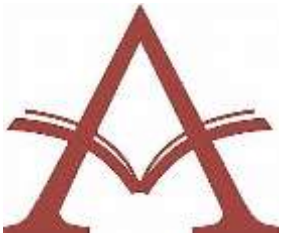
UNIVERSIDAD PERUANA DE LAS AMÉRICAS



ESCUELA PROFESIONAL DE DERECHO

TRABAJO DE INVESTIGACIÓN

El impacto del cibercrimen en delitos de estafa en el Distrito de Lima, 2021.

PARA OPTAR EL TÍTULO PROFESIONAL EN DERECHO

AUTOR:

IRMA GISELA HUAYRE TORRES

CÓDIGO ORCID: 0000-0002-4650-8972

ASESOR:

Dr. ANDRÉS BORCIC SANTOS

CÓDIGO ORCID: 0000-0003-1464-8759

LÍNEA DE INVESTIGACIÓN: DERECHO PENAL

LIMA, PERÚ

Diciembre, 2021

RESUMEN

Esta investigación tiene por objetivo examinar cual es el impacto social sobre las políticas criminales en delitos de estafa explorando las tendencias actuales de las comunicacio nes y la delincuencia cometida en el entorno de Internet. La metodología sigue un enfoque cualitativo, correlacional y descriptivo. Se usan los métodos explicativos, empíricos y hermenéuticos, además, se revisarán publicaciones científicas y relevantes sobre delitos informáticos. Este estudio desarrolla los conceptos de ciberdelincuencia como medio en el procedimiento delictual de estafa, se procede analizando las disposiciones legales existentes, normas e instrumentos que intervienen en la lucha contra los delitos informáticos. Esta investigación busca contribuir en la proposición de políticas de protección informática como estrategia de ciberseguridad.

Palabras Clave: Cibercrimen, delito de estafa, delitos informáticos.

ABSTRACT

The objective of this research is to examine what is the social impact on criminal policies in fraud crimes by exploring current trends in communications and crime committed in the Internet environment. The methodology follows a qualitative, correlational and descriptive approach. Explanatory, empirical and hermeneutical methods are used, in addition, scientific and relevant publications on computer crimes will be reviewed. This study develops the concepts of cybercrime as a means in the criminal fraud procedure, it proceeds by analyzing the existing legal provisions, rules and instruments that intervene in the fight against computer crimes. This research seeks to contribute to the proposition of computer protection policies as a cybersecurity strategy.

Key Words: Cybercrime, fraud crime, computer crimes.

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Investigar el delito cibernético se ha convertido en la actualidad en un gran desafío. Los delincuentes aprovechan cualquier dispositivo con internet para cometer estos delitos en forma anónima. Dada la gravedad de estos delitos informáticos y su naturaleza, se evidencia la necesidad crucial de entender el funcionamiento de esta actividad delictiva a nivel legal nacional e internacional para poder abordarla de manera eficaz. Por tanto, es de enorme importancia investigar hasta qué punto la legislación, las iniciativas, políticas criminales y procedimientos que ayuden a combatir estos delitos informáticos son coherentes en nuestra realidad nacional.

El objetivo de este trabajo es estudiar, analizar y comparar el impacto que tienen estos delitos informáticos en la jurisdicción de Lima en el año en curso que servirá para identificar en qué medida son coherentes entre sí, su alcance y sus limitaciones.

Este trabajo examina los enfoques utilizados para combatir el cibercrimen, en última instancia, el propósito es identificar las áreas donde se necesitan mejoras y de existir alguna modificación legal, resolverla.

Para cumplir con la finalidad del tema, se desarrollará el planteamiento del problema de investigación, describiendo la realidad problemática.

Se realiza un análisis de la realidad problemática, del marco teórico, detallando antecedentes de la investigación, aquellos de índole nacional e internacional, legislac ión aplicable al impacto del cibercrimen que conllevan a delitos de estafa.

Finalmente, se desarrolla el trabajo de campo, la cual analiza e interpreta el resultado de la investigación.

2. ANTECEDENTES

2.1. Internacionales.

Díaz, Angulo y Barboza (2018). *Repositorio: ¨Análisis del delito de fraude electrónico: modalidad tarjeta de crédito¨*. Planteaban esa línea de tiempo, la ausencia de una normativa que determine los delitos informáticos de índole financiero, pero alcanzando la supletoriedad de la ley especifica en las resoluciones que emitían los juzgados penales colombianos sobre estos delitos. Los autores explican que el código penal sanciona el ciberdelito pero no delimita las acciones típicas en delitos de fraudes informát icos financieros. Indican también, que las tarjetas bancarias son vulnerables en seguridad electrónica siendo de alcance del cibercriminal que usa distintos medios de acceso a información y datos personales aumentando los casos de fraude en la población colombiana. Como solución, el Estado promulgó una seria de leyes que ayudaron a combatir estos delitos, pero que en la práctica confiere tanto al banco emisor como al tenedor de la tarjeta bancaria, responsabilidad compartida respecto su uso y de su ciberseguridad.

Devia (2017), Tesis: Delito informático: *¨Estafa informática del artículo 248.2 del Código Penal.* Sustenta que la economía va de la mano con la tecnología, siendo una característica principal su crecimiento en el uso de la red informática a nivel mundia l, pero con consecuencias positivas como también negativas, se establece la correlación en la forma de realizar los delitos por medios informáticos siendo clasificados por la normativa penal de formas distintas según la locación donde se ejecuta el delito. Esto último dificulta las acepciones legales que tienen los juristas por la dinámica variante de estos delitos de fraude informático en su regulación, así como en su lucha y prevención. El autor concluye que la dificultad radica en la contraposición de la regulación de internet con los derechos fundamentales de libertad de expresión y otras libertades (intimidad, privacidad y anonimato) en las cuales los Estados no tienen alguna intervención. La defensa de la propiedad patrimonial existe desde cualquier acceso social como es el acceso informático, los derechos de cada persona que comparte datos sensibles como cuentas bancarias, personales o de identidad o en contrataciones virtuales donde prima la

buena fe, deben ser protegidas por la legislación mundial demarcándose de otros derechos que puedan ser reclamados cuando se atenten con la libertad de cada persona.

Mayer y Oliver (2020). Revista chilena de derecho y tecnología : *¨El delito de fraude informático: concepto y delimitación¨*. Los autores concluyen que siendo el fraude informático un delito en auge, no existen precisiones de las conductas que califiq uen dentro del marco normativo chileno, se confunden con otros delitos similares que no especifica el comportamiento exacto del fraude por internet. Los autores proponen delimitar los elementos del delito de la siguiente manera: verificando la manipulación de los sistemas informáticos del sujeto activo, provocando perjuicios patrimoniales en la victima o sujeto pasivo, para finalmente obtener algún beneficio, provecho o utilidad del ciberdelincuente.

Quevedo (2017). *¨Programa de Doctorado en Derecho y Ciencia Política de la Universidad de Barcelona: Investigación y prueba del ciberdelito¨*. De sus conclusio nes se esboza conocer a profundidad el manejo técnico básico de internet que permitan conocer y diferenciar de otros delitos informáticos la conducta de cada ciberdelito. La competencia de perseguir el cibercrimen del poder judicial español abarca según donde se produce el delito desde la tentativa hasta su consumación. Si el delito se comete en otro Estado, la ley penal considera la extradición de quienes lo cometan si estos se consideran terrorismo o delitos de pornografía infantil o cualquiera relativa a ella. El Estado español forma parte de organismos de investigaciones criminales que facilitan los convenios en tratamientos de acciones penales cometidos por ciudadanos europeos teniendo en cuenta los derechos fundamentales emitidas por la Constitución y la jurisprudencia. Estos controles del delito implican diligencias de intervención en las revisiones de las cuentas digitales con las respectivas autorizaciones judiciales. Las dificultades en la obtención de los medios probatorios radican en la inmaterialidad de los elementos del delito causado, siendo la receptación de los dispositivos informáticos utilizados en un proceso judicial.

2.2. Nacionales.

Reyes (2020). Tesis: *¨Los Delitos Informáticos y su influencia en la Integridad Personal, distrito de Chorrillos, Lima Metropolitana, 2019¨*. Percibe la alta tasa de criminal idad tecnológica con procedimientos que el Estado no puede controlar en la forma de aplicar justicia. La sociedad está desprotegida y al alcance de los cibercriminales que utilizan las redes informáticas para cometer los hechos ilícitos. Los actos criminales afectan no solo el patrimonio, sino también la honradez de las personas. La escasa investigación del delito en el distrito de Chorrillos sugiere al autor realizar el trabajo de campo para contribuir al futuro conocimiento de los estudiantes y poder aplicarla. El autor finaliza su investigación, recomendando a la Fiscalía la posibilidad de proponer capacitaciones del delito informático. De la misma manera, sugiere que el Estado ofrezca capacitaciones de especializaciones en cibercrimen con la tecnología correcta y en el uso de aplicacio nes digitales de prevención a la población.

Montoya, F. (2018). Afirma la ausencia en la definición y tipificación del delito de clonación de tarjetas bancarias, siendo escasa el campo de acción de la actual legislac ión penal contra la modalidad de inseguridad por los ciberdelincuentes. El autor propone una actualización de la normativa penal que incida en un acápite independiente que defina el ilícito de duplicidad de tarjetas con índole financiero con base al derecho comparado. Determina la insuficiencia de los elementos contenidos en la Ley N° 30096, siendo una norma muy general, que no regula específicamente el delito mencionado y pueda proteger al ciudadano de estos actos ilícitos.

Pardo (2018). Delimita la confusión que existe en los operadores jurídicos cuando aplican la legislación penal en delitos informáticos respecto al patrimonio. Con exactitud difiere de la norma de fraude informático en su generalización con otras acciones delictivas más complejas. El autor expresa que existen muchas lagunas jurídicas en la medida que se pueda sancionar delitos específicos que se caracterizan por su atipicidad, por ejemplo el delito de estafa no coincide con la ley de delitos informáticos, dificultando a los operadores de justicia poder aplicarla con eficiencia. Los ciberdelincuentes aprovechan estos vacíos legales para seguir delinquiendo de país en país en desventaja de las normas peruanas que no conectan de manera regular con las normas internacionales. La inclus ión de capacitaciones de derecho informático y de cursos básicos de informática ayudaría al

conocimiento y advertir de los delitos que puedan involucrar el uso de dispositivos electrónicos.

Gallardo (2020). Determina respecto al Convenio contra el Cibercrimen (Budapest), y la Resolución Legislativa N° 30913 (ratificado el año 2019), incorporando los delitos de falsificación informática, subsanando algunos artículos de la Ley de delitos informáticos, la valoración de los conceptos pertenecientes a la falsificación informática y su evaluación incluye una determinación explícita de las amenazas a la ciberseguridad para aclarar la inminencia originada por los ciberataques, así como la necesidad de una acción del Estado peruano, así como la difusión del Convenio de Budapest como una disposició n de derecho internacional para las definiciones aplicadas actualmente.

3. BASES TEÓRICAS.

3.1. Doctrina.

3.1.1. Delitos informáticos.

Las tecnologías y las comunicaciones están cambiando rápidamente en los tiempos modernos, lo que hace que los conceptos siempre variantes de delincuencia y criminal idad se adapten a un mundo informático. La prevalencia de las tecnologías y del Internet ha cambiado radicalmente la forma en que vivimos, nos comunicamos, viajamos, compartimos información, transferimos fondos, trabajamos y hacemos negocios (Oxman, 2013 - Revista de Derecho). Para comenzar a discutir el ciberdelito, la victimizac ión online y el uso de métodos de prevención del ciberdelito, es crucial comprender cómo surge el ciberespacio, la extensión de internet y cómo se regula. Un tercio de la población mundial (4,660 millones de personas) tiene acceso a Internet (Galeano, 2021), aproximadamente el 55% de todos los usuarios de Internet tienen menos de 25 años (Conapoc, 2020. Libro digital: *¨Diagnóstico Situacional Multisectorial sobre la Ciberdelincuencia en el Perú. Edición digital¨*). Como tal, particularmente en los más jóvenes, se vuelve menos común encontrar un crimen que no involucre algunos elementos de la conectividad a Internet. El entorno de la evolución de Internet y las tecnologías hace que la planificación y las predicciones en torno al ciberdelito sean inciertas, especialme nte para las fuerzas del orden. Como resultado, el campo del delito informático a menudo no está regulado o si lo está, será por estatutos obsoletos que no abarcan los desarrollos más nuevos. Los delitos cibernéticos con mayor impacto se han venido produciendo desde los primeros años de existencia de Internet.

Según Barrio (2015). Libro: *¨Ciberdelito: Amenazas Criminales del ciberespacio¨*. Los delitos informáticos son aquellas acciones delictivas reales que amenazan la seguridad ciudadana. Sin embargo, no todos los delitos cometidos en el ciberespacio están cubiertos por el término delito informático.

De acuerdo Mayer y Oliver (2020). Revista*: ¨El delito de fraude informático: concepto y delimitación¨*. El delito informático puede considerarse como aquel delito donde, un

dispositivo digital o informático media como herramienta incidental del delito. Sain (2018) define delito informático como el uso implícito de tecnologías digitales en la comisión de un delito, está dirigido a las propias tecnologías de la información y de sus comunicaciones. En nuestro país, los delitos informáticos son sancionados por la Ley N° 30096 (2013).

Aboso (2018). Libro: *¨Derecho penal cibernético: la cibercriminalidad y el Derecho Penal en la moderna sociedad de la información y la tecnología de la comunicación¨*. Clasifica el delito informático en tres categorías:

- Delitos donde la computadora y/o la red informática es el objetivo de la actividad delictiva, como por ejemplo: la piratería o el deterioro de los sistemas informáticos;
- Delitos comunes donde la computadora o dispositivo digital es la herramienta o medio utilizado para cometer el delito, como por ejemplo: la pornografía infant i l y el fraude por internet; y
- Delitos donde el uso de la computadora o dispositivo digital es un aspecto incidental en la comisión del delito, proporcionando evidencia del delito, como por ejemplo: direcciones encontradas de un sospechoso de asesinato.

Cabanellas y Palazzi (2004). Revista: *¨Delitos informáticos e internet, en Derecho de internet en Argentina¨*, Adoptan una clasificación similar:

- Delito que implica el uso de tecnologías digitales en la comisión del delito, como el fraude online y la difusión de materiales ofensivos por vía electrónica;
- Delitos que están dirigidos a las tecnologías informáticas y de comunicac ió n, incluido el acceso no autorizado a computadoras y redes de computadoras, delitos que involucran vandalismo e invasión del espacio personal como acoso cibernético; y
- Delito donde la tecnología de la información es incidental en la comisión de otros delitos.

Heredia (2015). Revista: *¨Política criminal de los delitos informáticos¨*. Sobre las tendencias en ciberseguridad establece que el cibercrimen evoluciona junto con las tecnologías y se vuelve cada vez más sofisticada. Los piratas informáticos ya no están explotando objetivos de oportunidad, sino que tienen la libertad de seleccionar personas,

empresas o servicios específicos que están disponibles a medida que las víctimas confían cada vez más en la información para estar seguras en Internet, lo que abre nuevas oportunidades para los delincuentes. Otro aspecto del entorno virtual que puede causar problemas potenciales es la inteligencia artificial y drones, que pueden usarse como vigilancia, violando la privacidad de las personas o incluso como un arma letal.

Crespo (2020). Revista: *¨La acción nuclear del delito informático en el novísimo código orgánico integral penal¨*. Afirma que el principal problema para estudiar el delito informático es la ausencia de definiciones actuales y coherentes del delito informático.

Ortiz (2019). Revista*: ¨Normativa Legal sobre Delitos Informáticos en Ecuador¨*. Señala que el término "delito informático" no tiene una definición específica en la ley, sin embargo, el término se usa a menudo en política, medios de comunicación y dentro del sistema de justicia penal. Crespo (2020), sugiere que en lugar de intentar conceptualizar el término "cibercrimen" o "ciberdelito" como un fenómeno único, debería verse como una gama de actividades en las que las redes de tecnología de la información y comunicación (TIC) o Internet son variables determinantes. Por otro lado, Utreras (2017). Tesis: *¨La necesidad de tipificar el delito de fraude informático en chile. Análisis jurisprudencial, doctrinario y normativo¨*. Define el cibercrimen como un término conceptualizado: actividades realizadas por medios o dispositivos informáticos que son ilegales o consideradas ilícitas en ciertos lugares y que se llevan a cabo a través de redes electrónicas a nivel global (p. 13). La definición proporcionada por muchos autores toma una distinción crucial entre delito (acto prohibido por la ley) y desviación social (acto que viola las normas sociales informales), lo cual es importante para una mayor reflexió n sobre su definición.

En primer lugar, no existe una definición universalmente aceptada. Si bien algunos países ya han avanzado relativamente en la persecución de los delitos informáticos con instrumentos jurídicamente vinculantes (como el Convenio de Budapest), otras regiones aún no han incluido la importancia de la ciberseguridad como un tema en su estrategia de seguridad nacional. Naturalmente, lo acompaña la falta de definiciones claras. Pero no es solo la indiferencia de los gobiernos nacionales lo que evitó los esfuerzos para implementar una definición legal; Uno de los principales problemas para definir adecuadamente el ciberdelito es la falta de datos estadísticos concretos sobre estos delitos.

Las empresas a menudo se abstienen de informar sobre estos ataques por temor a liberar datos confidenciales o perder la confianza de sus clientes. Dado que la denuncia de delitos hasta ahora es predominantemente voluntaria, es casi seguro que las cifras sean mucho más bajas que la ocurrencia real de delitos.

Además, el enjuiciamiento de los delitos informáticos sigue siendo un desafío para los Estados y los operadores jurídicos debido a una interconexión global inherente, sin fronteras. Esto refiere al hecho de ignorar criterios operativos tradicionales en los sistemas de justicia penal, como son la soberanía y el principio de territorialidad. Los delitos informáticos desafían los ámbitos jurisdiccionales convencionales de los estados soberanos cuando los ataques se originan en casi cualquier computadora o dispositivo digital del mundo, atraviesan múltiples fronteras nacionales o están diseñados para parecer que se originan en fuentes extranjeras, lo que crea incertidumbres con respecto a la jurisdicción competente.

Los problemas son también los niveles nacionales divergentes en la legislación, que facilitan la explotación de diversas lagunas en legislación penal de otros países sin enjuiciar debidamente a los criminales. La ausencia de armonización internacional puede crear "refugios contra el crimen" similares a los "refugios fiscales" creados por la legislación en ciertos estados.

La ilimitación de los delitos coexistentes con la ausencia de un régimen de derecho internacional en el ciberespacio provoca un dilema jurisdiccional. Por lo tanto, los Estados no pueden manejar el problema individualmente, sino que deben buscar la cooperación transnacional o global para abordar eficazmente los delitos informáticos.

Además de la problemática de la ilimitación de los delitos informáticos, la característica de ser innovador implica el entorno cambiante de las TIC. Los procedimientos de aplicación de la ley penal ajustados al mundo físico se enfrentan a nuevos desafíos en el mundo virtual. Ya sea que las pruebas se eliminen o alteren en las redes de informac ión o estas nuevas tecnologías diversifiquen el mercado constantemente, el marco legal debe cambiar para adaptarse a estos nuevos delitos.

Estos nuevos delitos dependientes de internet desafían el marco de la normativa penal debido a la ausencia de referencias en la ley. El delito informático en su origen podría tener ya una referencia en el derecho penal, por ejemplo, el fraude o el robo de propiedad. Aun así, estos delitos se persiguen en una nueva dimensión y conllevan nuevas opciones que no están contempladas en la legislación respectiva. No está claro en qué medida las referencias legales existentes sean aplicables a los delitos informáticos y especialmente a las formas de delitos dependientes del internet y habilitados por el sistema informát ico, lo que plantea complejidades no solo legales sino también técnicas en la persecución del delito informático. Esto es válido para el seguimiento de medios probatorios, ya que la naturaleza dinámica del ciberespacio dificulta la recopilación de todas las pruebas digitales relevantes de los delitos informáticos.

Se plantea la cuestión de la existencia de la ley de delitos informáticos en primer lugar y si esta ley es eficazmente aplicable en la normativa peruana. Los requisitos tecnológicos para realizar estos delitos se han vuelto más accesibles. En comparación con otros delitos que requieren una inversión menor y no está restringido por controles más estrictos.

Para concluir, los delitos informáticos difieren significativamente en su naturaleza de los delitos comunes que son visibles en cuatro aspectos principales: la falta de una definic ión clara como delito, su naturaleza "sin fronteras", los rápidos cambios técnicos y los recursos necesarios suficiente para causar daños.

3.1.2. Delito de estafa informática.

Según Lara y Albán (2017). Revista: *¨Los riesgos de las transacciones bancarias por Internet¨*. Lo definen como la realización ilegal e intencional de un engaño que causa perjuicio real potencial para en otra persona. Sus elementos son: ilegalidad, tergiversación, prejuicio e intención. Cevallos (2020), identifica el fraude informá t ico como "delitos informáticos que implican la tergiversación deliberada o alteración de datos con el fin de obtener algo lucrativo".

Asimismo, la normativa peruana sanciona estos delitos informáticos mediante Ley N° 30096, específicamente en el artículo 9° (suplantación de identidad) y el artículo 8° (fraude informático).

La estafa informática tiene características engañosas generalmente comunes del delito informático perpetrado dentro de una relación comercial con beneficio personal. Es un acto de engaño intencional utilizando información falsa (Ospina, Milton, y Sanabria, 2020). Por lo tanto, la estafa informática se describe generalmente como la utilización de servicios de internet donde se realizan transacciones comerciales dudosas con intenció n de engañar a personas, organizaciones o inclusive gobiernos (Heredia, 2015. Revista: *¨Política criminal de los delitos informáticos¨*).

La estafa informática también se describe como cualquier tipo de esquema de fraude que utiliza diversos componentes de la internet para realizar solicitudes y transacciones fraudulentas (Lara y Albán, 2017). Revista: *¨Los riesgos de las transacciones bancarias por Internet¨*). Se perpetra con diferentes camuflajes, formas o matices, usando páginas o redes sociales mayormente falsas. Estas formas comunes incluyen estafas y robos de identidad en línea. La penetración de Internet en la economía personal y el comercio han abierto vías para perpetrar estos delitos, escondiéndose detrás del anonimato cibernético (Mayer y Oliver, 2020). Concretándose la exposición a transacciones fraudulentas de estos usuarios con el uso de documentación falsa y robándose su identidad.

La estafa informática tiene diferentes dimensiones, intenciones y formas con efectos diversos en el comercio electrónico. Un tipo de estafa informática se da cuando esta variedad tienen la intención de defraudar al público, como estafas de trabajo desde casa, sorteos o concursos falsos u otros esquemas similares (Oxman, 2013). Links diversos compartidos por redes sociales, sitios web creados o web falsos de concursos y/o ventas, solicitando a los consumidores que se registren con una tarifa e información personal detallada, todo con el objetivo de engañarlos por dinero o información personal, como claves o contraseñas. Otra estafa informática es aquel del pago anticipado, cuando “los delincuentes convencen a las víctimas que paguen una tarifa por recibir algo de valor” (Ortiz, 2019). A los consumidores se les presentan documentos falsos, identidad y reclamos de algunos recursos valiosos que el consumidor puede desear desesperadamente.

El phishing es probablemente la variedad más común y extendida de fraude informát ico. Toma la forma de varios enlaces electrónicos, correos o sitios web falsos, cuyo objetivo

es inducir a los usuarios a revelar sus cuentas bancarias o contraseñas de estas cuentas, pueden utilizarse para debitarlas o realizar transacciones indebidas (Aboso, 2018).

3.1.3. Cibercrimen.

Este estudio cubre únicamente el término "cibercrimen", que refiere a una variedad de casos en los que se utiliza tecnología en la comisión de un delito, que a menudo tiene motivaciones financieras y abarca diferentes conceptos de distintos niveles de especificidad, por el público entre los medios de comunicación y el discurso profesiona l; apenas tiene un punto de referencia a documentos legales. Dado que en algunos casos la expresión incluso se usa indistintamente con "crimen informático", "crimen de alta tecnología" o "crimen digital", el discurso sobre una definición universalmente válida es llevada más lejos. En general, el ámbito de la cibercrimen contiene un gran conjunto de diferentes actividades delictivas en las computadoras y en los sistemas de informac ión que constituyen el objetivo o herramienta principal por donde se viabiliza el delito.

Para Mayer (2018), el cibercrimen tiene lugar en el ciberespacio, que viene a ser "lugar no físico" donde ocurren las comunicaciones electrónicas encontrándose en ella datos digitales. Se define el ciberespacio como "una inmensa red de redes que conecta a millones de usuarios en redes de información a miles de almacenes de datos electrónicos en todo el mundo".

Por lo tanto, el cibercrimen podría ser en primer lugar un delito común o "tradiciona l", que ahora se comete en el entorno de las TIC. Jara, Ferruzola y Rodríguez (2017). Se refieren a estos delitos como delitos informáticos, ya que el uso de las tecnologías de la información y en las comunicaciones no se inicia el delito, pero aumenta en gran medida la escala o el alcance permitiendo una nueva modalidad del acto criminal.

Estos son delitos que ya existen en el ámbito físico pero que ahora se llevan a cabo mediante sistemas informáticos. Dentro del alcance de esta categoría se incluyen los delitos informáticos como fraude y falsificación. A través del phishing, los delincue ntes intentan adquirir datos confidenciales de manera ilegal, como contraseñas o detalles de pago, disfrazándose como una entidad confiable en comunicaciones electrónicas.

Además, los delitos relacionados con el contenido suelen pertenecer a la misma categoría de delitos informáticos, aunque no están claramente clasificados como delitos tradicionales y abarcan la publicación de contenido ilegal en medios electrónicos, como la difusión de pornografía infantil, delitos de derechos de autor y los derechos de propiedad.

Los delitos cibernéticos también pueden ser delitos exclusivos del mundo de las TIC que se originan en la evolución digital. Según Sánchez (2012). Revista: *¨Ciberespacio y el crimen organizado¨*. Estas aplican tanto a la tipología de delitos dependientes de internet, ya que las TIC han permitido un nuevo campo de criminalidad. Estos delitos violan la confidencialidad, integridad o disponibilidad de las redes de sistemas informáticas y/o datos digitales dirigidos a sistemas informáticos. Los ejemplos más destacados de estos delitos son la piratería, spam o el bloqueo de servicios informáticos. Aunque estos delitos pueden estar dirigidos principalmente a dañar computadoras o redes, también podrían implicar resultados secundarios de delitos tradicionales como el fraude. Por lo tanto, la distinción es naturalmente borrosa y plantea desafíos a los sistemas de justicia penal que están sujetos al principio de derecho de que solo se puede perseguir un delito debidamente reconocido por la ley. Si bien una definición estrecha que solo se aplica a los delitos cibernéticos corre el riesgo de excluir los delitos dañinos, una definición amplia es criticada por ser vaga y, por lo tanto, sin sentido. Esta discusión muestra que si bien la amenaza del delito informático se conoce en general, alcance real del tema sigue siendo relativamente desconocido.

A pesar de los esfuerzos de muchos académicos por llegar a una definición concluye nte del fenómeno, Según Alonso y Esparza (2017). Revista: *¨Los retos procesales de la criminalidad informática desde una perspectiva española¨*. Creen que todavía existe una brecha en la comprensión de cómo se construye el término cibercrimen. El autor afirma que la ley carece de una definición clara, lo que lleva a que el público cree su propia percepción de lo que es el cibercrimen, creando posteriormente muchos mitos.

Por otro lado, Crespo (2020) sostiene que la amenaza del cibercrimen se está extendiendo y aumentando rápidamente. El autor afirma que el uso mayor de Internet a lo largo de la historia, creó circunstancias favorables en las cuales los delincuentes pasaron de delitos

callejeros a delitos informáticos porque es más seguro, no depende de la ubicación geográfica e incluso, internet ofrece más oportunidades como una red vulnerable.

Es fundamental establecer el uso real de Internet, los niveles de preocupación por el cibercrimen y las tasas reales de victimización en la población en general., Cabanellas y Palazzi (2004) proporcionaron algunos de los trabajos más contemporáneos que abordan las brechas más actuales en la teoría criminológica sobre el delito informático. Lara y Albán (2017) analizan el tema del ciberdelito desde varios ángulos, intentando demostrar que el cibercrimen debe ser visto como un tema interdisciplinario. Sus elementos como las leyes que lo rigen, las formas en que se regula el ciberespacio, la desviación social que lo contiene y la identidad en internet se revisa desde las perspectivas de la criminología, la sociología, la filosofía, la informática y otros campos de las ciencias sociales y jurídicas.

Esta investigación mostrará realmente lo complicado que puede ser el ciberdelito y por qué debe abordarse desde diferentes puntos de vista y diferentes ángulos filosóficos debido a su naturaleza en constante cambio. Una forma de ver el ciberdelito dentro del campo de la criminología es mediante la aplicación de las teorías tradicionales del cibercrimen, a las que muchos autores se han adherido.

Otra forma de entender el fenómeno del cibercrimen es examinando las regulaciones y leyes clave y sus cambios a lo largo del tiempo. Mayer (2018) sostiene que la ciberdelincuencia es un campo realmente poco explorado, con muchos desafíos y problemas que deben abordarse. Este autor refiere aspectos fundamentales e intrínsecos contenidos en el ciberespacio como son: la privacidad, el anonimato y derechos.
Proponiendo formas donde las leyes pueden estructurarse en base a todos estos princip ios que pueden aplicarse mejor a estos delitos, analizando formas que se manejan desde una perspectiva legal.

Jara, Ferruzola y Rodríguez (2017). Discuten este tema, intenta analizar cómo aborda la privacidad en el ciberespacio desde una perspectiva legal. Otro autor, Oxman, (2013) estudia el robo de datos para obtener la suplantación de identidad de víctimas en internet. Estos delitos se hicieron más frecuentes en el ciberespacio, abriendo nuevas oportunidades en estos delincuentes, aprovechando la demora de adaptación de la norma

penal. Analiza las fallas en la legislación en diferentes artículos legales, afirmando el amplio margen de interpretación y los diversos criterios judiciales de los jueces penales.

Finalmente, para Ospina, Milton, y Sanabria (2020), el ciudadano comienza a reconocer al delito de estafa informático como una amenaza real; sin embargo, cuando estos casos son llevados a los juzgados, son revisados como delitos comunes en lugar de Aplicar el delito informático. Si bien es cierto que afirman una mejoría en el tratamiento penal de los delitos de fraude informático, todavía hay numerosos desafíos que deben abordarse.

3.1.4. Ciberseguridad.

Con el crecimiento de la conectividad global, la vida social y política ha cambiado enormemente. Internet es utilizado como un instrumento eficaz de vigilancia y ataque a oponentes, también para cometer daño en cualquier forma posible. Si bien se afirma el grado de libertad que trajeron las redes de comunicación a los usuarios, también dio lugar a amenazas de seguridad que han sido utilizados contra el mismo ciudadano.

Sin embargo, el tema de las preocupaciones y las precauciones de seguridad siempre ha existido en un área de tensión con la defensa de la libertad. A menudo se percibe que las medidas de seguridad jurídica cuando se sancionan penalmente, éstas amenazan libertades y derechos garantizados por ley. Por lo tanto, cualquier acto legislativo del Estado adoptado en el contexto de la ciberdelincuencia debe ser examinado para verificar su compatibilidad con libertad y seguridad de los ciudadanos en el pleno cumplimie nto del Estado de Derecho y sus derechos fundamentales. Conseguir que los derechos individuales y preocupaciones por la seguridad sean coherentes es un desafío importante para los principios fundamentales democráticos.

Por tanto, se requieren amplias deliberaciones sobre ciberdelincuencia y el paradigma de seguridad en nuestro país. En los últimos años, las preocupaciones sobre la ciberdelincuencia se han convertido gradualmente en el centro de atención policia l, amenazando todos los servicios informáticos, afectando en última instancia a todos los ámbitos de la vida pública y en áreas fundamentales como políticas comerciales, seguridad y mercado interno. Por tanto, los derechos fundamentales como bienes superiores, están protegidos por un enfoque de seguridad común. Consecuentemente, la

ciberseguridad y el cibercrimen están ganando cada vez más atención en el discurso público. Sin embargo, prevalecen nociones divergentes de los conceptos, lo que plantea desafíos a la hora de abordar sistemáticamente este problema.

Debido al amplio alcance de la ciberseguridad, se utilizan varias definiciones dentro de la discusión académica internacional sobre el tema. Si bien algunos académicos se refieren a la ciberdefensa como componente que forma parte de una estrategia general de ciberseguridad, otros usan el término indistintamente, lo que ya indica desacuerdo al abordar el tema. Generalmente, la ciberseguridad se enfoca en la protección de computadoras, redes y datos contra el acceso, cambio o destrucción no intencional o no autorizada.

En el tiempo se ha encontrado una noción borrosa de ciberseguridad: "La cibersegur idad es la primera línea de defensa contra el cibercrimen". Esto se aclara aún más con Vega (2008) donde la ciberseguridad se define como "la seguridad en redes e informac ió n, aplicación de la ley y la defensa, que abarcan áreas políticas divergentes operando en el contexto de diferentes marcos legales".

Nuestra dependencia cada vez mayor del ciberespacio coloca a todos los Estados, empresas, organizaciones y usuarios individuales en riesgo de ataques informáticos. En efecto, significan preocupaciones sobre seguridad que afectan a todas las partes de la sociedad, no solo en la esfera económica y política, sino también a todos los ciudadanos en su ámbito privado. La importancia de la ciberseguridad gana más impulso en el ciudadano siendo víctimas de estos delitos informáticos, enfocados principalmente en estafas de tarjetas de crédito, robo de cuentas, transferencias interbancarias ilegales, etc.

3.2. Legislación.

¨LEY DE DELITOS INFORMÁTICOS
LEY N° 30096¨

FINALIDAD Y OBJETO DE LA LEY

¨**Artículo 1.** Objeto de la Ley¨

DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS

¨**Artículo 2.** Acceso ilícito¨

¨**Artículo 3.** Atentado a la integridad de datos informáticos¨

¨**Artículo 4.** Atentado a la integridad de sistemas informáticos¨

DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES

¨**Artículo 5.** Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos¨

DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES

¨**Artículo 6.** Tráfico ilegal de datos¨ (*)

(*) Artículo derogado por la Única Disposición Complementaria Derogatoria de la Ley N° 30171, publicada el 10 marzo 2014.

¨**Artículo 7.** Interceptación de datos informáticos¨

DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

¨**Artículo 8.** Fraude informático¨

DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA

¨**Artículo 9.** Suplantación de identidad¨

DISPOSICIONES COMUNES

¨**Artículo 10.** Abuso de mecanismos y dispositivos informáticos¨

¨**Artículo 11.** Agravantes¨

¨**Artículo 12.** Exención de responsabilidad penal¨

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. ¨Codificación de la pornografía infantil¨

SEGUNDA. ¨Agente encubierto en delitos informáticos¨

TERCERA. ¨Coordinación interinstitucional entre la Policía Nacional, el Ministerio Público y otros organismos especializados¨

CUARTA. ¨Cooperación operativa¨

QUINTA. ¨Capacitación¨

SEXTA. ¨Medidas de seguridad¨

SÉTIMA. ¨Buenas prácticas¨

OCTAVA. ¨Convenios multilaterales¨

NOVENA. ¨Terminología¨

DÉCIMA. ¨Regulación e imposición de multas por la Superintendencia de Banca, Seguros y AFP¨

UNDÉCIMA. ¨Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones¨

3.3. Jurisprudencia

3.3.1. EXP. N.° 01189-2019-PHC/TC LIMA MARCOS MORALES VARGAS, representado por WILLIAM BENARDINO GARCÍA ROSALES

En Lima, a los 10 días del mes de diciembre de 2020, el Pleno del Tribunal Constitucio nal, compuesta por los magistrados Ledesma Narváez, Ferrero Costa, Miranda Canales, Ramos Núñez, Sardón de Taboada y Espinosa-Saldaña Barrera, pronuncia la siguie nte sentencia. Se deja constancia de que el magistrado Blume Fortini votará en fecha posterior. ASUNTO Recurso de agravio constitucional interpuesto por don Willia m Benardino García Rosales, abogado de don Marcos Morales Vargas, contra la resolución con fojas 421, con fecha 5 de noviembre de 2018, cursada por la Segunda Sala Penal para Procesos con Reos Libre de la Corte Superior de Justicia de Lima, que declaró improcedente la demanda de habeas corpus de autos. ANTECEDENTES 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. Sostiene que mediante la sentencia de 16 de junio de 2017, se condenó al beneficiario a diez años de pena privativa de la libertad efectiva, que resultó de la sumatoria siguiente: ocho años por el delito de fraude informático y dos años de pena privativa de la libertad efectiva y falsificación de firma en documento privado. Posteriormente, mediante la Resolución de 26 de diciembre de 2017, se le redujo la pena a seis años de pena privativa de la libertad efectiva, por ambos delitos. Precisa que se condenó al beneficiario a través de una norma que no se encontraba vigente al momento que se cometieron los hechos delictuosos, pues tales hechos ocurrieron durante los meses de enero, febrero, marzo, julio, setiembre y octubre de 2013, pero fue condenado mediante la Ley 30096, que entró en vigencia el 23

de octubre de 2013, por lo que la norma aplicable era el artículo 185 del Código Penal, que en su forma agravada era el artículo 186, numeral 3 del referido código. La procuradora pública adjunta encargada de los asuntos judiciales del Poder Judicial (f. 61), solicita que la demanda sea declarada improcedente. Alega que el actor fue condenado mediante la Ley 30096, que sanciona el delito informático, la que estaba vigente desde el 23 de octubre de 2013; que se trata de un tipo penal prexistente al momento de lo comisión del evento delictivo; y que identificaba de forma clara la conducta objeto de investigac ión y su posterior juzgamiento. Los jueces demandados, señores Luis Antonio La Rosa Paredes, Gabino Alfredo Espinoza Ortiz y Andrés Avelino Cáceres Ortega a fojas 82, 136 y 138 de autos, expresan que el delito de fraude informático fue cometido por el beneficiario el año 2014, cuando ya se encontraba vigente la Ley 30096, por lo que solicita que la demanda sea desestimada.

Por estos fundamentos, el Tribunal Constitucional, con la autoridad que le confiere la Constitución Política del Perú, HA RESUELTO Declarar INFUNDADA la demanda.

3.3.2. Sentencia del Tribunal Constitucional del Peru, del 21 de enero de 2004. Expediente Nº 1219-2003-HD/TC, caso Nuevo Mundo Holdong S.A.

En Lima, a los 21 días del mes de enero de 2004, la Sala Primera del Tribuna l Constitucional, con la asistencia de los señores magistrados Aguirre Roca, Gonzales Ojeda y García Toma, pronuncia la siguiente sentencia. ASUNTO Recurso extraordinar io interpuesto por Nuevo Mundo Holding S.A. (NMH) contra la resolución de la Tercera Sala Civil de la Corte Superior de Justicia de Lima, de fojas 597, su fecha 23 de enero del 2003, que declaró infundada la acción de **hábeas data** de autos. ANTECEDENTES 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.

La demandada aduce que es falso que tenga la calidad de accionista del 99.9999% de las acciones representativas del capital social del Banco Nuevo Mundo (BNM), por lo que considera que la pretensión no tiene sustento, ni la actora legitimidad para interponer la, al carecer manifiestamente de la titularidad y/o legitimidad para formular las pretensiones reclamadas en el presente proceso. Añade que el BNM fue sometido a un régimen de intervención debido, única y exclusivamente, a la negligente administración del BNM, lo que incluso terminó con la apertura de un proceso penal ante el Trigésimo Séptimo Juzgado Penal de Lima contra el representante de NMH, señor Jaques Simón Levy Calvo, por la presunta comisión de delitos contra el orden financiero y monetario.

El Decimocuarto Juzgado Civil de Lima, con fecha 12 de agosto de 2002, declara fundado el hábeas data, por considerar que la demandada no ha cuestionado que no obren en su poder los documentos e informes solicitados en la carta de fojas 9, y porque la Ley General del Sistema Financiero y del Sistema de Seguros, ni ninguna otra ley, limita el ejercicio del derecho de pedir información sobre una empresa intervenida por dicho organismo.

La recurrida, revocando la apelada, declaró infundada la demanda, por considerar que existe un proceso penal contra el accionante por hechos que guardan relación con lo actuado en el proceso investigatorio efectuado por la SBS. Sostiene, asimismo, que la información requerida puede considerarse incluida en el secreto bancario, por lo que es preciso para su conocimiento el pedido previo del Juez, del Fiscal de la Nación o de una Comisión Investigadora del Congreso, como se establece en el párrafo final del inciso 5) del artículo 2° de la Constitución Política del Estado.

Con posterioridad a la vista de la causa, se solicitó que este Tribunal declarara la sustracción de la materia, lo que fue puesto en conocimiento del recurrente. FALLO Por los fundamentos expuestos, el Tribunal Constitucional, con la autoridad que la Constitución Política del Perú le confiere, Ha resuelto: 1. Declarar fundado el hábeas data. 2. Ordenar que la Superintendencia de Banca y Seguros proporcione a Nuevo Mundo Holding S.A. la documentación requerida, para lo cual, en ejecución de sentencia, el juez de primera instancia deberá obrar conforme a los fundamentos 15 y 16 de esta sentencia.

3.4. Tratado

3.4.1. El Convenio de Budapest o Convenio sobre o Convenio sobre Cibercrimen.

Naturalmente, el debate sobre la ciberseguridad no solo se lleva a cabo en el Perú sino también a nivel internacional dado su carácter transnacional. Aparte de innumerab les iniciativas de cooperación internacional o de acuerdos vinculantes, estos son raros debido a la naturaleza del derecho internacional. Un hito en el intento internacio nal de concebir el delito informático fue la adopción del Convenio sobre delitos informáticos del Consejo de Europa (Convenio de Budapest), de la cual el Perú está adherido desde el año 2019. Desde el año 2001, 64 países han ratificado este tratado internacional de justicia penal que se esfuerza principalmente por el establecimiento de política criminal destinada a la protección de la sociedad contra el delito informático, la ciberdelincuencia o cibercrime n, entre otras cosas mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional.

Con respecto a las disposiciones de derecho sustantivo, el Convenio de Budapest exige que los signatarios establezcan los delitos penales en la legislación nacional que se enumeran entre los artículos 2 al 13 dentro de cinco categorías: el Título 1 enumera los delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos que se aplica a la definición estricta de delito informático dirigido a las redes. Además, los títulos posteriores enumeran los delitos por medio de computadoras, centrándose en conductas que adquieren una nueva calidad cuando se cometen a través de estos dispositivos, delitos informáticos de falsificación y de fraude informático en el título 2, delitos relacionados con respecto al contenido en el título 3 y nuevamente en el título 4 por delitos relacionados con infracciones de derechos de autor y derechos conexos. Por lo tanto, la Convención adopta una definición amplia de delito informá t ico que clasifica no solo delitos cibernéticos sino también delitos tradicionales modificados en el ciberespacio como actos delictivos que deben perseguirse a nivel nacional. El derecho procesal también está regulado para permitir que las autoridades de justicia penal investiguen eficazmente delitos como el registro y la incautación de datos informát icos almacenados o la interceptación de comunicaciones. Además, se exige explícitamente la cooperación internacional.

Siendo el documento más sustancial sobre delitos informáticos a nivel internacional, el Convenio de Budapest sirve como base de referencia haciendo que muchos países lo utilicen como una "ley base o ley modelo" en la preparación de la legislación nacional. Incluso la Asamblea General de las Naciones Unidas recomendó "determinar si su país se ha desarrollado legislación para la investigación y el enjuiciamiento de la ciberdelincuencia, teniendo en cuenta los marcos existentes.

La ley sustantiva sobre delitos cibernéticos ha influido en la legislac ión nacional, con las normas emitidas a lo largo de nuestra normativa penal, sin embargo, es dudoso que la Convención realmente haya creado una eficacia a la hora de juzgar los delitos informáticos. La deficiencia del derecho internacional es visible en la falta de operadores de justicia competentes en esta rama nueva del derecho. La cooperación internacio nal apoya teóricamente pero difícil de lograr en la práctica debido a los esfuerzos nacionales divergentes en la ejecución de estas sugerencias. En ocasiones, incluso Gallardo (2020) declara que la Convención es solo de naturaleza simbólica sin ningún cambio real. Finalmente el Convenio de Budapest sirve como base al derecho penal peruano, ofreciendo un punto de partida desde una normativa mundial mucha más estricta de protección a la ciberseguridad.

4. CONCLUSIONES

A. En este mundo globalizado de vida diaria cada vez más digitalizada, los usuarios de las redes informatizadas, están preocupados por su seguridad personal y patrimonial, ya que hay una tendencia en crecimiento por el uso de las mismas (compras, pagos, comunicación, atención al usuario de los servicios básicos, etc.), en la que para todos estos servicios se utilizan nuestros datos. En la actualidad este es un gran problema, porque, en la medida que la tecnología avance, paralelamente también se desarrollaran los ciberdelincuentes en las diferentes modalidades.

B. Uno de los principales problemas para tener la definición adecuadamente del cibercrimen o ciberdelito es que no se tiene mayores datos estadísticos sobre estos delitos. Las empresas no dan mayor información ya que tienen el temor que los clientes o potenciales clientes se rehúsen a su uso, que en la actualidad ha crecido excesivamente, sobre todo como consecuencia de la pandemia por el COVID 19, se incrementó considerablemente el uso de las redes informatizadas.

C. Los ciberdelitos existentes, no están limitados en el derecho internacional, es por eso que provoca incertidumbre jurisdiccional. Los estados deben llegar a un consenso para buscar una cooperación global y así poder combatir los delitos informáticos que día a día los ciberdelincuentes van modificando su modus operandi.

D. La mayoría de delitos siguen existiendo, pero pasaron de ser delitos comunes a delitos informáticos porque para los ciberdelincuentes es más seguro, no registran ubicación, la red es vulnerable. La meta del estudio es buscar la seguridad en el ciberespacio, para que las personas puedan seguir usando Internet sin tener en cuenta la preocupación de toparse con ciberdelincuentes, y poder usar internet para todas las necesidades básicas, como la comunicación, compras, la banca, etc.

5. APORTE DE LA INVESTIGACIÓN

A. Como aporte científico, la investigación busca resolver la problemática legal de los delitos de estafa informática. Los ciudadanos están preocupados por su seguridad en el mundo virtual, mientras que su vida cotidiana se está digitaliza ndo de manera similar, teniendo en cuenta que casi todos los servicios públicos vitales se llevan a cabo mediante redes y datos informáticos conectados. Todas las áreas importantes de la vida pública dependen hasta cierto punto de las tecnologías de la información y la comunicación, lo que hace que la ciberseguridad sea uno de los temas más importantes en los próximos años.

B. El estudio del cibercrimen es de vital importancia en el uso actual de internet como servicio esencial teniendo su importancia frente al Covid-19, cuando ejemplarmente el sistema informático mundial está potencialmente expuesto a ciberdelincuentes, amenazando la seguridad patrimonial y social de los peruanos.

C. El aporte se justifica en la importancia de estar preparado académicamente de la mejor manera posible en los avatares de la delincuencia informática, conociendo los elementos de los delitos informáticos que día a día van modificando su modus operandi.

D. La meta del estudio es buscar la seguridad en el ciberespacio, para que las personas puedan seguir usando Internet sin tener en cuenta como la preocupación de toparse con ciberdelincuentes, y poder usar internet para todas las necesidades básicas, como la comunicación, compras y la banca.

6. RECOMENDACIONES

A. Se sugiere que, los profesionales del derecho (abogados, fiscales y jueces), así como los policías que investigan este tipo de delitos, revisión el marco legal existente para adaptarlo a las normas jurídicas (a través del congreso), los nuevos desafíos del derecho penal informático que permita mantener la confianza pública que proporcione seguridad y libertad digital, constituidos como objetivos fundamentales de la Constitución Política del Perú.

B. Mejorar la garantía de la seguridad jurídica ante el cibercrimen en delitos contra la fe pública, fraude y estafa, para los ciudadanos del mundo, ya que esta deficiencia perjudica gravemente el apoyo a nuevos procesos de integrac ión mundial al establecer una tipificación exacta de los delitos mencionados, en cada legislación de sus respectivos países que combata y reprima eficazmente la ciberdelincuencia.

C. Que, no solo debe existir responsabilidad y sanciones administrativas de las empresas que impulsan el uso de las redes informáticas (para sus ventas), así como el uso de tarjetas electrónicas como medios de pago, si no también sanciones dinerarias a favor del usuario perjudicado, porque son estas empresas las que deben adoptar todas las medidas necesarias para que no sean vulnerados sus clientes tan fácilmente.

D. Y, por último, emitir una regulación de protección para usuarios de servicios o comercio electrónico, y hacer cumplir que las personas jurídicas o naturales que brinden estos servicios cuenten con mecanismos de seguridad, en favor de sus usuarios.

7. REFERENCIAS

- Díaz, S., Angulo, J. & Barboza, M. (2018). Análisis del delito de fraude electrónico: modalidad tarjeta de crédito. Trabajo de investigación, X Semestre de la Facultad de Derecho de la Universidad Cooperativa de Colombia. Córdoba. Recuperado de: https://repository.ucc.edu.co/bitstream/20.500.12494/8381/1/2019_analisis_delito_fraude.pdf

- Devia, E. (2017). Delito informático: Estafa informática del artículo 248.2 del Código Penal. (Tesis para la obtención del Título de Doctor en Derecho). Repositorio institucional de la Universidad de Sevilla, recuperado de: https://idus.us.es/bitstream/handle/11441/75625/Tesis%20Edmundo%20Devia%20Completa%20Final%2031%20Mayo%202017.pdf?sequence=1&isAllowed=y

- Mayer, L., & Oliver, G. (2020). ¨El delito de fraude informático: concepto y delimitación¨. Revista chilena de derecho y tecnología, 9(1), 151-184, recuperado de: https://dx.doi.org/10.5354/0719-2584.2020.53447

- Quevedo, J. (2017). ¨Investigación y prueba del ciberdelito¨. Programa de Doctorado en Derecho y Ciencia Política de la Universidad de Barcelona, recuperado de: https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1&isAllowed=y

- Reyes, C. (2020). Los Delitos Informáticos y su influencia en la Integridad Personal, distrito de Chorrillos, Lima Metropolitana, 2019. (Tesis para optar el grado de bachiller en Derecho). Repositorio institucional de la Universidad Nacional Federico Villarreal, recuperado de: http://repositorio.ulasamericas.edu.pe/bitstream/handle/upa/937/T.%20INVESTIGACION-REYES%20VALDIVIA.pdf?sequence=1&isAllowed=y

- Montoya, F. (2018). ¨Regulación expresa del delito informático de clonación de tarjetas-Sede Divindat, 2017¨. (Tesis para obtener el título profesional de abogado). Repositorio institucional de la Universidad Cesar Vallejo, recuperado de: https://repositorio.ucv.edu.pe/handle/20.500.12692/39776

- Pardo, A. (2018). ¨Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018¨. (Tesis para optar el grado académico de Maestro en Derecho Penal y Procesal Penal). Repositorio institucional de la Universidad Cesar Vallejo, recuperado de: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_VA.pdf?sequence=1&isAllowed=y

- Gallardo, A. (2020). ¨ Innovaciones en la tipificación de delitos con la ratificación del convenio contra el cibercrimen, en el Perú el año 2019¨. (Tesis para optar el título profesional de abogado). Repositorio institucional de la Universidad Científica del Perú, recuperado de: http://repositorio.ucp.edu.pe/bitstream/handle/UCP/984/GALLARDO_DER_TESIS_TITULO_2020.pdf?sequence=1&isAllowed=y

- Oxman, N. (2013). ¨Estafas informáticas a través de Internet: acerca de la imputación penal del phishing y el pharming¨. Revista de Derecho Valparaiso, (XLI), 211-262, recuperado de: https://www.redalyc.org/articulo.oa?id=1736/173629692007

- Barrio, A. (2015). Ciberdelitos: Amenazas Criminales del ciberespacio. Madrid: Editorial Reus.

- CONAPOC (2020). Diagnóstico Situacional Multisectorial sobre la Ciberdelincuencia en el Perú. Edición digital. Lima: Minjus.

- Villavicencio, F. (2014). Delitos Informáticos, Cybercrimines. Revista Ius Et Veritas. Lima, recuperado de:

http://revistas.pucp.edu.pe/index.php/iusetveritas/article/download/13630/14253/

- Ministerio Público (2021). Informe de análisis N° 04, Ciberdelincuencia: Pautas para una investigación fiscal especializada. Lima.

- Sain, G. (2018). Cibercrimen y delitos informáticos: Los nuevos tipos penales en la era de internet. Buenos Aires: Errerius.

- Acurio Del Pino, S. (s/r). Delitos Informáticos. OAS, recuperado de: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

- Aboso, G. (2018). Derecho penal cibernético: la cibercriminalidad y el Derecho Penal en la moderna sociedad de la información y la tecnología de la comunicación. Buenos Aires: Euros editores.

- Galeano, S. (2021). ¨El número de usuarios de internet en el mundo crece un 7,3% y alcanza los 4.660 millones¨. Recuperado de: https://marketing4ecommerce.net/usuarios-de-internet-mundo/

- Cabanellas, G. & Palazzi, P. (2004). Delitos informáticos e internet, en Derecho de internet en Argentina. En Derecho de Internet. Buenos Aires: Heliasta.

- Heredia, S. (2015), Política criminal de los delitos informáticos. Revista del Foro, Colegio de Abogados de Lima.

- Crespo, L. (2020). La acción nuclear del delito informático en el novísimo código orgánico integral penal. Revista Tecnológica- Educativa Docentes 2.0, 9(1), 17-27, recuperado de: https://doi.org/10.37843/rted.v9i1.89

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

- Lara, E. & Albán, L. (2017). Los riesgos de las transacciones bancarias por Internet. Revista Publicando, 4 No 10. (1). 2017, 62-74.

- Cevallos, Y., Pupo, A., Calderon, M. & Ponce, D. (2020). La interpretación y la analogía de los delitos de estafa con documentos bancarios. Recimundo, 4(1), 4-12, recuperado de: https://doi.org/10.26820/recimundo/4.(1).esp.marzo.2020.4-12

- Ospina, M., & Sanabria, P. (2020). ¨Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia¨. Revista Criminalidad, 62(2), 199-217, recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199&lng=es&tlng=es

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

- Jara, L., Ferruzola, E. y Rodríguez, G. (2017). ¨Delitos a través redes sociales en el Ecuador: una aproximación a su estudio¨. I+D Tecnológico, 13(2), 111-122, recuperado de: https://revistas.utp.ac.pa/index.php/id-tecnologico/article/view/1721

- Sánchez, G. (2012). Ciberespacio y el crimen organizado. Los nuevos desafíos del siglo XXI. Revista Enfoques: Ciencia Política y Administración Pública, X (16), 71-87, recuperado de: https://www.redalyc.org/articulo.oa?id=960/96024266004

- Alonso L. & Esparza, I. (2017). Los retos procesales de la criminal idad informática desde una perspectiva española. Novum Jus, 11(1), 39-72, recuperado de: https://doi.org/10.14718/NovumJus.2017.11.1.2

- Vega, W. (2008). ¨Políticas y seguridad de la información. Fides et Ratio-Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia, 2(2), 63-69¨, recuperado de: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008&lng=es&tlng=es.