UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

La comisión del phishing: una revisión de su literatura científica, en el marco de la ley 30096

TRABAJO DE INVESTIGACIÓN PARA OBTENER GRADO ACADÉMICO DE:

Bachiller en Derecho

AUTOR:

Peralta Huaman, Alex Jaime (orcid.org/0000-0002-1532-8397)

ASESOR:

Dr. Riveros Tolentino, Edy Leonardo (orcid.org/0000-0002-6556-569X)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal, Procesal Penal, Sistema de Penas, Causas y Formas del Fenómeno Criminal

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía

LIMA – PERÚ

2024

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Autenticidad del Asesor

Yo, RIVEROS TOLENTINO EDY LEONARDO, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ATE, asesor de Trabajo de Investigación titulado: "La comisión del phishing: una revisión de su literatura científica, en el marco de la ley 30096.", cuyo autor es PERALTA HUAMAN ALEX JAIME, constato que la investigación tiene un índice de similitud de 15%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 16 de Junio del 2024

Apellidos y Nombres del Asesor:	**Firma**
RIVEROS TOLENTINO EDY LEONARDO **DNI:** 40541981 **ORCID:** 0000-0002-6556-569X	Firmado electrónicamente por: ERIVEROSTOL el 16-06-2024 20:34:25

Código documento Trilce: TRI - 0761452

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Originalidad del Autor

Yo, PERALTA HUAMAN ALEX JAIME estudiante de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ATE, declaro bajo juramento que todos los datos e información que acompañan el Trabajo de Investigación titulado: "La comisión del phishing: una revisión de su literatura científica, en el marco de la ley 30096.", es de mi autoría, por lo tanto, declaro que el Trabajo de Investigación:

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

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

Nombres y Apellidos	**Firma**
ALEX JAIME PERALTA HUAMAN **DNI:** 70037520 **ORCID:** 0000-0002-1532-8397	Firmado electrónicamente por: APERALTAH el 16-06-2024 19:08:02

Código documento Trilce: TRI - 0761453

INVESTIGA UCV

Índice de contenidos Pág.

Resumen

Este trabajo de revisión de la literatura está alineado con el Objetivo de Desarrollo Sostenible (ODS) centrándose en la alianza para lograr objetivos. El estudio, de tipo básico, utilizó recursos de plataformas académicas reconocidas como Scielo, Scopus y Dialnet. En consecuencia, problema general: Determinar la posibilidad de atribuir responsabilidad civil en el delito de Phishing a las entidades financieras. Objetivo específico 1: Analizar si son responsables civiles los bancos en los delitos de Phishing. Objetivo específico 2: Definir cuál es el tipo de responsabilidad que se atribuiría a los bancos en el delito de Phishing, en conclusión, que luego de realizar una revisión exhaustiva, el tipo de responsabilidad que les corresponde asumir a los bancos sería la de la responsabilidad civil y administrativa, tal y como se ha mencionado en líneas precedentes, ello en merito a que los bancos, son los encargados de dotar de seguridad a los usuarios.

Palabras clave: Responsabilidad civil, exhaustiva, phishing.

Asbtract

This literature review work is aligned with the Sustainable Development Goal (SDG) focusing on partnership to achieve objectives. The basic study used resources from recognized academic platforms such as Scielo, Scopus and Dialnet. Consequently, General problem: Determine the possibility of attributing civil liability for the crime of Phishing to financial entities. Specific objective 1: Analyze whether banks are civilly liable for Phishing crimes. Specific objective 2: Define the type of responsibility that would be attributed to banks in the crime of Phishing, in conclusion, that after carrying out an exhaustive review, the type of responsibility that banks must assume would be that of liability civil and administrative, as mentioned in previous lines, this is due to the fact that banks are in charge of providing security to users.

Keywords: Civil liability, exhaustive, phishing.

I. INTRODUCCIÓN

En lo que respecta a la **Realidad Problemática**, debemos de precisar que en la actualidad realizar actividades financieras han ido en constante cambio, ello se debe principalmente al contexto actual en el que nos desarrollamos, la rigidez para la obtención de una cuenta en un banco es nula todos los pasos son cortos y rápidos, realizar compras por internet, permiten al usuario realizar sus operaciones y transacciones de modo simple clic, situación que favorece en la temporalidad de las transacciones financieras, haciéndolas las útiles y con una fracción de tiempo menor a la de apersonarse a un establecimiento financiero, sin embargo realizar todo a través de un dispositivo electrónico también tiene sus riesgos si no se toman las previsiones del caso para evitar ser víctima de phishing, por lo general, en la comisión de delitos informáticos, no hay una sanción a las entidades financieras, siendo las ultimas las responsables de sus plataformas financieras, razón por la cual debe de existir la manera de sancionar a los bancos, por no otorgar garantías para el desenvolvimiento y correcto funcionamiento de la plataforma financiera.

En cuanto a la **Problemática y Contexto social**. La falta de autenticación por parte de las entidades financieras, permite que los ciberdelincuentes aprovechen el poco conocimiento de los usuarios, quienes desconocen la manera en la que se desarrollan sus actividades financieras, siendo más propensas a que los delincuentes aprovechen que en la actualidad robar información sensible y suplantar la identidad de una persona, lastimosamente es algo muy cotidiano, ello se debe a la optimización de los procesos para la apertura de una cuenta bancaria de cuentas, aplicaciones de índole financiero, los usuarios financieros son estafados a través de las plataformas financieras por inescrupulosos, quienes utilizan el espacio virtual para cometer ilícitos que perjudican finalmente a los usuarios de los proveedores de servicios, quien por lo general n cumplen su rol protector, ello debido a que son propietarios de los dominios de sus plataformas, al no existir una legislación uniforme que ampare a los consumidores en los casos de este tipo de delitos, los mecanismos de seguridad de las entidades financieras, no garantizan la seguridad de una transacción y al no tener algún tipo de responsabilidad, simplemente obvian su rol protector, razón por la cual el panorama actual es escaso por no decir nulo sobre otorgar sanciones civiles y administrativas a las entidades bancarias por no otorgar seguridad en las operaciones

financieras así como también resarcir el daño causado por incumplimiento de sus políticas de seguridad.

Formulación del Problema. Quintana (2008), nos señala que la formulación de un problema se basa en responder una pregunta o el problema planteado a investigar, en tal aspecto, se ha elaborado los siguientes cuestionamientos en la presente investigación: **problema general:** ¿Es posible atribuir responsabilidad civil en el delito de Phishing a las entidades financieras? objetivo específico 1: ¿Son responsables civiles los bancos en los delitos de Phishing? Objetivo específico 2: ¿Cuál es el tipo de responsabilidad que se atribuiría a los bancos en el delito de Phishing? Los cuestionamientos señalados, se basan a los resultados obtenidos en las investigaciones, tomando como referencia el contexto actual.

En esa línea de ideas tenemos como **Antecedentes Nacionales**, Paredes (2017), en su investigación titulada, los delitos cometidos con el uso de sistemas informáticos, concluye que en el caso del Phishing estos delitos constituyen una modalidad en la que el perfeccionamiento es tal que los usuarios creen que las plataformas son verdaderas, por ello confían en la procedencia de dichas plataformas.

Mori (2019), en su investigación titulada, Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de Lima, periodo 2008 al 2012, concluye que los jueces carecen de conocimiento claro respecto a este tipo de delitos, en tal aspecto al carecer de conocimiento los administradores de justicia hace más vulnerable la situación hacia las víctimas.

Hancco (2018), en su investigación que lleva por título, La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096, Perú – 2017, en nuestro país la estructura penal no tiene una conexión coherente con la sanción que se le otorga a los delincuentes informáticos, razón por la cual imputar estos delitos es casi imposible, situación que debe de ser revertida en todos sus extremos.

A decir de Espinoza (2017), en su investigación titulada, Derecho penal informático, existe mucho por hacer para efectivizar las normas en materia de delitos informáticos, ello se ve reflejado en los altos incides delictivos, la dación de normas tiene que ser dinámicas y ello será posible cuando se trabaje de manera multisectorial.

Se describen los **Antecedentes Internacionales**, que sustenta la presente investigación, según Herrera (2016), en su investigación titulada, El Phishing como Delito Informático, tuvo la siguiente conclusión, para que exista un trabajo conjunto se tienen que cumplir todos los estándares internacionales, para imputar delitos como el phishing y ello será posible, cuando las normas tengas que ser conjuntas.

Por otro lado, Terán (2016), en su investigación titulada, La necesidad de incorporar el Phishing, arribo a la siguiente conclusión, se debe de proteger el sistema penal tomando en consideración los aspectos criminógenos de la sociedad, razón por la cual se tiene que proteger a las víctimas de este tipo de delitos.

A decir de, Zapata (2019), en su investigación titulada: El delito de estafa en la modalidad Phishing, tuvo por conclusión, la obtención de la prueba digital constituye un paso importante para poder recrear el caso y llegar a la imputación necesaria en este tipo de delitos que dada su categoría se desarrollan de manera pluriofensiva, dado que convergen una serie de voluntades para causar un lucro a las víctimas.

En ese sentido, a decir de Flores (2017), en su investigación titulada, El phishing como comportamiento penalmente relevante, llego a la siguiente conclusión, el Phishing, tiene una serie de etapas o fases en la que se desarrolla, situación que merece un profundo estudio dado que para sancionar este delito se requiere una imputación objetiva.

Respecto a las teorías relativas al tema, Benavides et al. (2020) nos da una arista clara respecto a cómo se desarrolla este tipo de delitos, de esta manera a decir de Benavides, el delito de phishing requiere generar certeza de la veracidad de las plataformas o entidades que se suplantan, por ello las victimas creen estar en un espacio seguro y veraz, por ello este tipo de delitos es de perfeccionamiento. Del mismo modo, Hernández y Baluja (2021) mencionan que el phishing es calificado como un sistema conjunto de pequeños fraudes hasta lograr el objetivo de pescar a la víctima para lograr su cometido. La teoría de la ciberdelincuencia, señalada por Santos y Teixeira (2020) consiste en realizar engaños a las personas usuarios de plataformas digitales o físicas, quienes a través de mensajes, llamadas o links, creen que determinadas entidades son cierta accediendo a los requerimientos de los delincuentes informáticos quienes aprovechan de ese desconocimiento para causar

por lo general un lucro económico, Del mismo modo, Parada y Errecaborde (2018) señalan que a raíz de los avances tecnológicos, realizar transacciones operacionales es algo cotidiano por ello el avance significativo de estos delitos, muchas personas al considerar ofertas por internet proporcionan sus datos personales, los mismos que son aprovechados para realizar el delito de phishing. Igualmente, Cámara (2020), tuvo como aporte científico detallar la utilización de nuevas metodologías de delitos, para causar perjuicio económico a los usuarios, por ende, se debe de proteger la autenticación, en cada una de las operaciones que se realicen.

Justificación de la investigación: la presente investigación, parte de la postura de regular y proteger a los usuarios frente al delito de phishing, razón por la cual se debe de tener en consideración, que se debe de otorgar responsabilidad civil a los bancos entidades. En cuanto a la **Justificación Teórica**: La presente revisión de la literatura versa en la búsqueda y análisis de información científica. **Justificación Metodológica:** se ha empleado el método científico, para la elaboración de esta revisión de la literatura, consignando información relevante siguiendo líneas del rigor correspondiente. **Justificación Práctica:** al existir un defecto de la norma, se tiene que fortalecer el sistema legal, para dinamizar el actual nuestro marco normativo.

problema general: Determinar la posibilidad de atribuir responsabilidad civil en el delito de Phishing a las entidades financieras. **Objetivo específico 1:** Analizar si son responsables civiles los bancos en los delitos de Phishing. **Objetivo específico 2:** Definir cuál es el tipo de responsabilidad que se atribuiría a los bancos en el delito de Phishing.

II. METODOLOGÍA

Enfoque tipo y diseño de investigación. En ese sentido el enfoque cualitativo en que se basa la presente investigación. Para Fernández (2014) el enfoque cualitativo busca indagar y sistematizar la información desde la perspectiva de los participantes. El artículo de revisión de la literatura, fue de tipo básico. Según Álvarez (2020), señala que este tipo de investigación se orienta a obtener un nuevo conocimiento con el objetivo de incrementar el existente. Por ello, el autor señala que el tipo de investigación básica nos permite a través de la búsqueda de la información y los saberes previos, obtener una información con relevancia jurídica para abordar un tema de manera idónea. De la Espriela & Gomez (2022) en referencia al diseño de investigación de investigación consideramos que la teoría fundamentada: nos permite tener una conceptualización de las teorías cumpliendo todos los estándares de la investigación es decir mediante los datos obtenidos recabados en la búsqueda de la información nos permitirá comparar aspectos para fundamentar la información (p.1). Por ello, concuerdo con lo que señalado por los referidos autores, dado que este tipo de teoría nos permite tener idea clara dinamizando el proceso de investigación toda vez que mediante este diseño de investigación los resultados serán los deseados por el investigador partiendo desde las teorías recabadas en los antecedentes de la investigación.

En referencia a las **fuentes y base de datos**, debemos referir que la categoría Phishing informático, Hancco (2017), respecto al phishing, el autor refiere que este tipo de delitos constituye un perfeccionamiento de la acción penal ilícita toda vez que tiene faces o modalidades para lograr su objetivo, el mismo que dado los incides de criminalidad se aprecia que siempre busca la obtención de redito económico, como lo he señalado en líneas precedentes, estas actividades ilícitas primero buscar robar la identidad, luego las claves y finalmente aprovecharse económicamente de las victimas (p.33), en tal sentido de las fuentes consultadas son revistas indizadas cuya antigüedad es no mayor de cinco años, siendo fuentes con prestigio como Scielo, Scopus, Alicia, Redalyc, Tesis y Libros.

En relación al *volumen de publicaciones realizadas***,** fueron 30 fuentes consultadas, para darle mayor rigor científico a la investigación al trabajo de revisión de la literatura, en tal aspecto el volumen se cumple en lo estipulado en el marco de la investigación.

En cuanto a al objetivo específico 1 que consiste en analizar qué tipo de responsabilidad se debería aplicar a las Entidades financieras frente al delito de Phishing. Se ha trabajado con los siguientes antecedentes. Campos (2018), en su investigación titulada "El deber civil de las entidades financieras por el peligro de phishing", utilizó un enfoque cualitativo con el objetivo general de identificar patrones de fraude mediante el análisis de datos históricos de operaciones. Se concluyó que los bancos tienen deficiencias en la detección y verificación oportuna de retiros, y que es deber de las entidades bancarias asegurar que sus sistemas de protección contengan características que impidan la generación de diversos tipos de fraudes.

Por otra parte, Pardo (2017) en su investigación titulada "Procedimiento legal penal de los delitos informáticos contra el patrimonio en el Distrito Judicial de Lima, 2018", también utilizó un enfoque cualitativo. Su principal objetivo fue examinar cómo se trata legalmente los delitos informáticos contra el patrimonio en Lima. La conclusión resaltó la falta de eficacia del marco normativo actual para abordar de manera efectiva los delitos informáticos y sus variantes, como el fraude informático.

Finalmente, León (2018) en su estudio titulado "Vacíos jurídicos que limitan la imposición de sanciones por delitos informáticos según la Ley N° 30096 y sus modificaciones en el distrito de Lima Cercado en 2017", también empleó un enfoque cualitativo con el objetivo de identificar las lagunas legales que obstaculizan la aplicación de penalidades por delitos informáticos conforme a la legislación vigente. La conclusión fue que es crucial reforzar las políticas estatales y mejorar la gestión de la información para garantizar la seguridad y la integridad de los datos en las instituciones.

Abanto (2020), en su investigación titulada "La clonación de tarjetas de crédito y la responsabilidad civil de los bancos, Olivos año 2020", utilizó un enfoque cualitativo para examinar la responsabilidad civil de las entidades bancarias frente a la clonación de tarjetas de crédito en el distrito de Los Olivos. Concluyó que las entidades financieras deben asumir la responsabilidad por los cargos realizados mediante clonación una vez que el titular notifica y confirma las transacciones no reconocidas, conforme al protocolo de reclamo establecido. Sin embargo, observó que en ocasiones las entidades no cumplen esta obligación cuando el titular busca otros medios alternativos.

En cuanto al objetivo específico 2, que consistía en definir el tipo de responsabilidad aplicable al delito de phishing informático, se recurrió a varios antecedentes. Primero, Ruiz (2016) en su investigación titulada "Análisis de los delitos informáticos y su afectación a los derechos constitucionales de las personas", llevó a cabo un estudio cualitativo sobre el fraude informático y su impacto en los derechos constitucionales. Salas (2017) en su tesis "La responsabilidad civil de las entidades financieras frente a los consumidores por delitos informáticos", también utilizando un enfoque cualitativo, examinó la responsabilidad civil de las entidades financieras en casos de delitos informáticos. Concluyó que la responsabilidad civil debe ser objetiva para compensar los daños ocasionados por delitos informáticos, más allá de la responsabilidad subjetiva.

Hidalgo (2018), en su tesis "Los ilícitos informáticos y su repercusión en las relaciones legales", sostuvo que las entidades financieras tienen responsabilidad civil en casos de phishing, ya que deben proteger a los usuarios que desconocen los procedimientos financieros en línea. Finalmente, Coarite & Ramos (2022) en su tesis sobre Propusieron establecer una responsabilidad civil solidaria para las entidades financieras en casos de fraude informático mediante phishing, argumentando que estas entidades tienen la obligación de garantizar la seguridad de cada transacción financiera.

Estas investigaciones subrayan la importancia de establecer y fortalecer la responsabilidad civil de las entidades financieras en la protección de los usuarios contra los delitos informáticos, como el phishing.

En cuanto a las **consideraciones éticas**, destaca la rigurosidad empleada siguiendo las directrices empleadas por el lineamiento establecido mediante resolución académica, asegurando así la validez y fiabilidad de mi investigación. Además, he adherido a los lineamientos institucionales de nuestra universidad al recopilar la información necesaria, la cual guarda una estrecha relación con el enfoque y diseño de mi revisión de la literatura. Este enfoque ha resultado en el desarrollo de una investigación robusta, fundamentada en información veraz y orientada hacia la formulación de conclusiones legítimas.

III. RESULTADOS

En cuanto a al objetivo específico 1 que consiste en Analizar qué tipo de responsabilidad se debería aplicar a las Entidades financieras frente al delito de Phishing informático, desde el panorama nacional.

Luego del análisis correspondiente tomando la postura de los autores, quienes refieren que en los delitos informáticos existen ciertos vacíos que generan un perjuicio a las víctimas de phishing toda vez que no existe una uniformidad respecto a las decisiones judiciales de manera jurisprudencial, soy de la idea que los bancos deban resarcir el daño causado cuando se cometan estos delitos informáticos tomando en consideración la existencia del deber de idoneidad que los proveedores de servicios financieros deban de tener, en tal sentido, Paredes (2017), es de la idea de que se deba de proteger a las víctimas de delitos informáticos, creando mecanismos que garanticen la autenticación de las personas que realizan alguna operación financiera, mientras que Mori (2019), refiere las deficiencias a la hora de administrar justicia, sostiene que la falta de conocimiento por parte de los justiciables, no permite llegar a una sanción penal justa cuando se cometen este tipo de delitos que lesionan a las víctimas, Hancco (2018), Se ha determinado que en varios delitos no hay una correspondencia entre la gravedad de los actos y el veredicto, evidenciando que el derecho penal no diferencia entre barreras administrativas, infracciones penales y delitos. El término "penal" que se discute abarca todos los comportamientos que impactan en el "sistema", Finalmente, Espinoza (2017), nos refiere que en efecto las normas penales en materia de delitos informáticos son ineficiente.

Por todas las consideraciones antes planteadas soy de la idea que el actual marco normativo no cumple su rol garante de protección a las víctimas de delitos informáticos, considero que sería elemental que os proveedores de servicios financieros en atención a la naturaleza financiera en la que se desarrolla sus actividades, sean las encargadas de ser responsables solidariamente cuando exista un delito informático, por la lesión causada a sus usuarios, si las entidades financieras fueran responsables, tengo la plena seguridad que los altos incides de incidencia criminal disminuirían en gran porcentaje y eso se debería a que los proveedores, como los bancos tengas un nivel de seguridad mayor en todas sus plataformas financieras.

En cuanto al objetivo específico 2, que consiste en definir qué tipo de responsabilidad encuadraría en el delito de Phishing informático, comparto la postura de los autores, tales como Herrera (2016), quien sostiene que en el ecuador se han implementado herramientas, con el objetivo de proteger a los usuarios de las entidades financieras. Para enfrentar a este tipo de modalidades delictivas se requiere que las personas jurídicas, es decir las entidades financieras tengas que proteger a sus usuarios para proteger a los consumidores. Suscribo lo señalado por Terán (2016), quien señala que en efecto existe un vacío legal para proteger a los usuarios frente a la vulneración de delitos informáticos, las entidades financieras, deben tener cierto grado de responsabilidad frente a la existencia de estos delitos. A decir de, Zapata (2019), las entidades financieras deben ser responsables civilmente, por ende, se deberá de sancionar a los bancos para resarzan el daño causado a los usuarios. En ese sentido, a decir de Flores (2017), se debe de sancionar a las entidades financieras que incumplan su deber de idoneidad. Considero, que en efecto las entidades financieras deben de tener responsabilidad civil o administrativa, para resarcir de cierta manera el daño causado a las personas que sufren de estos delitos financieros que aunado a la incorrecta legislación hacen que las personas no obtengan justicia, soy de la postura de que se debe de perfeccionar el sistema penal para erradicar las acciones ilícitas, razón por la cual se debe de sancionar a las entidades financieras que no cautelen la seguridad en los servicios financieros que ofrecen.

Como resultado final de la presente investigación, relacionado a los objetivos planteados, en tal sentido en relación al primer objetivo planteado Analizar si son responsables civiles los bancos en los delitos de Phishing, se concluye que en efecto las entidades financieras deben tener cierto grado de responsabilidad dado que son los proveedores de servicios financieros, por ende, corresponde que se les atribuya responsabilidad, en relación al segundo objetivo, que versa sobre definir cuál es el tipo de responsabilidad que se atribuiría a los bancos en el delito de Phishing, se llega a la conclusión que luego de realizar una revisión exhaustiva, el tipo de responsabilidad que les corresponde asumir a los bancos sería la de la responsabilidad civil y administrativa, tal y como se ha mencionado en líneas precedentes, ello en merito a que los bancos, son los encargados de dotar de seguridad a los usuarios.

IV. CONCLUSIONES

En relación al **objetivo específico 1**, a decir de los autores, urge la necesidad de regular las conductas ilícitas de los sujetos activos que lesionen a los usuarios de las entidades financieras, para sancionar su conducta ilícita, de esta manera se debe de tomar en consideración que los bancos tienen grado de responsabilidad cuando se lesiona al usuario, para obtener estos resultados se ha sistematizado la información y se llega a la conclusión que las entidades financieras en los casos de delitos informáticos como lo son el Phishing, deben de responder civilmente, frente al aprovechamiento de los sujetos activos que buscan lucrar con las personas que desconocen las nuevas tecnologías.

En relación **objetivo específico 2,** se llega a la conclusión que, debido a la estructura de nuestro marco normativo, las entidades financieras podrían responder civilmente**,** toda vez que al ser proveedores de servicios tienen una relación contractual con las personas que son sus usuarios, razón por la cual son responsables civil y administrativamente, por ende, le corresponde al INDECOPI, realizar la defensa de los sujetos pasivos.

Objetivo general, Se llega a la conclusión, que a nivel normativo la legislación jurídica es nula y ello se refleja con la dación de normas que no contemplan la figura delictiva del delito de Phishing, razón por la cual se debe de legislar en materia informática, incluyendo en nuestra legislación la figura delictiva del Phishing informático dado que en efecto en nuestro país la legislación es nula Por otro lado, respecto a otorgar las entidades financieras responsabilidad de cualquier tipo, razón por la cual se debe de sancionar a las entidades financieras, para poder imputar sanciones a los proveedores de servicios financieros, las entidades financieras tienen grado de responsabilidad toda vez que ellos son los encargados de otorgar seguridad jurídica.

REFERENCIAS

Acosta, Benavides, García (2020). *Delitos Informáticos: Impunidad Organizacional Y Su Complejidad En El Mundo De Los Negocios.* https://www.redalyc.org/revista.oa?id=290

Álvarez. A (2020). *Clasificación de las investigaciones*. Universidad de Lima, Facultad de Ciencias Empresariales y Económicas, Carrera de Negocios Internacionales. https://repositorio.ulima.edu.pe/handle/20.500.12724/10818

Astete, J. (Ed.). (2023). *Los delitos informáticos con mayor incidencia y los bancos más afectados*. diario gestión. https://gestion.pe/peru/ciberataques-delitos-informaticos-con-mayor-incidencia-y-los-bancos-mas-afectados-mininter-gobierno-hackers-delincuentes-ciberneticos-noticia/

Cabrera, P. (2017). *Derecho Penal Parte Especia*l. Lima: Moreno

Espinoza (2017). *Derecho penal informático: deslegitimación del poder punitivo en la sociedad de control*.

Flores, C. (2017). *El phishing como comportamiento penalmente relevante*. http://opac.pucv.cl/pucv_txt/txt-4000/UCC4478_01.pdf

Fuentes Garrido, K. V. (2021). *Modificación de la Ley 30096 para incorporar los Delitos de Phishing, Pharming Y Carding como Delitos Penalizables con prisión, para reducir la ciberdelincuencia, Lima 2019* [Universidad Señor de Sipan].

Gamio, A. (2018). *Límites a la creación voluntaria de patrimonio de afectación para la salvaguarda de bienes*. Revista de derecho de la universidad de Montevideo, 147.

García Forero, L. F. G. (2020). *Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo.* [Tesis de grado. Universidad Piloto de Colombia]. http://repository.unipiloto.edu.co/handle/20.500.12277/9545

García, V. (Ed.). (2019). *¿cómo está avanzando la ciberseguridad en el Perú? breve aproximación al marco normativo*. Actualidad Jurídica Uría Menéndez.

Gupta, S., & Bansal, H. (2023). *Trust evaluation of health websites by eliminating phishing websites and using similarity techniques. Concurrency and Computation: Practice & Experience,* 35(21). https://doi.org/10.1002/cpe.7695

Hancco, E. (2018), en su investigación titulada, *La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096, Perú – 2017.* http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/6436/DEhazaey.pdf?sequence=1&isAllowed=y

Herrero, Torres, Vivas (2021). Smarthphone Addiction, Social Support, And Cybercrime Victimization: A Discrete Survival And Growth Mixture Model. https://www.redalyc.org/journal/1798/179870642005/

Hidalgo coronel, C. N., y Solano vidal, G. S. (2021). *El phishing como conducta delictiva no regulada en el ordenamiento jurídico peruano*. Propuesta de incorporación del artículo 7-a en la Ley de Delitos Informáticos 30096. [Tesis de 30 Grado, Universidad Nacional del Santa]. http://repositorio.uns.edu.pe/handle/UNS/3849

Ley Nº 30096 de 2013. *Ley de Delitos Informáticos*. 22 de octubre de 2013. Recuperado de https://spij.minjus.gob.pe/spij-ext-web/detallenorma/H1088463

Ley Nº 30171 de 2014. *Ley que modifica la Ley 30096, Ley de Delitos Informáticos.* 10 de marzo de 2014. https://repositorio.umsa.bo/bitstream/handle/123456789/13890/T4774.pdf?sequence=1&isAllowed=y

López, J. (2019). *Métodos y técnicas de detección temprana de casos de phishing*, Cataluña, Universitat Oberta de Catalunya.https://spij.minjus.gob.pe/spij-extweb/detallenorma/H1097704

Mayer, L. (2017). *El bien jurídico protegido en los delitos informáticos. Revista chilena de derecho,* 44(1), 261-285. Doi: http://dx.doi.org/10.4067/S0718-34372017000100011

Mayer, L. (2018). *Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. Ius et Praxis*, 24(1), 159- 206. https://dx.doi.org/10.4067/S0718-00122018000100159

Mayer, Oliver (2020). *El Delito De Fraude Informático: Concepto Y Delimitación.* https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S07192584202000010 0151&lang=es

Mengoa, M. (2021). *Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú.* https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/62379/Me ngoa_VMM-SD.pdf?sequence=1

Mori, F. (2019). *Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de Lima, periodo 2008 al 2012.* http://repositorio.unfv.edu.pe/bitstream/handle/UNFV/3519/UNFV_MORI _QUIROZ_FRANCISCO_MAESTRIA_2019%20%283%29.pdf?sequenc e=1&isAllowed=y

Opara, C., Chen, Y., & Wei, B. (2024). *Look before you leap: Detecting phishing web pages by exploiting raw URL and HTML characteristics. Expert Systems with Applications,* 236(121183), 121183. https://doi.org/10.1016/j.eswa.2023.121183

Ortiz Campos, N. J. (Ed.). (2019). *Normativa Legal sobre Delitos Informáticos en Ecuador Legal Regulations on Cybercrimes* in Ecuador (Vols. 4, No. 1, 2019). Rev. Hallazgos21, http://revistas.pucese.edu.ec/hallazgos21/

Palacios Rodríguez, Oscar Alejandro. (2021). *La teoría fundamentada: origen, supuestos y perspectivas. Intersticios sociales*, (22), 47-70. Epub 03 de noviembre de 2021. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-49642021000200047&lng=es&tlng=es.

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

Paredes, J. (2017). *De los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, en el período 2009-2010.* https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/10314/Paredes_pj.pdf?sequence=3&isAllowed=y

Salvi, M. (2019) *El Phishing en la Argentina* [Tesis de Grado, Universidad Siglo 21]. https://repositorio.uesiglo21.edu.ar/handle/ues21/16066

Shoaib, M., & Umar, M. S. (2023). *An investigation in detection and mitigation of smishing using machine learning techniques. Social Network Analysis and Mining,* 13(1).

Sowmya, Mary Anita, T. (2023) *International Journal of Intelligent Systems and Applications in Engineering*

Tacilio Yauli, E. F. (2016). *Metodología de la Investigación Científica. Universidad Jaime Bausate y Meza*. Recuperado de http://repositorio.bausate.edu.pe/handle/bausate/36

Tellez Valdés, J. (2008). *Derecho Informático. México*: Editorial Graw Hill.

Terán, T. (2016). *La necesidad de incorporar en el código penal el tipo penal de falsificación informática* (Phishing).

Tian, C. (annie), Jensen, M. L., & Durcikova, A. (2023). *Phishing susceptibility across industries: The differential impact of influence techniques. Computers & Security,* 135(103487), 103487. https://doi.org/10.1016/j.cose.2023.103487

Tóala, G. M. T., y Briones, A. A. M. (2019). *Importancia de la enseñanza de la metodología de la investigación científica en las ciencias administrativas. Dominio de las Ciencias*, 5(2), 56-70

Zapata, J. (2019). *El delito de estafa en la modalidad "Phishing" a través de internet y sus medios probatorios en Venezuela*. Universidad de Carabobo.

ANEXOS

Matriz de sistematización de fuentes referenciales

Tipo de fuente	Titulo	Fecha	Autor (es)	Editorial-URL-DOI-ISBN
Delitos Informáticos	*Impunidad Organizacional Y Su Complejidad En El Mundo De Los Negocios*	2020	Acosta, Benavides, García	https://www.redalyc.org/revista.oa?id=290.
Universidad de Lima, Facultad de Ciencias Empresariales y Económicas, Carrera de Negocios Internacionales	*Clasificación de las investigaciones*	2020	Álvarez. A	https://repositorio.ulima.edu.pe/handle/20.500.12724/10818
diario gestión	*Los delitos informáticos con mayor incidencia y los bancos más afectados*	2023	Astete, J.	https://gestion.pe/peru/ciberataques-delitos-informaticos-con-mayor-incidencia-y-los-bancos-mas-afectados-mininter-gobierno-hackers-delincuentes-ciberneticos-noticia/
Pontificia Universidad Católica de Valparaíso	. *El phishing como comportamiento penalmente relevante*	2017	Flores, C.	http://opac.pucv.cl/pucv_txt/txt-4000/UCC4478_01.pdf

Universidad Señor de Sipan	*Modificación de la Ley 30096 para incorporar los Delitos de Phishing, Pharming Y Carding como Delitos Penalizables con prisión, para reducir la ciberdelincuencia, Lima 2019*	2021	Fuentes Garrido, K. V.	https://repositorio.uss.edu.pe/handle/20.500.12802/8345
Tesis de grado. Universidad Piloto de Colombia.	*Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo*	2020	García Forero, L. F. G.	http://repository.unipiloto.edu.co/handle/20.500.12277/9545
Universidad nacional de san Agustín de Arequipa	*La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096*	2018	Hancco, E.	http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/6436/DEhazaey.pdf?sequence=1&isAllowed=y
Tesis de 30 Grado, Universidad Nacional del Santa	*El phishing como conducta delictiva no regulada en el ordenamiento jurídico peruano*. Propuesta de incorporación del artículo 7-a en la Ley de Delitos Informáticos 30096.	2021	Hidalgo coronel, C. N., y Solano vidal, G. S.	http://repositorio.uns.edu.pe/handle/UNS/3849
Universidad César Vallejo. (tesis)	Inversión pública y cobertura de los servicios básicos en la Municipalidad Provincial de Tocache, 2020	2021	Lozano Gago, G	https://repositorio.ucv.edu.pe/handle/20.500.12692/57807

Minjus	Ley Nº 30096 de 2013. *Ley de Delitos Informáticos*	2013	MINJUS	de https://spij.minjus.gob.pe/spij-ext-web/detallenorma/H1088463
scielo	*El Delito De Fraude Informático: Concepto Y Delimitación*	2020	Mayer, Oliver	https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S071925842020000100151&lang=es

PORCENTAJE DE TURNITIN

La comisión del phishing: una revisión de su literatura científica, en el marco de la ley 30096.

INFORME DE ORIGINALIDAD

15%	15%	1%	6%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.ucv.edu.pe Fuente de Internet	8%
2	hdl.handle.net Fuente de Internet	4%
3	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	3%
4	"Inter-American Yearbook on Human Rights / Anuario Interamericano de Derechos Humanos, Volume 16 (2000)", Brill, 2004 Publicación	<1%
5	www.dealerworld.es Fuente de Internet	<1%
6	www.ondanaranja.com Fuente de Internet	<1%
7	www.slideshare.net Fuente de Internet	<1%