FACULTAD DE DERECHO Y HUMANIDADES
ESCUELA PROFESIONAL DE DERECHO

TESIS

“La Ciberseguridad en el Comercio Electronico y los Riesgos de Phishing en tiempos de Pandemia. Chiclayo 2022”

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADA

Autora:

Bach. Zamora Vasquez Karin Junet

https://orcid.org/0000-0002-7581-4477

Asesora:

Mg. Delgado Fernandez Rosa Elizabeth

https://orcid.org/0000-0001-6995-3609

Línea de Investigación

Desarrollo Humano, Comunicación y Ciencias Jurídicas para enfrentar los Desafíos Globales

Sublínea de Investigación

Derecho público y Derecho privado

Pimentel – Perú

2024

DECLARACIÓN JURADA DE ORIGINALIDAD

Quien suscribe la DECLARACIÓN JURADA, soy la Bachiller **ZAMORA VASQUEZ KARIN JUNET,** de la Escuela Profesional de Derecho, Facultad de Derecho y Humanidades de la Universidad Señor de Sipán S.A.C, declaro bajo juramento que soy autora del trabajo titulado:

"LA CIBERSEGURIDAD EN EL COMERCIO ELECTRONICO Y LOS RIESGOS DE PHISHING EN TIEMPOS DE PANDEMIA. CHICLAYO 2022"

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética del Comité Institucional de Ética en Investigación de la Universidad Señor de Sipán, conforme a los principios y lineamientos detallados en dicho documento, en relación con las citas y referencias bibliográficas, respetando el derecho de propiedad intelectual, por lo cual informo que la investigación cumple con ser inédito, original y autentico.

En virtud de lo antes mencionado, firma:

Zamora Vasquez Karin Junet	DNI: 73967673	

Pimentel, 26 de mayo del 2024.

REPORTE DE SIMILITUD TURINITIN

Reporte de similitud

NOMBRE DEL TRABAJO
"La Ciberseguridad en el Comercio Electr onico y los Riesgos de Phishing en tiemp os de Pandemia. Chic

AUTOR
Karin Junet Zamora Vasquez

RECUENTO DE PALABRAS
18646 Words

RECUENTO DE CARACTERES
101051 Characters

RECUENTO DE PÁGINAS
59 Pages

TAMAÑO DEL ARCHIVO
127.9KB

FECHA DE ENTREGA
Oct 9, 2024 2:58 PM GMT-5

FECHA DEL INFORME
Oct 9, 2024 2:59 PM GMT-5

23% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 21% Base de datos de Internet
- 2% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 9% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 8 palabras)

“LA CIBERSEGURIDAD EN EL COMERCIO ELECTRONICO Y LOS RIESGOS DE PHISHING EN TIEMPOS DE PANDEMIA. CHICLAYO 2022”

Aprobación del jurado

MG. OBIOL ANAYA ERIK FRANCESC

Presidente del Jurado de Tesis

MG. INOÑAN MUJICA YANNINA JANNETT

Secretario del Jurado de Tesis

MG. DELGADO FERNANDEZ ROSA ELIZABETH

Vocal del Jurado de Tesis

“LA CIBERSEGURIDAD EN EL COMERCIO ELECTRONICO Y LOS RIESGOS DE PHISHING EN TIEMPOS DE PANDEMIA. CHICLAYO 2022”

Resumen

La investigación estableció como problema el incremento de los delitos cibernéticos *phishing* frente al comercio electrónico en tiempos de pandemia, Chiclayo, 2022, para ello estableció como objetivo general determinar si la ciberseguridad ayudara a mejorar el comercio electrónico y evitara los riesgos de phishing en tiempos de estado de emergencia, lo cual fue desarrollado con una metodología de tipo cualitativa, con el diseño no experimental, los cuales ayudaron a establecer como participantes a Jueces Penales, Abogados especialistas en derecho penal y fiscales, ya que a través de sus respuestas lograron sustentar correctamente que es necesario implementar sistema de seguridad digital para evitar el aumento de la ciberdelincuencia, llegando a la conclusión, que se ha logrado determinar que a través de una adecuada ciberseguridad se alcanzara a mejorar convenientemente el comercio electrónico, es por ello que se debió establecer mecanismos de actualizaciones de protección de datos digitales, capacitación al personal judicial y policial en delitos informáticos, a ello se le debe sumar la protección a través de software en las distintas empresas que manejan datos de clientes, ya que ha sido evidenciado durante el tiempo de pandemia que estos delitos se incrementaron, afectado directamente a la sociedad sin que existan mecanismos adecuados para su adecuada reducción.

Palabras claves: Phishing, Ciberseguridad, Comercio, electrónico

Abstract

The research established as a problem the increase in cybercrimes (phishing) in the face of electronic commerce in times of pandemic, Chiclayo, 2022, for this purpose it established as a general objective to determine if cybersecurity would help improve electronic commerce and avoid the risks of phishing in times of state of emergency, which was developed with a qualitative methodology, with a non-experimental design, which helped establish Criminal Judges, Lawyers specializing in criminal law and prosecutors as participants, since through their responses they achieved correctly support that it is necessary to implement a digital security system to avoid the increase in cybercrime, reaching the conclusion that it has been determined that through adequate cybersecurity it will be possible to conveniently improve electronic commerce, which is why it was necessary establish mechanisms for updating digital data protection, training judicial and police personnel in computer crimes, to this must be added protection through software in the different companies that handle customer data, since it has been evidenced over time During the pandemic, these crimes increased, directly affecting society without adequate mechanisms for their adequate reduction.

Keywords: Phishing, Cybersecurity, E-commerce

I. INTRODUCCIÓN

A nivel internacional se comprende que la ciberdelincuencia está dentro de uno de los desafíos más problemáticos que perjudica al mundo entero, y si a la par tenemos en consideración que los últimos años incremento la utilización del internet para efectuar un sinfín de actividades. Por lo cual la ciberdelincuencia actúa en un espacio radicalmente diferente a lo que comúnmente estamos familiarizados, esto es, un ámbito virtual, por lo que dicha característica promueve la impunidad.

En ese sentido, es importante reconocer lo mencionado por Mateos (2020) quien llega a definir a la ciberdelincuencia, como un conjunto de acciones realizadas por una propiedad o un sistema informático que se considera ilegal. En otras palabras, es el Departamento de Delincuencia Tradicional el que utiliza exponencialmente las nuevas tecnologías para difundir y desarrollar.

Así mismo, se puede asegurar que la ciberdelincuencia desarrollará conforme incremente la cantidad de usuarios, lo cual nos conlleva a pensar que por ende también incrementará la cantidad y modalidades de ciberdelincuencia. De acuerdo a lo que estamos señalando podemos darnos cuenta que los ciberdelitos se apoyan de cierto modo en la tecnología, lo cual conlleva que este en una evolución constante.

Sin embargo, sobre la naturaleza de la internet profunda, Devia (2021) precisa en principio, podemos decir que toda la superficie de contenido de Internet, que no forma parte del sitio web que se muestra o puede ser encontrada por varios motores de búsqueda, está oculta fuera del espacio general y público de la navegación específica del sitio web de Internet.

Es por ello que el desarrollo de la mayoría de nuestras actividades requiere del empleo de la internet superficial, como los que se mencionaran a continuación: enviar y recibir correos, realizar diversas búsquedas, ejecutar pagos, entre otros más; sin embargo también hay la internet profunda, que tiene también como objetivos, cometer ilícitos.

Además, la Unión Internacional de Telecomunicaciones (2014), mediante el informe Comprensión de ciberdelincuencia: fenómenos, dificultades y respuesta jurídica, precisa que el delito cibernético, en el verdadero sentido de la palabra

“delito informático”, implica cualquier actividad ilegal a través de sistemas electrónicos que amenace la seguridad de los sistemas informáticos y los datos que procesan. En general, el ciberdelito (delitos informáticos) implica cualquier actividad ilegal en un sistema informático o red informática o través de él, incluida la extracción y difusión ilegal de información o la difusión a través de sistemas informáticos o redes informáticas.

Al mismo tiempo, la ciberseguridad es el mecanismo apropiado para el progreso del análisis y gestión de riesgos relacionados al ciberespacio. En este aspecto, este mecanismo busca contrarrestar toda aquella amenaza que se desate del uso del ciberespacio. En ese orden de ideas, podemos llegar a la conclusión que la ciberseguridad, mediante un conjunto de actuaciones, trata de asegurar la información en el ciberespacio.

Tal cual hemos señalado, los ataques al ciberespacio han incrementado esto en relación a la cantidad como al procedimiento, y cada vez son mucho más sofisticados. Al respecto, Fernández y Martínez (2018) afirman que los *cybertocks* son ejemplos de amenazas cibernéticas para ataques de denegación de servicios y software de pago, asimismo para robo de datos e información piratería de dispositivos móviles y sistemas industriales e infraestructura crítica.

A nivel nacional se ha podido evidenciar que la ciberdelincuencia desde los inicios de la legislación peruana ha sido regulado en el artículo 186 en el inciso 3 dentro del código penal de 1991 en donde se consideraba como un delito autónomo y propio ya que existía un agravante del delito de hurto, por lo que se encontraba prescrito en el artículo 185 posterior a ello los delitos informáticos fueron previstos en el código penal en los artículos 207- A al 207 -D, es así que al encontrarse leyes especiales que contemplaban la denominada ley delitos informáticos se buscaba determinar los delitos contra los datos y los sistemas informáticos así como así como la libertad sexual y la indemnidad, posteriormente se promulgó la ley 30171 la cual modificó la ley de delitos informáticos con la finalidad de adecuar estándares de ciberdelincuencia para incorporar nueva tipificación de los delitos cibernéticos ilícitamente informáticos.

Esto comprende que a partir de nuestra legislación constitucional se ha venido reglamentando una serie de normas que, de algún modo, han reglamentado el manejo del uso de la tecnología de la información. En ese aspecto, por ejemplo, tenemos la promulgación de la ley de la acción constitucional de hábeas data; la ley sobre el derecho de autor o protección jurídica del software; la ley de firmas y certificados digitales, entre otras.

Todo este avance normativo se presenta cuando el estado peruano suscribe un Convenio de Budapest, instrumento internacional que busca combatir y erradicar la ciberdelincuencia. En ese entendido, definimos a los delitos informáticos no como nuevos comportamientos ilícitos, sino como nuevas formas en que se desarrollan los delitos mediante el uso de medios informáticos conectados a Internet o teniendo acceso físico a un dispositivo equipado con un puerto que permite la conexión al sistema y a los archivos contenidos en el mismo (Tenorio, 2020).

Es así que, con el avance de la tecnología se han presentado diversos grandes desafíos los cuales han expuesto a toda la sociedad a nivel mundial sin embargo el papel catalizador de la tecnología ha enfrentado colectivamente una crisis ya que existen grandes desafíos para las industrias y las organizaciones en brindar una mejor seguridad a la información que poseen pues la protección al sistema informático ha sido debilitado frente al incremento de diversos ciberataques durante la pandemia del 2020 sobre todo obligando adoptar nuevas formas de trabajo y acelerar una transformación digital.

Este medio tecnológico avanzado en el 2020 ha creado que delitos como el *phishing* se incrementen en tiempos de pandemia, ya que según el programa informático ESET analizó que dentro del 61% de las empresas peruanas que han sido encuestadas, sus políticas de seguridad indican que no cuentan con una seguridad de antivirus, tal es así que en el caso de los bancos se genera un modalidad de ciberdelincuencia muy novedosa y requiere que los delincuentes cibernéticos creen una página web falsa de una entidad bancaria para que el usuario, al actualizar sus datos, inconscientemente entregue las claves de sus cuentas bancarias, de modo que estas sean vaciadas (La Gestión, 2020)

Del mismo modo, el 49% de las empresas peruanas han visto un aumento en los ataques cibernéticos después de la pandemia, según el estudio Times of COVID-19 sobre los niveles de riesgo cibernético en América Latina. La encuesta también nos deja ver que el 21% considera que la ingeniería social (phishing) es el ciberataque que más ha aumentado en los últimos años, mientras que el 20% dice que es malware (Ormaza, et al.,2021).

De esta manera, el phishing implica la suplantación o clonación de ciertos sitios web, entre los cuales están, las páginas webs de las diversas entidades bancarias, pues algunos especialistas indican que dicho mecanismo puede ser considerado como una estafa informática, ya que en esta modalidad se caracteriza por utilizar un correo electrónico, un logotipo y un link similares o parecidos a los de la entidad financiera en cuestión, en función a ello, la investigación requiere que se cree un mecanismo de ciberseguridad con el fin de poder mejorar el comer electrónico en los tiempos de pandemia, evitando que se ejecute riesgos de phishing (Ormaza, et al.,2021).

Desde el **ámbito local**, en Lambayeque, se tiene que actualmente, las empresas están cada vez más expuestas al uso de telecomunicaciones y dispositivos personales, y hay un aumento significativo de los ciberataques ya que les preocupa que la epidemia haya aumentado su presupuesto de ciberseguridad en un 24% y lo haya reducido en un 10% (Ministerio de Justicia y Derechos humanos, 2022).

Esto ha generado que dentro de la región Lambayeque en el año 2020 se han presentado casos de phishing donde empresas como Claro, manifiestan que esta modalidad es una estafa virtual en donde suplantan la identidad a través de páginas web fraudulentas, para que ilegalmente obtengan acceso a los datos personales o cuentas financieras, a través de la suplantación de identidad de manera virtual, pues frente a este caso, la compañía determina que el usuario tiene que tener en cuenta la página que tengan certificado de seguridad (Ministerio de Justicia y Derechos humanos, 2022).

Finalmente se analiza que la utilización del internet tiene una considerable importancia en toda la humanidad actual, pues, con el paso de los años, la mayor

parte de nuestras actividades ostenta, en mayor o menor medida, un soporte virtual. No obstante, cabe mencionar que en estos últimos años también se han agudizado o surgido diversas modalidades de cibercriminalidad como él phishing. Entonces podemos darnos cuenta que, conforme la sociedad avanza con la tecnología también se incrementa a nuevas conductas delictivas, como la ciberdelincuencia (Roman, 2020).

Así mismo se tuvo, como antecedentes de estudio a Estrada, et al. (2021) en su artículo tiene como propósito principal, analizar al Phishing como delito en la legislación colombiana, para ello utilizo una estructura metodológica de tipo mixta, lo que permitió concluir que las personas que cometen o están cometiendo ciberdelitos son, en este caso particular, delitos fraudulentos, hackers o ciberdelincuentes que se benefician de sus conocimientos de los expertos en informática “networking, programación, etc”. sistema con el fin de obtener información privada. A partir del análisis realizado sobre diferentes tipos de delitos informáticos, el phishing es una actividad muy lucrativa y se considera ilegal en la mayoría de las leyes internacionales, que no están consagradas en nuestras normas penales.

Quevedo (2020) en su estudio planteo como objetivo principal, analizar la eficacia de la prueba del ciberdelito, para ello utilizo una estructura de análisis de documento, lo que permitió concluir que la actividad delictiva se ha visto significativamente afectada por la creación de nuevos tipos de delitos por Internet y sirviendo como herramienta para cometer otros delitos tradicionales. Por tanto, la investigación del llamado ciberdelito requiere el conocimiento de las características técnicas básicas de Internet (red global con conexiones instantáneas y marco de red descentralizado basado en la representación digital de la información) y permite conexiones en tiempo real entre personas, su ubicación.

Molinos (2020), busco analizar el fraude informático o ciberdelito desde la perspectiva penal, para ello utilizo una estructura metodología de tipo cuantitativa, lo que permitió concluir que la relación entre el delito y la informática se explica desde la perspectiva del delito tradicional, siendo la tecnología la herramienta para cometer los delitos. Cuando se utiliza la informática, ataca un sistema como datos o programas. La doctrina, al igual que la jurisprudencia, utiliza términos diferentes

para referirse al delito cibernético y, por otro lado, el interés legal, que proporciona diferentes clasificaciones y términos relacionados con él, a menudo tiene dificultades para vincular las nuevas estadísticas delictivas con las tasas de delitos cibernéticos, tanto debido a la diversidad como ciberdelincuencia.

Horianski (2020), en su investigación de la delincuencia cibernética y la protección penal ante los avances tecnológicos, la cual fue desarrollada con una estructura de tipo documental, lo que permitió concluir que el derecho penal tiene un papel fundamental que desempeñar y se debe avanzar lo suficiente en el proceso de investigación de los delitos cibernéticos. Una buena técnica para incluir el ciberdelito en el Código Penal debe ir acompañada de la técnica de procedimiento para investigar estos casos, muchas veces muy compleja, esto significa que los abogados y jueces especiales deben cumplir con normas penales especiales.

Torrente (2020), en su investigación, analiza las diversas actividades que se realizan online a través de un comercio electrónico en la ciudad de Panamá, pues frente a ello se utilizó una estructura de tipo descriptiva con enfoque cualitativo, donde llegó a concluir que las comunicaciones comerciales se pueden realizar entre países locales o diferentes, ahora la economía mundial está a la vanguardia de las grandes herramientas electrónicas, con la mejora de los estándares evolutivos a través del aumento de la tecnología y la cuarta industria, priorizando y tomando en cuenta el proceso global que se presenta en las grandes empresas con el fin de proteger el medio cibernético en que las empresas generan un aumento de calidad y de funcionalidad.

A nivel nacional Chávez (2020), en su investigación sobre la vulneración de la intimidad personal frente a los delitos de datos y sistemas informáticos, para ello se utilizó una estructura de análisis de documento, lo que permitió concluir que el Estado, a través del Poder Judicial, brinda capacitación permanente a los profesionales del derecho de la Corte Superior de Justicia de Lima Norte sobre los principios generales de protección de la información pública y privada (información sensible, control, restricción de la información). Los delitos contra la persona, la seguridad personal, los daños causados por el delito de Phishing a los datos y los

sistemas informáticos afectan significativamente al derecho fundamental a la privacidad personal.

Chuco (2023) en su investigación sobre el delito de fraude informático frente al Código Penal Peruano, para ello se utilizó una estructura de tipo básico con diseño fenomenológico, donde se llegó a concluir que la falta de información adecuada sobre la tecnología informática es un factor crítico en el impacto del ciberdelito en la sociedad en general, requiriendo cada vez más conocimientos en tecnologías de la información, lo que permite un marco contextual aceptable para hacer frente a este tipo de situaciones. Al realizar un análisis legal comparativo con otros países, se determinó que Perú es un país que ciertamente controla el ciberdelito de fraude informático, sin embargo, lo hace mal porque es común, lo que genera algunos vacíos legales, lo que imposibilita las investigaciones informáticas forenses.

Villavicencio (2020) en su artículo jurídico sobre los delitos informáticos como el *Phishing*, el cual fue desarrollado con una estructura metodología de tipo cualitativa con análisis documental, lo que permitió concluir que el objeto de la Ley de Delitos Cibernéticos es prevenir y sancionar las conductas ilícitas que afecten a los sistemas y datos informáticos, contra los bienes, la confianza pública y la libertad sexual cometidos mediante el uso de las TIC. Las estadísticas penales de acceso ilícito, controladas en el artículo 2, están tipificadas como delito de actividad normal, ya que este acto ilícito constituye una violación de las medidas de seguridad de un sistema informático.

Astorayme (2023) su estudio direccionado al análisis de los vacíos legales que presenta el delito informático Phishing en el Nuevo Código Penal peruano, para ello se utilizo una estructura de tipo básica con enfoque cualitativo, lo que permitió concluir que la falta de información adecuada sobre las limitaciones de la tecnología de la información es un factor crucial en el impacto del ciberdelito Phishing en la sociedad en general, requiriendo cada vez más conocimientos en tecnología de la información, lo que permite un marco contextual aceptable para hacer frente a tales situaciones. Las nuevas formas de comercio online son un claro ejemplo de cómo los delitos pueden manifestarse de diferentes formas, por lo que es necesario crear

herramientas legales efectivas para abordar esta problemática, cuyo único propósito es sustentar el marco legal.

Peralta y Roa (2020), en sus averiguaciones examinan el impacto que ha causado los presentes delitos cibernéticos en relación a los procedimientos que implica el comercio electrónico, es por ello que esta investigación ha sido debidamente presentada para obtener el título profesional de abogado de la prestigiosa Universidad de Córdova, en el cual se llega a la conclusión que los cambios precipitados resultantes de la globalización son incontables y por ende cada vez más interesantes, y destapan oportunidades esto es no solo económicas sino también culturales para toda la comunidad. Es de este modo que orientados por el progreso tecnológico de información y de comunicación, se ha logrado establecer una herramienta que acrecienta las relaciones, asimismo el conocimiento y por ende los aspectos del desarrollo personal, asimismo organizacional, local e internacional. Entonces debemos señalar que el comercio electrónico no solo crea sino también organiza una mejor manera de pensar que se acopla al mundo digital; asimismo podemos observar que las maneras tradicionales de hacer negociaciones se están dejando de lado, para reemplazarlas de manera gradual, esto por el hecho de que las negociaciones últimamente se transan de manera electrónica y por ende se puede tener en bases de datos informáticas sin que haya la existencia de documentos en físicos.

A nivel local, Alcantara & Delgado (2024) en su investigación comprenden la criminalidad que se presenta en lo informático y tecnológico a través del delito contra el sistema financiero, para ello se utilizó una estructura básica con enfoque cualitativo, en donde manifiestan que el uso de la informática ha permitido que surjan diversos delictivos que perjudiquen la integridad cibernética de la persona como es el caso del robo de identidades personas, frente a ello determina que el objetivo de la investigación es poder salvaguardar los interés de las personas dentro de un sistema financiero, ya sea aplicando una valoración economía frente a los daños ocasionados en el sistema informático, para ello toma como recomendación aplica dentro del sistema informático un AISI para reparar el daño ocasionado frente a un perjuicio tecnológico en donde se vele por la seguridad nacional y personal.

Parra (2020), en su investigación sobre la ciber seguridad y su proyecto legal como esquema nacional, para ello se utilizó una estructura de tipo básica con enfoque cuantitativo, donde concluye que una de las mejores formas de concienciar sobre la ciberseguridad es compartir experiencias de ciberataques (Phishing) con la población, hasta que salgan a la luz las vulnerabilidades de las empresas o estados afectados. La ciberdefensa tiene la función de protección, detección, respuesta y recuperación, mientras que la ciberseguridad será un paso para garantizar la protección de los ordenadores y sistemas cibernéticos a través de un andamiaje de herramientas que van desde el sistema legal hasta el medio técnico.

Llaque y Piñin (2020), en su investigación requieren aplicar un modelo de comercio electrónico dentro de la ciudad de Chiclayo, para ello se utilizó una estructura investigativa de tipo básica, donde se concluyó que dentro de la ciudad de Chiclayo, las compras online que se realizan no permiten seguridad a la sociedad, por lo que muchas veces, estas compras se han prestado para poder adquirir información personal del cliente, llegando a cometer un delito cibernético que pone en riesgo al consumidor y a la empresa que brinda el servicio de compra, tal es el caso que se recomienda que la empresa cuente con una seguridad cibernética para poder aumentar las motivación de poder consumir un producto seguro.

Villanueva (2023), en su investigación sobre la medida de prevención de los delitos informáticos establecidos en la Ley 30096 y el bloqueo dinámico del IP, para ello utilizo una estructura metodológica de tipo correlacional con enfoque cuantitativo, llegando a concluir que las transacciones electrónicas se protegerán bloqueando las direcciones IP dentro del comercio electrónico, ya que la autenticación por parte de un solo usuario e iniciar sesión en una dirección IP estática es la forma más eficiente de prevenir ataques de piratas informáticos, piratería informática o de contraataque. Teniendo en cuenta que se identificó que, por los resultados, bloquear IP dinámica dentro del soporte informático sería una medida de seguridad que previene el ciberdelito, con un 65% de los 20 jueces que creen que la propuesta de investigación es aplicable.

Delgado (2022), en su investigación interpreta los delitos informáticos que han sido cometido a través de las diversas redes sociales, para ello se utilizó una

estructura metodología de tipo básica con enfoque mixto, con análisis documental, en donde se concluye que los legisladores deben revisar la ley actual de delitos informáticos para ver si el tipo actual de delitos informáticos cubre todas las actividades que amenazan a los sistemas y computadoras con su uso adecuado, los ciudadanos de la rama. Análisis experto. Debe contener la naturaleza de la tecnología informática, asimismo los diversos pasos para restaurar evidencia informática, su indagación y los requisitos de un informe pericial que al mismo tiempo permita la credibilidad de la evidencia como medio de prueba

Respecto a las teorías relacionadas al tema es evidente que empleo de la internet tiene una considerable influencia en nuestro mundo actual, pues, con el transcurrir del tiempo, gran parte de actividades cotidianas requiere, ya sea en mucha o poca medida, un soporte virtual. La supeditación de este medio de comunicación se ve más acrecentado con la llegada de la pandemia por el COVID-19. Sin embargo, es importante resaltar que en los últimos años también se han agudizado o aparecido muchas modalidades de cibercriminalidad. Esto deja ver que, mientras la sociedad progresa con la tecnología también se logra ver la existencia de nuevas conductas delictivas, como la ciberdelincuencia. Cabe mencionar que, si bien hoy en día hay instrumentos de lucha contra este flagelo, no es menos cierto que las técnicas para la configuración de dichos delitos vienen innovando cada vez con más fuerza. En el presente documento desarrollaremos y analizaremos qué y cuales son la clase de delitos que se encuentran en evolución continua y por ende el origen de ellos.

En 1997, un grupo de expertos se reunió para debatir los problemas que incidían sobre la delincuencia en internet, y años después dicha reunión sirvió de base para el Convenio sobre Ciberdelincuencia, también conocido como Convenio de Budapest.

Tenorio (2020) señala que un nuevo comité se encargó de la elaboración de la herramienta con el asesoramiento de expertos y la participación de países miembros y no miembros del Consejo.

Así mismo ya en noviembre de 2001, se firmó el Consejo Europeo de Ciberdelincuencia en Budapest, y la ciberdelincuencia se clasificó en cuatro grupos

principales: 1) Delitos contra la confidencialidad, la integridad y el acceso a los datos y sistemas informáticos. 2) Delitos informáticos 3) Delitos relacionados con el contenido y 4) Delitos relacionados con la propiedad intelectual y la infracción de derechos relacionados.

Tenorio (2020), precisa que a este tratado se le considera que el primer acuerdo internacional sobre delitos cometidos a través de Internet y otros sistemas informáticos, que busca brindar herramientas básicas y procesales en derecho penal, así como potenciar la capacidad de cada país a través de la cooperación internacional en tiempo real en la lucha contra el ciberdelito.

El presente convenio surgió en un contexto donde el internet se desarrollaba tecnológicamente. Ahora la globalización término muy escuchado en los últimos años genera que el internet evolucione y logre cruzar las fronteras, lo que produce que se modifique parte de la economía.

Es así que Salom (2019) precisa que “El propósito de la Convención es legislar en diferentes países que aprueben no solo asuntos relacionados con el derecho penal significativo, sino también el procedimiento judicial para investigar tales delitos”. (p.136)

En el 2003 se estableció un protocolo complementario al convenio, y se incluyeron conductas como la apología del racismo y la xenofobia mediante el uso de sistemas informáticos, que constituyen una amenaza contra el Estado y la estabilidad democrática. Tales instrumentos internacionales advierten que la comisión de ilícitos se realiza también de modo virtual: los denominados “delitos informáticos”. De esta manera, podemos concluir que el Convenio de Budapest es considerado como el máximo referente que combate la delincuencia informática.

El Perú suscribió del Convenio de Budapest, instrumento internacional que busca combatir y erradicar la ciberdelincuencia. En este sentido, nos referimos al ciberdelito no como “nuevos comportamientos ilegales, sino como nuevas formas de cometer delitos mediante el uso físico de medios informáticos conectados a Internet o el acceso físico a un dispositivo con un puerto que permite una conexión al sistema que proporciona archivos (Tenorio, 2020).

Según Tenorio (2020) entre los principales delitos informáticos se encuentran los siguientes: delitos contra la intimidad; delitos relativos al contenido; delitos económicos, acceso no autorizado y sabotaje (como la piratería), y delitos contra la propiedad intelectual. Además, existe conexión entre la ciberdelincuencia y el delito informático, dado que ambos conceptos no se pueden excluir. (p.12)

Nuestro país integró los delitos informáticos mediante la Ley N° 30096, que fue proclamada el 22 de octubre del 2020; sin embargo, sobre dicha ley se realizaron diversas modificatorias, conforme detallamos a continuación.

El campo de actuación de la ciberdelincuencia es el medio virtual, ahí la persona oculta de alguna manera su identidad, lo cual provoca dificultad para una investigación futura. Por ejemplo, mediante la Deep Web, que también es conocida como internet profunda, que busca de algún modo crear perfiles falsos.

Hoy en día existen diversos procederes y situaciones particulares que no son populares hasta la fecha de hoy, lo cual es una situación que sigue generando de algún modo impunidad. Cabe resaltar que como la ciberdelincuencia se realiza en una plataforma virtual, es muy posible que este tipo de delitos se configuren con el apoyo de personas que se encuentran en diferentes Estados. Por lo tanto, es posible observar nuevos ataques masivos, lo que conlleva pensar que existe una organización criminal.

Para obstaculizar de alguna manera ser afectado de la cibercriminalidad se es recomendable considerar los consejos que se brindan a los usuarios, así como el sentido común que tenemos cada persona y el más importante “principio de desconfianza”, esto es más aun cuando se nos solicitan datos que no son habituales ni comunes. La naturaleza de la cibercriminalidad nos hace comprender que no conoce fronteras, es por ello, que se necesita de una lucha internacional contra estas organizaciones criminales.

Cabe resaltar que es sumamente necesario poner en ejecución la implementación internacional de un sistema que otorgue de alguna manera predisponer los ciberataques; ante ello, España ha creado el Centro Nacional de Protección de las Infraestructuras Críticas. Nuestra legislación sobre delitos informáticos propone un catálogo de sanciones de conductas ilícitas que buscan

evitar impunidad. Es necesario implementar una política criminal global que busque evitar la impunidad, esto es, que frente a problemas globales se busquen soluciones de características similares.

Existen diversas formas y métodos de ciberdelincuencia que constantemente están surgiendo y pueden ser consideradas como actos preparatorios de configuración de un ilícito penal. De ese modo, describiremos los siguientes: phishing, cartas nigerianas, chantajes informáticos, wannaCry, llamadas perdidas, SIM swapping, entre otras.

Las cartas nigerianas es una de las modalidades de ciberdelincuencia antigua, por lo que es distinta a las actuales modalidades que se caracterizan por ser más novedosas y elaboradas. Se le denomina así porque en un principio el remitente se hacía pasar por un ciudadano nigeriano o proveniente de países colindantes.

En términos sencillos, las cartas nigerianas consisten en la recepción de un correo electrónico con información de un usuario desconocido, y donde se anuncia información de alguna herencia o datos bancarios.

En esta modalidad, el tiempo juega un rol fundamental, ya que solicitan que se responda el correo en un plazo, por ejemplo, un día, y para hacerlo creíble envían documentos que aparentan ser oficiales y movimientos bancarios falsos, de modo que la víctima realice la transferencia de dinero.

Los chantajes informáticos son una de las modalidades de ciberdelincuencia muy extendida. Esta se realiza en una llamada donde se indica falsamente que un familiar es víctima de secuestro y se solicita cierta cantidad de dinero.

Hemos advertido, por los diferentes medios de comunicación, que este tipo de modalidad es muy frecuentemente empleada por los ciberdelincuentes. Cabe resaltar que, en esta modalidad, la organización criminal analiza una actividad previa, esto es, conseguir información privada.

Conocida también como secuestros informáticos, es un ataque cibernético que busca meterse de algún modo en la computadora o el ordenador de la siguiente víctima y dañar de algún modo los archivos, base de datos o determinados documentos.

El origen de este tipo de ciberdelincuencia es desconocido, aunque algunos expertos sostienen que, en sus inicios, se solicitaba un rescate mediantebitcoins. Si bien los documentos o archivos no se dañan, lo que sucede es que se convierten en inaccesibles.

Muchos países han incorporado en sus legislaciones tipos penales que buscan contrarrestar este avance criminal. En ese sentido, España ha tipificado esta conducta en el art. 264.1 de su Código Penal: “El que, por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesible datos informáticos”.

Es una de las modalidades de ciberdelincuencia mucho más usual. Consiste en la recepción de una llamada en un determinado teléfono móvil desde un número totalmente desconocido.

Es preciso señalar que, durante el transcurso de la llamada, se advierte que en un buzón de voz se ha dejado un mensaje, entonces al oír dicho mensaje, la persona se suscribe, sin saberlo, a un determinado servicio de mensajería, que pretende facturar un determinado porcentaje de dinero.

Es una modalidad de ciberdelincuencia actual que consiste en dejar sin cobertura a los teléfonos móviles y clonar o cancelar la tarjeta SIM.

Conforme hemos precisado, los ciberdelincuentes se apoyan en diversas modalidades para lograr nuevas formas y métodos de comisión de ilícitos, los mismos que en su mayoría son más calificados.

En el actual contexto del COVID-19, muchas personas, para realizar sus diversas actividades realizar pagos, entrar a una plataforma web para estudiar o trabajar, entre otros, se están apoyando en un soporte tecnológico. En ese sentido, los ciberdelincuentes se están aprovechando del incremento de tal dependencia para llevar a cabo estas prácticas y vulnerar la “seguridad informática”, así como la “integridad, confidencialidad y disponibilidad de los datos o sistemas informáticos”. (Jiménez, 2021)

El phishing es una modalidad de ciberdelincuencia muy novedosa y requiere que los delincuentes cibernéticos creen una página web falsa de una entidad

bancaria para que el usuario, al actualizar sus datos, inconscientemente entregue las claves de sus cuentas bancarias, de modo que estas sean vaciadas.

Respecto a la terminología de esta conducta, Paredes (2020), ha señalado que deriva:

La palabra phishing se utiliza para enviar un correo electrónico con el nombre de un banco que tiene una cadena y un sitio web falso que permite al usuario brindar información confidencial sobre sus cuentas bancarias, tarjeta de crédito o clave (p. 247).

De esta manera, esta modalidad implica la suplantación o clonación de determinados sitios web, entre ellos, las páginas webs de las entidades bancarias. Algunos expertos sostienen que dicho mecanismo puede ser considerado como una estafa informática.

Devia, (2021), precisa lo siguiente:

Esta técnica de registro ilegal de información personal se basa en la confianza de organizaciones confidenciales, y existen muchos tipos y métodos que se pueden usar porque el malware se puede instalar a través de programas maliciosos, como los que se usaban en el pasado. leer (troyanos, gusanos, etc.) en un sistema donde las víctimas tienen diferentes contraseñas (p. 106).

Hoy en día, el correo electrónico ha logrado reemplazar en su mayoría el envío de cartas mediante ciertas agencias, es por ello que hoy en día las entidades financieras emplean la vía electrónica. Este servicio lo que hace es facilitar la concurrencia de ilícitos, específicamente del phishing, puesto que esta modalidad utiliza un correo electrónico, un logotipo y un link similares a los de la entidad financiera.

Con relación al phishing a través de mensajes SMS de telefonía móvil, Salom (2019) indica: “El spam es un mensaje de texto que se envía desde el banco con una respuesta de la misma base de datos del banco”. (p.153)

El phishing es un delito que incentiva de alguna manera a las personas a compartir información netamente confidencial, como por ejemplo, contraseñas y

números de tarjetas de crédito. Al igual que la pesca, hay más de mil formas de atrapar presas, pero existe un método común que es el famoso phishing. Las víctimas de estos delitos reciben correos electrónicos o mensajes de texto a través de una persona u organización de buena reputación, como un asistente, un banco o una oficina gubernamental. Cuando la víctima abre un correo electrónico o un mensaje de texto, encuentra un mensaje para asustarla. El mensaje es que la víctima debe ir a un sitio web y actuar de inmediato o enfrentarse a las consecuencias

Si un usuario está conectado y hace clic en un enlace, será enviado a un sitio web que es una copia del sitio web legal. A partir de ahora, se le pedirá que inicie sesión con su nombre de usuario y contraseña. Si eres lo suficientemente simple, la información de inicio de sesión llegará al atacante, quien la utilizará para robar identidad, robar cuentas bancarias y vender información personal en el mercado negro.

En comparación de otros tipos de amenazas cibernéticas, el phishing no necesita tecnología especial. De hecho, Adam Kojawa, director de MalwareBites Labs, dice: "El phishing es la forma más simple de ciberataque y, al mismo tiempo, la más peligrosa y efectiva. Esto es debido a que ataca a la computadora más vulnerable y a la vez más poderosa del mundo: la mente humana. "En lugar de que los escritores de phishing quieran asumir un riesgo técnico para el sistema operativo de su dispositivo, utilice la 'ingeniería social'. De hecho, los atacantes a menudo recurren al phishing porque no pueden encontrar una falla técnica. ¿Por qué perder el tiempo cuando alguien puede engañarlo y ¿Darle la clave? Uno de los eslabones más débiles en un sistema de seguridad personal es que no verifica la fuente del correo electrónico, sino que es un error oculto en el código de la computadora.

Es fácil encontrar el nombre original "Phishing". El proceso de cometer una estafa de phishing es muy similar al proceso de pesca. Se instala un anzuelo que piensa en engañar a una presa, luego lanzarla y esperar a morderla. En el caso del dígito "ph" en lugar de "F", puede ser el resultado de una combinación de las palabras en inglés "fishing" y "pseudo", pero algunas fuentes se refieren a otra fuente.

En la década de 1970, existía una subcultura de trucos de bajo nivel para explotar el sistema telefónico. Los primeros hackers lo llamaron "Freaks", una combinación de las palabras en inglés "phone" y "freak". En una época en la que ya no se pueden robar computadoras conectadas a la red, enloquecer se ha convertido en una forma común de hacer llamadas gratuitas de larga distancia o comunicarse con números que no figuran en la lista.

Incluso antes de que desapareciera el término "phishing", se describió en detalle un esquema de phishing introducido en 1987 por el grupo internacional de usuarios HP en Interex.

El término ha sido acuñado por el famoso Khan C. Smith, spammer y hacker desde mediados de la década de 1990. Además, según informes en línea, la palabra phishing se utilizó y registró públicamente por primera vez el 2 de enero de 1996. Se realizó una visita a un equipo de noticias de Usenet llamado AOHell. En ese momento, América Online (AOL) era el proveedor de acceso a Internet número uno con millones de conexiones diarias.

Naturalmente, la popularidad de AOL la ha convertido en un objetivo de estafa. Los piratas informáticos y los piratas informáticos lo utilizaron para comunicarse entre sí, así como para realizar ataques de phishing contra usuarios legítimos. Cuando AOL tomó medidas para cerrar AOHell, los atacantes adoptaron otras técnicas. Envían mensajes a los usuarios de AOL que afirman ser empleados de la empresa, pidiéndoles que verifiquen sus cuentas y proporcionen información de facturación. Con el tiempo, el problema creció y AOL emitió advertencias a todas las aplicaciones de cliente de mensajería instantánea y correo electrónico: "Nadie en AOL quiere su contraseña o información de facturación".

En la década de 2000, el phishing se convirtió en el foco del sistema de pago en línea. Se hizo común que Fisher se dirigiera a los clientes de servicios bancarios y de pago en línea, algunos de los cuales, según experimentos posteriores, identificaron correctamente y se conectaron con el banco que realmente estaban usando. Asimismo, los sitios de redes sociales se han convertido en un objetivo importante para las estafas de phishing, lo que permite a los estafadores robar información personal publicada en estos sitios.

Los delincuentes registraron decenas de dominios que pretendían ser eBay y PayPal, y si no se los imitaba adecuadamente y no se les prestaba suficiente atención, parecerían reales. Luego, los clientes de PayPal reciben correos electrónicos de phishing (enlaces a sitios web falsos) pidiéndoles que actualicen sus números de tarjetas de crédito y otra información personal. El banquero (publicado por The Financial Times Ltd.) informó del primer ataque de phishing en un banco en septiembre de 2003.

A mediados de la década de 2000, el software de phishing "keykey" estuvo disponible en el mercado negro. Al mismo tiempo, los grupos de hackers comenzaron a organizarse para desarrollar negocios modernos de phishing. Las estimaciones del daño causado por el éxito de los ataques de phishing varían, y Gartner informa que, entre agosto de 2006 y agosto de 2007, 3,6 millones de adultos perdieron $ 3,2 mil millones.

En 2011, se descubrieron patrocinadores de phishing cuando un pirata chino atacó las cuentas de Gmail de altos funcionarios políticos y militares de Estados Unidos y Corea del Sur, así como de activistas políticos chinos.

En 2020, en un caso más común, se robaron 110 millones de archivos de clientes y tarjetas de crédito de clientes objetivo a través de la cuenta de un subcontratista de phishing.

Aún más famosa fue la campaña de phishing lanzada por Fancy Bear (un equipo de ciber espionaje afiliado al GRU de la Agencia Central de Inteligencia de Rusia) en el primer trimestre de 2016 contra la dirección de correo electrónico del Comité Nacional Demócrata. Especialmente después de la piratería de Hillary Clinton, John Podesta, el director de campaña, pirateó su Gmail y filtró la siguiente información, uniéndose a la forma antigua: el ataque de phishing, que afirmaba que se había perdido la contraseña de su correo electrónico, se vio comprometido (Haga clic aquí para cámbialo).

En 2017, los departamentos de contabilidad de Google y Facebook fueron engañados para que transfirieran más de $ 100 millones a cuentas bancarias extranjeras controladas por un pirata informático.

A pesar de la diversidad, el denominador común de todos los ataques de phishing es el uso de excusas falsas para obtener datos valiosos. Incluye algunas categorías básicas:

Muchas empresas de phishing envían cada vez más correos electrónicos a la mayoría de las personas, y el spear phishing es un ataque dirigido. El spear phishing se dirige a una persona u organización específica, a menudo este contenido es apropiado para la víctima o las víctimas. Es necesario espiar antes del ataque para encontrar el nombre, título, dirección de correo electrónico y otros elementos. Los piratas informáticos en Internet buscan lo que han aprendido sobre colegas profesionales específicos y los nombres y enlaces clave de empleados clave de sus organizaciones. Al hacer esto, el autor del correo electrónico de phishing crea un correo electrónico válido (Cadillo, 2022).

Por ejemplo, el lanzamiento de jabalina puede crear un empleado con responsabilidades que incluyen la capacidad de permitir que un estafador pague. El correo electrónico parece provenir de un gerente de la organización, el empleado debe realizar un pago significativo al gerente de la empresa o al vendedor (en realidad, cuando el enlace de pago malicioso lo envía al atacante).

El lanzamiento de jabalina es una seria amenaza para las empresas (y los gobiernos) y puede resultar costoso. Según un informe de investigación de 2016, el spear phishing fue responsable del 38% de los ciberataques a las empresas participantes en 2015. Además, para las empresas estadounidenses involucradas, el costo promedio de un ataque con pistola es de $ 8 millones por evento (Schroder, 2021).

En este ataque, los perpetradores crean una copia válida o un clon del correo electrónico que contiene el enlace o archivo adjunto. Luego, el autor reemplaza los enlaces o archivos adjuntos de phishing con contenido malicioso oculto y parece real. Los usuarios sospechosos pueden hacer clic en el enlace o abrir el archivo adjunto, lo que a menudo les permite controlar sus sistemas. El autor de Phishing puede reclamar falsamente la identidad de la víctima para aparecer como un remitente confiable para otras víctimas en la misma organización.

Los esfuerzos de phishing telefónico, a veces denominados phishing de voz o "lloriqueos", Fisher afirma representar a su banco, policía o agencia tributaria local. Te asustan con algún tipo de problema e insisten en que lo arregles de inmediato dando la información de tu cuenta o pagando una multa. Por lo general, te piden que pagues mediante transferencia bancaria o tarjeta de crédito (León, 2023).

El phishing a través de SMS o "reír" es un gemelo vicioso que realiza el mismo tipo de estafa (a veces para hacer clic en un enlace malicioso) a través de SMS.

Dentro de las técnicas utilizadas para la comisión del delito de fraude informático entendiendo por estas, al diseño, introducción, alteración, borrado, supresión, clonación de datos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, destacan las siguientes:

a) Bombas lógicas (logic bomb): Es aquella Rutina no concedida de un programa que trae consecuencias totalmente destructivas en un sistema en cierto momento determinado.
b) Caballo de Troya:(Trojan horse): Aquel que introduce una serie de instrucciones o hábitos a un determinado programa que en algunas ocasiones logra que actúe de forma diferente a lo esperado;
c) Puertas falsas: Este, introduce ciertos puntos de control para comprobar que los resultados intermedios sean correctos, que posterior, al no ser cerrados son utilizadas para fines ilícitos;
d) Fuga de información (data leakage): Aquella divulgación no autorizada de datos reservados;
e) Acceso no autorizado(piggybacking): Aquel acceso a determinadas áreas limitadas o restringidas;
f) Pinchazo en línea (Wiretapping): Aquellos pinchazos de líneas de determinada comunicación con el propósito de obtener información;
g) Simulación y Modelación: Pretende utilizar un ordenador para planificar y simular un delito que luego es ejecutado;
h) El Salami: Es aquella manipulación de un gran número de pequeños importes de dinero;
i) Skimming: Aquel robo de información contemplada en una tarjeta de crédito;

j) Recojo de información desechada (Scavenging): Es la obtención de determinada información desechada en la papelera de reciclaje;
k) Superzapping: Nos concede modificar ciertos archivos y bases de datos sin la necesidad de acceder a ellos;
l) El pharming: Un tipo de estafa electrónica que implica insertar una aplicación en la computadora de un usuario cuando envía un correo electrónico o accede de alguna forma a un sitio web, para registrar en este caso el movimiento de las llaves y poder transferir la información recopilada: número de tarjeta de crédito, contraseña, etc.;
m) El phishing: Cualquier otra empresa conocida por registrar ilegalmente datos personales relacionados con contraseñas para acceder a servicios bancarios y financieros, a través de correo electrónico o páginas web que imiten o copien la imagen o apariencia de una institución bancaria o cualquier otra reputación acreditada. Después de obtener las claves secretas, el dinero se retira mediante transferencia electrónica.

Se entiende por todas estas, a dicha operación que se efectua alterando las normas y protocolo bancarios mediante la manipulación de la red de TEF, empleando el código de transferencia bancaria sin soporte de papel y acreditarse montos de dinero en cuentas exprofesas para ser retirados por cómplices. Otra de las formas usuales es la transferencia de dinero de una cuenta a otra, lo cual se ejecuta desde un ordenador electrónico (celular, computadora, laptop, Tablet) en el cual el delincuente logra poder tener acceso a la cuenta de ahorros, corrientes, y con el acceso de la clave secreta logran su propósito de transferir dinero de una cuenta a otra, simulando ante la institución financiera, ser cliente de la misma.

El intercambio electrónico es un método que se realiza a través de un terminal electrónico, dispositivo telefónico o computadora. Esta licencia valida un préstamo o deuda contra una cuenta o institución financiera. Este método de transferencia de fondos es la transferencia de fondos de una cuenta a otra en la misma institución financiera, pública o privada, o la cuenta de otra institución financiera u otro tipo de institución (Salinas, 2020).

Por otro lado, tenemos el consumo o retiro con tarjetas clonadas que se realiza utilizando tarjetas de débito o de consumo previamente clonadas, usadas en

centros comerciales para adquirir o consumir diversos productos los cuales son cancelados mediante estos mecanismos electrónicos, asumiendo para ello (el agente) la identidad del usuario clonado. El retiro de dinero, en cajeros o tiendas comerciales, se realiza también con el uso de las claves secretas obtenidas, además de los mecanismos ya mencionados, muchas veces con la infidencia del interior del banco afectado (Salinas, 2020)

Toda vez que la finalidad del agente será siempre obtener un beneficio o provecho ilícito a su favor o de un tercero; en el delito de fraude informático, el objeto “material” o “inmaterial” será la sustracción de dinero o documentos; la sustracción de mercancías; la sustracción de valores negociables o documentos que sirvan de soporte para el intercambio de mercancías o de dinero; la sustracción de servicios y finalmente la sustracción de software25. Todos ellos, con un valor patrimonial o de intercambio para sus titulares y perfectamente negociables en el mercado negro.

El delito de fraude informático se entiende como aquel empleo indebido de un sistema informático, este a su vez no requiere para su configuración, la afluencia de los elementos propios de la estafa, tales como el engaño, el ardid y el error; puesto que la actuación del agente es sobre un ordenador, un sistema una máquina y no se emplea necesariamente la participación, en el otro extremo, de una persona humana, por cuanto la transferencia de datos y el desplazamiento patrimonial en perjuicio del sujeto pasivo, se da de forma automática y sin su participación o consentimiento (Adamu, 2022).

Por medio de la primera disposición complementaria y modificatoria de la Ley, se introdujo al delito informático como uno de los delitos pasibles del levantamiento del secreto de las comunicaciones, establecido en el artículo 1 de la Ley N.º 27697 para un abanico de delitos graves. Asimismo, mediante la modificación del numeral 09 del artículo 3 de la Ley N.º 30077, se estableció además que, para su investigación, le son aplicables las normas que regulan la investigación en los delitos de criminalidad organizada. En consecuencia, este tipo de delitos son investigados a la fecha por las Fiscalías Especializadas en Criminalidad Organizada con las exigencias establecidas por la norma, bajo las reglas del nuevo Código Procesal Penal. Con estas modificaciones, sin lugar a dudas, se ha otorgado de

nuevos mecanismos procesales idóneos y eficaces que buscan combatir esta nueva delincuencia moderna.

El ciberdelito incluye ahora delitos graves como secuestro, trata de personas, pornografía infantil, robo, extorsión, narcotráfico, tráfico migratorio, delitos de lesa humanidad, delitos contra la seguridad nacional y traición, terrorismo, delitos fiscales y aduaneros, blanqueo de capitales.

El delito de fraude informático, es una de las modalidades del cibercriminal es cualitativamente contrario a los delitos de hurto y estafa, de trascendencia internacional que se realiza o comete en el ciberespacio, el cual no conoce distancias geográficas.

Cabe señalar que comparte con los demás delitos informáticos un bien jurídico en común (que es el cuidado de los sistemas y datos informáticos en sus tres propiedades: integridad, confidencialidad y disponibilidad) además que protege en el caso específico el patrimonio (Lazaro, 2019).

Este es un delito doloso, con un elemento subjetivo adicional, el propósito de procurarse para sí o para otros un determinado provecho ilícito, lo cual lo diferencia del “hacking ético”. Para su consumación requiere la existencia objetiva de un daño patrimonial.

Antes de abordar este tópico, comencemos por definir el concepto de un contrato electrónico. Espinoza (2019) Un contrato electrónico significa "el uso de cualquier elemento electrónico, declaración o similar que pueda tener un impacto real y directo en la construcción, desarrollo o interpretación del futuro acuerdo. En un entorno típico o ambos de forma electrónica” (p.282).

Simón (2020) define al contrato electrónico en sentido amplio y estricto: “Podemos hablar de un contrato electrónico en el sentido más amplio, cuando en él se incluyen todos los contratos celebrados electrónicamente, o solo los acuerdos electrónicos celebrados por el intercambio electrónico entre dos ordenadores. Los contratos electrónicos incluyen todas las etapas del contrato” (p. 376).

El principal inconveniente que genera la contratación electrónica tiene que ver con la dificultad de identificar de manera fehaciente al usuario de la tarjeta de crédito

cuando se realiza una contratación a través de Internet, pese a los mecanismos de seguridad como los certificados de firma digital. Este tema lo trataremos en el apartado siguiente cuando analicemos el tipo penal de defraudación cometido mediante el uso de tarjetas de crédito.

Dentro de la Legislación extranjera, el delito de defraudación en el Código Penal argentino y el empleo de tarjetas bancarias; para ello, brinda una base conceptual desde la óptica del derecho civil-comercial de lo que es el sistema de tarjetas bancarias, teniendo en consideración para esto lo aportado por la doctrina, la legislación nacional e internacional, es así que llega a la conclusión que se trata de un acto complejo el cual rompe los parámetros clásicos del contrato y por ende requiere de una regulación propia y autónoma.

Sobre la base de esto plasma desde el marco del Derecho Penal la actual problemática en relación a las defraudaciones cometidas mediante el empleo de tarjetas bancarias, las cuales a criterio de la autora son uno de los pilares básicos de la actividad económica actual y por ello la necesidad de emplear mecanismos jurídicos que permitan abordar la creciente criminalidad referida a los delitos de defraudación cometidos mediante el empleo de tarjetas bancarias. Así, la autora considera que la incorporación del tipo penal de defraudación mediante el uso de tarjetas bancarias como mecanismo jurídico ha logrado cubrir un vacío normativo, pues se deja atrás así el antiguo debate en el que hechos similares eran encuadrados bajo la figura de estafa, hurto o falsificación de instrumento privado, problemática que se dejó de lado actualmente por la incorporación de la ley en mención y que se encuentran abarcados por un tipo penal autónomo que responde a la necesidad de proteger con mayor intensidad el tráfico comercial.

El crédito es uno de los pilares básicos de la actividad económica en la sociedad actual. Ello pone de manifiesto la necesidad imperiosa de proteger al individuo de los comportamientos delictivos relacionados con la actividad comercial. Aquí se hace innegable la intervención del derecho penal, tomando como punto de partida la preocupación de emplear mecanismos jurídicos que permitan abordar la creciente criminalidad referida a los delitos informáticos, en particular nos detendremos en las defraudaciones especiales cometidas mediante el empleo de

tarjetas de compra, crédito o débito, tipo legal incorporado al Código Penal argentino en el artículo 173, inciso 15 mediante la Ley N.º 25.930 en el año 2004.

Aboso (2019), comprende que la categoría de ciberdelito debe reconocerse únicamente cuando el propósito de la acción lo determina la red informática o su uso, es decir, no todos los intermediarios en el ordenador indican necesariamente que se trata de un ciberdelito. (p.641)

Con anterioridad a esta reforma, hechos similares eran encuadrados bajo la figura de estafa, hurto o falsificación de instrumento privado. Entre estos delitos mediaba un concurso real. Actualmente estos supuestos se encuentran abarcados por un tipo penal autónomo que responde a la necesidad de proteger con mayor intensidad el tráfico comercial.

El objeto del presente trabajo es comenzar, en primer término, desde la óptica civil, realizando un análisis contractual del "sistema de tarjetas de crédito y débito", enfocado en la doctrina nacional y considerando la regulación del Código Civil y Comercial argentino en materia de contratos bancarios y su estrecha relación con el derecho de los consumidores y usuarios para luego, dentro del marco del derecho penal, exponer la actual problemática delictiva en relación a las defraudaciones cometidas mediante el empleo de tarjetas bancarias.

El derecho a la intimidad se encuentra recogido en el art. 2 de nuestra Constitución Política y busca proteger el aspecto reservado de la vida de cada persona, mediante la protección de los datos personales que forman parte de la esfera privada.

En ese orden de ideas, Fernández y Martínez (2019) señalan:

El propósito de reconocer la privacidad personal y familiar es respetar al individuo como persona y asegurar que el individuo tenga un área separada de la vida a la que esté vinculado, frente a las actividades y el conocimiento de los demás (p. 140).

Los ciberdelincuentes utilizan la información del entorno íntimo de la víctima para realizar la conducta ilícita, por ejemplo, intentan tener en su poder los datos personales, bancarios, académicos… de la víctima. En ese sentido, la información

recopilada coadyuva a que el mecanismo empleado no pueda ser advertido por la víctima.

Respecto al sentido de la palabra “comunicación”, Fernández y Martínez (2019) señalan lo siguiente:

Por “comunicación” considera la doctrina mayoritaria que deben entenderse incluidos todos los medios de comunicación, no existe un numerus clausus respecto de los medios de comunicación que pueden ser objeto de vigilancia; y para que haya comunicación se exige una distancia real entre los comunicantes y que se realice por canal cerrado. (p.141)

Cuando los ciberdelincuentes poseen toda la información necesaria para realizar la actividad criminal, vulneran algunos derechos constitucionales como el secreto de las comunicaciones.

Ahora bien, el derecho a la libertad de expresión e información en el transcurso del tiempo, ya que implica en términos sencillos la no afectación del derecho a la intimidad. En virtud de ello, los ciberdelincuentes obtienen la información de la víctima sin su consentimiento y utilizan dicha información para cometer un ilícito.

De acuerdo con lo descrito se plantea el problema general de la investigación: **¿De qué manera la Ciberseguridad ayudará a mejorar el comercio electrónico para evitar los casos de phishing en tiempos de pandemia, Chiclayo, 2022?**

A su vez, se plantean los siguientes problemas específicos:

a. ¿Cuáles son las medidas de seguridad que se pueden implementar en el comercio electrónico?
b. ¿Qué trascendencia tiene la figura jurídica del phishing y su impacto en la pandemia de la Covid 19?
c. ¿Cuáles serían las mejoras en la ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico?

d. ¿Cómo se puede garantizar la seguridad jurídica desde la normativa del comercio electrónico en cuanto a la figura jurídica del phishing y su impacto en la pandemia de la Covid 19?

Como objetivo general se planteó, Determinar si la ciberseguridad ayudara a mejorar el comercio electrónico y evitara los riesgos de phishing en tiempos de pandemia.

Y como específicos:

a. Identificar qué medidas de seguridad se pueden implementar en el comercio electrónico.
b. Analizar la figura jurídica del phishing y su impacto en la pandemia de la Covid 19.
c. Analizar que mejoras se puede aplicar en la ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico.
d. Establecer mejoras en la Ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico.

Es importante tener en cuenta que con la pandemia de COVID-19 y la cuarentena, los delitos informáticos han aumentado en el Perú y el mundo. Uno de los delitos que más se ha disparado es el *phishing,* es por ello que la investigación pretende estudiar los tipos o modalidades y su impacto en la sociedad actual. Asimismo, advierte la poca preocupación de las autoridades en actualizar la legislación para una eficiente persecución y sanción de este tipo de delitos.

Como justificación legal, es necesario mencionar que el fraude informático es uno de los delitos que atenta contra el patrimonio de una persona natural o jurídica. Su componente principal es el ánimo de lucro. Este delito se fundamenta en tres supuestos: 1) engaño, 2) error y 3) disposición del dinero e individuo que realice este acto ilícito. Muchas veces, las legislaciones no están acorde con el contexto social, debido a que están desfasadas frente a estos tipos de delitos, en consecuencia, existen individuos inescrupulosos que se aprovechan de los vacíos legales para ejecutar ilícitos penales en diferentes modalidades. Una de estas

modalidades es el phishing, que se apoya en los sistemas informáticos de alta gama.

Por consiguiente, los fraudes informáticos se han incrementado a un nivel exponencial en tiempos de pandemia de COVID-19. Las noticias evidencian el aumento de casos de ciudadanos que denuncian haber sido víctimas de ciberdelincuentes. Sin embargo, ¿qué han hecho las entidades financieras y las instituciones del Estado para prevenir y sancionar estos delitos? Hasta el momento la ayuda es escasa y el marco jurídico que tenemos respecto a los delitos informáticos es muy general.

Como bien se sabe muchas personas ahora tienen la capacidad de transferir e indagar información, lo cual puede provocar la pérdida de datos importantes y la piratería de contraseñas, es por esto que uno de los mayores riesgos que se presentan dentro del estado peruano son lo delitos cibernéticos.

Como justificación teórica, menciona que actualmente el incremento de estos delitos se ha generado por la pandemia Covid- 19, donde como consecuencias se observan la vulnerabilidad al comercio electrónico, ya que la compra y venta virtual muchas veces conlleva a que se apliquen delitos cibernéticos, es así que esta propuesta de investigación quiere aplicar la ciberseguridad con el fin de proteger el comercio electrónico y evitar los riesgos de phishing en tiempo de pandemia (Hernández, 2018).

Salom (2019), explicita que desde el aspecto social el aumento, a nivel mundial, del *phishing* atenta contra la seguridad y confianza que debe de tener todo usuario al momento de utilizar el internet como medio para hacer operaciones bancarias. De acuerdo a estudios realizados, lo que una persona valora y desea es la total privacidad de sus estados de cuentas. Así, el 60 % asegura que no realiza compras online por temor a ser estafado. Manifiestan, además, que utilizarían una aplicación de manera frecuente si estas contaran con sistemas de control de seguridad más confiables. El 82 % de los ataques cibernéticos son a través de la modalidad del *phishing*.

Como justificación metodológica se tiene el análisis de la Sentencia Penal N.° 463/2018, esta sentencia a sido interpuesta y como materia de delito de estafa,

constituida en una modalidad cibernética, principalmente en el delito de phishing, ante esta materia de análisis se tuvo en cuenta la manipulación informática, la valorización de la prueba

Además, esta investigación ayuda a que los jueces, fiscales, peritos y abogado sean capacitados para poder determinar la ciberseguridad y que se pueda proponer mejores ideas sobre cómo prevenir este tipo de robos y fraudes informáticos.

La novedad que brinda mi investigación es crear un sistema de ciber seguridad teniendo en cuenta que los casos de phishing han aumentado con el uso de aplicaciones, páginas webs, mensajes de texto. La falta de una regulación acorde al nuevo contexto global ha ocasionado el incremento de los fraudes informáticos, no solo a nivel nacional, sino también mundial.

El aporte aplicable de mi investigación es solucionar problemas mediante una profunda investigación para el desarrollo y bienestar de los medios informáticos que se ejecutan en el comercio electrónico, así como también brindar la tranquilidad de compra y venta virtual, ya que la informática dentro de la sociedad a menudo genera mayor oportunidad y facilidad.

II. MATERIALES Y MÉTODO

La presente investigación es de enfoque **cualitativo** mediante la aplicación de entrevistas y de análisis documental. Esta indagación es de tipo descriptiva, porque se basa específicamente en un estudio del caso. Además, la investigación que se realiza es básico. porque se aborda una temática trascendental para la sociedad, como lo es la ciberseguridad y el phishing en el Perú.

Conforme lo menciona Hernández (2020), las investigaciones cualitativas tienen por finalidad la interpretación de información, sin la necesidad de emplear parámetros numéricos. Del mismo modo existen tipos para realizar la investigación, una de ellas es aplica, las cuales se enfocan en brindar soluciones o propuestas a un fenómeno de la realidad.

La Investigación además es **tipo básico** por cuanto no se centra en resolver un problema en específico; si no más bien lo que busca es contribuir teóricamente a futuras investigaciones realizadas a las temáticas tratadas. (Arias,2020.p.43)

En la presente investigación se desarrolla un diseño **no experimental**, según Hernández (2020) señala que es un diseño de investigación donde no existe la manipulación de alguna variable, en la misma que se podrá analizar la ciberseguridad y el phishing en el Perú (p. 174).

Esta investigación se desarrolló dentro de la ciudad de Chiclayo, en donde se toma en cuenta la aplicación de los instrumentos dentro de la cuidad de Chiclayo, tomándolo como distrito judicial, pues aquí se va aplicar la entrevista para tomar en cuenta la relevancia del fenómeno de estudio.

Conforme a ello se llega a comprender que la población es todo aquel conjunto de persona que tienen en común un tema denominado a través de un espacio, en donde expertos, como el caso de jueces, fiscales y abogados serán generados a través del Derecho Penal, teniendo como expertos a los jueces, fiscales y abogados especialistas en Derecho Penal, del distrito judicial de Chiclayo (José, 2020).

Se analiza que la muestra es una parte de la población, en muchas ocasiones se tiene como especialista a los expertos como expertos a los jueces,

fiscales y abogados especialistas en Derecho Penal, del distrito judicial de Chiclayo, con la finalidad de presentar mejores conocimientos de manera estadística a la población (Hernández, 2020).

Asimismo se le aplicara una entrevista a fin de poder recolectar información útil y relevante en relación al fenómeno de estudio, dicha información complementara al análisis documental realizado.

Se tuvo como técnica la **Entrevista**: Según el autor Bustos (2021) señala que la entrevista es utilizada como un método de recolección de datos para obtener una información, asimismo esta técnica suele ser utilizado de forma virtual o presencial en comunicación con el entrevistado, en el cual se usa un cuestionario que contiene una serie de preguntas que son validadas por un letrado.

Y como instrumento la Guía de entrevistas: Según Lázaro (2021) es el listado de preguntas que efectúa el investigador para realizárselas al entrevistado.

El procedimiento para la recolección de datos en el presente estudio se efectuó a través de la búsqueda de doctrina, legislación y jurisprudencia relacionada con el tema materia de estudio, así como la intervención de especialistas de materia penal a quienes se les aplicó una entrevista en donde se obtienen los resultados que complementan el estudio materia de investigación.

Los datos se analizan tomando en cuenta el modelo cualitativo, ya que es necesario sintetizar a través de una encuesta e informar por escrito que los datos no son números, pero es necesario llevar estos resultados a los estándares y escala que se deben investigar con ciber implementación de la seguridad en el comercio electrónico y los riesgos de phishing durante la pandemia, dado esto, es importante que uno de los pasos a tomar sea la recolección de datos, que luego ayudarán a la investigación a lograr criterios importantes en los que una persona pueda responder a todas las preguntas se basa en el conocimiento que cada experto ha involucrado, por lo que esta información es procesada y analizada de manera consistente y coordinada. interpretar cada fenómeno para obtener resultados favorables (Lerma, 2022).

Se tuvo como criterios éticos a la beneficencia, el respecto la justicia, la confidencialidad y la originalidad.

III. RESULTADOS Y DISCUSIÓN

3.1. Resultados

Objetivo General: Determinar si la ciberseguridad ayudara a mejorar el comercio electrónico y evitara los riesgos de phishing en tiempos de pandemia.

Tabla 1

¿Por qué debe existir mecanismos de ciberseguridad dentro del comercio electrónico?

Entrevistado	**Ideas fuerza**
Salazar Maza Geiner Vidal	Deben existir mecanismos de seguridad para poder hacer las compras a través de aplicaciones sin tener miedo de ser víctimas de este tan sonado delito como lo es el phishing.
Vasquez Chavarri Cesar Ágel	El comercio electrónico es una modalidad de compra virtual que la gran mayoría de personas realizan como parte de sus actividades diarias, sin embargo, existe una gran cantidad de población que exige que existan mejores mecanismos de ciberseguridad, ya que han sido víctimas de distintos delitos de ciberdelincuencia.
Chavez Rojas Magaly del Roció	Para permitir que muchas de nuestras transacciones o actividades que tengan que ver con los medios electrónicos, sean seguros y así brindar una mayor confianza al momento de emplear un medio tecnológico, con la esperanza de no ser víctimas de este tipo de delitos que cada día van acrecentando.
Benavides Pérez Liliana Maribel	Deben de existir mejores mecanismos de ciberseguridad, para que las personas que realizan estas actividades virtuales, puedan estar seguras y protegidas ante cualquier delito cibernético que puedan atentar contra su bienestar.
Chero Villegas Wilfredo	Para evitar la comisión de actos ilícitos que perjudiquen el interés personal, empresarial o societario.

Irigoin Fallaque Gilmer	Los mecanismos de ciberseguridad, ayudaran rotundamente a la sociedad a realizar toda actividad electrónica de una forma segura y viable, de igual manera estos mecanismos también evitasen que las personas que están acostumbradas a cometer estos actos delictuosos no puedan atentar contra el bienestar de la sociedad.

Nota. Elaboración Propia

Nota. Es importante reconocer que en la actualidad a causa del surgimiento del Covid-19, la vida cotidiana que antes conocíamos ha dado un giro inesperado, ocasionando que todo el mundo se adecue de una manera inesperada e inmediata a las normas aplicadas por el estado, sin embargo, se puede evidenciar que dentro estos cambios la sociedad ha tenido que buscar alternativas para nuevos ingresos económicos, en el cual radica el problema ya que la sociedad no se encuentran segura frente a los mecanismos de ciberseguridad dentro del comercio electrónico; es por ello que al tener en cuenta lo señalado por los distintos expertos que han formado parte de la entrevista, es necesario que deban existir nuevos mecanismos de seguridad frente a los delitos cibernéticos, por el tan solo hecho de brindar una correcta y adecuada seguridad a la sociedad que puedan realizar sus actividades electrónicas de una manera justa y segura.

Tabla 2

¿Cuáles son los beneficios de aplicar mecanismos de ciberseguridad dentro del comercio electrónico?

Entrevistado	**Ideas fuerza**
Salazar Maza Geiner Vidal	• No ser víctimas de phishing • Compras online seguras • Derecho a reclamos y devoluciones online
Vasquez Chavarri Cesar Ágel	Evitará que las personas que realizan actividades de comercio electrónico no sean víctimas de estos actos ilícitos.
Chavez Rojas Magaly del Roció	• Mayor Confiabiabilidad • Mayor utilización del comercio electrónico • Brindar una mayor seguridad a los usuarios
Benavides Pérez Liliana Maribel	Mediante los mecanismos de ciberseguridad se logrará mejorar el comercio electrónico brindando así una seguridad a las personas que realizan sus actividades por una computadora o instrumento electrónico.
Chero Villegas Wilfredo	Que brinda seguridades tecnológicas y garantía jurídica para los usuarios del sistema informático
Irigoin Fallaque Gilmer	• Seguridad en las actividades electrónicas • Fiabilidad en el comercio electrónico

Nota. Elaboración Propia

Nota. En la actualidad las actividades del comercio electrónico han aumentado de una forma exponencial, considerándose así el mecanismo más oportuno frente a la actual pandemia para que no existe un contacto directo con las personas, evitando

así el incremento del Covid-19, es por ello que la sociedad necesita estar segura frente a las actividades del comercio electrónico. Los mecanismos de protección frente a los delitos cibernéticos son: evitar el contagio o el incremento del Covid-19, una seguridad frente a todas las transacciones realizadas en un comercio electrónico, una mayor confiabilidad, derecho a reclamos y devoluciones online, compras seguras de forma online y entre otros beneficios que de una u otra manera.

Objetivo Especifico 1: Identificar qué medidas de seguridad se pueden implementar en el comercio electrónico.

Tabla 3

¿Cuáles considera usted que son las medidas que se pueden implementar para mejorar el comercio electrónico y evitar los riesgos del phishing?

Entrevistado	**Ideas fuerza**
Salazar Maza Geiner Vidal	Yo considero que las plataformas deben ser más seguras, asimismo debe haber un estricto cumplimiento en lo que respecta a los datos personales de los usuarios, y así evitar que personas inescrupulosas aprovechen de eso para cometer actos ilícitos.
Vasquez Chavarri Cesar	Una de las principales medidas es que el estado peruano debe implementar es una adecuada orientación a la población de cómo actúan y como protegerse ante estos delitos cibernéticos.
Chavez Rojas Magaly del Roció	A manera de implementar y mejorar así el comercio electrónico, yo propondría que se implemente el uso biométrico, asimismo el otro punto que yo propondría sería una mayor exigencia de los datos de quienes realizan las transacciones, a manera de evitar ser víctimas de este tipo de personas inescrupulosas.
Benavides Pérez Liliana Maribel	Considero que todas las entidades que involucre un comercio electrónico deban mejorar sus filtros para la confirmación de la actividad a realizar, teniendo en cuenta que esta confirmación deberá estar acorde con la entidad bancaria.

Chero Villegas Wilfredo	• Establecer filtros para la información. • Establecer la reserva informática en la POLICIA NACIONAL Y EL PODER JUDICIAL. • Creación de anillos de seguridad tecnológica.
Irigoin Fallaque Gilmer	Deberán mejorar todos los filtros que se solicitan al realizar alguna actividad dentro del comercio electrónico, como es el mejoramiento de la confirmación de la compra y que las entidades que investigan estos delitos ataquen directamente a los números telefónicos y los correos electrónicos que están involucrados en el delito de phishing

Nota. Elaboración Propia

Nota. Es importan reconocer que hoy en día las actividades de comercio electrónico son alternativas consideradas eficientes solamente en su rapidez, sin embargo, al hablar de su protección o seguridad frente a sus actividades se puede poner en tela de juicio su eficacia, es por ello que a través de las respuestas de los entrevistados que han formado parte de la investigación se ha podido demostrar la necesidad de establecer nuevos y adecuados filtros para el comercio electrónico, orientación a la población de cómo actúan y como protegerse ante estos delitos cibernéticos, la implementación del uso biométrico, una mayor exigencia de los datos y entre otras medidas de seguridad. Esto quiere decir que las actividades del comercio electrónico aun presentan vacíos para su adecuada viabilidad, generando así que existe una desconfianza en todas las actividades que involucren actividades electrónicas.

Tabla 4

¿De qué manera el Estado peruano podría brindar una adecuada protección tecnológica frente a los fraudes electrónicos?

Entrevistado	**Ideas fuerza**
Salazar Maza	A opinión personal, yo considero que se deben imponer penas más severas, esto con el fin de causar mayor temor en los

Geiner Vidal	delincuentes y evitar así que siga acrecentando el porcentaje de delitos informáticos.
Vasquez Chavarri Cesar Ágel	El estado influirá de manera positiva al capacita adecuadamente a las personas que investigan este delito, orientando a la misma población de cómo actúan estos delitos cibernéticos y por último al mejorar las herramientas de las DIVINDAT y otras entidades que investigan estos actos delictuosos.
Chavez Rojas Magaly del Roció	El estado podría asegurar en parte una mejor protección a los usuarios, brindando un mayor equipamiento al nivel de tecnología digital; asimismo como recalque en líneas anteriores; exigiendo una mayor identificación de los usuarios.
Benavides Pérez Liliana Maribel	El estado puede influir de una manera positiva, ya que puede brindar mejores herramientas electrónicas para la correcta investigación de estos delitos.
Chero Villegas Wilfredo	Entidades públicas que diseñen políticas de confidencialidad, respeto a la información de los usuarios, implicando a ello dotación de recursos y capacitaciones constantes para el personal que atiende el servicio público.
Irigoin Fallaque Gilmer	Capacitando adecuadamente a las personas que investigan estos delitos cibernéticos como son los de la DIVINDAT, al Ministerio Publico para que de esta manera puedan detener a las personas que realizan estos delitos.

Nota. Elaboración Propia

Nota. El estado peruano tiene la obligación de proteger y hacer respetar los derechos fundamentales de la ciudadanía, es por ello que el estado peruano tiene el deber de brindar una adecuada protección del comercio electrónico frente a los delitos cibernéticos, es por ello que se pueda tomar en cuenta las respuesta de los expertos en la materia, los cuales señalan que deberán imponer penas más severas, capacitar adecuadamente a las personas que investigan este delito, orientar a la misma población de cómo actúan estos delitos cibernéticos, mejorar

las herramientas de las DIVINDAT y otras entidades que investigan estos actos delictuosos, mejorando el equipamiento al nivel de tecnología digital y entre otros aspectos.

Objetivo Especifico 2: Analizar la figura jurídica del phishing y su impacto en la pandemia de la Covid 19.

Tabla 5

¿Por qué ha aumentado de manera considerable los delitos informáticos que atentan contra el patrimonio en tiempos de Covid 19?

Entrevistado	**Ideas fuerza**
Salazar Maza Geiner Vidal	Si bien es cierto; con la llegada de la pandemia, muchas personas nos hemos tenido que aislar privándonos de hacer muchas actividades que realizábamos con frecuencia; empleando de manera más continuada los medios tecnológicos; lo cual acrecentó de manera considerable a que se cometan muchos más delitos informáticos.
Vasquez Chavarri Cesar Ágel	Se ha llegado aumentar de manera considerable estos actos delictuosos por el confinamiento ocasionado por el Covid-19, ya que la gran mayoría de la población comenzó a realizar actividades de comercio electrónico y es ahí donde los delitos informáticos se han aprovechado de los ciudadanos por su falta de experiencia en estas actividades.
Chavez Rojas Magaly del Roció	Se ha visto un gran aumento en relación a este tipo de delitos, debido a que la pandemia. De por sí nos envió a aislarnos, incitándonos de tal modo a realizar nuestras actividades a través de los medios

	tecnológicos; generando a que haya un mayor porcentaje de víctimas y que los delincuentes saquen mayor provecho.
Benavides Pérez Liliana Maribel	Se ha aumentado de forma considerable a causa de la pandemia del Covid-19, ya que sociedad comenzó a realizar todas tus actividades por medios de los servicios tecnológicos, generando ser propenso a los delitos.
Chero Villegas Wilfredo	Por qué no existió preparación, control y reserva en las entidades del estado, lo que ha generado la invasión de instrumentos que vulneran el sistema informático Estatal.
Irigoin Fallaque Gilmer	Estos delitos cibernéticos han aumentado de forma exponencial, a causa del confinamiento del Covid-19, los cuales ocasionado que toda persona realice transacciones virtuales.

Nota. Elaboración Propia

Nota. Como se ha venido desarrollando en toda la investigación el comercio electrónico se ha vuelto una alternativa eficaz frente a su rapidez, de igual forma se ha establecido como una herramienta favorable frente a la reducción del incremento del Covid-19, sin embargo, estas actividades electrónicas se han visto incrementado gracias al confinamiento realizado por el estado peruano, teniendo en cuenta que no existió preparación, control y reserva en las entidades del estado, lo que ha generado la invasión de instrumentos que vulneran el sistema informático Estatal. A través de las respuestas de los entrevistados se puede evidenciar de una manera unánime, las personas están de acuerdo en que los delitos cibernéticos se han incrementado a causa de la pandemia del Covid-19.

Tabla 6

¿De qué manera se puede controlar el aumento de delitos informáticos que atentan contra el patrimonio?

Entrevistado	**Ideas fuerza**

Salazar Maza Geiner Vidal	Creando y mejorando estrategias positivas, para que cada vez sean menos los usuarios víctimas de personas inescrupulosas, que lo único que buscan es beneficiarse a costa de otras personas, perjudicándolas gravemente.
Vasquez Chavarri Cesar Ágel	Los delitos cibernéticos se lograrán controlar de manera adecuada, cuando el estado peruano tome interés en capacitar adecuadamente a las personas que investigan estos delitos, de igual forma orientando a la ciudadanía de cómo realizar sus actividades y de igual forma que las entidades bancarias entre otras de índole similar ayuden a orientar a sus clientes.
Chavez Rojas Magaly del Roció	Capacitando a las personas a que tengan un mayor cuidado en lo que respecta el uso de los medios tecnológicos, así como el uso de las tarjetas y no atendiendo a cualquier solicitud que se les sea enviada a su correo o teléfono celular, las cuales solo son propagandas engañosas que buscan obtener un provecho perjudicando gravemente a la otra persona.
Benavides Pérez Liliana Maribel	Estos delitos podrán ser controlados a través de una adecuada orientación y capacitación a la ciudadanía de cómo actúa estos criminales frente a las actividades electrónicas.
Chero Villegas Wilfredo	A través de una campaña pública de una campaña pública de prevención y que las sanciones sean severas y efectivas.
Irigoin Fallaque Gilmer	Se podrá controlar el aumento de delitos informáticos, cuando se mejore las herramientas de trabajo de las entidades que investigan estos delitos

Nota. Elaboración Propia

Nota. El aumento de los delitos informáticos se podrá controlar o reducir de manera eficiente, cuando el estado peruano tome conciencia de la gran cantidad de los delitos cibernéticos que se vienen realizando en la actualidad, es por ello que

se tendrá en cuenta lo obtenido por las respuestas de los entrevistados que están de acuerdo en que exista una adecuada orientación y capacitación a la ciudadanía de cómo actúa estos criminales frente a las actividades electrónicas, creando y mejorando estrategias positivas, capacitando adecuadamente a las personas que investigan estos delitos, del igual forma que las entidades bancarias entre otras de índole similar ayuden a orientar a sus clientes y entre otros aspectos.

Objetivo específico 3: Analizar que mejoras se puede aplicar en la ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico.

Tabla 7

¿Qué mejoras puede aplicar el legislador en la Ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico?

Entrevistado	**Ideas fuerza**
Salazar Maza Geiner Vidal	El legislador lo que debe hacer en este caso es aplicar penas restrictivas de libertas más altas a las ya impuestas, con el propósito de crear cierto temor en los delincuentes.
Vasquez Chavarri Cesar Ágel	La ley deberá ser más rigurosas con sus penas, para que de esta manera se pueda sancionar de forma adecuada a las personas que cometen este delito.
Chavez Rojas Magaly del Roció	A mi criterio personal; lo que se podría hacer para brindar una mayor seguridad y así proteger a los clientes seria brindar una mayor prevención y difusión en el cuidado al memento de emplear los diversos medios electrónicos.
Benavides Pérez Liliana	Incorporar políticas de prevención para la adecuada investigación de estos delitos cibernéticos.

Maribel	
Chero Villegas Wilfredo	El legislador debe tomar en cuenta la intensidad e inmensidad de los delitos informáticos, para cambiar la legislación en la materia.
Irigoin Fallaque Gilmer	Debe de existir una adecuada modificatoria de la ley que regula los delitos informáticos para que de esta manera se pueda incrementar la pena de estos actos delictuosos.

Nota. Elaboración Propia

Nota. Teniendo en cuenta las respuestas de los entrevistados es evidente que de forma unánime los expertos manifiestan estar de acuerdo en que se deba incrementar la condena aplicada hacia las personas que cometen estos actos delictuosos, teniendo en cuenta la intensidad e inmensidad de los delitos informáticos. Es importante reconocer que el estado peruano deberá tomar un mejor interés frente a estos asuntos de manera judicial, ya que de esta manera se podrá evitar que se vulneren los derechos de las personas que realizan sus actividades de comercio electrónico.

Tabla 8

¿A qué se debe la inseguridad del comercio electrónico en el Perú?

Entrevistado	**Ideas fuerza**
Salazar Maza Geiner Vidal	A que los dominios de las plataformas son inseguros, Lo cual crea a que los delincuentes saquen mayor provecho y así cometan este tipo de delitos con mayor frecuencia.
Vasquez Chavarri Cesar Ágel	Esta inseguridad se debe a que las plataformas virtuales no brindan una seguridad viable hacia la población, ya que es evidente del incremento de estos delitos.

Chavez Rojas Magaly del Roció	Básicamente a un desconocimiento de la utilización de los medios electrónicos, pues recordemos que con la llegada de la pandemia toda nuestra vida comenzó a girar en base a la tecnología, provocando esto a que haya una mayor demanda en lo que respecta la utilización de los medios tecnológicos.
Benavides Pérez Liliana Maribel	Existe una inseguridad al realizar estas actividades, por el tan solo hecho de que la sociedad está enterada del incremento de los delitos cibernéticos, y peor aun cuando se investiga estos casos en muchas oportunidades la persona afectada no recupera lo perdido.
Chero Villegas Wilfredo	Por la falta de una legislación adecuada y de una política de prevención de estos delitos, sin dejar de lado la falta de sanción oportuna para los autores.
Irigoin Fallaque Gilmer	Esta inseguridad se debe a que existe un desconocimiento adecuado de las herramientas que protegen estas actividades virtuales.

Nota. Elaboración Propia

Nota. Las actividades de comercio electrónico hoy en día han sido la alternativa más adecuada a la situación del Covid-19, sin embargo existe una inseguridad que surge a través del comercio electrónico que es a causa de que existe un incremento exponencial de los delitos cibernéticos, el cual genera que exista una incertidumbre frente a las actividades electrónicas, peor aun cuando la sociedad se entera que las entidades que se encuentran involucraras en este comercio no brindan una adecuada protección a sus clientes, generando así una disconformidad frente a sus actuaciones.

Objetivo Especifico 4: Establecer mejoras en la ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico

Tabla 9

¿Cuáles son los estándares de seguridad que debe buscar el Estado para proteger a los clientes o usuarios en el comercio electrónico?

Entrevistado	**Ideas fuerza**
Salazar Maza Geiner Vidal	Yo creo; que se debe mejorar las medidas de acción para así identificar las compras fraudulentas y que muchas más personas sean víctimas de este tipo de delitos.
Vasquez Chavarri Cesar Ágel	Unos de los estándares de seguridad que debe mejora o buscar el estado peruano, es el incremento de la condena, mejor comunicación de las empresas que brindar el servicio y sus clientes.
Chavez Rojas Magaly del Roció	Que haya una mayor exigibilidad entre las partes intervinientes y una mayor difusión a través de los medios tecnológicos.
Benavides Pérez Liliana Maribel	Los estándares de seguridad que el estado debe asegurar, es la adecuada comunicación directa como segura entre las entidades y las mismas personas que realizan cualquier actividad electrónica, para que de esta manera se pueda proteger el comercio electrónico.
Benavides Pérez Liliana Maribel	La interconexión electrónica general. Tema de identificación y confidencialidad.
Irigoin Fallaque Gilmer	Los estándares de seguridad, deben mejorar desde la perspectiva en el mejoramiento de las herramientas para su investigación, orientación de los usuarios y por último el incremento de la pena.

Nota.: Elaboración Propia

Nota. El estado peruano debe buscar adecuados estándares de seguridad, que ayuden a mejorar y proteger las actividades de comercio electrónico, es por ello

que al tener en cuenta lo señalado por los expertos entrevistados están de acuerdo en que se mejore las medidas de acción para así identificar las compras fraudulentas y evitar que muchas más personas sean víctimas de este tipo de delitos, de igual forma consideran que se deba incrementar la condena, mejorar la comunicación de las empresas que brindar el servicio y sus clientes.

Tabla 10

¿Qué se debe implementar dentro de la norma de delitos informáticos para poder tener un mayor resguardo del patrimonio ante la comisión de delitos cibernéticos?

Entrevistado	**Ideas fuerza**
Salazar Maza Geiner Vidal	• Realizar copias de seguridad fiables, • Contar con servidor propio. • Instalación de antivirus y antispam. • Contar periódicamente con contraseñas para mejorar la seguridad con respecto al acceso ilícito de cuentas electrónicas.
Vasquez Chavarri Cesar Ágel	Se debe implementar correctamente a todas las personas involucradas en el delito como autores y coautores del delito.
Chavez Rojas Magaly del Roció	Que haya una política de prevención
Benavides Pérez Liliana Maribel	La ley de delitos informáticos deberá incrementar sus condenas y mejorar las políticas de prevención
Benavides Pérez Liliana	Se debe considerar a los autores y cómplices de los hechos, así como a los terceros beneficiarios dentro o fuera del Estado.

Maribel	
Irigoin Fallaque Gilmer	Incorporar políticas que prevengan estos delitos

Nota. Elaboración Propia

Nota. Unas de las principales medidas que el estado peruano debe implementar dentro de la normatividad que regula los delitos informáticos, son las políticas de prevención, ya que de esta manera se podrá generar un mayor resguardo del patrimonio ante la comisión de delitos cibernéticos, lo cual ayudará a brindar una seguridad a la ciudadanía para que puedan realizar sus actividades electrónicas, sin que existe la desconfianza de que puedan ser víctimas de los delitos cibernéticos. Teniendo en cuenta todas las respuestas otorgadas por los entrevistados se puede establecer que hoy en día el comercio electrónico es una alternativa eficiente para el desarrollo económico, sin embargo, esta situación tiene la necesidad de prevenir y controlar los actos delictivos que atentan contra el patrimonio de los ciudadanos.

Tabla 11

Criterios de interpretación de técnicas de estudio de caso y fuente documental

Estudio de caso	Análisis documental
Tomando en cuenta al objetivo general el cual considera el análisis del Expediente Nº 1219-2003-HD/TC, señala que se interpuso un recurso de apelación en contra de la empresa Nuevo Mundo Holding S.A. (NMH), sobre la decisión del Juzgado Tercero de Instancia de la Audiencia Nacional	Tomando en cuenta el objetivo general es conveniente analizar lo investigado por el maestro Tenorio (2020), el cual hace referencia que los delitos cibernéticos atentan contra la intimidad, economía, propiedad intelectual y entre otros aspectos que perjudican directamente el bienestar de la sociedad, teniendo en cuenta que existe

de Lima, donde el demandado dijo que era falso que tenía una participación del 99,9999% en el Banco Nuevo Mundo (BNM), lo que supuso no tenía fundamento, o que se agregaron los derechos del proponente, ya que faltaba. Titularidad clara y / o legitimidad para generar reclamos. Agregó que el BNM fue colocado en un sistema de injerencia solo por las sentencias del BNM, lo que incluso condujo a la apertura de una causa penal ante el Juzgado Trigésimo Séptimo de lo Penal de Lima contra el representante del NMH, Sr. Jaques Simón Levy Calvo, acusado de mala conducta contra el sistema financiero; el cual fue declarado fundado el hábeas data y ordenando a la Superintendencia de Bancos y Seguros que facilite a Nuevo Mundo Holding SA la documentación necesaria, para lo cual, en la ejecución de la sentencia, el juez de primera instancia deberá actuar de conformidad con las causales 15 y 16.	conexión entre la ciberdelincuencia y el delito informático, dado que ambos conceptos no se pueden excluir, así mismo otra teoría que respalda a objetivo general es lo señalad por Tenorio (2020), el cual señala que la ciberseguridad es la mejor manera de promover el análisis y la gestión de los riesgos asociados con el entorno de la red. En este sentido, este proceso tiene como objetivo reducir las amenazas que surgen del uso de Internet. De igual forma Villanueva (2023), manifiesta acerca de las medidas de prevención en la ley de delitos informáticos. Teniendo en cuenta que se identificó que, por los resultados, bloquear IP dinámica dentro del soporte informático sería una medida de seguridad que previene el ciberdelito, con un 65% de los 20 jueces que creen que la propuesta de investigación es aplicable. De acuerdo al primer objetivo específico, el cual tendrá como base lo señalado por Hernández (2020), el cual señala que el aumento de estos delitos se debe a la pandemia Covid-19, que ha resultado en un comercio electrónico débil, ya que las compras y ventas virtuales a menudo conducen a delitos cibernéticos, por lo que esta propuesta de investigación tiene como objetivo utilizar la ciberseguridad para proteger el comercio electrónico, evitando así las transacciones fraudulentas durante el comercio y la distribución
Al tomar en consideración lo señalado en el objetivo específico 1,2, y 3, se ha tomado en cuenta lo señalado por el CN Civil - N. N, 25/01/2005 – Argentina, el cual hace mención La entidad financiera demandada es	

netamente responsable por los daños derivados de la extracción fraudulenta de los fondos que poseía un cliente en una caja de ahorros, aun cuando este, a consecuencia de un engaño, señaló su clave a quienes fueron responsables de extraer su dinero a través de la duplicación de su tarjeta de débito, pues el banco procedió de manera negligente al no contar con medios de seguridad eficientes para evitar la operatoria de 'confección de tarjetas mellizas', y no tomó en cuenta las medidas necesarias para de algún modo evitar extracciones luego que el cliente efectuara la denuncia policial".	Haciendo referencia al segundo objetivo específico se tendrá en cuenta lo señalado por Mateos (2020) Define el ciberdelito, que es una serie de actos en los que se considera ilegal una propiedad o un sistema informático. En otras palabras, el sistema criminal tradicional se utilizará para expandir y desarrollar rápidamente nuevas actividades delictivas. Para finalizar se tendrá en cuenta al tercer objetivo específico, teniendo como base lo señalado por Jiménez (2021), el cual señala que en el trasfondo de COVID-19, muchas personas dependen del apoyo de la tecnología para realizar sus diversas actividades, pagar, acceder a la plataforma en línea para estudiar o trabajar. En este sentido, los ciberdelincuentes aprovechan esta adicción para cometer tales acciones y violar la "seguridad informática" así como para "violar la integridad, confidencialidad y existencia de datos o sistemas informáticos".

Nota. Fuente propia

Nota. Para el adecuado análisis de lo obtenido se tendrá en cuenta las fuentes documentales, para sustentar lo que busca el objetivo principal que es determinar si la ciberseguridad ayudara de una manera adecuada a mejorar la estabilidad del comercio electrónico, evitando a tal manera los riesgos de phishing en tiempos de pandemia, es por ello que al realizar un análisis del Expediente Nº 1219-2003-HD/TC y a la vez lo analizado por Tenorio (2020), el cual hace referencia que los delitos cibernéticos atentan contra la intimidad, economía, propiedad intelectual y entre otros aspectos que perjudican directamente el bienestar de la sociedad, teniendo en cuenta que existe conexión entre la ciberdelincuencia y el delito

informático, dado que ambos conceptos no se pueden excluir, es por ello que a través de lo expresado en el expediente se puede señalar que en la actualidad los delitos cibernético están al paso de cada movimiento que realiza la sociedad, sin embargo hasta el día de hoy se ha visto que estos actos no son sancionado correctamente ya que en algunas circunstancias las personas que cometen este delito, no solo quedan impune sino que siguen cometiendo los mismos delitos, esto sucede a causa de que el estado peruano no presenta una adecuada legislación frente a estos delitos y peor aún no incorpora políticas de prevención para una adecuada ciberseguridad.

Teniendo en cuenta lo señalado en el CN Civil - N. N, 25/01/2005 – Argentina, y lo que busca el primero objetivo, el cual busca un adecuado análisis de la figura del del phishing y su impacto en la pandemia de la Covid 19, se logró determinar que dentro de la legislación argentina hasta el momento aún persisten estos delitos, sin embargo, las condenas son consideras más drásticas al estado peruano, de igual manera existe otro punto a favor es que cuando existen o surgen estos casos de ciberdelincuencia las personas que han sido afectada o se les ha vulnerado sus derechos, reciben una reparación acorde a lo sucedido, entonces al compararlo con lo que sucede en el estado peruano se puede evidenciar que en muchas oportunidades las personas que han vivido estos delitos han sido desprotegido por el estado peruano y nunca se logra a resolver las estos problemas afectando directamente a parte de las personas involucradas. Cabe resaltar lo señalado por Hernández (2020), el cual señala que el aumento de estos delitos se debe a la pandemia Covid-19, que ha resultado en un comercio electrónico débil, ya que las compras y ventas virtuales a menudo conducen a delitos cibernéticos, por lo que esta propuesta de investigación tiene como objetivo utilizar la ciberseguridad para proteger el comercio electrónico; es importante determinar que a través de los sucedido por la pandemia la gran mayoría de personas optaron por realizar sus actividades de manera virtual sin embargo el estado peruano no realizo o aplicado ninguna medidas de prevención para disminuir la ciberdelincuencia.

Continuando con el segundo especifico el cual busca un adecuado análisis para encontrar mejoras que puedan se aplicables frente a la ley que regula los delitos informáticos, ya que de esta manera se podrá respaldar la finalidad de

buscar los estándares adecuados para la protección de los clientes y a la vez de los usuarios en el comercio electrónico, para ello se tendrá en cuenta lo sustentado por CN Civil - N. N, 25/01/2005 – Argentina y lo investigado por Hernández (2020), el cual señala que el aumento de estos delitos se debe a la pandemia Covid-19, que ha resultado en un comercio electrónico débil, ya que las compras y ventas virtuales a menudo conducen a delitos cibernéticos, es preciso señalar que a causa del surgimiento de esta pandemia mundial, todos los estados has tenido que adecuarse de una manera inmediata a la situación, es por ello que el estado peruano ha tomado como base realizar sus actividades por medio del comercio electrónico para que de esta manera se pueda obtener beneficios dinerarios para la sostenibilidad alimenticia, sin embargo es evidente que no solo la población se ha adecuado a esta pandemia sino que las personas del mal vivir de igual forma se han venido adecuándose, es por ello el incremento de los delitos cibernéticos que afectan directamente a la población.

Para finalizar tendremos en cuenta el tercer objetivo específico el cual busca la adecuada propuesta de mejoras frente a la ley que regula los delitos informáticos, ya que tiene la finalidad de mejorar los estándares de seguridad que brinda el estado para proteger tanto a los clientes o usuarios que realizan sus actividades en el comercio electrónico, de igual forma se tendrá en cuenta lo señalado por el CN Civil - N. N, 25/01/2005 – Argentina y lo investigado por Jiménez (2021), el cual señala que en el trasfondo de COVID-19, muchas personas dependen del apoyo de la tecnología para realizar sus diversas actividades, pagar, acceder a la plataforma en línea para estudiar o trabajar. En este sentido, los ciberdelincuentes aprovechan esta adicción para cometer tales acciones y violar la “seguridad informática”, sin embargo, a sabiendas de estos actos delictuosos el estado peruano hasta el momento no ha realizado ninguna mejora en la ley, ya que es evidente que muchas personas al realizar sus actividades por medio del comercio virtual se han visto perjudica, sin que existe una solución factible y favorable para la víctima.

Al tener en cuenta todo lo obtenido en la investigación, se puede evidenciar que el estado peruano hasta el momento no toma interés de mejorar o crear políticas de prevención para que de esta manera se logre evitar cualquier acción

que pueda perjudicar a la sociedad frente a la realización de tus actividades en el comercio electrónico.

3.2. Discusión

Acerca del objetivo general: **Determinar si la ciberseguridad ayudara a mejorar el comercio electrónico y evitara los riesgos de phishing en tiempos de pandemia**, es correcto afirmar que de acuerdo a la información obtenida por la correcta aplicación de la entrevista se puede evidenciar la necesidad de determinar si la ciberseguridad ayudara a mejorar el comercio electrónico, es por ello que de acuerdo a lo obtenido en la Tabla N°1 se puede confirmar que es importante reconocer que en la actualidad a causa del surgimiento del Covid-19, la vida cotidiana que antes conocíamos ha dado un giro inesperado, ocasionando que todo el mundo se adecue de una manera inesperada e inmediata a las normas aplicadas por el estado, sin embargo, se puede evidenciar que dentro estos cambios la sociedad ha tenido que buscar alternativas para nuevos ingresos económicos, en el cual radica el problema ya que la sociedad no se encuentran segura frente a los mecanismos de ciberseguridad dentro del comercio electrónico; es por ello que al tener en cuenta lo señalado por los distintos expertos que han formado parte de la entrevista, es necesario que deban existir nuevos mecanismos de seguridad frente a los delitos cibernéticos, por el tan solo hecho de brindar una correcta y adecuada seguridad a la sociedad que puedan realizar sus actividades electrónicas de una manera justa y segura. Es importante confirmar que, en el contexto actual, debido al impacto del Covid-19, la vida diaria ha experimentado cambios drásticos, obligando a todos a adaptarse rápidamente a nuevas normativas estatales. Sin embargo, esta adaptación ha generado desafíos significativos, especialmente en términos de seguridad cibernética en el comercio electrónico. Es crucial reconocer la necesidad urgente de implementar nuevos y efectivos mecanismos de seguridad para proteger a la sociedad de los delitos cibernéticos. Expertos enfatizan la importancia de asegurar un entorno electrónico justo y seguro, permitiendo así que las actividades cotidianas puedan realizarse con confianza y protección adecuada.

Los resultados previamente mostrados, se asemejan con lo sustentado por Chávez (2020), en su investigación sobre la vulneración de la intimidad personal

frente a los delitos de datos y sistemas informáticos, para ello se utilizó una estructura de análisis de documento, lo que permitió concluir que el Estado, a través del Poder Judicial, brinda capacitación permanente a los profesionales del derecho de la Corte Superior de Justicia de Lima Norte sobre los principios generales de protección de la información pública y privada (información sensible, control, restricción de la información). Los delitos contra la persona, la seguridad personal, los daños causados por el delito de Phishing a los datos y los sistemas informáticos afectan significativamente al derecho fundamental a la privacidad personal. Es importante reconocer que la ciberseguridad es una de los principales mecanismos que ayudara rotundamente en mejorar el comercio electrónico, dado que en la realidad y a causa del covid-19, se ha evidenciado gran cantidad de casos donde los ciudadanos han sido víctima de algún tipo de delito cibernético como es el caso del phishing, originando de esta manera una inseguridad a todos los ciudadanos, pues ya no confían en el sistema actual a causa de falta de mecanismos que protejan correctamente todas sus acciones electrónicas.

El cuanto al primer objetivo específico: **Analizar la figura jurídica del phishing y su impacto en la pandemia de la Covid 19**, se ha alcanzado a obtener resultados excelentes para la investigación, ya que de esta manera se logró determinar la necesidad de una adecuada prevención por medio de la ciberseguridad. Este objetivo tiene total respaldo con lo obtenido en la Tabla N° 5 donde se muestra que el comercio electrónico se ha vuelto una alternativa eficaz frente a su rapidez, de igual forma se ha establecido como una herramienta favorable frente a la reducción del incremento del Covid-19, sin embargo, estas actividades electrónicas se han visto incrementado gracias al confinamiento realizado por el estado peruano, teniendo en cuenta que no existió preparación, control y reserva en las entidades del estado, lo que ha generado la invasión de instrumentos que vulneran el sistema informático Estatal. A través de las respuestas de los entrevistados se puede evidenciar de una manera unánime, las personas están de acuerdo en que los delitos cibernéticos se han incrementado a causa de la pandemia del Covid-19. De forma similar, tiene total semejanza con lo obtenido en la Tabla N° 6 donde se muestra que el aumento de los delitos informáticos se podrá controlar o reducir de manera eficiente, cuando el estado peruano tome conciencia de la gran cantidad de los delitos cibernéticos que se

vienen realizando en la actualidad, es por ello que se tendrá en cuenta lo obtenido por las respuestas de los entrevistados que están de acuerdo en que exista una adecuada orientación y capacitación a la ciudadanía de cómo actúa estos criminales frente a las actividades electrónicas, creando y mejorando estrategias positivas, capacitando adecuadamente a las personas que investigan estos delitos, del igual forma que las entidades bancarias entre otras de índole similar ayuden a orientar a sus clientes y entre otros aspectos.

Es importante explicar que en estos resultados se destaca el comercio electrónico como una alternativa efectiva debido a su rapidez y su papel en la mitigación del Covid-19. Sin embargo, el incremento de estas actividades durante el confinamiento en Perú reveló vulnerabilidades debido a la falta de preparación y control por parte de las entidades estatales, permitiendo la infiltración de amenazas al sistema informático estatal. Es importante mencionar que los entrevistados concuerdan en que los delitos cibernéticos han aumentado significativamente debido a la pandemia. Así mismo, es esencial que el estado peruano tome conciencia de esta situación para implementar orientación y capacitación adecuada a la ciudadanía, así como estrategias mejoradas para combatir estos delitos, involucrando tanto a investigadores como a entidades bancarias para proteger a los usuarios de actividades electrónicas.

Los resultados que han sido previamente obtenidos, se asemejan con lo sustentado por Chuco (2023) en su investigación sobre el delito de fraude informático frente al Código Penal Peruano, para ello se utilizó una estructura de tipo básico con diseño fenomenológico, donde se llegó a concluir que la falta de información adecuada sobre la tecnología informática es un factor crítico en el impacto del ciberdelito en la sociedad en general, requiriendo cada vez más conocimientos en tecnologías de la información, lo que permite un marco contextual aceptable para hacer frente a este tipo de situaciones. Al realizar un análisis legal comparativo con otros países, se determinó que Perú es un país que ciertamente controla el ciberdelito de fraude informático, sin embargo, lo hace mal porque es común, lo que genera algunos vacíos legales, lo que imposibilita las investigaciones informáticas forenses.

Cabe precisar que el phishing, es una forma de fraude informático mediante la cual los delincuentes engañan a las personas para que divulguen información personal y confidencial como contraseñas o números de tarjetas de crédito, ha tenido un impacto significativo durante la pandemia de Covid-19. Con el aumento masivo del trabajo remoto y la dependencia creciente de plataformas y servicios en línea, los ataques de phishing se han intensificado, aprovechando la incertidumbre y el miedo asociados con la crisis sanitaria global. Los estafadores han utilizado temas relacionados con el virus, como ofertas de equipos de protección personal o falsas campañas de donación, para engañar a las personas y empresas. Este tipo de fraudes no solo compromete la seguridad de los datos personales y financieros, sino que también socava la confianza en las comunicaciones digitales y representa una amenaza continua para la ciberseguridad en un entorno cada vez más digitalizado y vulnerable.

Prosiguiendo con la contrastación de los resultados, se tuvo en mención el segundo objetivo específico, **Analizar que mejoras se puede aplicar en la ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico**, cabe señalar que este objetivo busca un adecuado análisis para la correcta mejora de la ley. Es importante precisar que el objetivo previamente mostrado, tiene respaldo con lo obtenido en la Tabla N° 7 donde se muestra que las respuestas de los entrevistados son evidentes que de forma unánime los expertos manifiestan estar de acuerdo en que se deba incrementar la condena aplicada hacia las personas que cometen estos actos delictuosos, teniendo en cuenta la intensidad e inmensidad de los delitos informáticos. Es importante reconocer que el estado peruano deberá tomar un mejor interés frente a estos asuntos de manera judicial, ya que de esta manera se podrá evitar que se vulneren los derechos de las personas que realizan sus actividades de comercio electrónico. Cabe precisar que el resultado indica que los expertos entrevistados están unánimemente a favor de aumentar las penas para quienes cometen delitos informáticos, dada la gravedad y el alcance de estos actos. Así mismo, también se destaca la necesidad urgente de que el estado peruano intervenga más efectivamente en el ámbito judicial para abordar estos problemas. Esto no solo ayudaría a disuadir a los delincuentes, sino que también protegería los

derechos de las personas que realizan transacciones comerciales electrónicas, asegurando un entorno digital más seguro y justo para todos los usuarios.

Cabe reconocer que, este resultado se asemeja con lo sustentado por Villavicencio (2020) en su artículo jurídico sobre los delitos informáticos como el Phishing, el cual fue desarrollado con una estructura metodología de tipo cualitativa con análisis documental, lo que permitió concluir que el objeto de la Ley de Delitos Cibernéticos es prevenir y sancionar las conductas ilícitas que afecten a los sistemas y datos informáticos, contra los bienes, la confianza pública y la libertad sexual cometidos mediante el uso de las TIC. Las estadísticas penales de acceso ilícito, controladas en el artículo 2, están tipificadas como delito de actividad normal, ya que este acto ilícito constituye una violación de las medidas de seguridad de un sistema informático.

Es importante precisar que para mejorar la ley de delitos informáticos y garantizar estándares de seguridad efectivos en el comercio electrónico, es crucial implementar varias estrategias. En primer lugar, se debe fortalecer la legislación existente mediante la incorporación de penas más severas y proporcionales a la gravedad de los delitos cibernéticos, como el robo de datos personales o fraudes financieros. Además, es fundamental actualizar continuamente estas leyes para abordar las nuevas amenazas y técnicas utilizadas por los delincuentes digitales. Esto incluye establecer normativas claras sobre la protección de datos personales y exigir a las empresas que implementen medidas robustas de seguridad cibernética. Promover la educación y concienciación pública sobre prácticas seguras en línea también es esencial para empoderar a los usuarios y prevenir engaños como el phishing. Asimismo, facilitar la colaboración entre sectores público y privado para compartir información sobre amenazas y mejorar la respuesta ante incidentes fortalecerá aún más la defensa contra los ataques cibernéticos. Finalmente, asegurar que las instituciones judiciales cuenten con recursos y capacitación adecuados en delitos informáticos permitirá una aplicación más efectiva de la ley y una mayor protección para todos los involucrados en el comercio electrónico.

Para finalizar, se tuvo en cuenta al último objetivo específico, el cual busca **Proponer mejoras en la ley de delitos informáticos con la finalidad de buscar**

estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico, es preciso señalar que las leyes actuales que regulan los delitos cibernéticos no protegen adecuadamente a la ciudadanía, es por ello la necesidad de mejoras. Este objetivo tiene como respaldo a lo obtenido en la Tabla N° 10 donde se llega a mostrar que unas de las principales medidas que el estado peruano debe implementar dentro de la normatividad que regula los delitos informáticos, son las políticas de prevención, ya que de esta manera se podrá generar un mayor resguardo del patrimonio ante la comisión de delitos cibernéticos, lo cual ayudará a brindar una seguridad a la ciudadanía para que puedan realizar sus actividades electrónicas, sin que existe la desconfianza de que puedan ser víctimas de los delitos cibernéticos. Teniendo en cuenta todas las respuestas otorgadas por los entrevistados se puede establecer que hoy en día el comercio electrónico es una alternativa eficiente para el desarrollo económico, sin embargo, esta situación tiene la necesidad de prevenir y controlar los actos delictivos que atentan contra el patrimonio de los ciudadanos.

Este resultado, se asemeja con lo sustentado por Astorayme (2023) su estudio direccionado al análisis de los vacíos legales que presenta el delito informático Phishing en el Nuevo Código Penal peruano, para ello se utilizó una estructura de tipo básica con enfoque cualitativo, lo que permitió concluir que la falta de información adecuada sobre las limitaciones de la tecnología de la información es un factor crucial en el impacto del ciberdelito Phishing en la sociedad en general, requiriendo cada vez más conocimientos en tecnología de la información, lo que permite un marco contextual aceptable para hacer frente a tales situaciones. Las nuevas formas de comercio online son un claro ejemplo de cómo los delitos pueden manifestarse de diferentes formas, por lo que es necesario crear herramientas legales efectivas para abordar esta problemática, cuyo único propósito es sustentar el marco legal.

Es importante precisar que para fortalecer la ley de delitos informáticos y mejorar los estándares de seguridad en el comercio electrónico, es fundamental implementar varias medidas clave. Primero, actualizar y ampliar las penalidades para los delitos cibernéticos, asegurando que sean proporcionales a la gravedad de los ataques y fraudes. Segundo, establecer normativas estrictas sobre la

protección de datos personales y la seguridad de la información en línea, obligando a las empresas a adoptar prácticas de seguridad robustas y transparentes. Tercero, promover la colaboración entre el sector público y privado para compartir información sobre amenazas y desarrollar respuestas conjuntas frente a incidentes cibernéticos. Cuarto, invertir en educación y concienciación pública sobre los riesgos cibernéticos y las mejores prácticas para proteger la información personal y financiera. Estas acciones no solo fortalecerán la confianza de los consumidores en el comercio electrónico, sino que también reducirán significativamente la incidencia de fraudes y delitos informáticos.

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

1. Se ha logrado determinar que a través de una adecuada ciberseguridad se alcanzara a mejorar convenientemente el comercio electrónico, es por ello que se debió establecer mecanismos de actualizaciones de protección de datos digitales, capacitación al personal judicial y policial en delitos informáticos, a ello se le debe sumar la protección a través de software en las distintas empresas que manejan datos de clientes, ya que ha sido evidenciado durante el tiempo de pandemia esos delitos se incrementaron, afectado directamente a la sociedad sin que existan mecanismos adecuados para su adecuada reducción.
2. De acuerdo al análisis realizado a la figura jurídica del delito de Phishing, se pudo determinar que el Estado Peruano y las empresas privadas no estuvieron preparadas para afrontar una pandemia, desde el punto de vista de seguridad digital, a ello se le sumo el desconocimiento y la falta de capacitación de los órganos administradores de justicia y también falto un control y supervisión de las entidades financieras.
3. Para mejorar los estándares de seguridad del Estado peruano, respecto al uso de la tecnología para fines delictivos, se deben implementar mecanismos de control que ayuden a disminuir los delitos cibernéticos, así mismo se debe buscar que las entidades financieras busquen adecuar sus políticas de seguridad bajo un sistema unificado de datos, ello con la finalidad de proteger y brindar seguridad a sus usuarios.
4. Conforme a todo lo desarrollado en la investigación, se ha logrado demostrar que las mejoras que se deben implementar son:
    a) Mejoras en software informáticos de control y seguridad en las entidades financieras
    b) Mejor capacitación a los peritos policiales y fiscales en delitos de phishing
    c) Actualizaciones constantes de bases de datos.
    d) Plantear que se incorpore a la Ley de delitos informáticos la criminalidad organizada en los delitos de fraude informático.

4.2. Recomendaciones

1. Es de vital importancia que el Estado peruano, implemente mecanismos de control, adecuado sistemas de capacitación al personal de justicia, las entidades financieras y los propios usuarios con la finalidad de proteger su integridad patrimonial en las compras virtuales que estos realicen, del mismo modo buscar implementar la agravante de pluralidad de agentes en la ley de delitos informáticos.
2. Dentro de la legislación peruana el poder ejecutivo deberá incorporar adecuadas políticas de ciberseguridad en la ley que regula y sanciona los delitos cibernéticos, para que de esta manera se pueda reducir exponencialmente estos delitos que atentan contra el bienestar de toda una población que realizan sus actividades por medio del comercio electrónico.
3. El estado peruano deberá brindar adecuada información para la correcta capacitación hacia la población entera de cómo actúan las personas que realizan estos actos delictivos, para que de esta manera tenga mejor prevención al realizar alguna actividad dentro del comercio electrónico.
4. Que los filtros actuales que se encuentran predeterminados para la realización del comercio electrónico, sean mejorados desde una perspectiva de una comunicación tanto desde el cliente y la empresa que está brindando el servicio, para que de esta manera se pueda mejorar la seguridad de la transacción.

REFERENCIAS

Aboso, G. (2019). *La nueva regulación de los llamados 'delitos informáticos' en el Código Penal argentino*, Revista de Derecho Penal.

Adamu (2022) "Concern for e-Commerce Security"

Alcantara, F.E., Delgado, R.E., (2024). Análisis de la ley 30096 de delitos informáticos en su aplicación a los delitos de fraude informático en el Perú, 2022. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/12384/Alcantara%20Diaz%2C%20Fabian%20Eduardo.pdf?sequence=1&isAllowed=y

Arias, J (2020). "Proyecto de tesis Guía para la elaboración". p.43; 48.

Astorayme, J.L. (2023). Ciberdelincuencia y la implementación de Fiscalías Especializadas en San Juan de Miraflores, 2022. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/121896/Astorayme_SJL-SD.pdf?sequence=1

Bustos, M. (2021) Técnicas e instrumentos para recoger datos del hecho social educativo. Revista Científica Retos de la Ciencia, 5(10), 50-61. https://acortar.link/xNu5SZ

Cadillo, B. A., (2022). La evidencia digital en el cibercrimen Perú 2022. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.upn.edu.pe/bitstream/handle/11537/32802/Cadillo%20Quispe%2C%20Bryan%20Antonio.pdf?sequence=1&isAllowed=y

Campos, A., Hernández, M. A., & Aniceto, P. F. (2021). Análisis documental del concepto estrategias de aprendizaje aplicado en el contexto universitario.

PSICUMEX, 11. Obtenido de https://www.scielo.org.mx/pdf/psicu/v11/2007-5936-psicu-11-e395.pdf

Chávez Rodríguez, E. G. (2020). *El delito contra datos y sistemas informáticos en el derecho fundamental a la intimidad personal en la corte superior de justicia de lima norte, 2017*, [Tesis de doctorado, Universidad Nacional Federico Villareal] http://repositorio.unfv.edu.pe/bitstream/handle/UNFV/2704/CHAVEZ%20RODRIGUEZ%20ELIAS%20GILBERTO%20-%20DOCTORADO.pdf?sequence=1&isAllowed=y

Chuco, E.Y. (2023). Análisis del delito de fraude informático y hurto como delito previo, Cercado de Lima – 2020. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/125058/Chuco_REY-SD.pdf?sequence=1&isAllowed=y

Delgado, F.J. (2022). El tratamiento penal de los delitos informáticos contra el patrimonio de las personas naturales y jurídicas en la corte superior de justicia del santa – Chimbote. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/10400/Delgado%20Benites%2C%20Francisco%20Javier.pdf?sequence=1&isAllowed=y

Devia Gonzales, E. A. (2021). *Delito informático: estafa informática del artículo 248.2 del Código Penal*, Sevilla, [Tesis de doctorado, Universidad de Sevilla] https://acortar.link/OncayJ

Espinoza Céspedes, J. F. (2019). *Contratación electrónica, medidas de seguridad y derecho informático*, Editora Raó.

Estrada, R.D., Unás, J.L., Flórez, O.E. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2422-42002021000300098

Fernández Bermejo, D. y Martínez Atienza, G (2019). *Ciberseguridad, ciberespacio y ciberdelincuencia*, Editorial Aranzadi.

Hernandez, Sampieri, R. (2020). *Metodología de la investigación científica*, Interamericana Editores.

Horianski, J. E. (2020). *La protección penal ante el avance tecnológico y la delincuencia cibernética,* [Tesis de pre grado, Universidad siglo 21] https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/14687/HORIANSKI%20JORGE.pdf?sequence=1&isAllowed=y

Jiménez Herrera, J. C. (2021). *Manual de derecho penal informático*, Jurista Editores.

La Gestión (11 de diciembre 2020). *Ciberseguridad en el Perú: ¿Qué tan preparados estamos para enfrentar la ciberdelincuencia?*, https://gestion.pe/publirreportaje/ciberseguridad-en-el-peru-que-tan-preparados-estamos-para-enfrentar-la-ciberdelincuencia-noticia/?ref=gesr

Lazaro (2019) “Medios técnicos en la investigación de los delitos informáticos”. Especial referencia a la tecnovigilancia, Consejo General del Poder Judicial, Madrid.

Lázaro, R. (2021). Entrevistas estructuradas, semi-estructuradas y libres. Análisis de contenido. Ediciones de la Universidad de Castilla-La Mancha. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=7993166

León, Y.A. (2018). Bloqueo del ip dinámico dentro del comercio electrónico como medida de prevención de los delitos informáticos de la Ley 30096. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/5463/Le%C3%B3n%20Ochoa%20Yorli%20Adrian.pdf?sequence=1&isAllowed=y

Llaque Facho, N. I. y Piñin Morocho, D. A. (2020). *Aplicación de un modelo de aceptación de comercio electrónico en la ciudad de Chiclayo*, [Tesis de pre grado, Universidad Católica Santo Toribio de Mogrovejo] http://tesis.usat.edu.pe/bitstream/20.500.12423/2630/1/TL_LlaqueFachoNahomi_Pi%c3%b1inMorochoDaniela.pdf

Madariaga, M. (1988). *Reflexiones sobre delitos relacionados con tarjetas de crédito*, Revista La Ley.

Mateos Pascual, I. (2020). *Ciberdelincuencia. Desarrollo y persecución tecnológica*, [Tesis de pre grado, Universidad Politécnica de Madrid], https://oa.upm.es/22176/1/PFC_IVAN_MATEOS_PASCUAL.pdf

Ministerio de Justicia y Derechos humanos (2022). Ciberdelincuencia reporte de información estadística y recomendaciones para la prevenció. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf

Molinos, A. (2020). El Fraude Informático y Telemático, Perspectiva Penal. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://uvadoc.uva.es/bitstream/handle/10324/46997/TFG-D_01089.pdf?sequence=1&isAllowed=y

Ormaza, J.G., López, C.I., Muñoz, L., Zambrano, A.D. (2021). Ataques informáticos en tiempos de pandemia COVID19 en Latinoamérica: Revisión Bibliográfica. chrome-

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.espam.edu.ec/recursos/sitio/informativo/archivos/ponencias/sigloxxi/XI/CIDEIT/S3/CIDEIT-S3-009.pdf

Paredes Pérez, J. M. (2020). *De los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, en el periodo 2009-2010*, Lima, [Tesis de maestría, Universidad Nacional Mayor de San Marcos] https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/10314/Paredes_pj.pdf?sequence=3&isAllowed=y

Parra Perea, R. G. (2020). *Proyecto legal para un esquema nacional de ciber seguridad*, [Tesis de pre grado, Universidad de San Martín de Porres] https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/2051/parra_prg.pdf?sequence=1&isAllowed=y

Peralta Cuadrado, M. L. y Roa Ibarra, E. E. (2020). *El impacto del delito cibernético en las operaciones de comercio electrónico*, [Tesis de pre grado, Universidad de Córdova] https://repositorio.unicordoba.edu.co/bitstream/handle/ucordoba/3949/EL%20IMPACTO%20DEL%20DELITO%20CIBERN%C3%89TICO%20EN%20LAS%20OPERACIONES%20DE%20COMERCIO%20ELECTR%C3%93NICO%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y

Pereyra, G. (2012). *México: violencia criminal y guerra contra el narcotráfico*. Revista Mexicana de Sociología.

Quevedo Gonzales, J. M. (2020). *Investigación y prueba del ciberdelito,* [Tesis de pre grado, Universidad de Barcelona] https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1&isAllowed=y

Roman, E.H. (2020). Modificación legislativa de la ley 30096 de delitos informáticos para su eficacia contra la ciberdelincuencia en la ciudad de Chiclayo. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/10463/Roman%20Cruz%20Eucario%20Hector.pdf?sequence=1&isAllowed=y

Salinas Siccha, R. (2020). *Derecho penal. Parte especial*, Editorial Grijley.

Salom Closet, J. (2019). *El ciberespacio y el crimen organizado*, Revista Jurídica

Schroder, H. Z. (2021). Las normas técnicas en el Perú: marco teórico y legal. Lima : Foro jurídico (Lima), N° 16.

Simón Hocsman, H. (2020). *Los contratos electrónicos, Comercio electrónico. Estructura operativa y jurídica*, Hammurabi

Tenorio Pereyra, J. E. (2019). *Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia*, Academia Diplomática del Perú Javier Pérez de Cuéllar, http://repositorio.adp.edu.pe/bitstream/handle/ADP/71/2018%20Tesis%20Tenorio%20Pereyra%2c%20Julio%20Eduardo.pdf?sequence=1&isAllowed=y

Torrente, M. (2020). *El comercio electrónico a través del consumidor en las empresas que desarrollan actividades de ventas online en la ciudad de Panamá*, [Tesis de pre grado, Universidad Internacional de Ciencia y Tecnología] http://www.idi-unicyt.org/wp-content/uploads/2020/10/Mayra-Torrente-TG-Definitivo.pdf

Unión Internacional de Telecomunicaciones (2014). *Comprensión de ciberdelito: fenómenos, dificultades y respuesta jurídica*, Ginebra, Oficina de Desarrollo de las Telecomunicaciones.

Villanueva, J.A., (2023). Ley de delitos Informáticos N° 30096 y su influencia en La Población de Chiclayo en tiempos de Covid-19. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/10627/Villanueva%20Calderon%20Juan%20Amilcar.pdf?sequence=1&isAllowed=y

Villavicencio Terreros, F. (2020). *Delitos Informáticos*, [Tesis de pre grado, Universidad Nacional de San Marcos], https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

ANEXOS

Anexo 01: Resolución de aprobación de Tema de Investigación

Universidad Señor de Sipán

FACULTAD DE DERECHO Y HUMANIDADES
RESOLUCIÓN N° 0954-2023/FADHU-USS

Pimentel, 20 de octubre del 2023

VISTO:
El oficio N° 0524-2023/FADHU-ED-USS de fecha 13 de octubre del 2023, presentado por la Escuela Profesional de Derecho, quien informa que la (los) estudiante **ZAMORA VASQUEZ KARIN JUNET**, solicita el cambio de TÍTULO de **Investigación (tesis)**; Y,

CONSIDERANDO:
Que, la Constitución Política del Perú en su Artículo 18° establece que: *"La educación universitaria tiene como fines la formación profesional, la difusión cultural, la creación intelectual y artística y la investigación científica y tecnológica (...)".*

Que, acorde con lo establecido en el Artículo 8° de la Ley Universitaria, Ley N° 30220, *"La autonomía inherente a las Universidades se ejerce de conformidad con lo establecido en la Constitución, la presente ley demás normativa aplicable. Esta autonomía se manifiesta en los siguientes regímenes: normativo, de gobierno, académico, administrativo y económico"*. La Universidad Señor de Sipán desarrolla sus actividades dentro de su autonomía prevista en la Constitución Política del Estado y la Ley Universitaria N° 30220.

Que, acorde con lo establecido en la Ley Universitaria N°30220; indica:
- Artículo N° 6°: Fines de la Universidad, Inciso 6.5) "Realizar y promover la investigación científica, tecnológica y humanística la creación intelectual y artística".

Según lo establecido en el Artículo 45° de la Ley Universitaria, Ley N° 30220, *"Obtención de Grados y Títulos; Para la obtención de grados y títulos se realiza de acuerdo a las exigencias académicas que cada universidad establezca en sus respectivas normas internas.*

Que, el Reglamento de Investigación de la USS Versión 8, aprobado con Resolución de Directorio N°015-2022/PD-USS, señala:

- Artículo 72°: Aprobación del tema de investigación: El Comité de Investigación de la escuela profesional eleva los temas del proyecto de investigación y del trabajo de investigación que esté acorde a las líneas de investigación institucional a Facultad para la emisión de la resolución.

- Artículo 73°: Aprobación del proyecto de investigación El (los) estudiante (s) expone ante el Comité de Investigación de la escuela profesional el proyecto de investigación para su aprobación y emisión de la resolución de facultad.

Que, Reglamento de Grados y Títulos Versión 09 aprobado con resolución de directorio N° 0120-2022/PD-USS, señala:
- Artículo 21°: "Los temas de trabajo de investigación, trabajo académico y tesis son aprobados por el Comité de Investigación y derivados a la facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El periodo de vigencia de los mismos será de dos años, a partir de su aprobación (...).

- Artículo 24°: *"La tesis, es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela académico profesional (...)".*

- Artículo 25°: *"El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C".*

Que, mediante Resolución N° 0935-2023/FADHU-USS de fecha 16 de octubre del 2023, se resuelve aprobar el tema de investigación (tesis) denominado: **"CYBERSEGURIDAD PARA MEJORAR EL COMERCIO ELECTRÓNICO Y EVITAR LOS RIESGOS DE PHISHING EN TIEMPOS DE PANDEMIA.CHICLAYO 2021"**, presentado por la estudiante **ZAMORA VASQUEZ KARIN JUNET**.

Universidad Señor de Sipán

RESOLUCIÓN N° 0954-2023/FADHU-USS

Que, mediante el oficio N° 0524-2023/FADHU-ED-USS de fecha 13 de octubre del 2023, remitido por la Escuela Profesional de Derecho, quien eleva la solicitud presentada por la (el) estudiante **ZAMORA VASQUEZ KARIN JUNET**, en donde solicita el cambio del tema de investigación (tesis) denominado: "**CYBERSEGURIDAD PARA MEJORAR EL COMERCIO ELECTRÓNICO Y EVITAR LOS RIESGOS DE PHISHING EN TIEMPOS DE PANDEMIA.CHICLAYO 2021**", por el denominado: **"LA CIBERSEGURIDAD EN EL COMERCIO ELECTRONICO Y LOS RIESGOS DE PHISHING EN TIEMPOS DE PANDEMIA. CHICLAYO 2022"**.

Estando a lo expuesto y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes.

SE RESUELVE:

ARTÍCULO PRIMERO: **AUTORIZAR** y **APROBAR** el **cambio del tema de investigación Tesis** del denominado: "**CYBERSEGURIDAD PARA MEJORAR EL COMERCIO ELECTRÓNICO Y EVITAR LOS RIESGOS DE PHISHING EN TIEMPOS DE PANDEMIA.CHICLAYO 2021**", por el denominado: **"LA CIBERSEGURIDAD EN EL COMERCIO ELECTRONICO Y LOS RIESGOS DE PHISHING EN TIEMPOS DE PANDEMIA. CHICLAYO 2022**" presentado por la (los) estudiante **ZAMORA VASQUEZ KARIN JUNET**.

ARTÍCULO SEGUNDO: **DEJAR SIN EFECTO** la Resolución N° 0935-2023/FADHU-USS de fecha 16 de octubre del 2023.

ARTÍCULO TERCERO: **DISPONER** que las áreas competentes tomen conocimiento de la presente resolución con la finalidad de dar las facilidades para la ejecución de la presente Investigación

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Dra. Dioses Lescano Nelly
Decana de la Facultad de Derecho y Humanidades

Mg. Delgado Vega Paula Elena
Secretaria Académica Facultad de Derecho y Humanidades

Anexo 02: Acta de Aprobación de Asesor

Universidad Señor de Sipán

ACTA DE APROBACIÓN DEL ASESOR

Yo **Mg. Delgado Fernández Rosa Elizabeth,** quien suscribe como asesor designado mediante Resolución de Facultad Nº 0955-2023/FADHU-USS del proyecto de investigación titulado " **"La Ciberseguridad en el Comercio Electrónico y los Riesgos de Phishing en tiempos de Pandemia. Chiclayo 2022"** desarrollado por el estudiante: **Bach. Zamora Vásquez Karin Junet**, del programa de estudios de **Derecho de la Universidad Señor de Sipán**, acredito haber revisado, y declaro expedito para que continúe con el trámite pertinentes.

En virtud de lo antes mencionado, firma:

Mg. Delgado Fernández Rosa Elizabeth	DNI: 16452199	

Pimentel, 11 de junio de 2024.

Anexo 03: Acta de Originalidad

USS	ACTA DE SEGUNDO CONTROL DE REVISIÓN DE SIMILITUD DE LA INVESTIGACIÓN	Código:	F3.PP2-PR.02
		Versión:	02
		Fecha:	18/04/2024
		Hoja:	1 de 1

Yo, **Martha Olga Marruffo Valdivieso** , coordinadora de investigación del Programa de Estudios de derecho, he realizado el segundo control de originalidad de la investigación, el mismo que está dentro de los porcentajes establecidos para el nivel de Pregrado según la Directiva de similitud vigente en USS; además certifico que la versión que hace entrega es la versión final del informe titulado: **"LA CIBERSEGURIDAD EN EL COMERCIO ELECTRONICO Y LOS RIESGOS DE PHISHING EN TIEMPOS DE PANDEMIA. CHICLAYO 2022"**

Elaborado por el Bachiller **ZAMORA VASQUEZ KARIN JUNET**

Se deja constancia que la investigación antes indicada tiene un índice de similitud del **23%**, verificable en el reporte final del análisis de originalidad mediante el software de similitud TURNITIN.

Por lo que se concluye que cada una de las coincidencias detectadas no constituyen plagio y cumple con lo establecido en la Directiva sobre índice de similitud de los productos académicos y de investigación vigente.

Pimentel, 09 de octubre de 2024

Mg. Martha Olga Marruffo Valdivieso
Coordinador de Investigación
Escuela Profesional de Derecho
DNI N° 43647439

Anexo 04: Instrumento

Entrevista

"LA CIBERSEGURIDAD EN EL COMERCIO ELECTRONICO Y LOS RIESGOS DE PHISHING EN TIEMPOS DE PANDEMIA. CHICLAYO 2022"

Estimado (a): Se le solicita su valiosa colaboración para que absuelva las preguntas de acuerdo a su criterio y experiencia profesional. Esta técnica de recolección de datos de entrevista de profundidad, posteriormente será analizada e incorporada a la investigación con el título descrito líneas arriba. Donde todo lo obtenido será utilizado para la investigación respetando los criterios de confidencialidad.

Guía de entrevista

TÍTULO: "La Ciberseguridad en el Comercio Electronico y los Riesgos de Phishing en tiempos de Pandemia. Chiclayo 2022"

Entrevistado: ……..…….

Cargo/ Profesión/ Grado académico: …….....

Institución:

OBJETIVO GENERAL

DETERMINAR SI LA CIBERSEGURIDAD AYUDARA A MEJORAR EL COMERCIO ELECTRÓNICO Y EVITARA LOS RIESGOS DE PHISHING EN TIEMPOS DE PANDEMIA.

Preguntas:

1. ¿Por qué debe existir mecanismos de ciberseguridad dentro del comercio electrónico?

   ……
   ……
   ……
   ……
   ……
2. ¿Cuáles son los beneficios de aplicar mecanismos de ciberseguridad dentro del comercio electrónico?

   ……
   ……
   ……

OBJETIVO ESPECÍFICO 1

IDENTIFICAR QUÉ MEDIDAS DE SEGURIDAD SE PUEDEN IMPLEMENTAR EN EL COMERCIO ELECTRÓNICO.

3. ¿Cuáles considera usted que son las medidas que se pueden implementar para mejorar el comercio electrónico y evitar los riesgos del phishing?

   ……
   ……
   ……
   ……
   ……

4. ¿De qué manera el Estado peruano podría brindar una adecuada protección tecnológica frente a los fraudes electrónicos?

   ……
   ……
   ……
   ……
   ……

OBJETIVO ESPECÍFICO 2

ANALIZAR LA FIGURA JURÍDICA DEL PHISHING Y SU IMPACTO EN LA PANDEMIA DE LA COVID 19.

Preguntas:

5. ¿Por qué ha aumentado de manera considerable los delitos informáticos que atentan contra el patrimonio en tiempos de Covid 19?

   ……
   ……
   ……
   ……
   ……

6. ¿De qué manera se puede controlar el aumento de delitos informáticos que atentan contra el patrimonio?

   ……
   ……
   ……
   ……
   ……

OBJETIVO ESPECÍFICO 3

ANALIZAR QUE MEJORAS SE PUEDE APLICAR EN LA LEY DE DELITOS INFORMÁTICOS CON LA FINALIDAD DE BUSCAR ESTÁNDARES DE SEGURIDAD PARA PROTEGER A LOS CLIENTES O USUARIOS EN EL COMERCIO ELECTRÓNICO

Preguntas:

7. ¿Qué mejoras puede aplicar el legislador en la Ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico?

   ……
   ……
   ……
   ……
   ……

8. ¿A qué se debe la inseguridad del comercio electrónico en el Perú?

   ……
   ……
   ……
   ……
   ……

OBJETIVO ESPECÍFICO 4

PROPONER MEJORAS EN LA LEY DE DELITOS INFORMÁTICOS CON LA FINALIDAD DE BUSCAR ESTÁNDARES DE SEGURIDAD PARA PROTEGER A LOS CLIENTES O USUARIOS EN EL COMERCIO ELECTRÓNICO.

9. ¿Cuáles son los estándares de seguridad que debe buscar el Estado para proteger a los clientes o usuarios en el comercio electrónico?

   ……
   ……
   ……
   ……
   ……

10. ¿Qué se debe implementar dentro de la norma de delitos informáticos para poder tener un mayor resguardo del patrimonio ante la comisión de delitos cibernéticos?

    ……
    ……
    ……
    ……
    ……

- **Guías de análisis documental realizadas**

FICHA DOCUMENTAL 1

OBJETIVO GENERAL
Determinar si la ciberseguridad ayuda a mejorar el comercio electrónico para evitar los riesgos de phishing en tiempos de pandemia

Fuente	Expediente Nº 1219-2003-HD/TC
Contenido de la fuente	Con fecha 21 de agosto de 2001, el recurrente interpone acción de hábeas data contra la Superintendencia de Banca y Seguros (SBS), con el objeto de que se le proporcione la información denegada por carta notarial, de fecha 18 de julio de 2001. Alega que se vulnera su derecho de acceso a la información documentada, por cuanto no se le han proporcionado copias de los documentos que los interventores designados por la SBS en el Banco Nuevo Mundo (BNM) entregaron al Banco Interamericano de Finanzas (BIF). Agrega que el pedido incluye copias sobre cualquier data informática y las claves o códigos de acceso a información del BNM que pudiera habérseles entregado.
Análisis	Señala que se interpuso un recurso de apelación en contra de la empresa Nuevo Mundo Holding S.A. (NMH), sobre la decisión del Juzgado Tercero de Instancia de la Audiencia Nacional de Lima, donde el demandado dijo que era falso que tenía una participación del 99,9999% en el Banco Nuevo Mundo (BNM), lo que supuso no tenía fundamento, o que se agregaron los derechos del proponente, ya que faltaba. Titularidad clara y / o legitimidad para generar reclamos. Agregó que el BNM fue colocado en un sistema de injerencia solo por las sentencias del BNM, lo que incluso condujo a la apertura de una causa penal ante el Juzgado Trigésimo Séptimo de lo Penal de Lima contra el representante del NMH, Sr. Jaques Simón Levy Calvo, acusado de mala conducta contra el sistema financiero; el cual fue declarado fundado el hábeas data y ordenando a la Superintendencia de Bancos y Seguros que facilite a Nuevo Mundo Holding SA la documentación necesaria, para lo cual, en la ejecución de la sentencia, el juez de primera instancia deberá actuar de conformidad con las causales 15 y 16.
Recensión critica	Independientemente de que entre la recurrente en este proceso y la investigada en el proceso penal no exista identidad -si es que acaso, tal identidad sea necesaria-, resulta claro, a partir de todo lo expuesto, que el artículo 73° del Código de Procedimientos Penales no es aplicable al caso de autos. En efecto, sucede que, de conformidad con el inciso 4) del artículo 139°, uno de los principios que informan todo proceso judicial es su publicidad, salvo que exista disposición contraria de la ley. Y si bien el artículo 73° del Código de Procedimientos Penales ha establecido, con carácter general (generalidad que ahora este Tribunal no va a juzgar), que la "instrucción tiene carácter reservado", tal reserva no se extiende a toda actuación procesal.

FICHA DOCUMENTAL 2

OBJETIVO ESPECIFICO 1
Analizar la figura jurídica del phishing y su impacto en la Covid 19

Fuente	CN Civil - N. N, 25/01/2005 – Argentina

Contenido de la fuente	Se debe pagar una indemnización por el daño a la economía que tenga, ya que el error en la emisión de una tarjeta de crédito a nombre del jugador como consecuencia de la negligencia del demandante, demuestra que bien mantenido, brindando inteligencia o esfuerzo para evitarlo, también afectará la dignidad o la belleza del jugador disfruta de su negocio. (CN Civil, sala H, Magarelli, Sergio Gustavo, Tarshop S.A. s/ daños y perjuicios, 24/10/2012, publicado en: La Ley Online, cita online: ar/jur/62242/2012).
Análisis	La entidad financiera demandada es responsable por los daños derivados de la extracción fraudulenta de los fondos que poseía un cliente en una caja de ahorros, aun cuando este, a raíz de un engaño, reveló su clave a quienes luego extrajeron su dinero a través de la duplicación de su tarjeta de débito, pues el banco actuó de manera negligente al no disponer de medios de seguridad eficientes para evitar la operatoria de 'confección de tarjetas mellizas', y no tomó las medidas necesarias para evitar extracciones luego que el cliente efectuara la denuncia policial".
Recensión	En una afectación que ha generado daños y perjuicios a una cuenta corriente bancaria mediante la presentación de un DNI falso, la negativa del actor frente al pedido formulado por el banco demandado para que presente copias certificadas de determinada documentación, no exime a aquel de responsabilidad ni justifica su actitud pasiva respecto a la tramitación tendiente a que se excluya al actor de la lista de inhabilitados del sistema financiero ya que, la documentación requerida pudo ser solicitada por el banco a los organismos públicos correspondientes, sin perjuicio de lo cual, la actitud renuente del actor puede ser ponderada como atenuante al momento de la cuantificación de las eventuales indemnizaciones.

FICHA DOCUMENTAL 3

OBJETIVO ESPECIFICO 2
Analizar las posibles mejoras en la legislación de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger de manera efectiva a los clientes o usuarios en el comercio electrónico.

Fuente	EXP. N.° 01189-2019-PHC/TC
Contenido de la fuente	Con fecha 18 de julio de 2018, don William Benardino García Rosales interpone demanda de habeas corpus a favor de don Marcos Morales Vargas (f. 31) y la dirige contra los jueces integrantes de la Primera Sala Penal de la Corte Superior de Justicia de Lima Norte y la jueza a cargo del Décimo Juzgado Penal de Lima Norte. Solicita que se declare la nulidad de: (i) la sentencia de 16 de junio de 2017 (f. 3), que condenó al beneficiario por los delitos de fraude informático y falsificación de firma en documento privado; y (ii) la Resolución de 26 de diciembre de 2017 (f. 73), que confirmó la precitada sentencia en cuanto a la condena, pero la revocó respecto a la pena; y, reformándola, le impuso ocho años de pena privativa de la libertad efectiva (Expediente 9405-2014). Se alega la vulneración de los derechos a la libertad personal, al debido proceso y a la tutela jurisdiccional efectiva, así como del principio de legalidad penal.
Análisis	El objeto de la demanda es que se declare la nulidad de: (i) la sentencia de 16 de junio de 2017, que condenó a don William Benardino García Rosales por los delitos de fraude informático y falsificación de firma en documento privado; y, (ii) la Resolución de 26 de diciembre de 2017, que confirmó la precitada sentencia en cuanto a la condena, pero la revocó respecto a la

	pena; y reformándola, le impuso seis años de pena privativa de la libertad efectiva (Expediente 9405-2014). Se alega la vulneración de los derechos a la libertad personal, al debido proceso y a la tutela jurisdiccional efectiva, así como del principio de legalidad penal.
Recensión	Por tanto, resulta igualmente claro que la dimensión subjetiva del derecho a la legalidad penal no puede estar al margen del ámbito de los derechos protegidos por la justicia constitucional, frente a supuestos como la creación judicial de delitos o faltas y sus correspondientes supuestos de agravación o, incluso, la aplicación de determinados tipos penales a supuestos no contemplados en ellos. El derecho a la legalidad penal vincula también a los jueces penales y su eventual violación posibilita obviamente su reparación mediante este tipo de procesos de tutela de las libertades fundamentales.

FICHA DOCUMENTAL 4

OBJETIVO ESPECIFICO 3
Proponer mejoras en la legislación de delitos informáticos para que brinden una protección a los usuarios en el comercio electrónico.

Fuente	RECURSO DE NULIDAD N.° 206-2019
Contenido de la fuente	Se imputó al procesado don David Ricardo Moretti Valdivia que junto a otros coprocesados efectuó operaciones fraudulentas de los fondos de las tarjetas de débito y crédito del Banco Interbank, cuyo titular es don Mario Enrique Granda Cueto; se realizó transferencias y pagos entre los meses de noviembre y diciembre de dos mil diez, por montos ascendentes a diecisiete mil ciento veinte soles y seiscientos sesenta y ocho dólares estadounidenses, para lo cual habrían obtenido el número de la tarjeta y la clave token del agraviado, por medio de páginas web falsas, creadas con el fin de acceder a la cuenta bancaria del agraviado, además se actualizó el número del teléfono del contacto del Banco Interbank para recabar la clave a través de mensajes de textos.
Análisis	Además, debe tenerse en cuenta que es línea pacifica en la jurisprudencia de esta Instancia Suprema la imposición de reparación civil en los delitos de peligro, como se recoge en el Recurso de Nulidad N.° 1895-2016-Callao, del treinta de mayo de dos mil diecisiete, en cuyo fundamento tres punto cuatro se reconoce que existen daños a la sociedad que no pueden ser viables de cuantificar, por lo que cabe de que la reparación se determine objetivamente en consideración a “la gravedad del delito”, su trascendencia y de tal forma que no resulte un monto ínfimo.
Recensión	La adquisición de la nueva tecnología para la lucha contra el crimen organizado, para optimizar y fortalecer acciones contra la delincuencia, así como su ejecución de operaciones diversas, constituye el daño emergente.

- **Ficha de estudio del caso**

Título:

SENTENCIA DEL TRIBUNAL CONSTITUCIONAL

Fuente	Expediente Nº 1219-2003-HD/TC
Contenido de la fuente	Con fecha 21 de agosto de 2001, el recurrente interpone acción de hábeas data contra la Superintendencia de Banca y Seguros (SBS), con el objeto de que se le proporcione la información denegada por carta notarial, de fecha 18 de julio de 2001. Alega que se vulnera su derecho de acceso a la información documentada, por cuanto no se le han proporcionado copias de los documentos que los interventores designados por la SBS en el Banco Nuevo Mundo (BNM) entregaron al Banco Interamericano de Finanzas (BIF). Agrega que el pedido incluye copias sobre cualquier data informática y las claves o códigos de acceso a información del BNM que pudiera habérseles entregado.
Análisis	Señala que se interpuso un recurso de apelación en contra de la empresa Nuevo Mundo Holding S.A. (NMH), sobre la decisión del Juzgado Tercero de Instancia de la Audiencia Nacional de Lima, donde el demandado dijo que era falso que tenía una participación del 99,9999% en el Banco Nuevo Mundo (BNM), lo que supuso no tenía fundamento, o que se agregaron los derechos del proponente, ya que faltaba. Titularidad clara y / o legitimidad para generar reclamos. Agregó que el BNM fue colocado en un sistema de injerencia solo por las sentencias del BNM, lo que incluso condujo a la apertura de una causa penal ante el Juzgado Trigésimo Séptimo de lo Penal de Lima contra el representante del NMH, Sr. Jaques Simón Levy Calvo, acusado de mala conducta contra el sistema financiero; el cual fue declarado fundado el hábeas data y ordenando a la Superintendencia de Bancos y Seguros que facilite a Nuevo Mundo Holding SA la documentación necesaria, para lo cual, en la ejecución de la sentencia, el juez de primera instancia deberá actuar de conformidad con las causales 15 y 16.
Recensión critica	Independientemente de que entre la recurrente en este proceso y la investigada en el proceso penal no exista identidad -si es que acaso, tal identidad sea necesaria-, resulta claro, a partir de todo lo expuesto, que el artículo 73° del Código de Procedimientos Penales no es aplicable al caso de autos. En efecto, sucede que, de conformidad con el inciso 4) del artículo 139°, uno de los principios que informan todo proceso judicial es su publicidad, salvo que exista disposición contraria de la ley. Y si bien el artículo 73° del Código de Procedimientos Penales ha establecido, con carácter general (generalidad que ahora este Tribunal no va a juzgar), que la "instrucción tiene carácter reservado", tal reserva no se extiende a toda actuación procesal.

FICHA DE ESTUDIO DE CASO 2

SENTENCIA DEL TRIBUNAL CONSTITUCIONAL

Fuente	EXP. N.° 01189-2019-PHC/TC

Contenido de la fuente	Con fecha 18 de julio de 2018, don William Benardino García Rosales interpone demanda de habeas corpus a favor de don Marcos Morales Vargas (f. 31) y la dirige contra los jueces integrantes de la Primera Sala Penal de la Corte Superior de Justicia de Lima Norte y la jueza a cargo del Décimo Juzgado Penal de Lima Norte. Solicita que se declare la nulidad de: (i) la sentencia de 16 de junio de 2017 (f. 3), que condenó al beneficiario por los delitos de fraude informático y falsificación de firma en documento privado; y (ii) la Resolución de 26 de diciembre de 2017 (f. 73), que confirmó la precitada sentencia en cuanto a la condena, pero la revocó respecto a la pena; y, reformándola, le impuso ocho años de pena privativa de la libertad efectiva (Expediente 9405-2014). Se alega la vulneración de los derechos a la libertad personal, al debido proceso y a la tutela jurisdiccional efectiva, así como del principio de legalidad penal.
Análisis	El objeto de la demanda es que se declare la nulidad de: (i) la sentencia de 16 de junio de 2017, que condenó a don William Benardino García Rosales por los delitos de fraude informático y falsificación de firma en documento privado; y, (ii) la Resolución de 26 de diciembre de 2017, que confirmó la precitada sentencia en cuanto a la condena, pero la revocó respecto a la pena; y reformándola, le impuso seis años de pena privativa de la libertad efectiva (Expediente 9405-2014). Se alega la vulneración de los derechos a la libertad personal, al debido proceso y a la tutela jurisdiccional efectiva, así como del principio de legalidad penal.
Recensión	Por tanto, resulta igualmente claro que la dimensión subjetiva del derecho a la legalidad penal no puede estar al margen del ámbito de los derechos protegidos por la justicia constitucional, frente a supuestos como la creación judicial de delitos o faltas y sus correspondientes supuestos de agravación o, incluso, la aplicación de determinados tipos penales a supuestos no contemplados en ellos. El derecho a la legalidad penal vincula también a los jueces penales y su eventual violación posibilita obviamente su reparación mediante este tipo de procesos de tutela de las libertades fundamentales.

Anexo 05: Validación del instrumento

1/1

USS | UNIVERSIDAD SEÑOR DE SIPÁN

FICHA DE VALIDACIÓN DE INSTRUMENTO POR JUICIO DE EXPERTOS

7. NOMBRE DEL EXPERTO		Robinson Bamio De Mendoza Vásquez
8.	PROFESIÓN	· Abogado
	ESPECIALIDAD	Derecho Constitucional y Gobernabilidad
	GRADO ACADÉMICO	Doctor
	EXPERIENCIA PROFESIONAL (AÑOS)	17 años
	CARGO	Docente de la USS

TÍTULO DE LA INVESTIGACIÓN:

"LA CIBERSEGURIDAD EN EL COMERCIO ELECTRÓNICO Y LOS RIESGOS DE PHISHING EN TIEMPOS DE PANDEMIA. CHICLAYO 2022"

9. DATOS DEL TESISTA		
3.1	NOMBRES Y APELLIDOS	KARIN JUNET ZAMORA VASQUEZ
3.2	ESCUELA PROFESIONAL	DERECHO
10. INSTRUMENTO EVALUADO		5. Entrevista (x) 6. Cuestionario ( ) 7. Lista de Cotejo ( ) 8. Diario de campo ( )
11. OBJETIVOS DEL INSTRUMENTO		GENERAL: Determinar si la ciberseguridad ayudara a mejorar el comercio electrónico y evitara los riesgos de phishing en tiempos de pandemia.
		ESPECÍFICOS: • Identificar qué medidas de seguridad se pueden implementar en el comercio electrónico.

	• Analizar la figura jurídica del phishing y su impacto en la pandemia de la Covid 19. • Analizar que mejoras se puede aplicar en la ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico. • Proponer mejoras en la ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico.

A continuación se le presentan los indicadores en forma de preguntas o propuestas para que usted los evalúe marcando con un aspa (x) en "A" si está de ACUERDO o en "D" si está en DESACUERDO, SI ESTÁ EN DESACUERDO POR FAVOR ESPECIFIQUE SUS SUGERENCIAS

N°	12. DETALLE DE LOS ITEMS DEL INSTRUMENTO	ALTERNATIVAS
01	¿Por qué debe existir mecanismos de ciberseguridad dentro del comercio electrónico?	A (✓) D ( ) SUGERENCIAS: ....
02	¿Cuáles son los beneficios de aplicar mecanismos de ciberseguridad dentro del comercio electrónico?	A (✓) D ( ) SUGERENCIAS: ....

03	¿Cuáles considera usted que son las medidas que se pueden implementar para mejorar el comercio electrónico y evitar los riesgos del phishing?	A (✓) D ( ) SUGERENCIAS: .....
04	¿De qué manera el Estado peruano podría brindar una adecuada protección tecnológica frente a los fraudes electrónicos?	A (✓) D ( ) SUGERENCIAS: .....
05	¿Por qué ha aumentado de manera considerable los delitos informáticos que atentan contra el patrimonio en tiempos de Covid 19?	A (✓) D ( ) SUGERENCIAS: .....

06	¿De qué manera se puede controlar el aumento de delitos informáticos que atentan contra el patrimonio?	A(4 D( ) SUGERENCIAS: .....
07	¿Qué mejoras puede aplicar el legislador en la Ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico?	A( ) D( ) SUGERENCIAS: .....
08	¿A qué se debe la inseguridad del comercio electrónico en el Perú?	A( ) D( ) SUGERENCIAS: .....

09	¿Cuáles son los estándares de seguridad que debe buscar el Estado para proteger a los clientes o usuarios en el comercio electrónico?	A (X) D ( ) SUGERENCIAS:
10	¿Qué se debe implementar dentro de la norma de delitos informáticos para poder tener un mayor resguardo del patrimonio ante la comisión de delitos cibernéticos?	A (X) D ( ) SUGERENCIAS:

PROMEDIO OBTENIDO:	A (X) D ( )

7.COMENTARIOS GENERALES

LAS INTERROGANTES FUERON MUY PERTINENTES Y ACERTADAS PARA LOGRAR LOS PROPÓSITOS DE LA PRESENTE INVESTIGACIÓN

9. OBSERVACIONES:

NINGUNA

Juez Experto

Dr. Robinson Barrio De Mendoza Vásquez
Reg. Ical N°3482

USS | UNIVERSIDAD SEÑOR DE SIPÁN

FICHA DE VALIDACIÓN DE INSTRUMENTO POR JUICIO DE EXPERTOS

7. NOMBRE DEL EXPERTO		Carlos Andree Rodas Quintos.
8.	PROFESIÓN	Abogado
	ESPECIALIDAD	Derecho Civil - Procesal Civil
	GRADO ACADÉMICO	Magister
	EXPERIENCIA PROFESIONAL (AÑOS)	13 años.
	CARGO	Docente.

TÍTULO DE LA INVESTIGACIÓN:

"LA CIBERSEGURIDAD EN EL COMERCIO ELECTRÓNICO Y LOS RIESGOS DE PHISHING EN TIEMPOS DE PANDEMIA. CHICLAYO 2022"

9. DATOS DEL TESISTA		
3.1	NOMBRES Y APELLIDOS	KARIN JUNET ZAMORA VASQUEZ
3.2	ESCUELA PROFESIONAL	DERECHO
10. INSTRUMENTO EVALUADO		5. Entrevista (x) 6. Cuestionario ( ) 7. Lista de Cotejo ( ) 8. Diario de campo ( )
11. OBJETIVOS DEL INSTRUMENTO		GENERAL: Determinar si la ciberseguridad ayudara a mejorar el comercio electrónico y evitara los riesgos de phishing en tiempos de pandemia.
		ESPECÍFICOS: • Identificar qué medidas de seguridad se pueden implementar en el comercio electrónico.

	• Analizar la figura jurídica del phishing y su impacto en la pandemia de la Covid 19. • Analizar que mejoras se puede aplicar en la ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico. • Proponer mejoras en la ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico.

A continuación se le presentan los indicadores en forma de preguntas o propuestas para que usted los evalúe marcando con un aspa (x) en "A" si está de ACUERDO o en "D" si está en DESACUERDO, SI ESTÁ EN DESACUERDO POR FAVOR ESPECIFIQUE SUS SUGERENCIAS

N°	12. DETALLE DE LOS ITEMS DEL INSTRUMENTO	ALTERNATIVAS
01	¿Por qué debe existir mecanismos de ciberseguridad dentro del comercio electrónico?	A (✓) D ( ) SUGERENCIAS: ....
02	¿Cuáles son los beneficios de aplicar mecanismos de ciberseguridad dentro del comercio electrónico?	A (✓) D ( ) SUGERENCIAS: ....

03	¿Cuáles considera usted que son las medidas que se pueden implementar para mejorar el comercio electrónico y evitar los riesgos del phishing?	A (✓) D ( ) SUGERENCIAS: .....
04	¿De qué manera el Estado peruano podría brindar una adecuada protección tecnológica frente a los fraudes electrónicos?	A (✓) D ( ) SUGERENCIAS: .....
05	¿Por qué ha aumentado de manera considerable los delitos informáticos que atentan contra el patrimonio en tiempos de Covid 19?	A (✓) D ( ) SUGERENCIAS: .....

06	¿De qué manera se puede controlar el aumento de delitos informáticos que atentan contra el patrimonio?	A(4 D( ) SUGERENCIAS: .....
07	¿Qué mejoras puede aplicar el legislador en la Ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico?	A( ) D( ) SUGERENCIAS: .....
08	¿A qué se debe la inseguridad del comercio electrónico en el Perú?	A( ) D( ) SUGERENCIAS: .....

09	¿Cuáles son los estándares de seguridad que debe buscar el Estado para proteger a los clientes o usuarios en el comercio electrónico?	A (X) D ( ) SUGERENCIAS:
10	¿Qué se debe implementar dentro de la norma de delitos informáticos para poder tener un mayor resguardo del patrimonio ante la comisión de delitos cibernéticos?	A (X) D ( ) SUGERENCIAS:

PROMEDIO OBTENIDO:	A (X) D ( )

7.COMENTARIOS GENERALES

LAS INTERROGANTES FUERON MUY PERTINENTES Y ACERTADAS PARA LOGRAR LOS PROPÓSITOS DE LA PRESENTE INVESTIGACIÓN

9. OBSERVACIONES:

NINGUNA

Juez Experto
Hg. Carlos Andres Reda Quintero
Reg. ICOL: 5126.

89

USS | UNIVERSIDAD SEÑOR DE SIPÁN

FICHA DE VALIDACIÓN DE INSTRUMENTO POR JUICIO DE EXPERTOS

7. NOMBRE DEL EXPERTO		CABRERA LEONARDO, W. DAVID
8.	PROFESIÓN	ABOGADO
	ESPECIALIDAD	D° CONSTITUCIONAL.
	GRADO ACADÉMICO	MAGISTER
	EXPERIENCIA PROFESIONAL (AÑOS)	35 AÑOS
	CARGO	DOCENTE
TÍTULO DE LA INVESTIGACIÓN: "LA CIBERSEGURIDAD EN EL COMERCIO ELECTRÓNICO Y LOS RIESGOS DE PHISHING EN TIEMPOS DE PANDEMIA. CHICLAYO 2022"		
9. DATOS DEL TESISTA		
3.1	NOMBRES Y APELLIDOS	KARIN JUNET ZAMORA VASQUEZ
3.2	ESCUELA PROFESIONAL	DERECHO
10. INSTRUMENTO EVALUADO		5. Entrevista (x) 6. Cuestionario ( ) 7. Lista de Cotejo ( ) 8. Diario de campo ( )
11. OBJETIVOS DEL INSTRUMENTO		GENERAL: Determinar si la ciberseguridad ayudara a mejorar el comercio electrónico y evitara los riesgos de phishing en tiempos de pandemia. ESPECÍFICOS: • Identificar qué medidas de seguridad se pueden implementar en el comercio electrónico.

	• Analizar la figura jurídica del phishing y su impacto en la pandemia de la Covid 19. • Analizar que mejoras se puede aplicar en la ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico. • Proponer mejoras en la ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico.

A continuación se le presentan los indicadores en forma de preguntas o propuestas para que usted los evalúe marcando con un aspa (x) en "A" si está de ACUERDO o en "D" si está en DESACUERDO, SI ESTÁ EN DESACUERDO POR FAVOR ESPECIFIQUE SUS SUGERENCIAS

N°	12. DETALLE DE LOS ITEMS DEL INSTRUMENTO	ALTERNATIVAS
01	¿Por qué debe existir mecanismos de ciberseguridad dentro del comercio electrónico?	A (✓) D ( ) SUGERENCIAS: ....
02	¿Cuáles son los beneficios de aplicar mecanismos de ciberseguridad dentro del comercio electrónico?	A (✓) D ( ) SUGERENCIAS: ....

03	¿Cuáles considera usted que son las medidas que se pueden implementar para mejorar el comercio electrónico y evitar los riesgos del phishing?	A (✓) D ( ) SUGERENCIAS: ....
04	¿De qué manera el Estado peruano podría brindar una adecuada protección tecnológica frente a los fraudes electrónicos?	A (✓) D ( ) SUGERENCIAS: ....
05	¿Por qué ha aumentado de manera considerable los delitos informáticos que atentan contra el patrimonio en tiempos de Covid 19?	A (✓) D ( ) SUGERENCIAS: ....

06	¿De qué manera se puede controlar el aumento de delitos informáticos que atentan contra el patrimonio?	A(4 D( ) SUGERENCIAS: ....
07	¿Qué mejoras puede aplicar el legislador en la Ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico?	A( ) D( ) SUGERENCIAS: ....
08	¿A qué se debe la inseguridad del comercio electrónico en el Perú?	A( ) D( ) SUGERENCIAS: ....

09	¿Cuáles son los estándares de seguridad que debe buscar el Estado para proteger a los clientes o usuarios en el comercio electrónico? --- --- ---	A(X) D( ) SUGERENCIAS: --- ---
10	¿Qué se debe implementar dentro de la norma de delitos informáticos para poder tener un mayor resguardo del patrimonio ante la comisión de delitos cibernéticos? --- --- ---	A(X) D( ) SUGERENCIAS: --- ---

PROMEDIO OBTENIDO:	A(X) D( )

7.COMENTARIOS GENERALES

LAS INTERROGANTES FUERON MUY PERTINENTES Y ACERTADAS PARA LOGRAR LOS PROPÓSITOS DE LA PRESENTE INVESTIGACIÓN

9. OBSERVACIONES:

NINGUNA

Juez Experto

DANIEL CABRERA L.

CAL. 1097

Anexo 06: Declaración de Consentimiento de los entrevistados

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE DERECHO. ESCUELA DE DERECHO

DECLARACION DE CONSENTIMIENTO

Yo, **GEINER VIDAL SALAZAR MAZA**, identificado con DNI N.° 45288195, con Registro ICAL 8613, con Domicilio en la av. calle Virrey Toledo N° 1022 - Provincia de Chiclayo, manifiesto mi Consentimiento para participar en la presente entrevista aplicada por la Estudiante de Derecho: **Zamora Vasquez Karin Junet** de la facultad de Derecho de la Universidad Señor de Sipán en la investigación denominada: **"La Ciberseguridad en el Comercio Electronico y los Riesgos de Phishing en Tiempos de Pandemia. Chiclayo 2022"**, quien me ha explicado el procedimiento de entrevista, el cual he entendido claramente.

Se que la información que le brindo al estudiante, al cual declaro que es verdadera y corresponde a mi experiencia como profesional de Derecho, será utilizada como fuente de información y posterior análisis para su investigación. Además, la información que brindo será utilizada de manera confidencial, y solo para los fines señalados.

He leído y comprendido íntegramente este documento y en consecuencia acepto su contenido y las consecuencias que de él se deriven, y accedo a lo anteriormente mencionado.

Chiclayo, 17 de junio del 2022

Geiner V. Salazar Maza
ABOGADO
ICAL: 8613

Entrevistado

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE DERECHO. ESCUELA DE DERECHO

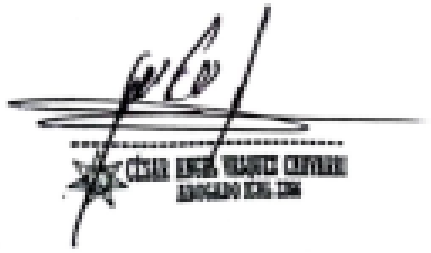
DECLARACION DE CONSENTIMIENTO

Yo, **CESAR ANGEL VASQUEZ CHAVARRI**, identificado con DNI N.° 41902142, con Registro ICAL 3366, con Domicilio en la Av. José Leonardo Ortiz N° 158 - Provincia de Chiclayo, manifiesto mi Consentimiento para participar en la presente entrevista aplicada por la Estudiante de Derecho: **Zamora Vasquez Karin Junet** de la facultad de Derecho de la Universidad Señor de Sipán en la investigación denominada: **"La Ciberseguridad en el Comercio Electronico y los Riesgos de Phishing en Tiempos de Pandemia. Chiclayo 2022"**, quien me ha explicado el procedimiento de entrevista, el cual he entendido claramente.

Se que la información que le brindo al estudiante, al cual declaro que es verdadera y corresponde a mi experiencia como profesional de Derecho, será utilizada como fuente de información y posterior análisis para su investigación. Además, la información que brindo será utilizada de manera confidencial, y solo para los fines señalados.

He leído y comprendido íntegramente este documento y en consecuencia acepto su contenido y las consecuencias que de él se deriven, y accedo a lo anteriormente mencionado.

Chiclayo, 14 de junio del 2022



Entrevistado

UNIVERSIDAD SEÑOR DE SIPÁN
FACULTAD DE DERECHO. ESCUELA DE DERECHO

DECLARACION DE CONSENTIMIENTO

Yo, **CHAVEZ ROJAS MAGALY DEL ROCÍO**, identificado con DNI N.° 16797537, con Registro ICAL 2002, con Domicilio en la av. San José 257 - Provincia de Chiclayo, manifiesto mi Consentimiento para participar en la presente entrevista aplicada por la Estudiante de Derecho: **Zamora Vasquez Karin Junet** de la facultad de Derecho de la Universidad Señor de Sipán en la investigación denominada: **"La Ciberseguridad en el Comercio Electronico y los Riesgos de Phishing en Tiempos de Pandemia. Chiclayo 2022"**, quien me ha explicado el procedimiento de entrevista, el cual he entendido claramente.

Se que la información que le brindo al estudiante, al cual declaro que es verdadera y corresponde a mi experiencia como profesional de Derecho, será utilizada como fuente de información y posterior análisis para su investigación. Además, la información que brindo será utilizada de manera confidencial, y solo para los fines señalados.

He leído y comprendido íntegramente este documento y en consecuencia acepto su contenido y las consecuencias que de él se deriven, y accedo a lo anteriormente mencionado.

Chiclayo, 10 de junio del 2022

MAGALY DEL ROCIO CHAVEZ ROJAS
ABOGADA
ICAL 2002

Entrevistado

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE DERECHO. ESCUELA DE DERECHO

DECLARACION DE CONSENTIMIENTO

Yo, **WILFREDO CHERO VILLEGAS**, identificado con DNI N.° 16584572, con Registro ICAL 1198, con Domicilio en la av. calle Elias Aguirre 1161- Provincia de Chiclayo, manifiesto mi Consentimiento para participar en la presente entrevista aplicada por la Estudiante de Derecho: **Zamora Vasquez Karin Junet** de la facultad de Derecho de la Universidad Señor de Sipán en la investigación denominada: **"La Ciberseguridad en el Comercio Electronico y los Riesgos de Phishing en Tiempos de Pandemia. Chiclayo 2022"**, quien me ha explicado el procedimiento de entrevista, el cual he entendido claramente.

Se que la información que le brindo al estudiante, al cual declaro que es verdadera y corresponde a mi experiencia como profesional de Derecho, será utilizada como fuente de información y posterior análisis para su investigación. Además, la información que brindo será utilizada de manera confidencial, y solo para los fines señalados.

He leído y comprendido íntegramente este documento y en consecuencia acepto su contenido y las consecuencias que de él se deriven, y accedo a lo anteriormente mencionado.

Chiclayo, 13 de junio del 2022

Entrevistado

UNIVERSIDAD SEÑOR DE SIPÁN
FACULTAD DE DERECHO. ESCUELA DE DERECHO

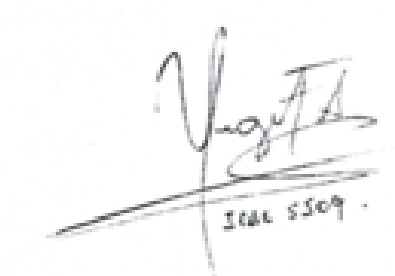
DECLARACION DE CONSENTIMIENTO

Yo, **GILMER IRIGOIN FALLAQUE**, identificado con DNI N.° 44174800, con Registro ICAL 5509, con Domicilio en la Av. calle 30 de AgostoN°159, Urb. Villarreal - Chiclayo, manifiesto mi Consentimiento para participar en la presente entrevista aplicada por la Estudiante de Derecho: **Zamora Vasquez Karin Junet** de la facultad de Derecho de la Universidad Señor de Sipán en la investigación denominada: **"La Ciberseguridad en el Comercio Electronico y los Riesgos de Phishing en Tiempos de Pandemia. Chiclayo 2022"**, quien me ha explicado el procedimiento de entrevista, el cual he entendido claramente.

Se que la información que le brindo al estudiante, al cual declaro que es verdadera y corresponde a mi experiencia como profesional de Derecho, será utilizada como fuente de información y posterior análisis para su investigación. Además, la información que brindo será utilizada de manera confidencial, y solo para los fines señalados.

He leído y comprendido íntegramente este documento y en consecuencia acepto su contenido y las consecuencias que de él se deriven, y accedo a lo anteriormente mencionado.

Chiclayo, 11 de junio del 2022



Entrevistado

Anexo 07: Matriz de Consistencia

TÍTULO:

"La Ciberseguridad en el Comercio Electrónico y los Riesgos de Phishing en tiempos de Pandemia. Chiclayo 2022"

PROBLEMA	OBJETIVOS	TIPO DE ESTUDIO Y DISEÑO DE LA INVESTIGACION	ESCENARIO DE ESTUDIO- CARACTERIZACION DE SUJETOS
¿De qué manera la Ciberseguridad ayuda a mejorar el comercio electrónico para evitar los casos de phishing en tiempos de pandemia, Chiclayo, 2022?	**Objetivo general:** Determinar si la ciberseguridad ayudara a mejorar el comercio electrónico y evitara los riesgos de phishing en tiempos de pandemia. **Objetivos específicos:** • Analizar la figura jurídica del phishing y su impacto en la pandemia de la Covid 19. • Analizar que mejoras se puede aplicar en la ley de delitos informáticos con la finalidad de buscar estándares de	**Tipo de Estudio** **Enfoque:** Conforme lo menciona Hernández (2018), las investigaciones cualitativas tienen por finalidad la interpretación de información, sin la necesidad de emplear parámetros numéricos. **Tipo: Básico** La Investigación es tipo básico por cuanto no se centra en resolver un problema en específico; si no más bien lo que busca es contribuir teóricamente a	**Escenario de Estudio** Esta investigación se desarrolló dentro de la ciudad de Chiclayo, en donde se toma en cuenta la aplicación de los instrumentos dentro de la cuidad de Chiclayo, tomándolo como distrito judicial, pues aquí se va aplicar la entrevista para tomar en cuenta la relevancia del fenómeno de estudio. **Caracterización de Sujetos** Se analiza que la muestra es una parte de la población, en muchas ocasiones se tiene como especialista a los expertos como expertos a los jueces, fiscales y abogados especialistas en Derecho Penal, del distrito judicial de Chiclayo, con la finalidad de presentar mejores conocimientos de manera estadística a la población

	seguridad para proteger a los clientes o usuarios en el comercio electrónico. • Proponer mejoras en la ley de delitos informáticos con la finalidad de buscar estándares de seguridad para proteger a los clientes o usuarios en el comercio electrónico.	futuras investigaciones realizadas a las temáticas tratadas. (Arias,2020.p.43) **Diseño: No Experimental** En la presente investigación se desarrolla un diseño **no experimental**, según Hernández (2018) señala que es un diseño de investigación donde no existe la manipulación de alguna variable, en la misma que se podrá analizar la ciberseguridad y el phishing en el Perú (p. 174).	