UNIVERSIDAD PARTICULAR DE CHICLAYO

FACULTAD DE DERECHO Y EDUCACION

ESCUELA PROFESIONAL DE DERECHO

TESIS:

"COMERCIO ELECTRÓNICO Y LOS PROBLEMAS DE LA CIBERDELINCUENCIA EN TIEMPOS DE COVID-19"

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

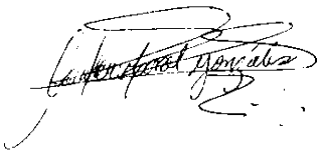
BACHILLER:

CAROL MARILIN GONZALES CHAVEZ

ASESOR

MG. JAVIER SORIANO DIAZ DIAZ

Pimentel, Perú, 2021



---------- ----------

Mg. Javier Soriano Diaz Diaz
ASESOR

Carol Marlín Gonzales Chevez
BACHILLER

APROBADO POR EL JURADO:

---------- ---------- ----------

Mg. Eleo Mitrídates Grillo Paico
SECRETARIO

Dr. Enrique Rodas Ramírez
PRESIDENTE

Mg. José Donald Gutiérrez Vega
VOCAL

DEDICATORIA

Se la dedico de manera especial a mi madre Elena Chávez Mogrovejo, pues ella es mi principal cimiento para la construcción de mi vida profesional, inculcándome siempre como base primordial la responsabilidad y deseos de superación, sobre todo sacándome adelante sola con esa fuerza que una madre entrega a sus hijos. Lo que de manera absoluta a contribuido siempre en cada paso que he dado para cumplir mis metas trazadas en lo largo de mi vida.

AGRADECIMIENTO

En primer lugar, agradezco a Dios mi padre celestial por haberme permitido llegar a este paso tan importante en mi vida, a mi abuela Luz Estela, mis tías Carmen Rosa y Susana, a mi hermano Mauricio por el apoyo brindado todos estos años de mi vida universitaria pues sin ellos no hubiera sido posible este momento.

A mi universidad por permitirme lograr ser un profesional con alto nivel humano y competitivo y a todos los brillantes docentes académicos que fueron parte de este proceso integral de mi formación que deja como producto esta tesis que durara dentro de los conocimientos y desarrollo de las demás generaciones futuras.

Y finalmente a todas esas personas que de una u otra manera contribuyeron con este gran sueño de cumplir mi meta para desarrollarme en los que más me apasiona.

INDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE ABREVIATURAS

Código Penal ……..…..…. C.P

Código Procesal Penal …….. C.P.P

Código de Procedimiento Civil ……..C.P.C

Tribunal Constitucional …….T.C

RESUMEN

La investigación presenta como problemática los problemas que se generan ante la ciberdelincuencia en tiempos de Covid- 19 y el comercio electrónico, es por ello que esta investigación desarrolla un modelo de influencia multinivel para explorar cómo los ciberdelincuentes están explotando la pandemia de COVID-19 evaluando factores situacionales, identificando víctimas, haciéndose pasar por fuentes confiables, así mismo se presenta como aspecto metodológico, una investigación de tipo aplicada, de diseño no experimental, con una muestra de 50, donde se considera a fiscales, jueces y abogados especialistas en derecho penal como expertos especialistas en la investigación, donde se llega a concluir que al identificar los problemas de ciberdelincuencia en tiempos de COVID-19, se mejora el comercio electrónico brindando una mayor seguridad a la información y neutralizando toda aquella amenaza que se desprenda del uso tecnológico, finalmente, la investigación analiza el comercio electrónico y los problemas de la ciberdelincuencia en tiempos de COVID-19 con el fin de establecer las normas de protección y defensa de los consumidores, así como asegura que todos los consumidores tengan acceso a los mecanismos de protección de sus derechos para que incurran en ciber delincuencia.

Palabras claves: comercio, comercio electrónico, ciberdelincuencia, ciberdelito.

ABSTRAC

The research presents as problematic the problems that are generated by cybercrime in times of Covid-19 and electronic commerce, that is why this research develops a multilevel influence model to explore how cybercriminals are exploiting the COVID-19 pandemic by evaluating situational factors, identifying victims, posing as reliable sources, likewise a methodological aspect is presented as an applied research, of non-experimental design, with a sample of 50, where prosecutors, judges and lawyers specializing in criminal law are considered as experts specialized in research, where it is concluded that by identifying cybercrime problems in times of COVID-19, electronic commerce is improved by providing greater information security and neutralizing any threat arising from technological use, finally, the research analyzes electronic commerce and the The problems of cybercrime in times of COVID-19 in order to establish the norms for the protection and defense of consumers, as well as ensure that all consumers have access to the mechanisms to protect their rights to incur cybercrime.

Keywords: commerce, e-commerce, cybercrime, cybercrime

I. INTRODUCCIÓN

Para poder analizar los problemas que se presentan frente a la ciberdelincuencia en los tiempos de Covid-19, se determina primero que este comercio electrónico se genera a partir de la revolución tecnológica dada aproximadamente por la revolución industrial del siglo XIX, de igual modo este avance tecnológico ha permitido de que la informática sea un elemento central para la vida cotidiana de la humanidad, pues con el avance del tiempo se han creado diversos aparatos tecnológicos que facilitan la vida diaria de las personas.

A su vez, la ciberseguridad es el mecanismo idóneo para el desarrollo del análisis y gestión de riesgos relacionados al ciberespacio. En ese sentido, este mecanismo busca neutralizar toda aquella amenaza que se desprenda del uso del ciberespacio. En ese orden de ideas, podemos afirmar que la ciberseguridad, mediante un conjunto de actuaciones, busca asegurar la información en el ciberespacio.

Pese a ello en la sociedad moderna actual con el vertiginoso avance de la ciencia y la tecnología de la comunicación y la informática, junto a sus beneficios, trajo consigo una serie de peligros que, en el campo del derecho penal, se materializan en la ciberdelincuencia a cuyas garras se exponen los usuarios al acceder a las redes sociales online, para el desarrollo de sus actividades cotidianas, delitos que por lo demás, no tienen fronteras, no exigen inmediación entre el agente y su víctima, permiten actuar en el anonimato y entre sus víctimas no distinguen estrato social, edades, credo religioso o color de piel (Gil, 2012, p. 87).

Es así que a nivel internacional, se determina que el bloque latinoamericano para lo cibercriminales es una de las grandes oportunidades que se genera para poder tener ganancias altas y esto se debe a que en la región la economía que se tiene es una de las más importantes en el mundo considerándose dentro de las veinte más importantes, al mismo tiempo existe un riesgo de que las personas que se involucran en estos delitos cibernéticos tienen que ser investigados, luego procesados para que posteriormente sean sentenciado, tal y como ocurre en el país de EE. UU. y en la Unión Europea, en donde se presenta que la migración de la delincuencia informática es un sistema de efectividad criminalizada (Martin, 2015, p. 1).

Sin embargo, en algunos sectores se determina que no existe una capacidad conductiva en el ciberespacio, los cual algunos estados no tienen los implementos tecnológicos necesarios para poder hacer frente a los individuos que se encuentran en constante conocimientos y actualizados.

Tal como es en el caso de los Estado Unidos, el delito cibernético es un acto ilegal en el que se utiliza una computadora como medio para cometer un delito contra una persona, propiedad o el gobierno, pese a ello, para el autor Sukhai explicó que una encuesta anual del FBI y del Computer Security Institute de 520 empresas e instituciones informaron más del 60% de uso no autorizado de sistemas informáticos durante un período de 12 meses y el 57% de todos los robos involucraron Internet. Aunque estos números parecen grandes, describen alrededor del 60% de los ciberataques ni siquiera se detectan. Las

investigaciones indican que solo alrededor del 15% de las personas expuestas (Sukhai, 2004).

Dicho de otro modo, los inventos tecnológicos en muchas ocasiones apoyan a la informática, así como en la comunicación mundial, pues en las últimas décadas la comunicación se ha expandido como un nuevo paradigma sociológico en donde se puede interactuar con la sociedad a la través de la informativa, es así que esta revolución industrial basada en la información, ayuda a que la información sea procesada, almacena, recuperar ya sea de una forma ilimitada o independiente pues esto será conforme el tiempo de la forma y la distancia en que se encuentre, por otra parte los nuevos sistemas sociales se basan en los servicios en donde el capital y el trabajo se centran en el conocimiento teórico (Anarte, 2016, p. 191).

De esta forma, queda claro que el poder es cada vez menor, ya que muchas personas consideran como propiedad a los elementos físicos como la tierra, los recursos naturales, las máquinas y los factores no físico, en donde se basan el uso de la alta tecnología, la información, la comunicación, la publicidad y el dominio financiero, de esta manera, se desmaterializa, no se toman más billetes ni lingotes, sino, solo se utiliza enviando mensajes digitales que actúan como moneda, que en este caso ayudan a la información financiera. (Choncho, 2003, p. 124)

Como se observa, tanto para los consumidores como para el Gobierno central, el comercio electrónico de bienes y servicios resulta ser una actividad relevante

para la continuidad del flujo de bienes y servicios, así como para reactivar nuestra economía.

Esta desconfianza *a priori* del consumidor peruano, que aún no ha comprado por Internet, se ve afianzada cuando al realizar un pedido de compra en los *hot days*, o durante esta época de cuarentena por el COVID-19, sufre una mala experiencia de compra. Por ejemplo, en el Perú, ante el incremento de las compras por Internet por el COVID-19, también aumentaron los reclamos de los consumidores por la falta o demora en la entrega de los productos que habían adquirido; falta de idoneidad del producto recibido; la entrega de pedidos de compra incompletos o distintos a los de sus carritos de compra; o la cancelación de las compras por falta de stock. En este escenario, surgen interrogantes respecto al rol que puede o no desempeñar el Estado para promover el desarrollo del comercio electrónico, que a su vez reditúa en el PBI nacional, resguardando a la par, la protección de los consumidores.

Por esta razón, resulta que los ataques más comunes continúan enfocándose en intereses económicos contra el sector financiero, que es utilizado por la clase media a diario. Por tanto, ante la importante inversión económica por parte del sector privado en los últimos años, los esfuerzos iniciales para crear medidas preventivas se han centrado en los clientes y titulares de cuentas de las instituciones bancarias, mientras que las autoridades han dedicado mucho tiempo a la campaña de alerta, las cuales hasta el momento no han podido calmar

la ciber delincuencia. Para acceder a sus cuentas financieras personales, para identificar la información proporcionada por medios no físicos.

Estos esfuerzos decididos han alertado a miles de víctimas potenciales; Sin embargo, si bien la campaña ha mantenido la misma estructura a lo largo de los años, el uso de Internet se ha acelerado lentamente, llegando a la conectividad ante una era permanente, pues son los ciberdelincuentes quienes tienen acceso a herramientas, que perjudican la seguridad financiera de las personas y que el control de la integridad física.

Ante ello, la investigación analiza el comercio electrónico y los problemas de la ciberdelincuencia en tiempos de COVID-19 con el fin de establecer las normas de protección y defensa de los consumidores, así como asegura que todos los consumidores tengan acceso a los mecanismos de protección de sus derechos para que incurran en ciber delincuencia, pues se observa que los consumidores peruanos perciben que la falta de cumplimiento normativo por parte de las empresas se debe principalmente por la falta de fiscalización del Estado, cuestionándose el cumplimiento de la política pública expuesta.

Frente al problema se genera la siguiente interrogante: ¿Qué problemas de ciberdelincuencia en tiempos de COVID-19, genera el comercio electrónico?, ante esta pregunta se establece como objetivo general: Analizar el comercio electrónico y los problemas de la ciberdelincuencia en tiempo de COVID -19, no obstante, para el cumplimiento de este objetivo, se toma en cuenta los específicos: Identificar los problemas de la ciberdelincuencia en tiempos de

COVID-19, examinar el comercio electrónico y su regulación en el estado peruano y determinar si el comercio electrónico se ve afectado ante los problemas de la ciberdelincuencia en tiempos de COVID-19.

Frente a estos objetivos se tiene como hipótesis, que, si se identifican los problemas de ciberdelincuencia en tiempos de COVID-19, entonces se mejorar el comercio electrónico brindando una mayor seguridad a la información y neutralizando toda aquella amenaza que se desprenda del uso tecnológico.

II. MARCO TEÓRICO

2.1. Antecedentes

Torrente, analiza como investigación las diversas actividades que se realizan online a través de un comercio electrónico en la ciudad de Panamá, pues frente a ello la investigación ha sido presentada para poder optar el título profesional de abogado de la Universidad Internacional de Ciencia y Tecnología, en donde se concluye 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 (Torrente, 2020).

Hernández y Mendoza, en su investigación analizan el funcionamiento que tiene el comercio electrónico, así como las categorías que se aplican para dar una seguridad a los usuarios y demografías de los usos habituales, esta investigación a sido presentada por la Universidad Autónoma del Estado de México, en donde se puede concluir que el uso de Internet es común a todos los ciudadanos y que la forma en que enfrentamos el mundo está cambiando. En todo este trabajo, la sociedad está cambiando y se observa la búsqueda de nuevos métodos

comerciales. Además, debido a los avances tecnológicos, se debe tener cuidado al operar en cada región, ya que puede comprometer la integridad del ejecutante (Hernández y Mendoza, 2018).

Quevedo, en su investigación realizada hacia la prueba del ciberdelito, la cual ha sido aplicada a través de la Universidad de Barcelona para poder optar el título profesional de abogado, se llega a la conclusión que el internet ha afectado gravemente a la sociedad al crear nuevos tipos de delincuentes y actuar como herramienta de transmisión de determinadas costumbres tradicionales, por ello la investigación del llamado ciberdelito requiere identificar las características esenciales de Internet, como la red mundial o afiliados en este caso. Las imágenes son llevadas a los seleccionados por la web en base a esto también verifique la representación digital de la información que permite diferentes conexiones en tiempo real entre personas y lugares (Quevedo, 2017).

Peralta y Roa, en su investigación analizan el impacto que ha generado los delitos cibernéticos dentro de las operaciones de comercio electrónico en Colombia, así esta investigación ha sido presenta para poder optar el título profesional de abogado de la Universidad de Córdova, en donde se concluye que los cambios acelerados resultantes de la globalización son innumerables y cada vez más atractivos, y abren oportunidades económicas y culturales ilimitadas para toda la humanidad. Así, guiados por el avance tecnológico de la información y de la comunicación, se han podido determinar que una herramienta que desarrolla las

relaciones, el conocimiento y el desarrollo personal, organizacional, local e internacional. El comercio electrónico crea y estructura la mejor forma de pensar que se adapta al mundo digital; Las formas tradicionales de hacer negocios están siendo reemplazadas gradualmente por el hecho de que los negocios se realizan electrónicamente y se pueden mantener en bases de datos informáticas sin la necesidad de documentos físicos (Peralta y Roa, 2020).

Camargo, en su investigación comprende la ciberseguridad y el teletrabajo dentro de los tiempos de pandemia, investigación que ha sido resuelta para poder optar el título profesional de abogado de la Universidad del Rosario, en donde se concluye que, el informe digital, presentado durante la pandemia, denominado ciberseguridad y redes durante COVID-19, es parte de una “colección” de podcasts ya publicados. En cumplimiento de la normativa, este podcast no se expuso a terceros distintos al nivel de proyecto, y muestra la importancia de proteger los datos personales en todos los sectores, tanto personales como empresariales (Camargo, 2020).

Romero, en su investigación interpreta los delitos informáticos que han sido cometido a través de las diversas redes sociales, para poder efectuar un eficaz tratamiento en el ministerio público de la ciudad de Huánuco, esta investigación ha ido presenta para poder obtener el título profesional de abogado de la Universidad de Huánuco, 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. Esto debe incluir la naturaleza de la tecnología informática, los pasos para restaurar la evidencia informática, su investigación y los requisitos de un informe pericial que permita la confiabilidad de la evidencia como medio de evidencia (Romero, 2017).

2.2. Base teórica

Cibercriminología desde la perspectiva de Latinoamérica

Durante casi una década, algunas o todas las escenas del crimen propiciaron un foro de diálogo entre otros para explorar los métodos de búsqueda, especialmente en México. Por lo tanto, algunos de nuestros temas relacionados con la ciencia están cambiando lenta pero seguramente y también se conocen como términos de investigación tanto a nivel académico como en las habilidades de investigación de América Latina (Cámpoli, 2005).

En cuanto al desarrollo de la cibercriminología, se puede aclarar que este tema ha avanzado poco en la literatura española. Esto permite a los estudiantes o investigadores comenzar con los conceptos básicos de la publicación de su trabajo y completar documentos previamente preparados de otras fuentes en el

campo durante la última década. que puede ser útil para criminales e investigadores forenses (Lira, 2010).

El bloque latino representa una buena oportunidad para que los emprendedores obtengan mayores ganancias porque la región es una de las 20 economías más importantes del mundo y al mismo tiempo tiene la economía más baja. Los riesgos están representados por la identidad, el enjuiciamiento y el enjuiciamiento de delitos informáticos menores en comparación con los delitos existentes en los Estados Unidos y la Unión Europea. Como resultado, las cajas de las computadoras van a esta parte del mundo a los estados, territorios y supersticiones. Por lo tanto, muchos de estos consejos carecen de experiencia suficiente en la investigación de comportamientos no relacionados en el medio ambiente y cuentan con el equipo técnico y técnico adecuado para tratar con personas con infraestructura mejorada (Martin, 2015).

El Perú cuenta con tecnología de detección de delitos de alta tecnología DIRINCRI-PNP, pero incluso hay intentos, por apoyo material, presupuesto, espacio limitado y medicina negra que aún refuerza este delito.

Al mismo tiempo, los miembros del parlamento enfrentan una serie de desafíos al considerar si deben llevar a cabo tal conducta, si es que lo hacen, si es necesario cambiar a lo que ya está previsto en el derecho penal. Discutir el

desarrollo de nuevas leyes y los peligros de no poder aprobar leyes que no sean penales (Rodríguez, 2013).

La criminalidad tecnológica en su máxima extensión

Para poder comprender lo referido en el titulo se cita a Mateo, quien menciona que:

> Baumann describe la transición de la luz a los tiempos modernos como una nueva apreciación del espacio, pretendiendo ser el fin de los tiempos. Inicialmente, para quienes se comportan, la mejora de la comunicación significa que permite el acceso global "instantáneo" y la invisibilidad de esos usuarios para los usuarios que no tienen acceso a esos métodos. En segundo lugar, significa una pérdida de valor del espacio. Todos tienen valor fetiche. Desde el punto de vista de George Simmel, la naturaleza no tiene precio y esto puede variar miles de kilómetros (Mateo, 2013, p. 11).

Es cierto, es cierto, pero es la magia en tiempo real la que ha traído innumerables satisfacciones a las necesidades sociales, pero esto todavía está en uso hoy en día.

Esto es Internet, correo electrónico, Facebook, Instagram, Twitter, WhatsApp, blogs, sitios web, democracia. Las cosas se crean como teléfonos. Es una herramienta para movilizar y lesionar a personas o grupos sociales, utilizar las

TIC para cometer ciberdelitos y mostrar una cultura de ambición, repetición y crueldad.

Por lo tanto, es un deseo poco común creer que la tecnología del delito cibernético permite a los expertos comprender todos los delitos cibernéticos. Aunque se incluyen muchas actividades (por ejemplo, fraude, base de datos, suplantación de identidad), la complejidad del delito cibernético y estas dinámicas cambian a través de la continuación del estudio del autor que muestran los buscadores. Tienes que elegir el crimen al aire. El acceso a los servicios (por ejemplo, delitos sexuales, abuso infantil, acceso a información pública, ataques políticos, etc.) y otras áreas requiere un mayor escrutinio en algunos casos.

El delito informático como una manifestación de una sociedad de riesgo

La sociedad moderna actual con el vertiginoso avance de la ciencia y la tecnología de la comunicación y la informática, junto a sus beneficios, trajo consigo una serie de peligros que, en el campo del derecho penal, se materializan en la ciberdelincuencia a cuyas garras se exponen los usuarios al acceder a las redes sociales online, para el desarrollo de sus actividades cotidianas, delitos que por lo demás, no tienen fronteras, no exigen inmediación entre el agente y su víctima, permiten actuar en el anonimato y entre sus víctimas no distinguen estrato social, edades, credo religioso o color de piel (Gil, 2012).

Es decir, los avances tecnológicos están respaldados por la tecnología y las telecomunicaciones globales, y con su incremento en las últimas décadas, ha dado lugar a un nuevo paradigma político denominado Sociedad del Conocimiento y / o de la Información. El nuevo modelo de negocio se basa en información que se puede procesar, almacenar, acceder y comunicar de manera oportuna, independientemente del tiempo o la distancia. El nuevo sistema social es compatible con los servicios. El principio del eje ya no se centra en el capital y el trabajo en la teoría.

De esta manera, el poder omnipresente del propietario de valiosos recursos naturales y tecnológicos, se ha convertido en un maestro de la ciencia, la tecnología, la información, las telecomunicaciones, el marketing y las finanzas inmobiliarias. De esta manera, la economía se degrada físicamente, los bancos y las balas ya no se llevan, y los mensajes digitales que parecen enviarse, pues el dinero se ve obstaculizado por la información (Choncol, 2003).

Es así que, en el derecho penal, Silva Sánchez señala en su libro Expansión del Derecho Penal que el ciberdelito y los delitos cibernéticos, llamados ciberdelitos, son los mejores ejemplos de la evolución de los delincuentes peligrosos. Esto puede conducir a una mejor comprensión del entorno local del entorno, como un entorno global peligroso o una comunidad informática peligrosa.

Ciberdelincuencia en tiempos de covid-19

Evidentemente, el uso del internet tiene una notable importancia en nuestra sociedad actual, pues, con el transcurso de los años, la mayoría de nuestras actividades posee, en mayor o menor medida, un soporte virtual. La dependencia a este medio de comunicación se acentúa más en el contexto de la pandemia de COVID-19. No obstante, en estos últimos tiempos también se han agudizado o surgido diversas modalidades de cibercriminalidad. Es decir, conforme la sociedad avanza con la tecnología también se expone a nuevas conductas delictivas, como la ciberdelincuencia. Si bien existen instrumentos de lucha contra este flagelo, no es menos cierto que las técnicas para la configuración de dichos delitos vienen evolucionando. En el presente artículo desarrollaremos cuáles y qué clase de delitos están en constante evolución y la naturaleza de ellos

Características de la conducta de la ciberdelincuencia

El campo de actuación de la ciberdelincuencia es la plataforma virtual, allí el sujeto oculta su identidad, lo que genera obstáculo para una futura investigación. Por ejemplo, mediante la Deep Web, también conocida como internet profunda, se busca crear perfiles falsos.

Aún existen comportamientos y situaciones particulares que no son conocidas a la fecha, situación que sigue generando impunidad. Ahora bien, como la ciberdelincuencia se desarrolla en una plataforma virtual, es posible que estos delitos se configuren con la colaboración de diversos sujetos que se encuentran

en diferentes Estados. Por lo tanto, es posible advertir ataques masivos, lo que significa que existe una organización criminal.

Para evitar ser víctima de la cibercriminalidad se recomienda tomar en cuenta los consejos que se proporcionan a los usuarios, así como el sentido común y el “principio de desconfianza”, más aún cuando nos solicitan datos que no son habituales ni comunes. La naturaleza de la cibercriminalidad nos hace entender que no conoce fronteras, por ello, se necesita de una lucha internacional contra estas organizaciones criminales.

Es necesario la implementación internacional de un sistema que busque prevenir los ciberataques; por ejemplo, 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.

Objeto material del delito del fraude informático

En las computadoras fraudulentas, los artículos "esenciales" o "no esenciales" son dinero o documentos, porque la intención del abogado es siempre obtener intereses o intereses de manera ilegal para beneficio propio o de terceros. Robar cosas; Robar valores o documentos de seguridad para ayudar en el intercambio

de bienes o fondos. Robo de trabajo y eventualmente robo de software. Todos tienen su propia familia o valor de cambio para sus dueños y son muy comunicativos en el mercado negro.

El delito de fraude informático entendida esta como la utilización indebida de un sistema informático, no requiere para su configuración, la concurrencia de los elementos propios de la estafa, tales como el engaño, el ardid y el error; toda vez que la actuación del agente es sobre un ordenador, un sistema una máquina y no se requiere 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 produce de forma automáticas sin su participación o consentimiento.

Mediante 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. Por otro lado, mediante la modificatoria 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, estos delitos vienen siendo 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.

Actualmente, el delito cibernético incluye hurto, malversación de fondos, pornografía infantil, hurto, hurto, tráfico de drogas, inmigración, delitos humanos, delitos de seguridad y sedición, terrorismo, delitos fiscales y morales, blanqueo de capitales Se incluyen delitos combinados.

El delito de fraude informático, una de las modalidades del cibercriminal es cualitativamente diferente a los delitos de hurto y estafa, de trascendencia internacional que se comete en el ciberespacio, el cual no reconoce fronteras geográficas.

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

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

Diferencia entre el delito informático y cibercrimen

A partir de una lectura de la ley, el Dr. Romeo, encuentra que es imposible hablar de juicios informáticos en uno porque tiene mucha modalidad y es apto como material legal. Hablando de ciberdelito, la ley del mismo nombre llevó más tarde al nombre de Julis. Así, como señalan los educadores, es menos probable que todas las organizaciones ofrezcan relaciones amistosas en relación con el crimen, la doctrina, la política, el crimen y la ley. Por lo tanto, el ciberdelito se ha adoptado como un nuevo término para distinguir los delitos de próxima generación relacionados con el uso de nuevas tecnologías de la información y la comunicación. El término se incorporó al derecho internacional y más tarde fue adoptado por la Constitución de Budapest (Romero, 2006).

Estas observaciones terminológicas resultan importantes por cuanto la ley de delitos informáticos, al extraer cada uno de los verbos rectores propuestos por dicho convenio para la configuración del delito de fraude informático, ubica a este, dentro de un contexto mayor, el cibercrimen; por ello, entendemos que el delito de fraude informático, cualitativamente supera en exceso el campo normativo regulado dentro del derogado delito de hurto agravado.

En este sentido, hemos identificado el ciberdelito como una de las formas más comunes de fraude, por lo que lo entendemos como un medio de acciones relacionadas con el acceso, engaño, intercambio y acceso a la información,

siguiendo a los Dres. Romero Casabona. La participación de la comunidad se lleva a cabo sin el permiso o permiso requerido o el uso de información sobre actividades ilegales que puedan violar diferentes requisitos legales de ética o de alto riesgo (Romero, 2006).

En consecuencia, el citado autor sostiene que los ciberdelitos, aunque coexistan en el tiempo con los llamados delitos informáticos, configuran una generación posterior cuyos problemas jurídicos están relacionados con las insuficiencias de la aplicación de la ley penal en el ámbito espacial de su vigencia y superar los límites de la extraterritorialidad que los mismos plantean, advirtiendo que Los nuevos signos de delincuencia en Internet requieren un tratamiento legal desde una perspectiva global, ya que la acción del gobierno por sí sola, la implementación de la aplicación de la ley penal, se ha debilitado en su posición (Casabona, 2006).

Bien jurídico protegido en los delitos informáticos

Desde su origen, tanto en el mundo como en el Perú, se ha discutido si el delito informático debe ser considerado como una infracción penal independiente y, en consecuencia, con un bien jurídico particular, o, si se trataba únicamente de una nueva forma o medio de comisión de delitos que ya se encontraban regulados en la ley penal.

Dr. García Cantizano, quien era el segundo al mando en ese momento, dejó en claro que el derecho penal no tiene una definición única de delito informático, que es un delito cometido contra su finalidad. Sistema automático de procesamiento o distribución de datos. Dr. Bramont-Arias Torres hizo lo propio cuando dijo: "De hecho, la caja de la computadora en sí no existe, por lo que la caja de la computadora no tiene protección legal. Él es el titular de un equipo legal que ya goza de la protección de los delincuentes. Sin sentido común". de lo que fueron los delitos informáticos, porque se reducen los delitos informáticos. Tiene acciones complejas o se puede combinar para hacer una interpretación única, definida como informática como el procesamiento de datos o los sistemas de transmisión de datos utilizados para tal fin" (Bramont, 1997).

Por su parte para el doctor argentino, Gustavo Eduardo Aboso, el bien jurídico protegido sería "la información y su transmisión a través de los sistemas telemáticos". Por otro lado, la Ley N.º 19.223 sobre delitos informáticos chileno, en su momento, señaló como objeto de la misma "Mantener nuevas características legales creadas con la última tecnología informática: calidad, pureza e idoneidad de la propia información. Se integra en el propio sistema automatizado de procesamiento de la información, del producto derivado de su funcionamiento" (Gustavo, 2006, p. 16).

Por nuestra parte, siguiendo al Dr. Reyna Alfaro, podemos señalar que, respecto del reconocimiento del bien jurídico en estos delitos, existen tres sectores bien

diferenciados. En primer lugar, niega la existencia del delito cibernético y luego ve el "delito cibernético" como una nueva forma delictiva de manejar el equipo legal que ya ha sido sancionado y no hay dinero asegurado legalmente. Una segunda posición, sin embargo, advierte que habría que diferenciar los delitos computacionales (donde se utiliza como media una computadora o afines), de los delitos informáticos propiamente dichos, los que sí, tienen un nuevo bien jurídico, que debe ser regulado legislativamente.

El maestro argentino, siguiendo a su vez a Andrzej Adamski, propone como bien jurídico en esta clase especifica de delitos la información como valor económico de empresa, clasificando en tres las conductas criminales que afectan este novedoso bien jurídico en sus tres propiedades confidencialidad, integridad y disponibilidad:

a. Acciones que violan la confidencialidad de la información (software espía o interferencia informática),

b. Comportamientos que comprometen la integridad de la información (bombas frontales y virus informáticos),

c. Conductas lesivas a la información (electronic mail, bombing y spam).

Una tercera postura, que señala que el delito informático tiene tres dimensiones: la primera, la computadora es el medio para cometer el delito;

en la segunda, el objeto del delito es la información contenida en los sistemas informáticos; finalmente la tercera dimensión, los ordenadores tendrán una transcendencia probatoria.

En Perú, la ley establece que su propósito es prevenir y sancionar las actividades ilícitas que dañen los sistemas informáticos, los datos y otras características legales de los delincuentes mediante el uso de tecnologías de la información y la comunicación. De la lucha contra el ciberdelito, se desprende que los instrumentos legales han sido establecidos por los sistemas informáticos y de datos de las fuerzas del orden, y otros asuntos legales relacionados con los delincuentes como los instrumentos y la confianza pública.

El delito informático y los problemas sobre su regulación

Desde su origen, tanto en el mundo como en el Perú, se ha discutido si el delito informático debe ser considerado como una infracción penal independiente y, en consecuencia, con un bien jurídico particular merecedor de una legislación especial, o, si se trataba únicamente de una nueva forma o medio de comisión de delitos que ya se encontraban regulados en la ley penal.

Si bien es cierto, se viene reconociendo la autonomía jurídico-penal de los delitos informáticos; sin embargo, aún no se puede distinguir a ciencia cierta, cuando estamos frente a uno. En efecto, ¿cuál es el criterio para diferenciarlos de los

delitos comunes?: ¿será por el bien jurídico afectado?, ¿la modalidad o instrumento utilizado para su comisión?, ¿será la calidad o particularidad del agente especializado en informática para su comisión?, ¿o será el rango nacional o internacional de sus efectos dañinos?, los mecanismos procesales especializados para su investigación? Lo cierto es que nos encontramos frente a una institución jurídico-penal compleja, donde cada uno de los criterios señalados ciertamente resultan útiles para su identificación y tratamiento.

Históricamente, el criterio que ha sido utilizado hasta la fecha por el legislador para ordenar dentro del Código Penal cada uno de los delitos clasificándolos, ha sido el bien jurídico protegido. Así tenemos que los delitos contra el patrimonio como el robo o el hurto, se diferenciaban sin mayor problema de los delitos contra la fe pública y estos a su vez de los delitos contra la indemnidad y libertad sexual. Sin embargo, con el nacimiento de los delitos informáticos, este criterio clasificatorio se difumina, por cuanto estos, con la implacable fuerza de la diosa Shiva recorren cada uno de los bienes jurídicos protegidos en casi todos los títulos del Código Penal vulnerándolos.

Por ello, quizás fracasó en su momento la intención del legislador nacional, al tratar de ponerle camisa de fuerza y regularlo dentro del Código Penal asignándole un nuevo bien jurídico mediante la Ley 27309 ya que cada día nacía un nuevo delito informático que, sin embargo, vulneraba un bien jurídico preexistente. Entonces se pasaron a regular esas nuevas figuras dentro del

capítulo correspondiente al bien jurídico afectado, tipificándolas como agravante de los delitos correspondientes cuando en realidad se trata de nuevas modalidades del mismo delito.

Posteriormente, ante la transcendencia mundial de los delitos informáticos, el legislador, procedió a regularlos en una ley especial LDI inspirada en los lineamientos del Convenio de Budapest. Sin embargo, las nuevas modalidades y formas criminales siguen apareciendo, por lo que subsiste el siguiente cuestionamiento: ¿cómo se tienen que regular esas nuevas figuras?

Al respecto, considero que, en principio y, de todas maneras, el legislador nacional debe abstenerse de incurrir nuevamente en la opción de tipificar una misma conducta, en dos tipos y leyes penales diferentes, tal como se ha denunciado en la introducción del presente trabajo con el child grooming. Consideración que debe tomarse en cuenta si anotamos que, en el Código Penal, aún subsisten algunas figuras que, a pesar de ser cometidos mediante el uso de TIC, no han sido incorporados en la Ley de Delitos Informáticos y sería, por decir lo menos, antitécnico incorporarlos en la LDI.

A nuestro criterio, respecto de los delitos informáticos, en un intento de clasificarlos, podemos anotar que del universo de ellos: en principio, todos son delitos complejos en cuanto a su investigación requiere el manejo de las TIC; el agente, que puede ser una persona o una organización criminal, siempre utiliza

como medio de comisión las TIC. Luego, dentro de este amplio campo que comparten ambas características, deben distinguirse dos parcelas bien diferenciadas: las nuevas modalidades de delitos preexistentes donde se vulnera el bien jurídico preexistente y por otro lado, las nuevas formas criminales que, en una sociedad moderna, surgen por el uso cotidiano de las TIC en el que se vulnera un nuevo bien jurídico que puede concurrir con la afectación de otros preexistentes. Así, el child grooming, viene a ser un delito preexistente, el cual adquiere una nueva modalidad mediante el uso de la TIC.

Técnicas y modalidades comprendidas dentro del delito de fraude informático

Errores u omisiones en la comprensión, procesamiento, recuperación, edición, eliminación, duplicación de datos o el uso de sistemas informáticos y estos, dentro de los cuales se utiliza tecnología para eliminar los casos de fraude informático, destacan las siguientes:

a) Bombas lógicas (logic bomb): Rutina no autorizada de un programa que produce consecuencias destructivas en un sistema en un momento determinado;

b) Caballo de Troya:(Trojan horse): Introduce un conjunto de instrucciones o hábitos a un programa que en algunos casos hace que actúe de forma diferente a lo esperado;

c) Puertas falsas: Ingrese el punto de juicio para asegurarse de que las respuestas intermedias sean correctas. Los resultados internos no están cerrados y se utilizan incorrectamente para fines.;

d) Fuga de información (data leakage): Divulgación no autorizada de datos reservados;

e) Acceso no autorizado(piggybacking): Acceso a áreas restringidas;

f) Pinchazo en línea (Wiretapping): Pinchazos de líneas de comunicación con el objeto de obtener información;

g) Simulación y Modelación: Utilizar un ordenador para planificar y simular un delito que luego es llevado a cabo;

h) El Salami: Manipulación de un gran número de pequeños importes de dinero;

i) Skimming: Robo de información contenida en una tarjeta de crédito;

j) Recojo de información desechada (Scavenging): obtención de información desechada en la papelera de reciclaje;

k) Superzapping: Permite modificar archivos y bases de datos sin acceder a ellos;

l) El pharming: Una estafa electrónica implica colocar una aplicación en la computadora de un usuario cuando envía un correo electrónico o accede a

un sitio web, para registrar el movimiento de las llaves y transferir la información recopilada: número de tarjeta de crédito, contraseña, etc.;

m) El phishing: Puede registrar ilegalmente sus datos personales relacionados con contraseñas para acceder a bancos y servicios financieros a través de correo electrónico o páginas web que siguen o copian las imágenes y apariencia de cuentas bancarias u otros nombres conocidos.

Entendiendo por estas, a aquella operación que se ejecuta alterando las normas y protocolo bancarios mediante la manipulación de la red de TEF, utilizando el código de transferencia bancaria sin soporte de papel y acreditarse montos de dinero en cuentas exprofesas para ser retirados por cómplices. Otra forma es la transferencia de dinero de una cuenta a otra que se ejecuta desde un ordenador electrónico (celular, computadora, laptop, tablet) en el que el delincuente logra ingresar a la cuenta de ahorros, corrientes, y con el acceso de la clave secreta logran transferir dinero de una cuenta a otra, aparentando ante la institución financiera, ser cliente de la misma.

El intercambio electrónico es un proceso que tiene lugar a través de una terminal electrónica, un teléfono móvil o una computadora. Esta licencia habilita un préstamo o crédito a su cuenta o institución financiera. Este método de envío de dinero, ya sea público o privado, consiste en transferir dinero de una cuenta financiera a otra, u otra cuenta de una institución financiera o de algún otro tipo de institución financiera (Salinas, 2013).

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, 2013, p.225)

III. METODOLOGÍA

3.1. Tipo y diseño de investigación:

Tipo: La presente investigación es aplicada debido a que se busca analizar comercio electrónico y los problemas de la ciberdelincuencia en tiempos de covid-19, además se constituye como una investigación mixta, es decir se basara principalmente en el aspecto cualitativo y cuantitativo, en función al análisis de datos y a la información propuesta por el investigador.

Diseño: La investigación tiene un diseño no experimental lo cual se basará principalmente en tener en cuenta si existe una vulnerabilidad del comercio electrónico frente a los problemas de la ciberdelincuencia en tiempos de covid-19

3.2. Categorías, subcategorías y matriz de categorización apriorísticas

Variable Independiente: Comercio electrónico

Variable Dependiente: Ciberdelincuencia en tiempos de COVID -19

Variables	Dimensiones	Indicadores	Ítem / Instrumento
Variable Independiente: Comercio electrónico	Compra y venta de productos por Internet	Intercambio de datos	Encuesta
	Sistema informático	Pagos electrónicos	
	Seguridad de los sistemas informáticos	Contratación electrónica	
Variable Dependiente: Ciberdelincuencia en tiempos de COVID -19	Delito cibernético	Actividad ilegal	Encuesta
	Políticas de seguridad	Falta de Seguridad tecnológica	
	Robos electrónicos	Estafas virtuales	

3.3. Escenario de estudio

Distrito judicial de Lambayeque -Chiclayo

3.4. Participante

Estuvo compuesta por 50 sujetos siendo todos especialistas en sus materias, en tal sentido son fiscales, jueces y abogados especialistas en derecho penal del distrito judicial de Chiclayo en donde se llega a determinar una totalidad de:

Tabla N. 1.- Población

Descripción	Cantidad	%
Fiscales	6	12%
Jueces	4	8%
Abogados especialistas en derecho penal	40	80%
Total, de informantes (N)	50	100

Fuente: *Propia de la Investigación.*

Muestra: De acuerdo a la muestra, se tiene que tomar en cuenta la totalidad de la población en función a los especialistas en derecho penal con un total de 50 personas.

Muestreo: Se considerará como muestreo el total de 50 informantes.

3.5. Técnicas e instrumentos de recolección de datos

Encuesta: será aplicable para poder tener una respuesta rápida de la solución del problema planteado, esta encuesta será resuelta por los jueces y Fiscales, abogados que laboran o tienen casos en los juzgados del Distrito judicial de Chiclayo los cuales tiene que tener la especialidad de derecho penal, para que puedan brindar una mejor confiabilidad.

Entrevista: la envista consta de pregunta que se realizaran a expertos para que se pueda evaluar el nivel de conocimiento que tienen los investigadores ante el problema, así mismo la validación del instrumento de trabajo fue a través de “juicio de expertos”.

Análisis documental: es la investigación de los documentos tanto en el aspecto doctrinal, legislativo como jurisprudencial para poder determinar la ciberdelincuencia y la vulneración que se está brindando ante el comercio electrónico.

3.6. Procedimientos

Los datos se obtuvieron mediante el uso de tecnología y métodos de recolección de datos aplicados a los recursos o sociedades ya mostrados. Se evalúa e incluye en la búsqueda de empleo como información relevante que permite diferenciar el supuesto del real. Los datos recopilados expuestos al porcentaje de compresión se presentan como una pregunta en forma de tablas, números de imágenes.

La información se presenta como resúmenes, tablas y gráficos que se analizan sin ningún propósito. Los estudios basados en información sobre los dominios de las subhipótesis se utilizan como referencia para la subhipótesis. Los resultados de la prueba hipotética proporcionan la base para dar forma a los resultados.

El resultado final se utilizará como un sitio de prueba para el concepto de globalización. Los resultados de probar la hipótesis hipotética (que pueden ser pruebas globales, pruebas seleccionadas y ficción, o un complemento real) proporcionan la base para dar forma al resultado del estudio.

3.7. Rigor científico

Tomando en cuenta la investigación mixta aplicada, se llega a corroborar que existe una validez y confiabilidad frente a la ampliación de la búsqueda de la investigación, donde los errores tienen mayor relevancia y confiabilidad.

Fiabilidad:

Es la certeza que los expertos mencionado en la población brindan a la investigación, esta certeza se actúa bajo la aplicabilidad de sus firmas dentro del instrumentos, pues a través de este instrumento se puede poder corroborar la opinión de los expertos en función al problema propuesto. (Hernández, 2018, p. 101)

Muestreo:

La investigación presenta un muestro no probabilístico, ya que por un lado toma en cuenta conocimiento obtenidos a través de libros, informes, revistas, periódicos, entre otros medios, con el fin de no llegar a manipular las variables ante la averiguación de la solución de la problemática (Hernández, 2018, p. 101)

Generalización:

Este aspecto es basado en la razón y el pensamiento que se genera a través de la resolución del instrumento que realizan los expertos mencionados en la población, pues con esto nos va a permitir tener un conocimiento más amplio y de manera significativa ante la discusión que generan uno o dos autores. (Hernández, 2018, p. 101)

3.8. Método de análisis de la información

Métodos Generales.

a) **El Método Inductivo:** Parte de lo particular para llegar a lo general.

b) **El Método Deductivo:** Parte de lo general para llegar a lo particular.

Métodos Específicos.

a) **El Método Inductivo:** Parte de lo particular para llegar a lo general.

b) **El Método Deductivo**: Parte de lo general para llegar a lo particular.

3.9. Aspectos éticos

a. Dignidad Humana:

Se basa principalmente en tener en cuenta el criterio de dignidad humana, teniendo en cuenta un análisis jurisprudencia y la normativa vigente

b. Consentimiento informado

Se aplica a través de la firma de los especialistas en derecho penal dentro, con la finalidad de darle una posible solución al problema planteado

c. Información

La información que se tomara en cuenta se tiene que analizar e interpretar, en función al análisis de la jurisprudencia, doctrina y legislación.

d. Voluntariedad

Se considera el actuar de la persona principalmente de los expertos en materia penal dentro de la aplicación del tema que se está investigando.

e. Beneficencia:

En la presente investigación será en beneficio de toda la comunidad jurídica para analizar comercio electrónico y los problemas de la ciberdelincuencia en tiempos de covid-19.

f.Justicia:

Se tiene en cuenta que no solo ayudara a la población jurídica sino a todo el Estado y al análisis jurisprudencial del análisis del comercio electrónico y los problemas de la ciberdelincuencia en tiempos de covid-19.

.

IV. RESULTADOS Y DISCUSION

Tabla 1

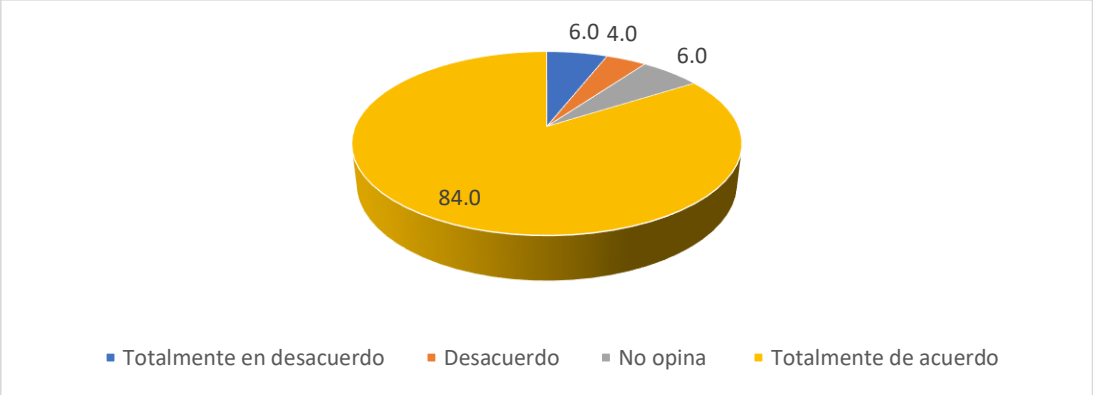
Comercio electrónico.

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	3	6.0
Desacuerdo	2	4.0
No opina	3	6.0
Totalmente de acuerdo	42	84.0
Total	50	100.0

Nota: Encuesta aplicada a Fiscales, Jueces penales y Abogados especialistas en derecho penal.

Figura 1.

Comercio electrónico.



Nota: El 84% de los Fiscales, Jueces penales y Abogados especialistas en derecho penal, manifiestan estar totalmente de acuerdo que la delincuencia en el comercio electrónico aumentando a causa del Covid-19, en caso contrario se tiene un 6.0% de la población que prefieren no opinar sobre el tema, sin embargo, como resultado negativo tenemos al 4.0% que está en desacuerdo y el 6.0% que están totalmente en desacuerdo.

Tabla 2

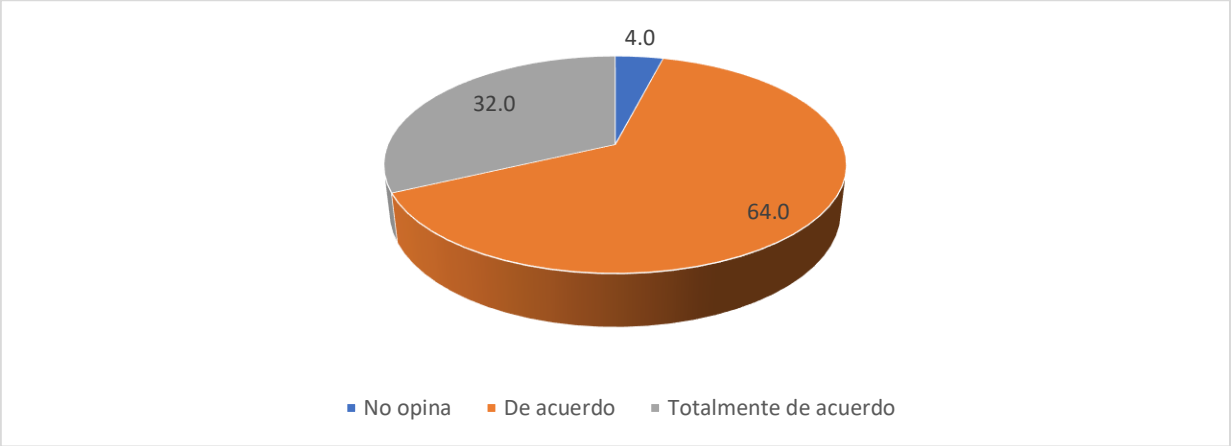
Ciberdelincuencia.

Descripción	Frecuencia	Porcentaje
No opina	2	4.0
De acuerdo	32	64.0
Totalmente de acuerdo	16	32.0
Total	50	100.0

Nota: Encuesta aplicada a Fiscales, Jueces penales y Abogados especialistas en derecho penal.

Figura 2.

Ciberdelincuencia.



Nota: El 64% de los Fiscales, Jueces penales y Abogados especialistas en derecho penal, manifiestan estar de acuerdo que a causa del surgimiento del Covid-19 se deba realizar un adecuado análisis al comercio electrónico para evitar la ciberdelincuencia, así mismo se tiene un resultado similar con un 32% que manifiestan estar totalmente de acuerdo, en caso contrario se tiene un 5.0% de la población que prefieren no opinar sobre el tema del análisis del comercio electrónico.

Tabla 3

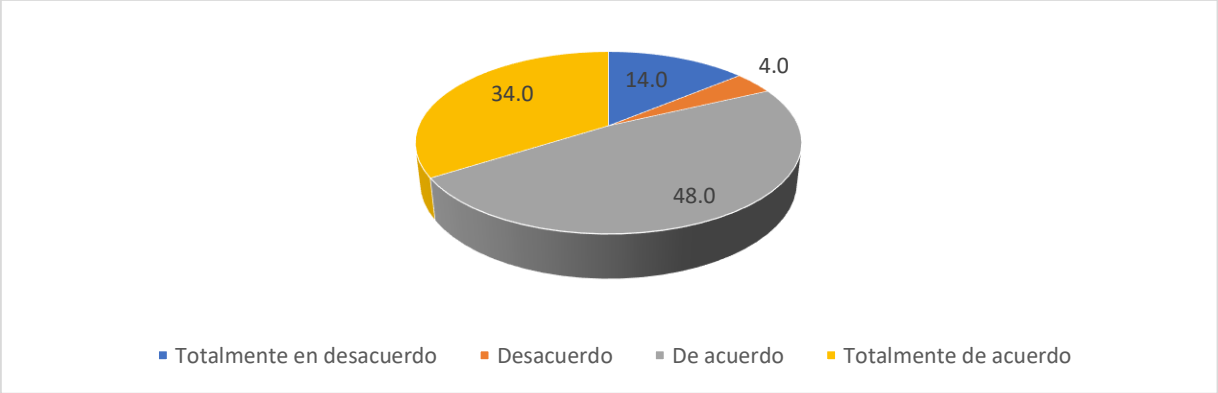
Problemas existentes.

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	7	14.0
Desacuerdo	2	4.0
De acuerdo	24	48.0
Totalmente de acuerdo	17	34.0
Total	50	100.0

Nota: Encuesta aplicada a Fiscales, Jueces penales y Abogados especialistas en derecho penal.

Figura 3.

Problemas existentes.



Nota: El 48% de los Fiscales, Jueces penales y Abogados especialistas en derecho penal, manifiestan estar de acuerdo que se deba identificar los problemas existentes de la ciberdelincuencia, así mismo se tiene un resultado similar con un 34% que manifiestan estar totalmente de acuerdo, en caso contrario se tiene un 14% de la población que se encuentran totalmente en desacuerdo, teniendo otro resultado negativo tenemos el 4.0% que está en desacuerdo.

Tabla 4

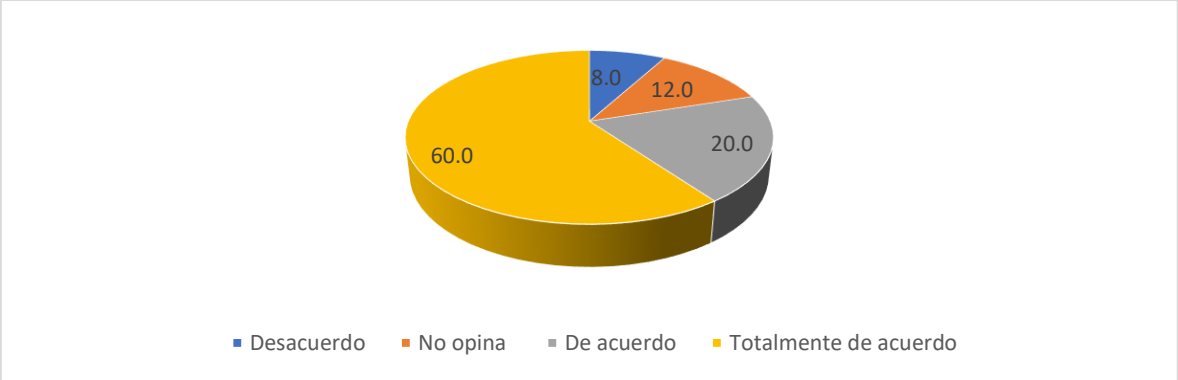
Comercio electrónico.

Descripción	Frecuencia	Porcentaje
Desacuerdo	4	8.0
No opina	6	12.0
De acuerdo	10	20.0
Totalmente de acuerdo	30	60.0
Total	50	100.0

Nota: Encuesta aplicada a Fiscales, Jueces penales y Abogados especialistas en derecho penal.

Figura 4.

Comercio electrónico.



Nota: El 60% de los Fiscales, Jueces penales y Abogados especialistas en derecho penal, manifiestan estar totalmente de acuerdo que se deba examinar cómo se encuentra regulado el comercio electrónico en el estado peruano, así mismo se tiene un resultado similar con un 20% que manifiestan estar de acuerdo, en caso contrario se tiene un 12% de la población que prefieren no opinar sobre la pregunta establecida, sin embargo, como resultado negativo tenemos el 8.0% que se encuentran en desacuerdo.

Tabla 5

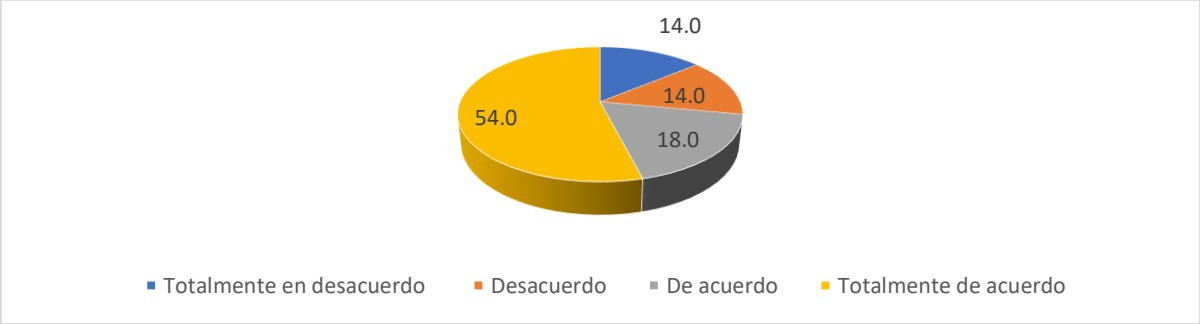
Tiempos de Covid – 19.

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	7	14.0
Desacuerdo	7	14.0
De acuerdo	9	18.0
Totalmente de acuerdo	27	54.0
Total	50	100.0

Nota: Encuesta aplicada a Fiscales, Jueces penales y Abogados especialistas en derecho penal.

Figura 5.

Tiempos de Covid – 19.



Nota: El 54% de los Fiscales, Jueces penales y Abogados especialistas en derecho penal, manifiestan estar totalmente de acuerdo que el comercio electrónico se encuentra afectado y vulnerado mediante la ciberdelincuencia en tiempos de Covid – 19, de igual forma se tiene un resultado similar con un 18% que manifiestan estar de acuerdo, en caso contrario se tiene dos resultados negativos los cuales serían el 14% de la población que están totalmente en desacuerdo y de igual manera se tiene 14% que está en desacuerdo.

Tabla 6

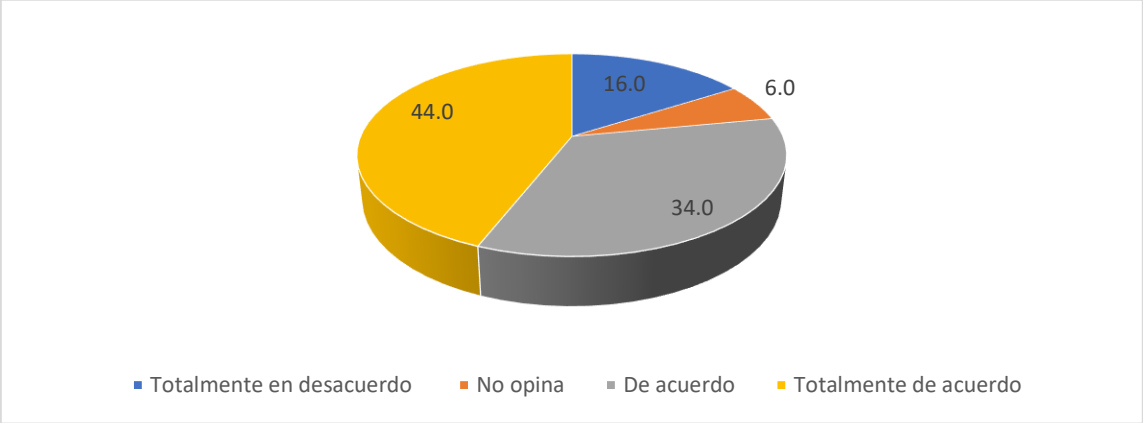
Delincuencia cibernética.

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	8	16.0
No opina	3	6.0
De acuerdo	17	34.0
Totalmente de acuerdo	22	44.0
Total	50	100.0

Nota: Encuesta aplicada a Fiscales, Jueces penales y Abogados especialistas en derecho penal.

Figura 6.

Delincuencia cibernética.



Nota: El 44% de los Fiscales, Jueces penales y Abogados especialistas en derecho penal, manifiestan estar totalmente de acuerdo que el surgimiento del Covid-19 ha generado el aumento de la delincuencia cibernética, así mismo se tiene un resultado similar con un 34% que manifiestan estar de acuerdo, en caso contrario se tiene un 6.0% de la población que prefieren no opinar sobre el tema, sin embargo, como resultado negativo tenemos el 16% que está totalmente en desacuerdo.

Tabla 7

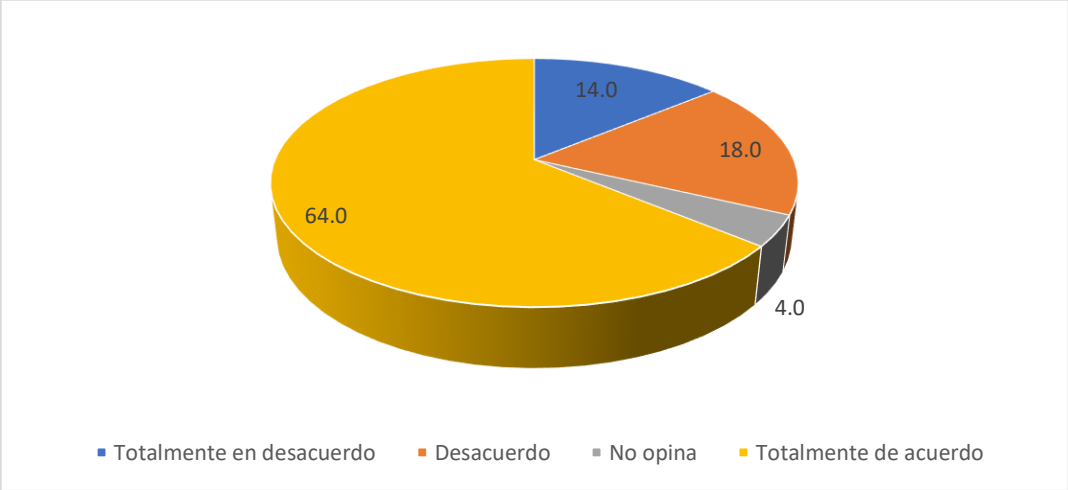
Regulación de la ciberdelincuencia.

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	7	14.0
Desacuerdo	9	18.0
No opina	2	4.0
Totalmente de acuerdo	32	64.0
Total	50	100.0

Nota: Encuesta aplicada a Fiscales, Jueces penales y Abogados especialistas en derecho penal.

Figura 7.

Regulación de la ciberdelincuencia.



Nota: El 64% de los Fiscales, Jueces penales y Abogados especialistas en derecho penal, manifiestan estar totalmente de acuerdo la ciberdelincuencia se encuentra bien regulado, sin embargo, existe un 4% de la población que prefieren no opinar sobre el tema, en caso contrario se tiene como resultado negativo tenemos el 18% que está en desacuerdo y 14% de igual forma está totalmente en desacuerdo.

Tabla 8

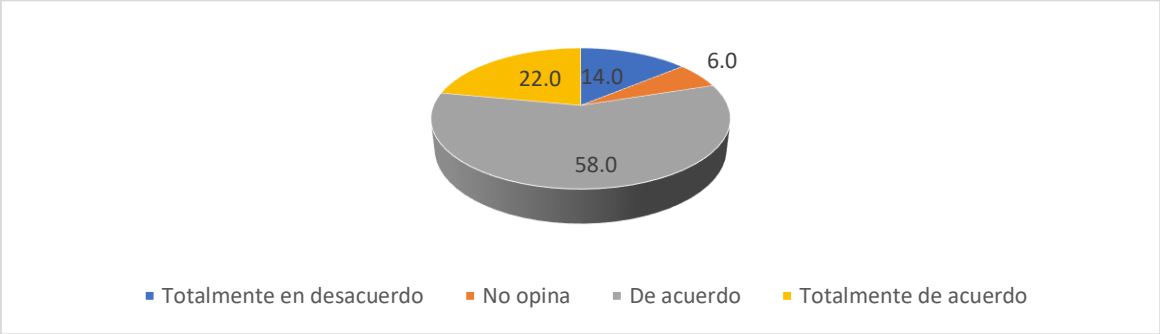
Gestión de riesgos.

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	7	14.0
No opina	3	6.0
De acuerdo	29	58.0
Totalmente de acuerdo	11	22.0
Total	50	100.0

Nota: Encuesta aplicada a Fiscales, Jueces penales y Abogados especialistas en derecho penal.

Figura 8.

Gestión de riesgos.



Nota: El 58% de los Fiscales, Jueces penales y Abogados especialistas en derecho penal, manifiestan estar de acuerdo que la ciberseguridad es el mecanismo idóneo para el desarrollo del análisis y gestión de riesgos relacionados al ciberespacio, así mismo se tiene un resultado similar con un 22% que manifiestan estar totalmente de acuerdo, en caso contrario se tiene un 6.0% de la población que prefieren no opinar sobre el tema, sin embargo, como resultado negativo tenemos el 14% que está totalmente en desacuerdo.

Tabla 9

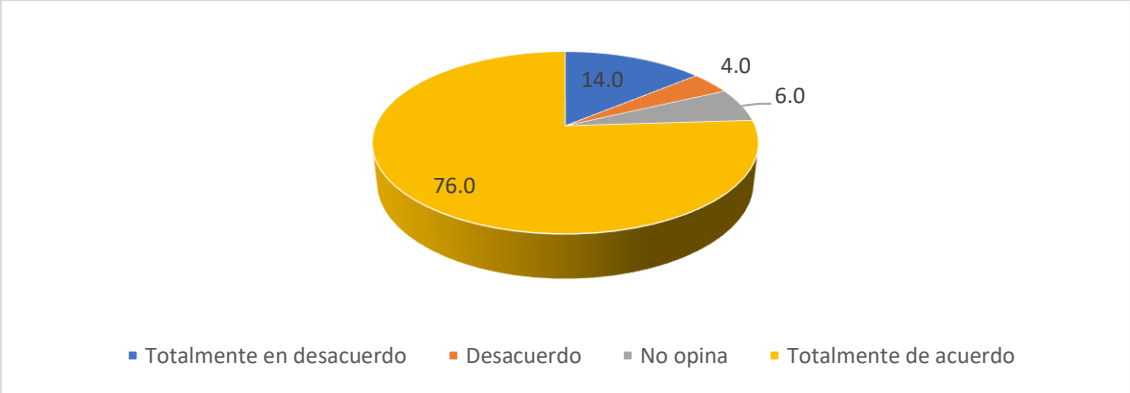
Estado peruano.

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	7	14.0
Desacuerdo	2	4.0
No opina	3	6.0
Totalmente de acuerdo	38	76.0
Total	50	100.0

Nota: Encuesta aplicada a Fiscales, Jueces penales y Abogados especialistas en derecho penal.

Figura 9.

Estado peruano.



Nota: El 76% de los Fiscales, Jueces penales y Abogados especialistas en derecho penal, manifiestan estar totalmente de acuerdo que el estado peruano ha dejado de tomar en cuenta la ciberdelincuencia, en caso contrario se tiene un 6.0% de la población que prefieren no opinar sobre el tema, sin embargo, como resultado negativo tenemos el 14% que está totalmente en desacuerdo y 4.0% que está en desacuerdo

Tabla 10

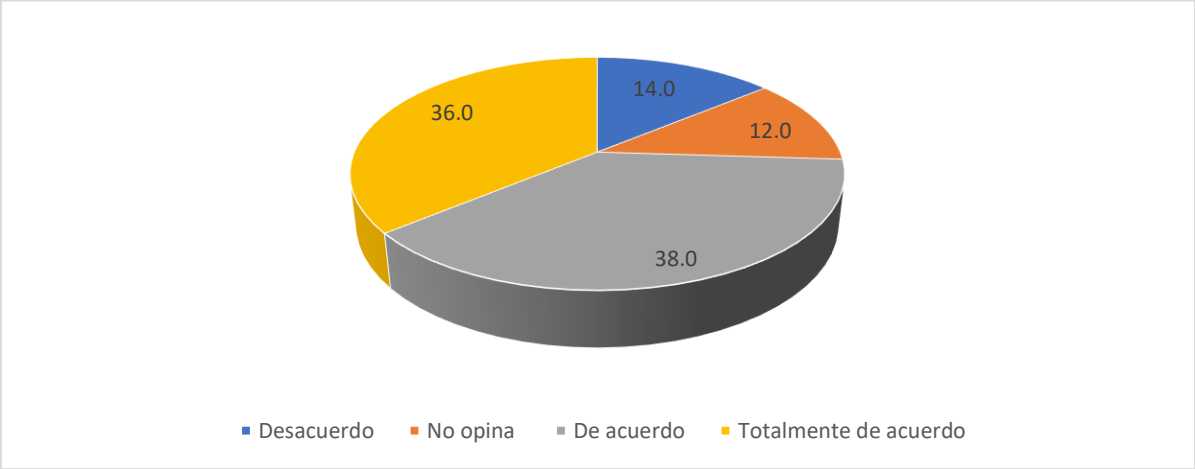
Estabilidad económica.

Descripción	Frecuencia	Porcentaje
Desacuerdo	7	14.0
No opina	6	12.0
De acuerdo	19	38.0
Totalmente de acuerdo	18	36.0
Total	50	100.0

Nota: Encuesta aplicada a Fiscales, Jueces penales y Abogados especialistas en derecho penal.

Figura 10.

Estabilidad económica.



Nota: El 38% de los Fiscales, Jueces penales y Abogados especialistas en derecho penal, manifiestan estar de acuerdo que la ciberdelincuencia vulnera la estabilidad económica en el comercio electrónico, así mismo se tiene un resultado similar con un 36% que manifiestan estar totalmente de acuerdo, en caso contrario se tiene un 12% de la población que prefieren no opinar sobre el tema, sin embargo, como resultado negativo tenemos el 14% que están en desacuerdo.

DISCUSIÓN

Conforme a los resultados obtenidos se puede resaltar lo obtenido mediante la pregunta numero 1 el cual señala un resultado favorable hacia la investigación por el hecho que el 84% de los Fiscales, Jueces penales y Abogados especialistas en derecho penal expresan estar totalmente de acuerdo en que hoy en día la delincuencia dentro del comercio electrónico aumentado a causa del surgimiento del Covid-19, sin embargo en caso contrario existen especialistas que prefieren no expresar su opinión sobre la pregunta planteada, el cual el porcentaje restante manifiestan estar con un 4.0% en desacuerdo y 6.0% totalmente en desacuerdo.

Estos resultados favorecen rotundamente a la investigación por el hecho de dar a conocer que la delincuencia electrónica es un factor que se debe tomar en cuenta para la seguridad de las personas en sus compras para que de esta manera evitar el aumento del contagio del Covid-19, este resultado al ser comparado en lo investigado por Torrente, analiza como investigación las diversas actividades que se realizan online a través de un comercio electrónico en la ciudad de Panamá

Pues frente a ello la investigación ha sido presentada para poder optar el título profesional de abogado de la Universidad Internacional de Ciencia y Tecnología, en donde se concluye 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 (Torrente, 2020). Cabe resaltar que hoy en día el mundo se mueve mediante la tecnología, sin embargo, al tener conocimiento de ello se puede evidenciar que el estado peruano no presenta mecanismos idóneos con el objetivo de respaldar toda acción realizada por medio de la tecnología.

Prosiguiendo con los resultados se puede hacer referencia a la tabla N° 2 el cual da a conocer resultado que el 64% de los expertos que fueron encuestados manifiestan estar de acuerdo en que se deba realizar un adecuado análisis a las normas que regulan el comercio electrónico con el objetivo de evitar que la ciberdelincuencia aumente, así mismo existe un 32% que de igual forma se encuentran de acuerdo, sin embargo, existe un 5.0% de los expertos que prefieren no expresar su opinión sobre la realización del análisis a la normatividad del comercio electrónico.

Estos resultados obtenidos dan a conocer que en la actualidad la normatividad que regula y protege el comercio electrónico se considera ineficaz por el hecho del aumento de la ciberdelincuencia que ha sido a causa del Covid-19, estos resultados al compararlo con lo investigado por Peralta y Roa, en su investigación analizan el impacto que ha generado los delitos cibernéticos dentro de las

operaciones de comercio electrónico en Colombia, así esta investigación ha sido presenta para poder optar el título profesional de abogado de la Universidad de Córdova, en donde se concluye que los cambios acelerados resultantes de la globalización son innumerables y cada vez más atractivos, y abren oportunidades económicas y culturales ilimitadas para toda la humanidad.

Así, guiados por el avance tecnológico de la información y de la comunicación, se han podido determinar que una herramienta que desarrolla las relaciones, el conocimiento y el desarrollo personal, organizacional, local e internacional. El comercio electrónico crea y estructura la mejor forma de pensar que se adapta al mundo digital; Las formas tradicionales de hacer negocios están siendo reemplazadas gradualmente por el hecho de que los negocios se realizan electrónicamente y se pueden mantener en bases de datos informáticas sin la necesidad de documentos físicos (Peralta y Roa, 2020).

Esta comparación realizada por los resultados obtenido y lo investigado por Peralta y Roa dan a conocer que mediante la pandemia del Covid-19 se ha generado un aumento exponencial sobre la delincuencia electrónica afectando directamente a las personas que desean realizar sus trabajos, compras, entre otras actividades que puedan mejorar su economía sin correr el riesgo del contagio.

Continuando con los resultados se puede hacer referencia la importancia de lo obtenido en la tabla N° 3 el cual establece que el 48% de los especialistas en el derecho penal se encuentra de acuerdo en la importancia de identificar cuáles

son los problemas que generan la ciberdelincuencia, de igual manera se tiene otro resultado favorable que es el 34% que expresan estar totalmente de acuerdo en que se deba detectar las problemáticas generadas por estos actos de delincuencia cibernética, sin embargo un 14% se encuentra totalmente en desacuerdo y el 4.0% restante en desacuerdo.

Este resultado expresa la necesidad de realizar la correcta identificación de los problemas que genera la ciberdelincuencia frente la estabilidad del comercio electrónico, teniendo en cuenta generar una correcta protección y subsanar los vacíos el cual se aprovechan los delincuentes para cometer sus delitos, entonces al compararlo con lo investigado por Romero, en su investigación interpreta los delitos informáticos que han sido cometido a través de las diversas redes sociales, para poder efectuar un eficaz tratamiento en el ministerio público de la ciudad de Huánuco, esta investigación ha sido presenta para poder obtener el título profesional de abogado de la Universidad de Huánuco, 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.

Esto debe incluir la naturaleza de la tecnología informática, los pasos para restaurar la evidencia informática, su investigación y los requisitos de un informe pericial que permita la confiabilidad de la evidencia como medio de evidencia (Romero, 2017). Mediante el análisis realizado a lo obtenido por la encuesta y lo

investigado por el autor antes mencionado se puede señalar que el ministerio público es un factor fundamental frente a los delitos cibernéticos, sin embargo, se puede evidenciar que en la actualidad no cuentan con las herramientas idóneas para combatir estos delitos que vulneran los derechos de las personas que realizan sus actividades con la tecnología.

Para finalizar la discusión es importante analizar lo establecido en la tabla N° 5 el cual señala que el 54% de los Fiscales, Jueces penales y Abogados especialistas en derecho penal, expresaron estar totalmente de acuerdo en que el comercio electrónico se encuentre y seguirá siendo afectado como vulnerado mediante la ciberdelincuencia, así mismo se obtuvo un resultado similar el cual es el 18% que manifiesta estar de acuerdo en que el comercio electrónico aún sigue estando vulnerado, sin embargo existen dos resultados en contra el cual es el 14% que están totalmente en desacuerdo y el 14% restante en desacuerdo, se da a conocer mediante este último resultado que la gran mayoría de los experto en la materia expresan que existe una vulneración al comercio electrónico afectando directamente a la sociedad dejándolos vulnerable en toda actividad electrónica.

Es por ello que al compararlo con lo investigado por Quevedo, en su investigación realizada hacia la prueba del ciberdelito, la cual ha sido aplicada a través de la Universidad de Barcelona para poder optar el título profesional de abogado, se llega a la conclusión que el internet ha afectado gravemente a la sociedad al crear nuevos tipos de delincuentes y actuar como herramienta de transmisión de

determinadas costumbres tradicionales, por ello la investigación del llamado ciberdelito requiere identificar las características esenciales de Internet, como la red mundial o afiliados en este caso.

Las imágenes son llevadas a los seleccionados por la web en base a esto también verifique la representación digital de la información que permite diferentes conexiones en tiempo real entre personas y lugares (Quevedo, 2017). Para finalizar es importante resaltar que a través de la encuesta realizada se ha logrado obtener resultado que dan a conocer que hoy en día mediante la pandemia del Covid-19 se ha generado un gran aumento de la delincuencia cibernética afectado directamente a la sociedad, sin embargo, el estado peruano no ha generado ningún plan de contingencia con el objetivo de disminuir o contrarrestar estos actos delincuenciales.

V. CONSIDERACIONES FINALES

a. Se analiza que el comercio electrónico se está viendo afectado, por los problemas de la ciberdelincuencia que se están presentando durante el tiempo de covid-19, estos problemas facultan que el consumidor tenga una mala experiencia de compra y que incurran como víctima de los delitos cibernéticos, sin embargo la normativa actual no contempla todos los problemas que se evidencia en relación a los delitos informáticos, es por ello que identificando los delitos se está modificando la norma para incluir los nuevos problemas informáticos y así mejorar la seguridad a la información y todo tipo de amenaza que se desprenda del uso tecnológico.

b. Los problemas de la ciberdelincuencia en tiempos de COVID-19 frente al acceso del comer electrónico, son la falta de idoneidad del producto seleccionado, clonación de tarjetas, robo de cuentas bancarias, robo de identidad personal, acceso a cuentas personales, falta de seguridad financiera, defraudación de las telecomunicaciones, delitos contra la intimidad, entre otros medios que se pueden identificar que desprotegen las compras y el comercio electrónico.

c. El comercio electrónico es una de las nuevas modalidades de compra que sean presentado en los últimos tiempos, particularmente porque

el avance tecnológico y la pandemia actual han permitido que las compras se lleven de manera virtual, sin embargo, frente a esta nueva modalidad el Estado peruano no presenta regulación, más aún frente a las nuevas modalidades de robo, esto se debe a la falta de información y especialistas cibernéticos.

d. Frente a los nuevos problemas que se presentan en la ciberdelincuencia durante los tiempos de COVID-19, el ente más afectado es el comercio electrónico, principalmente porque se están ejecutando ante los nuevos medios de contratación y falsificaciones cibernéticas que no se encuentran estipulada en la norma, ni mucho menos ante los parámetros de los juzgadores penales.

VI. RECOMENDACIONES

a. Identificar los problemas actuales que se suscitan frente a la ciberdelincuencia para incurrir dentro de la norma los nuevos delitos y proteger la ejecución del comercio electrónico dentro del estado peruano, ejecutando una seguridad cibernética y una mejor protección tecnológica.

b. El Estado debe de capacitar a sus operadores de justicia para que conozcan los nuevos delitos cibernéticos, así como sus modalidades de operación y los problemas que dificultan acceder a realizar una compra virtual.

c. Proponer un proyecto de ley que incorpore las nuevas modalidades de delitos cibernéticos a la normativa actual y sus modalidades de robo informático frente a la ciberdelincuencia en tiempos de COVID-19

REFERENCIAS BIBLIOGRAFICAS

Anarte, E. (2016). Incidencia de las nuevas tecnologías en el sistema penal. aproximación al derecho penal en la sociedad de la información", Ius Juristas.

Bramont-Arias, L. (1997). El delito informático en el código penal peruano, 1.a ed., PUCP, Lima

Camargo, L. (2020). Ciberseguridad Y Teletrabajo En Tiempos de COVID-19, Universidad del Rosario, https://repository.urosario.edu.co/bitstream/handle/10336/25394/laura%20camargo%20r%20maestria%20proyecto%20de%20grado.-ciber.pdf?sequence=2&isAllowed=y

Cámpoli, G. (2005). Delitos informáticos en la legislación mexicana, México: Instituto Nacional de Ciencias Penales

Casabona, C. (2006). De los delitos informáticos al cibercrimen. una aproximación conceptual y político-criminal, en El cibercrimen. Nuevos retos jurídicos-penales, Comares, Granada.

Chonchol, J. (2003). Sociedad, Estado y tecnología: ¿qué pasa hoy con nuestras sociedades?, Revista de sociología, N.o 17, Facultad de ciencias sociales– Universidad de Chile

Chonchol, J. (2003). Sociedad, Estado y tecnología: ¿qué pasa hoy con nuestras sociedades?, Revista de sociología, N.o 17, Facultad de ciencias sociales– Universidad de Chile.

Gil, A. (2012). El fenómeno de las redes sociales y los cambios en la vigencia de los derechos fundamentales, Revista de derecho UNED, España.

Gil, A. (2012). El fenómeno de las redes sociales y los cambios en la vigencia de los derechos fundamentales, Revista de derecho UNED, España.

Gustavo, A. (2006). Cibercriminalidad y derecho penal. Editorial Montevideo, Buenos Aires.

Hernandez. D y Mendoza. G. (2018). El funcionamiento del comercio electrónico, categorías seguridad para usuarios y demografía de usos habituales, Universidad Autónoma del Estado de México, http://ri.uaemex.mx/bitstream/handle/20.500.11799/95210/TESIS-COMERCIO-ELECTRONICO.-Definitivo...pdf?sequence=1&isAllowed=y

Lira, O. (2010). Cibercriminalidad: fundamentos de investigación en México, México: Instituto Nacional de Ciencias Penales

Martin, P. (2015). “Inseguridad cibernética en América Latina: líneas de reflexión para la evaluación de riesgos”, en el portal web del Instituto Español de Estudios Estratégicos, Madrid

Martin, P. (2015). Inseguridad cibernética en América Latina: líneas de reflexión para la evaluación de riesgos, Instituto Español de Estudios Estratégicos, Madrid

Mateo, J. (2013). Zygmunt Bauman: una lectura líquida de la posmodernidad, Revista Académica de Relaciones Internacionales, Madrid

Peralta, M y Roa, E. (2020). El impacto del delito cibernético en las operaciones de comercio electrónico en Colombia, Universidad de Córdoba, 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

Quevedo, J. (2017). Investigación y prueba del ciberdelito, Universidad de Barcelona, España, https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1&isAllowed=y

Sukhai, N. (2004). Hacking and cyber crime. New York, NY. ACM Press.

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

ANEXOS

ANEXO N° 01 – DECLARATORIA DE AUTENTICIDAD DEL AUTOR

DECLARACIÓN DE AUTENTICIDAD

Carol Marilin Gonzales Chávez, identificado con DNI N° 45363605, a efecto de cumplir con las disposiciones vigentes consideradas en el Reglamento de Grados y Títulos de la Universidad Particular de Chiclayo, Facultad de Derecho y Educación, Escuela de Derecho, declaro bajo juramento que toda la documentación que acompaño es veraz y auténtica.

Así mismo, declaro también bajo juramento que todos los datos e información que se expone en la presente tesis son legítimos y ciertos.

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

Pimentel

GONZÁLES CHÁVEZ CARO MARILIN
DNI N° 45363605

Bach. Carol Marilin Gonzáles Chávez

ANEXO N° 02 – DECLARATORIA DE AUTENTICIDAD DEL ASESOR

DECLARACIÓN DE AUTENTICIDAD

……., identificado con DNI N°……..., a efecto de cumplir con las disposiciones vigentes consideradas en el Reglamento de Grados y Títulos de la Universidad Particular de Chiclayo, Facultad de Derecho y Educación, Escuela de Derecho, declaro bajo juramento que toda la documentación que acompaño es veraz y auténtica.

Así mismo, declaro también bajo juramento que todos los datos e información que se expone en la presente tesis son legítimos y ciertos.

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

Pimentel

_____

ASESOR

ANEXO N° 03 – MATRIZ DE CONSISTENCIA

PROBLEMA DE INVESTIGACIÓN	OBJETIVO GENERAL	HIPÓTESIS	VARIABLES E INDICADORES	TIPO DE INVESTIGACIÓN	DISEÑO DE INVESTIGACIÓN	METODOLOGÍA
¿Qué problemas de ciberdelincuencia en tiempos de COVID-19, genera el comercio electrónico?	Analizar el comercio electrónico y los problemas de la ciberdelincuencia en tiempo de COVID -19 **OBJETIVOS ESPECÍFICOS** 1. Identificar los problemas de la ciberdelincuencia en tiempos de COVID-19. 2. Examinar el comercio electrónico y su regulación en el estado peruano.	Si se identifican los problemas de ciberdelincuencia en tiempos de COVID-19, entonces se mejorar el comercio electrónico brindando una mayor seguridad a la información y neutralizando toda aquella amenaza que se desprenda	**VARIABLE 1** **Comercio electrónico** **VARIABLE 2** **Ciberdelincuencia en tiempos de COVID -19**	La presente investigación es aplicada debido a que se busca analizar comercio electrónico y los problemas de la ciberdelincuencia en tiempos de covid-19, además se constituye como una investigación mixta, es decir se basara principalmente en el aspecto cualitativo y cuantitativo, en función al análisis de datos y a la información propuesta por el investigador	La investigación tiene un diseño no experimental lo cual se basará principalmente en tener en cuenta si existe una vulnerabilidad del comercio electrónico frente a los problemas de la ciberdelincuencia en tiempos de covid-19	Descriptivo

	3. Determinar si el comercio electrónico se ve afectado ante los problemas de la ciberdelincuencia en tiempos de COVID-19	del uso tecnológico				
INSTRUMENTO		**MÉTODOS DE ANÁLISIS DE DATOS**				
Encuesta: será aplicable para poder tener una respuesta rápida de la solución del problema planteado, esta encuesta será resuelta por los jueces y Fiscales, abogados que laboran o tienen casos en los juzgados del Distrito judicial de Chiclayo los cuales tiene que tener la especialidad de derecho penal, para que puedan brindar una mejor confiabilidad. **Entrevista:** la envista consta de pregunta que se realizaran a expertos para que se pueda evaluar el nivel de conocimiento que tienen los investigadores ante el problema, así mismo la validación del instrumento de		Los datos plasmados en esta investigación serán obtenidos a través de los instrumentos y las técnicas de recolección los cuales ya previamente se han identificado tal es así que se tomará en cuenta toda aquella información que ayude a contrarrestar la hipótesis de la realidad problemática además estos datos se van a presentar a través de tablas y gráficos estadísticos utilizando el programa SPSS con la finalidad de generar una confiabilidad frente a lo manifestado por los expertos penales				

trabajo fue a través de “juicio de expertos”. **Análisis documental:** es la investigación de los documentos tanto en el aspecto doctrinal, legislativo como jurisprudencial para poder determinar la ciberdelincuencia y la vulneración que se está brindando ante el comercio electrónico.	

ANEXO N° 04 – INSTRUMENTO DE RECOLECCIÓN DE DATOS

UNIVERSIDAD PARTICULAR DE CHICLAYO

FACULTAD DE DERECHO

COMERCIO ELECTRÓNICO Y LOS PROBLEMAS DE LA CIBERDELINCUENCIA EN TIEMPOS DE COVID-19

Estimado (a): Se le solicita su valiosa colaboración para que marque con un aspa el casillero que crea conveniente de acuerdo a su criterio y experiencia profesional, puesto que, mediante esta técnica de recolección de datos, se podrá obtener la información que posteriormente será analizada e incorporada a la investigación con el título descrito líneas arriba.

NOTA: Para cada pregunta se considera la escala de 1 a 5 donde:

1	2	3	4	5
TOTALMENTE EN DESACUERDO	**EN DESACUERDO**	**NO OPINA**	**DE ACUERDO**	**TOTALMENTE DE ACUERDO**

ITEM	TD	D	NO	A	TA
1. ¿Considera usted que la delincuencia en el comercio electrónico aumentando a causa del Covid-19?					
2. ¿Cree usted que a causa del surgimiento del Covid-19 se deba realizar un adecuado análisis al comercio electrónico para evitar la ciberdelincuencia?					
3. ¿Considera usted se deba identificar los problemas existentes de la ciberdelincuencia?					
4. ¿Cree usted se deba examinar cómo se encuentra regulado el comercio electrónico en el estado peruano?					
5. ¿Considera usted que el comercio electrónico se encuentra se encuentra afectado y vulnerado					

	mediante la ciberdelincuencia en tiempos de Covid – 19?					
6.	¿Cree usted que el surgimiento del Covid-19 ha generado el aumento de la delincuencia cibernética?					
7.	¿Considera usted que la ciberdelincuencia se encuentra bien regulado?					
8.	¿Cree usted que la ciberseguridad es el mecanismo idóneo para el desarrollo del análisis y gestión de riesgos relacionados al ciberespacio?					
9.	¿Considera usted que el estado peruano ha dejado de tomar en cuenta la ciberdelincuencia?					
10.	¿Cree usted que la ciberdelincuencia vulnera la estabilidad económica en el comercio electrónico?					