informático en sus diferentes modalidades? Explique.	
		Daño extra patrimonial	¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños de naturaleza extra patrimoniales, como por ejemplo la afectación psicológica del agraviado, ocasionados por el fraude informático en sus diferentes modalidades? Explique.	

		Canales de atención	¿Considera Ud. que los bancos tienen responsabilidad civil, cuando se utilizan sus canales digitales de atención para la comisión del fraude informático en sus diferentes modalidades? Explique.	
		Operaciones no reconocidas	¿Considera Ud. que los bancos tienen responsabilidad civil, ante el daño causado por las operaciones no reconocidas de sus clientes, ocasionados por el fraude informático en sus diferentes modalidades? Explique.	
		Omisión de deber de protección	¿Considera usted que los bancos ejecutan eficientemente los estándares de idoneidad respecto a los métodos de seguridad para proteger las cuentas del usuario? Explique	

OBJETIVO ESPECIFICO 4: Proponer alternativas de solución en beneficio de los usuarios de las entidades financieras inmersos en la comisión del fraude informático a través del phishing.

MATRIZ DE CATEGORIZACIÓN DE ENTREVISTA				
CATEGORÍA	SUB CATEGORÍA	INDICADORES	ÍTEMS	INSTRUMENTO
Fraude informático	Propuesta	Políticas de responsabilidad	En su opinión ¿Se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la información y seguridad suficiente a sus usuarios frente a los riesgos existentes en la red? ¿Por qué?	Guía de entrevista
		Alternativas de solución	Considera Ud. ¿Que se debería establecer explícitamente dentro del contrato un apartado de la responsabilidad que tendría la entidad bancaria frente a los fraudes informáticos? Explique	
		Reconocimiento facial o biométrico	Considera Ud. ¿Qué se debería implementar la seguridad de las transacciones virtuales mediante un reconocimiento facial o biométrico? explique	

ANEXO 19

Entrevista

Título: La responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

I. Datos generales de los investigadores entrevistado (a):

Fecha: ..... Hora: .....

Lugar: .....

Entrevistadores: .....

Entrevistado: …..

Edad: ..... Género: .....

Puesto: .....

II. Instrucciones:

Leer detenidamente cada interrogante de la presente entrevista y responda desde su experiencia, conocimiento, opinión con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para corroborar nuestros objetivos.

OBJETIVO ESPECIFICO 2:

Identificar los fundamentos para imputar responsabilidad civil de las entidades financieras ante la comisión del fraude informático a través del phishing.

1. **¿Considera Ud. que los bancos no cumplen correctamente la comprobación de legitimidad para las transacciones virtuales? Justifique su respuesta.**

   _____

   _____

   _____

   _____

2. **¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños patrimoniales, ocasionados por el fraude informático en sus diferentes modalidades? Explique**.

   _____

   _____

   _____

3. **¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños de naturaleza extra patrimoniales, como por ejemplo la afectación psicológica del agraviado, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**

4. **¿Considera Ud. que los bancos tienen responsabilidad civil, cuando se utilizan sus canales digitales de atención para la comisión del fraude informático en sus diferentes modalidades? Explique.**

5. **¿Considera Ud. que los bancos tienen responsabilidad civil, ante el daño causado por las operaciones no reconocidas de sus clientes, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**

6. **¿Considera usted que los bancos ejecutan eficientemente los estándares de idoneidad respecto a los métodos de seguridad para proteger las cuentas del usuario? Explique**

OBJETIVO ESPECIFICO 4:

Proponer alternativas de solución en beneficio de los usuarios de las entidades financieras inmersos en la comisión del fraude informático a través del phishing.

7. **En su opinión ¿Se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la información y seguridad suficiente a sus usuarios frente a los riesgos existentes en la red?**

   _____
   _____
   _____
   _____

8. **Considera Ud. ¿Que se debería establecer explícitamente dentro del contrato un apartado de la responsabilidad que tendría la entidad bancaria frente a los fraudes informáticos? explique**

   _____
   _____
   _____
   _____

9. **Considera Ud. ¿Qué se debería implementar la seguridad de las transacciones virtuales mediante un reconocimiento facial o biométrico? explique**

   _____
   _____
   _____
   _____

ANEXO 20

GUIA DE ANALISIS DE FUENTE DOCUMENTAL

Título de la investigación: La responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

Guía de análisis de fuente documental

Objetivo:

Legislación comparada	País	Fuente	Análisis del contenido
Nacional	Perú		
Internacional	España		
	Colombia		
	Chile		

ANEXO 21: Encuesta desarrollada por los especialistas (policías, fiscal, Juez y trabajadores del banco)

ENTREVISTA 01

Título: La responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

I. Datos generales de los investigadores entrevistado (a):

Fecha: 19MAR2022 **Hora:** 09:00

Lugar: Central Operativa de Investigación Criminal PNP Tacna

Entrevistadores: - Br. COARITE ESPONIZA, Betsabe Celeste
- Br. RAMOS FLORES, Daniel Andrés

Entrevistado: Superior PNP Oscar RODRIGUEZ URRUTIA

Edad: 50 años **Género:** Masculino

Puesto: Jefe de la OIDCLS-DEPINCRI-DIVINCRI-PNP-TACNA

II. Instrucciones:

Leer detenidamente cada interrogante de la presente entrevista y responda desde su experiencia, conocimiento, opinión con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para corroborar nuestros objetivos.

OBJETIVO ESPECIFICO 2:

Identificar los fundamentos para imputar responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

1. **¿Considera Ud. que los bancos no cumplen correctamente la comprobación de legitimidad para las transacciones virtuales? Justifique su respuesta.**

   Si cumple, porque cada operación bancaria te envía un mensaje para verificar si está de acuerdo o no con dicha transacción.

2. **¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños patrimoniales, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**

   Si, ya que deberían hacerse cargo de los daños económicos como informáticos sustraídos a las entidades bancarias de la información bajo su cuidado.

3. **¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños de naturaleza extra patrimoniales, como por ejemplo la afectación psicológica del agraviado, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**

   Si, deberían hacerse cargo de los gastos ocasionados por los clientes afectados por dichos fraudes.

4. **¿Considera Ud. que los bancos tienen responsabilidad civil, cuando se utilizan sus canales digitales de atención para la comisión del fraude informático en sus diferentes modalidades? Explique.**

   Si, ya que deberían cuidar celosamente dicha información que podría ser utilizada maliciosamente por algún delincuente informático.

5. **¿Considera Ud. que los bancos tienen responsabilidad civil, ante el daño causado por las operaciones no reconocidas de sus clientes, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**

   Si tienen responsabilidad y deberían hacerse cargo de las sustracciones del dinero de las cuentas de los clientes, así como de su información.

6. **¿Considera usted que los bancos ejecutan eficientemente los estándares de idoneidad respecto a los métodos de seguridad para proteger las cuentas del usuario? Explique**

   Si, pero les falta mayor celo en el cuidado del dinero así como de la

información de los clientes, deberían tener lo último de seguridad informática en sus agencias.

OBJETIVO ESPECIFICO 4:

Proponer alternativas de solución en beneficio de los usuarios de las entidades financieras inmersos en la comisión del fraude informático a través del phishing.

7. **En su opinión ¿Se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la información y seguridad suficiente a sus usuarios frente a los riesgos existentes en la red?**
   Si, deben asumir el total de la sustracción del capital de las cuentas bajo cuidado de las agencias bancarias.

8. **Considera Ud. ¿Que se debería establecer explícitamente dentro del contrato un apartado de la responsabilidad que tendría la entidad bancaria frente a los fraudes informáticos? Explique**
   Si, debería registrarse clausulas en los contratos de uso de las cuentas bancarias a favor de los clientes y que estas sean claras para que ellos tomen la decisión de poner su capital o no en dicha entidad bancaria.

9. **Considera Ud. ¿Qué se debería implementar la seguridad de las transacciones virtuales mediante un reconocimiento facial o biométrico? explique**

   Si, eso sería lo ideal y de esta manera se evitaría los delitos de fraude informáticos, ya que existiría mayor control y habría mayor seguridad para el usuario.

ENTREVISTA 02

Título: La responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

I. Datos generales de los investigadores entrevistado (a):

Fecha: 25 de marzo del 2022 **Hora:** 10:00

Lugar: Central Operativa de Investigación Criminal PNP Tacna.

Entrevistadores: - Br. COARITE ESPINOZA, Betsabe y
- Br. RAMOS FLORES, Daniel

Entrevistado: S2 PNP Juan Raúl SOTO DE LA SOTA.

Edad: 35 AÑOS **Género:** Masculino.

Puesto: Investigador Especializado en DIVINCRI - TACNA

II. Instrucciones:

Leer detenidamente cada interrogante de la presente entrevista y responda desde su experiencia, conocimiento, opinión con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para corroborar nuestros objetivos.

OBJETIVO ESPECIFICO 2:

Identificar los fundamentos para imputar responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

1. **¿Considera Ud. que los bancos no cumplen correctamente la comprobación de legitimidad para las transacciones virtuales? Justifique su respuesta.**

   --- Si, para la perpetración del delito informático conocido como Phishing, los datos de acceso a una operación bancaria que han sido obtenidos ilegalmente (número de cuenta, nombre, contraseña, fecha o CCV), son los mismo que se requieren para una operación legal ya que el protocolo de las operaciones son espontáneos y sin saber si son legales o ilegales, en todo caso se debiera incrementar otro tipo de requerimientos para estas

operaciones virtuales, lo cual no es de conveniencia a la entidad bancaria ya que en todo momento buscan simplificar las operaciones y en la simplificación se encuentran los peligros utilizados por la cyber delincuencia.

2. **¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños patrimoniales, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**

   --- Si, únicamente que los mecanismos jurídicos frente a la responsabilidad civil no están claros al respecto, la responsabilidad de las entidades bancarias frente a este delito es que siendo que los bancos reciben el dinero de las personas en calidad de DEPOSITOS, la salida de los activos sean físicos o de forma virtual, es responsabilidad del que posee el bien, en tal sentido los bancos deberían preocuparse más en asegurar las operaciones que en simplificarlas, así como implementar no solo la seguridad en las operaciones, sino en el uso de sus dominios ya que es de esa forma en la cual los ciber delincuentes obtienen ilegalmente los datos que utilizaran para las operaciones.

3. **¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños de naturaleza extra patrimoniales, como por ejemplo la afectación psicológica del agraviado, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**

   --- Si, los daños ocasionado no solamente se centran en lo patrimonial, también afectan a la persona agraviada psicológicamente, incluso sin tener contacto con ellas, y en el caso del phishing los agraviados se ven afectados emocionalmente por la pérdida del dinero, ya que en un gran porcentaje saben que no volverán a recuperarlo, por otro lado el banco sin ser el autor de los hechos, por ser un delito informático viene siendo víctima al vulnerarse sus sistemas de seguridad, pero por su posición frente al patrimonio de las victimas debiera asumir responsabilidad al menos en lo civil.

4. **¿Considera Ud. que los bancos tienen responsabilidad civil, cuando se utilizan sus canales digitales de atención para la comisión del fraude informático en sus diferentes modalidades? Explique.**

   --- Si, como explique en la respuesta número "1" la atención de las operaciones virtuales se hacen sin el conocimiento de que sean ilegales, ya que al tener los requisitos para la operación es factible llevarla a cabo, por otro lado las investigaciones no debieran centrarse en la operación sino en la obtención de los datos para la posterior perpetración de la operación ilegal, para lo cual la ciber delincuencia no utiliza las plataformas de los bancos, sino que construye plataformas virtuales similares o idénticas con el fin de que los usuarios ingresen sus datos y ellos poder utilizarlos en las plataformas verdaderas

5. **¿Considera Ud. que los bancos tienen responsabilidad civil, ante el daño causado por las operaciones no reconocidas de sus clientes, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**

   --- Sería muy arbitrario responsabilizar a la entidad bancaria por operaciones únicamente NO REONOCIDAS, las cuales debiera reunir una serie de requisitos para generar sospecha y determinar la ilegitimidad de la operación.

6. **¿Considera usted que los bancos ejecutan eficientemente los estándares de idoneidad respecto a los métodos de seguridad para proteger las cuentas del usuario? Explique**

   --- No, en mi opinión, los bancos no están centrados en brindar seguridad en las operaciones, sino en simplificarlas, ya que por su naturaleza una operación bancaria suele verse como tediosa y complicada y las entidades bancarias quieren hacerlas más simples para que sean utilizadas por mayor cantidad de personas y es allí donde se aprovecha para la perpetración de los diferentes delitos informáticos. Mi opinión es incrementar los medios de seguridad y no solo buscar su simplificación.

OBJETIVO ESPECIFICO 4:

Proponer alternativas de solución en beneficio de los usuarios de las entidades financieras inmersos en la comisión del fraude informático a través del phishing.

7. **En su opinión ¿Se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la información y seguridad suficiente a sus usuarios frente a los riesgos existentes en la red?**

   --- Si, de hecho, la información respecto a una operación sospechosa o ilegal, es algo que los propios dueños de las cuentas no logran obtener de forma idónea y eso debe ser sancionado, asimismo el no brindar la seguridad al patrimonio de los usuarios es su responsabilidad.

8. **Considera Ud. ¿Que se debería establecer explícitamente dentro del contrato un apartado de la responsabilidad que tendría la entidad bancaria frente a los fraudes informáticos? Explique**

   --- Si, debiera ser parte de todo contrato que un usuario acepta frente a una entidad bancaria para establecer correctamente los límites de la responsabilidad del usuario y la del banco frente al patrimonio y no únicamente ofrecer los famosos seguros anti robo, que al final el usuario viene pagando.

9. **Considera Ud. ¿Qué se debería implementar la seguridad de las transacciones virtuales mediante un reconocimiento facial o biométrico? explique**

   --- Si, mi punto en todas las respuestas ha sido incrementar los medios de seguridad y no simplificarlos, la incrementación del reconocimientos biométricos faciales y dactilares es algo que ya se utiliza en gran porcentaje de los teléfonos celulares de la población, por lo tanto hacer de eso un paso más para realizar una operación sería útil y reduciría la perpetración de gran parte de los delitos informáticos.

SA - 31499721
Juan Raúl SOTO DE LA SOTA
S2 PNP
INVESTIGADOR DEL AREA DE DELITOS CONTRA EL PATRIMONIO PNP TACNA

ENTREVISTA 03

Título: La responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

I. Datos generales de los investigadores entrevistado (a):

Fecha: 25 de marzo del 2022 **Hora:** 11:00

Lugar: Sede del Ministerio Publico de Tacna.

Entrevistadores: - Br. COARITE ESPINOZA, Betsabe y
- Br. RAMOS FLORES, Daniel Andrés

Entrevistado: Abg. Christian Miguel Carrillo Maydana

Edad: 44 **Género:** Masculino

Puesto: Fiscal Adjunto Provincial de la fiscalía provincial Penal Corporativa de Tacna

II. Instrucciones:

Leer detenidamente cada interrogante de la presente entrevista y responda desde su experiencia, conocimiento, opinión con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para corroborar nuestros objetivos.

OBJETIVO ESPECIFICO 2:

Identificar los fundamentos para imputar responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

1. **¿Considera Ud. que los bancos no cumplen correctamente la comprobación de legitimidad para las transacciones virtuales? Justifique su respuesta.**
   Si, en razón que no se advierte un sistema de seguridad confiable que permita a los usuarios de las entidades financieras, poder acceder en forma segura a realizar diversas operaciones o transacciones virtuales, generando más bien el incremento de fraudes o hurtos informáticos.

2. **¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños patrimoniales, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**

Si, considero que al carecer las entidades financieras de un sistema de seguridad confiable y seguro, permite que se ocasionen perjuicios económicos en sus usuarios, lo cual conlleva y genera una responsabilidad civil por parte de la entidad bancaria, más aun que como se advierte en la actualidad, estos delitos son realizados por personas especializadas en informática y tecnología, ante lo cual no existe la información necesaria hacia los usuarios de las entidades financieras.

3. **¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños de naturaleza extra patrimoniales, como por ejemplo la afectación psicológica del agraviado, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**
   Si, también consideramos que si el problema se inicia por sistemas de las entidades financieras, inseguros, porque pueden ser clonados, copiados, a través de páginas web, correos electrónicos, llamadas telefónicas y mensajes de textos, con creaciones de links u otros, que permiten que los delincuentes hurten el patrimonio de los usuarios, ello en definitiva va afectar psicológicamente a los agraviados; debiendo tener en cuenta que el en estos delitos, se realizan en su mayoría las sustracciones del total de fondos de las cuentas bancarias.

4. **¿Considera Ud. que los bancos tienen responsabilidad civil, cuando se utilizan sus canales digitales de atención para la comisión del fraude informático en sus diferentes modalidades? Explique.**
   Si, en razón de que si un usuario ingresa a través de un medio o canal digital de una entidad bancaria para realizar una transacción y operación financiera, lo realiza en la confianza de seguridad que debe tener este tipo de medio ofrecido por la entidad.

5. **¿Considera Ud. que los bancos tienen responsabilidad civil, ante el daño causado por las operaciones no reconocidas de sus clientes, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**
   Si, siempre y cuando se haya llegado a determinar la manera en que los usuarios fueron víctimas de fraudes informáticos, y si es evidente que el usuario a pesar de aplicar un deber de cuidado de sus bienes, no pudo advertir el engaño o fraude en que fui inducido a incurrir.
6. **¿Considera usted que los bancos ejecutan eficientemente los estándares**

de idoneidad respecto a los métodos de seguridad para proteger las cuentas del usuario? Explique

No, ya como se ha señalado precedentemente, las estadísticas de criminalidad, llegan a determinar que los sistemas de seguridad utilizados por las entidades financieras, no son confiables, es decir son inseguras, conllevando al aumento de incidencia de los delitos informáticos.

OBJETIVO ESPECIFICO 4:

Proponer alternativas de solución en beneficio de los usuarios de las entidades financieras inmersos en la comisión del fraude informático a través del phishing.

7. **En su opinión ¿Se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la información y seguridad suficiente a sus usuarios frente a los riesgos existentes en la red?**

   Si, definitivamente, teniendo en cuenta el avance de la tecnología digital actual y la modernidad en el uso de los sistemas, aplicativos, app y otros, utilizados por las entidades financieras, estas entidades en la obligación de brindar y proporcionar toda esta información a través entre otros de los medios de comunicación (televisión, radio, prensa escrita, redes sociales y otros), sin embargo, no se advierten estas políticas de información en forma idónea por parte de las entidades.

8. **Considera Ud. ¿Que se debería establecer explícitamente dentro del contrato un apartado de la responsabilidad que tendría la entidad bancaria frente a los fraudes informáticos? Explique**

   Si, porque ello serviría para delimitar las responsabilidades de los usuarios y de las entidades financieras, en forma expresa.

9. **Considera Ud. ¿Qué se debería implementar la seguridad de las transacciones virtuales mediante un reconocimiento facial o biométrico? Explique**

   Si, porque son métodos de seguridad que deben adoptar las entidades financieras en beneficio y salvaguarda de sus usuarios; lo cual impediría las suplantaciones de identidad, y otras formas de fraude informático.

Abog. CHRISTIAN MIGUEL CARRILLO MAYDANA
FISCAL ADJUNTO PROVINCIAL
Fiscalia Provincial Penal Corporativa de Tacna

ENTREVISTA 04

Título: La responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

I. Datos generales de los investigadores entrevistado (a):

Fecha: 28 de marzo del 2022 **Hora:** 18:00

Lugar: Sede del Poder Judicial Tacna.

Entrevistadores: - Br. COARITE ESPINOZA, Betsabe y
- Br. RAMOS FLORES, Daniel Andrés

Entrevistado: Abg. Rogelio Alberto ZEA CATACORA

Edad: 44 **Género:** Masculino

Puesto: Juez (P) del Segundo Juzgado Civil Transitorio de Tacna

II. Instrucciones:

Leer detenidamente cada interrogante de la presente entrevista y responda desde su experiencia, conocimiento, opinión con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para corroborar nuestros objetivos.

OBJETIVO ESPECIFICO 2:

Identificar los fundamentos para imputar responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

1. **¿Considera Ud. que los bancos no cumplen correctamente la comprobación de legitimidad para las transacciones virtuales? Justifique su respuesta.**
   Considero que ante el avance de la tecnología y la aparición de nuevas formas de criminalidad “ciberdelincuencia”, las entidades bancarias en general deben fortalecer sus mecanismos de seguridad, atendiendo como entidades del sistema financiero administran los fondos de sus clientes.

2. **¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños patrimoniales, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**

En la medida que las entidades bancarias no cuenten con una adecuada seguridad, ella podría generar una responsabilidad civil, dado que como administradores de los fondos de sus clientes deben adoptar las medidas necesarias para evitar el fraude informático.

3. **¿Considera Ud. que los bancos tienen responsabilidad civil frente a los daños de naturaleza extra patrimoniales, como por ejemplo la afectación psicológica del agraviado, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**
   Es posible que concurran daños extra patrimoniales, según cada caso en concreto en la medida que en las entidades financieras hayan actuado con dolo o culpa y se encuentren presente los demás elementos de la responsabilidad civil.

4. **¿Considera Ud. que los bancos tienen responsabilidad civil, cuando se utilizan sus canales digitales de atención para la comisión del fraude informático en sus diferentes modalidades? Explique.**
   Debemos de partir que se genera responsabilidad civil, cuando concurren determinados aspectos, como el daño, la antijuricidad, el nexo causal, factor de atribución, de ahí que en la medida que las entidades bancarias no otorguen las debidas seguridades en la atención de sus canales digitales, según el caso concreto puede generar responsabilidad civil.

5. **¿Considera Ud. que los bancos tienen responsabilidad civil, ante el daño causado por las operaciones no reconocidas de sus clientes, ocasionados por el fraude informático en sus diferentes modalidades? Explique.**
   En tanto, puede establecerse que las operaciones en efecto, no han sido realizadas por sus clientes, y en tanto aparezcan los elementos de la responsabilidad civil, daño, la antijuricidad, el nexo causal, factor de atribución.

6. **¿Considera usted que los bancos ejecutan eficientemente los estándares de idoneidad respecto a los métodos de seguridad para proteger las cuentas del usuario? Explique**
   Entiendo que cada banco tienen sus propios mecanismos de seguridad que, para poder arribar a referida conclusión, habría que tener conocimiento de los mismos; sin embargo, consideramos que esos mecanismos de seguridad deben ser eficaces y eficientes.

OBJETIVO ESPECIFICO 4:

Proponer alternativas de solución en beneficio de los usuarios de las entidades financieras inmersos en la comisión del fraude informático a través del phishing.

7. **En su opinión ¿Se debe aplicar políticas de responsabilidad que sancionen a los bancos por no otorgar la información y seguridad suficiente a sus usuarios frente a los riesgos existentes en la red?**
   Sí, en la medida que los bancos prestan un servicio a sus clientes, están obligados a adoptar adecuados mecanismos de seguridad, máxime si en una relación de consumo quien presta un servicio debe realizarlo con idoneidad.

8. **Considera Ud. ¿Que se debería establecer explícitamente dentro del contrato un apartado de la responsabilidad que tendría la entidad bancaria frente a los fraudes informáticos? Explique**

   Considero que si resultaría factible, sería necesario realizar una propuesta legislativa en ese sentido, para obligatoriedad de cláusulas específicas en los contratos bancarios; ello también generaría un mayor compromiso de las entidades financieras.

9. **Considera Ud. ¿Qué se debería implementar la seguridad de las transacciones virtuales mediante un reconocimiento facial o biométrico? Explique**
   Es una alternativa, que puede ser utilizada, debemos tener presente que la tecnología en estos tiempos ha sido de gravital importancia para la realización de diferentes tramites de los ciudadanos, como de hacer diferentes transacciones civiles, comerciales, tributarias, etc.; en ese sentido, la utilización de la tecnología para fortalecer la seguridad de las transacciones bancarias, así como otras medidas que pueden tomarse para dotar de mayor seguridad.

Abg. Rogelio A. ZEA CATACORA
JUEZ (P) DEL SEGUNDO JUZGADO
CIVIL TRANSITORIO DE TACNA

ENTREVISTA N°05

Título: La responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

I. Datos generales de los investigadores entrevistado (a):

Fecha: 25-03-2022 **Hora:** 10:00

Lugar: Oficina del Banco de Crédito del Perú (BCP) – SEDE TACNA

Entrevistadores: Br. COARITE ESPINOZA Betsabe y
Br. RAMOS FLORES Daniel

Entrevistado: Lady del Pilar Ramos Damián

Edad: 33 **Género:** FEMENINO

Puesto: Asesora del ventas y servicios – División de Canales de Atención BCP

II. **Instrucciones:**

Leer detenidamente cada interrogante de la presente entrevista y responda desde su experiencia, conocimiento, opinión con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para corroborar nuestros objetivos.

OBJETIVO ESPECIFICO 3:

Determinar los métodos más frecuentes derivada de la comisión del fraude informático inmersos en las entidades financieras.

1. **¿Considera usted que el phishing es un método frecuente del fraude informático? explique**

   Sí, nuestros clientes reciben correos electrónicos falsos que los dirigen a una página web que simula ser del BCP donde los estafadores les solicitan "actualizar tus datos" donde buscan obtener sus claves secretas, número de tarjeta, fecha de vencimiento, código de seguridad y clave token. Nuestros

clientes ingresan al enlace y llenan sus datos creyendo que es de nuestro banco y nosotros jamás pedimos esta información a través de un mail.

2. **¿Considera usted que el pharming es un método frecuente del fraude informático? explique**

   Sí, hoy en día he sabido de algunos casos en mi entidad financiera.

3. **¿Considera usted que el smishing es un método frecuente del fraude informático? explique**

   Sí, los estafadores envían sms falsos a nuestros clientes haciéndose pasar por nosotros indicando que tienen transferencias retenidas o solicitando la actualización de datos inmediata para evitar el bloqueo de sus tarjetas. Nuestros clientes se alarman e ingresan rápidamente al enlace que está en esos sms, cayendo en esta modalidad de fraude.

4. **¿Qué otros métodos conoce usted que sean frecuentes para la comisión del fraude informático?**

   El vishing, nuestros clientes reciben llamadas telefónicas de los estafadores haciéndose pasar por colaboradores de nuestro banco donde les solicitan datos confidenciales y ellos brindan esa información, es allí donde son víctimas de esta modalidad de fraude.

Lady Ramos D.
Asesor de Ventas y Servicios
DNI 45305964 / MAT 122511
División de Canales de Atención

ENTREVISTA N° 06

Título: La responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

I. Datos generales de los investigadores entrevistado (a):

Fecha: 20-03-2022 **Hora:** 09:00 am

Lugar: Banco de la Nación de Tarata - Tacna

Entrevistadores: Br. COARITE ESPINOZA Betsabe y
Br. RAMOS FLORES Daniel

Entrevistado: Yajahira Pinto Oviedo

Edad: 27 **Género:** Femenino

Puesto: Administrador del Banco de la Nación – SEDE Tarata - Tacna

II. **Instrucciones:**

Leer detenidamente cada interrogante de la presente entrevista y responda desde su experiencia, conocimiento, opinión con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para corroborar nuestros objetivos.

OBJETIVO ESPECIFICO 3:

Determinar los métodos más frecuentes derivada de la comisión del fraude informático inmersos en las entidades financieras.

1. **¿ Considera usted que el phishing es un método frecuente del fraude informático? explique**

   Si, pues el phishing como tal es una de las modalidades más utilizadas en los últimos tiempos utilizando información confidencial, generando pérdidas económicas a los usuarios de diversas entidades financieras.

2. **¿ Considera usted que el pharming es un método frecuente del fraude informático? explique**

Si, este método de delito desvía a los clientes a páginas fraudulentas generando así pérdidas económicas por la malversación de información, este delito de fraude informático viene operando día a día con mayor énfasis.

3. **¿Considera usted que el smishing es un método frecuente del fraude informático? explique**

   Si, ya que comúnmente recibimos publicidad o anuncios de las entidades financieras mediante los equipos móviles y con la practicidad de esto muchas veces optamos por acceder, siendo estas no siempre las legítimas emitidas por las entidades financieras.

4. **¿Qué otros métodos conoce usted que sean frecuentes para la comisión del fraude informático?**

   También son conocidos los fraudes por redes sociales, las instalaciones de software malintencionados y el vishing.

ENTREVISTA N°07

Título: La responsabilidad civil de las entidades financieras derivada de la comisión del fraude informático a través del phishing.

I. Datos generales de los investigadores entrevistado (a):

Fecha: 27-03-2022 **Hora:** 19:45

Lugar: Oficina del Banco de la Nación – SEDE TACNA

Entrevistadores: Br. COARITE ESPINOZA Betsabe y
Br. RAMOS FLORES Daniel

Entrevistado: MOISES MARIN ROMERO

Edad: 38 **Género:** MASCULINO

Puesto: JEFE DE SECCIÓN CAJA DEL BANCO DE LA NACIÓN

II. **Instrucciones:**

Leer detenidamente cada interrogante de la presente entrevista y responda desde su experiencia, conocimiento, opinión con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para corroborar nuestros objetivos.

OBJETIVO ESPECIFICO 3:

Determinar los métodos más frecuentes derivada de la comisión del fraude informático inmersos en las entidades financieras.

1. **¿Considera usted que el phishing es un método frecuente del fraude informático? explique**

   Sí, porque el estafador o delincuente hace que el cliente divulgue su información personal haciéndolo vulnerable; por ejemplo: número de tarjeta, clave, cvv2, fecha de caducidad del plástico, DNI. Información que se requiere para vaciar los fondos del cliente.

2. **¿Considera usted que el pharming es un método frecuente del fraude informático? explique**

   Sí, porque este fraude informático es a través de páginas fraudulentas las que no están autorizadas por los Bancos; siendo toda responsabilidad del tarjetahabiente por ingresar a páginas a través de buscadores.

3. **¿Considera usted que el smishing es un método frecuente del fraude informático? explique**

   Sí, es fraude a través de los dispositivos móviles donde el cliente de igual forma brinda toda su información vulnerando así sus datos personales para que puedan ingresar a sus cuentas.

4. **¿Qué otros métodos conoce Ud. que sean frecuentes para la comisión del fraude informático?**

   No, los que vemos constantemente en el Banco son los anteriormente mencionados.