FACULTAD DE DERECHO

ESCUELA ACADÉMICO PROFESIONAL DE DERECHO

“La aplicación de la ley Nº. 30096 -Ley de delitos informáticos respecto a su regulación en el derecho penal peruano”

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogada

AUTORA:

Díaz Bohórquez, Cinthya Zari (ORCID: 0000-0002-1002-9128)

ASESORA:

Mg. Palomino Gonzales, Lutgarda (ORCID: 0000-0002-5948-341X)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal

LIMA – PERÚ

2019

Dedicatoria

El presente trabajo de investigación está dedicado a mi familia, a mis padres Carmen y Zacarías, y en especial a mi adorable hijo Nícolai, que con sus 07 meses de nacido ilumina mi vida.

Agradecimiento

A mi asesora Lutgarda Palomino G., por sus enseñanzas y dedicación para poder realizar y culminar el presente trabajo de investigación, y a la vida por ofrecer diariamente un nuevo comienzo para el logro de objetivos.

Página del Jurado

Declaratoria de Autenticidad

Yo, **Cinthya Zari Diaz Bohorquez** con DNI N° **45552884**, afecto con cumplir con las disposiciones vigentes consideradas en el reglamento de grados y títulos de la universidad Cesar Vallejo de Lima Este, facultad de derecho, escuela académica profesional de derecho, declaró bajo juramento que toda la documentación que acompaño es veraz u autentico.

Asimismo, declaro también bajo juramento que todos los datos e información que se presenta en la presente tesis son auténticos y veraces.

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

Lima 08 **de** Julio **del 2019**

Cinthya Zari Diaz Bohorquez

DNI. N°45552884

Presentación

Señores miembros del jurado:

Yo, Cinthya Zari Díaz Bohórquez, identificada con D.N.I N° 45552884, con código de estudiante Nº 6500044091, presento a ustedes mi tesis titulada *"La aplicación de la ley Nº. 30096 - Ley de delitos informáticos respecto a su regulación en el derecho penal peruano".* La presente tesis se encuentra desarrollada bajo los parámetros legales vigentes, ello en cumplimiento del Reglamento de grados y Títulos de la Universidad César Vallejo -Facultad de Derecho.

La Autora.

Índice

Resumen

La presente investigación tiene como objetivo general el determinar la eficacia de la ley Nº. 30096 - Ley de delitos informáticos respecto a su regulación en el derecho penal peruano. Para el cual se utilizó una serie de métodos de investigación, propias de la investigación cualitativa, de nivel descriptivo. Se utilizó como técnica la entrevista con su respectivo instrumento de recolección de datos, la guía de entrevista, con el cual se recopiló información de los expertos sobre el tema, llegándose a conclusiones precisas. En tal sentido, el tratamiento jurídico penal de los delitos informáticos es ineficaz, toda vez que no existe una fiscalía especializada que se avoque a aquel tipo penal por el cual genera inseguridad jurídica ya que existe una ineficiente investigación a nivel preliminar por lo que no se logra una sanción efectiva de los delitos informáticos contra los bienes jurídicos protegidos en la ley especial- Ley Nº. 30096.

***Palabras claves*:** Delito informático, investigación preliminar, bienes jurídicos.

Abstract

The present investigation has as general objective to determine the effectiveness of the law Nº. 30096 - Law on cybercrime regarding its regulation in Peruvian criminal law. For which a series of research methods, typical of qualitative research, of descriptive level was used. The interview with its respective data collection instrument, the interview guide, was used as a technique, with which information was collected from the experts on the subject, reaching precise conclusions. In this sense, the criminal legal treatment of cybercrime is ineffective, since there is no specialized prosecutor's office in that criminal type for which it generates insecurity in the investigation at the preliminary level so that an effective sanction of the crimes is not achieved IT against legal assets protected in the special law - Law Nº. 30096.

Keywords: Computer crime, preliminary investigation, legal goods

I. Introducción

Es importante iniciar mencionando que en cuanto al análisis que se le realiza a los delitos informáticos, se puede apreciar que son diversos los elementos que vigorizan la necesidad e importancia de implementar y considerar sistemas informáticos que brinden resultados rápidos y precisos a la hora de identificar este delito con todas sus características, además de permitir que las autoridades efectúen sanciones efectivas, empero es preciso mencionar que la informática es un área del conocimiento que se caracteriza por una alta especificación y complejidad técnica, viéndose refleja en el uso de una terminología y de diversos códigos distintos unos de otros, ya que prácticamente componen un idioma propio, poniendo de esta forma una dificultad engorrosa a los operadores de derecho a la hora de buscar la sanción correspondiente.

El delito informático o también llamado ciberdelito, es un tipo de problema que vienen enfrentado distintos países, siendo esta una acción antijurídica que realiza una determinada persona a través de la plataforma del internet, es decir de un espacio digital toda vez que, este tipo de delito se origina por el avance tecnológico de la época, por el crecimiento en el uso de esta ventana virtual, por lo que se ha generado que los delincuentes amplíen su campo de acción, amenazando la seguridad de las personas en las mismas, bajo ese mismo concepto, se refleja que países como en España donde ya se encuentra regulado este tipo de delitos, se poder advertir que no solo basta la implementación de la norma, sino que ellos han visto necesarios implementar mecanismos o medidas, para la correcta aplicación de la misma, llegando a controlar el avance de este delito, dado que el uso de estas medidas ayudan a que las acciones tomadas para identificar el delito faciliten la tipificación de las mismas, brindando de esta manera una efectiva tutela jurisdiccional el mismo que es un derecho constitucional que le asiste a la víctima.

En este mismo contexto es preciso mencionar que, en el país de México, entre los años 2013 al 2017 se produjo un incremento en este delito, motivo por la cual se implementó las herramientas y sistemas necesarios para el control de la misma, ya que por ejemplo uno de los principales problemas para tipificar este delito era la identificación del autor o autores del mismo, y encontrándose a que la mayoría de los hechos denunciados se realizaban en contra de los que resulten responsables, por ello, en consecuencia este tipo de casos era una traba al momento de castigar a los responsables por dicha acción ilícita.

De la misma manera, en el Perú este tipo de delito ha ido aumentando de manera desmedida la tecnología sistemática e informática, generando un problema grave en la actualidad, ya que, involucra la utilización y capacitación en el apoyo teórico – práctico en el campo tecnológico, toda vez que, para los operadores de justicia que actúan y luchan de forma incansable contra los delitos informáticos, los mismos tienen una tarea importante y difícil de solucionar, asumiendo esta importante misión la Policía Nacional del Perú, la Fiscalía y el Poder Judicial, estando estos comprometidos a afrontar la ya mencionada problemática.

Además, por lo anteriormente expuesto es importante precisar que la mayor limitación que se presenta para acabar con este delito es la falta de implementación de herramientas que ayude y facilite la sanción del mismo, dado que, muchas de las denuncias presentadas por este delito no han podido ser acusadas por el representante de Ministerio Público en su calidad de fiscal penal, ya que, no ha sido una tarea fácil identificar e individualizar al o a los sujetos autores del mismo, teniendo que archivarlos por el motivo indicado anteriormente, siendo esto el resultado de la falta de distintas herramientas que aquel tipo penal requiere.

En el Perú la ley de delitos informáticos, Ley N.° 30096, ha sido creada a fin de legislar y garantizar la lucha eficaz contra el ciberdelito, siendo preciso mencionar que, ocurrió una modificación de la ley antes mencionada a través de la ley 30171, modificando los artículos 2, 3, 4, 5, 7, 8 y 10. Este delito cibernético tiene como bien jurídico dañado: el patrimonio, la confidencialidad, integridad, disponibilidad de la información, toda vez, que las víctimas de este caso ven violado su información personal, generando vulneración a aquellos derechos protegidos especialmente por la legislación constitucional y penal, donde el autor del daño tiene la intención y voluntad propia de causar un perjuicio a su víctima, por lo que se configura como un delito doloso, así mismo, en la actualidad se ha implementado una división integrada por el personal policial especializado, siendo este la División de Investigación de Alta Tecnología de la PNP – siendo sus siglas DIVINDAT.

La justificación de esta investigación ha sido elegida debido al pleno desarrollo de las nuevas tecnologías de la información, dentro las cuales se encuentran los delitos

informáticos como nuevo concepto equiparable, se hace necesario y es menester de las ciencias jurídicas proteger al ser humano en su total dimensión en sociedad. Ello se puede plasmar en la realidad que, durante la década posterior a la incorporación de los delitos informáticos en el Código Penal el número de aquellos delitos se incrementó. Así, entre enero de 2000 y diciembre de 2010, se registraron 9075 denuncias por delitos informáticos en 27 distritos judiciales, pero sólo se formalizaron el 32.3% de aquellas. (Ministerio Público. "Persecución estratégica del delito", 2011, p. 8).

En el plano Internacional como antecedente se tiene a Arocena. (2012), en su artículo "La regulación de los delitos informáticos en el código penal argentino. Introducción a la ley nacional núm. 26.388", en la revista Boletín Mexicano de Derecho Comparado, mencionó que en este delito es importante el poder generar técnicas que faciliten la aplicación de las normas, en razón de que, para la solución de este tipo de problema no vasta la normativa sino generar una forma correcta, verídica y certera, que muestre la información que necesita el fiscal para poder formalizar su denuncia y de esta forma plantear su acusación.

Di lorio. (2017), manifestó en su libro de la Universidad fasta Ediciones, Mar del Plata, Argentina titulado "El rastro digital del delito, aspecto técnico, legales y estratégicos de la Informática Forense", que durante una investigación penal pueden presentarse escenarios donde la información se encuentre ubicada fuera de la República Argentina, planteándose en ese momento dificultades que representan desafíos para los investigadores. Existen convenios bilaterales y tratados de asistencia recíproca entre algunos países en lo que respecta a medidas de investigación y de prueba. La normatividad internacional que se avoca a esta dificultad es la Convención de Cibercriminalidad de la Unión Europea-Convenio de Budapest.

Espinoza. (2016), en el artículo científico "La tecnología de la información como herramienta construccionista para el autor financiero híbrido", publicado en la revista Fides Et Radtio, volumen 11, mencionó que es importante tener claramente cuáles son los hechos delictivos, teniendo en cuenta que estos hechos siempre son repetitivos, es ahí donde es sumamente necesario el empleo de instrumentos y sistemas para poder reconocer claramente dichos indicios y de esta forma tipificar de forma correcta el delito tecnológico y evitar que este se quede en esta epata o sea archivado por la autoridad.

Jiménez. (2018), en su tesis titulada “Desarrollo de una aplicación de uso didáctico para comunicación segura de datos a través de la red”, sustentada en la Escuela Politécnica Nacional de Quito; mencionó que, en los servicios de integridad la función que cumple el algoritmo “Un algoritmo Hash es una función que toma una cadena o mensaje de longitud variable y produce un valor hash de longitud fija, también llamado resumen de mensaje, que se emplea para verificar la integridad de los datos y mensaje, se representa como una cadena corta de letras aleatorias y números, es como una huella digital de mensajes, es un proceso unidireccional, pues no es posible crear el texto original utilizando cualquier función del hash inverso.

Justo. (2017), mencionó en su investigación el trabajo “Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal”, correspondiente al proyecto financiado por Ford Foundation, donde dicha investigación enfatiza la importancia y facultades en el ámbito procesal penal que deben de tener los investigadores en las diferentes modalidades del cibercrimen tales como procesos, servicios, actividades o manejo de información que se realizan en línea, considerándose que un mismo ilícito se puede realizar en diferentes jurisdicciones (países), por la propia naturaleza del internet.

Lasso. (2017), presentó una monografía para optar al título de Especialista en Seguridad Informática de la Universidad Nacional Abierta y a Distancia -UNAD en la Escuela de Ciencias Básicas e Ingeniería especialización en Seguridad Informática Villavicencio en el país de Colombia, titulada “Estado del peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia”, al respecto precisa que el estudio del fenómeno, denominado comúnmente delincuencia o criminalidad informática, y la motivación de contar con una capacidad de respuesta legal adecuada, ha permitido que se dé solución jurídica a muchos de los aspectos concernientes al cibercrimen tanto desde una perspectiva del Derecho Penal como en el Derecho Procesal Penal.

Manjarrés. (2012), en el artículo titulado “Caracterización de los delitos informáticos en Colombia”, publicado en la revista Pensamiento Americano, precisó que la incesante evolución de la criminalidad informática y la salida al mercado de nuevas tecnologías, se produce tanto a los métodos utilizados como la aplicación de la misma, generándose así posibles víctimas, considerando que dichas acciones pueden generar un perjuicio

importante para los mismos, toda vez que, se puede afectar el ámbito personal, tales como la intimidad, lo económico y hasta lo patrimonial, pudiendo además traer un perjuicio a su seguridad física.

Mayer. (2017), en el artículo "El bien jurídico protegido en los delitos informáticos", publicado en la revista chilena de derecho, volumen 44, numeral 1, indicó que los delitos informáticos comprenden dos tipos de teorías, distintas entre ellas, empero sumamente vinculadas siendo esta la norma descrita que limita esta conducta delictuosa y la otra es las herramientas y/o instrumentos que es la parte operativa que identifica el delito y ayuda a la aplicación de la primera; siempre preciso mencionar que una no podría llegar a sus objetivos sin la otra, toda vez que el trabajo en conjuntos de las ya mencionas son las que generan resultados favorecedores y adecuados para la sanción del autor que provocó dicho delito informático.

Mayer. (2018), en la revista Ius et Praxis, publicó el artículo "Elementos Criminológicos para el análisis jurídico –penal de los delitos informáticos", en el cual mencionó que, este delito constituye una materia que se viene presentando en tiempos recientes por el crecimiento de la tecnología, concentrando a la criminología en estos ámbitos también, es decir que a medida que evoluciona la tecnología también está evolucionando la delincuencia, razón por la cual las normas también tiene que abarcar esos ámbitos y de igual forma generar sistemas en los que se apoyen para poder controlar el incremento de dicho delito.

Ojeda, Arias, Rincón y Daza. (2010), en el artículo titulado "Delitos informáticos y entorno jurídico vigente en Colombia", publicado en la revista Cuad. Contab, volumen 11, número 28, indicó que, es necesario e importante poder conocer el contexto que presenta este delito, dado que está orientado a posibles acciones y respuestas que se enfocan a prevenir y dar el tratamiento debido, haciendo una revisión de las normas que han sido implementadas para controlar el mismo, contrastando la ley con los recursos que se tienen para la aplicación de la misma.

Ramírez. (2018), realizó un Informe final de proyecto aplicado para optar el título de Especialista en Seguridad Informática titulado "Análisis de la Evidencia Digital en Colombia como soporte judicial de Delitos Informáticos mediante cadena de custodia", correspondiente a la Universidad Nacional Abierta y a Distancia -UNAD en la Escuela de Ciencias Básicas e Ingeniería especialización en Seguridad Informática Villavicencio en el país de Colombia. El informe define la finalidad de la cadena de custodia indicando que en esencia es mantener y preservar la integridad física, así como lógica de una posible prueba o evidencia. Esta preservación debe realizarse desde el mismo instante de la recopilación o registro, su almacenamiento, transporte y análisis hasta finalizar con su entrega a la autoridad judicial.

Rico. (2012), en la revista IUS, artículo titulado "Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos", indicó que, este es un infracción que se encuentra dentro de los delitos informáticos, siendo que el pago electrónico, generado por el avance tecnológico a propiciado que personas inescrupulosas tengan conductas que dañen los derechos de la otra parte, siendo que en estos casos a través de esos sistemas se pueden rastrear qué daño es el ocasionado, cuánto es la gravedad que presenta, quién la cometió o la cometieron, para la toma de acciones inmediatas y que el daño no alcance la gravedad límite.

Como antecedente nacional, se tiene a Jiménez. (2017), quien presentó el libro de ediciones Jurista editores E.I.R.L., titulado "Manual de Derecho Penal Informático", al respecto hace referencia sobre, los lineamientos generales de la criminalidad informática y sugiere el modelo europeo como mejor alternativa a seguir para una actuación globalizada contra la ciberdelincuencia transnacional, por las nuevas formas de colaboración entre estados europeos, quienes con una visión integradora, parten del deseo común de llegar a conclusiones semejantes, sobre cuál debe ser el tratamiento adecuado de determinados fenómenos en aras de una mayor eficacia.

Nessi. (2017), presentó el proyecto de apoyo al sector Justicia American Bar Association Rule of lawInitiative aba roli Perú, Ministerio Publico y Policía Nacional del Perú, titulado "Manual de Evidencia Digital", al respecto precisa que, debe tenerse en cuenta que quienes participen en los diferentes actos, ya sean estos estrictamente de aseguramiento o análisis

de la evidencia o de conducción de la investigación penal, lo harán bajo las prescripciones del Nuevo Código Procesal Penal Decreto Legislativo N° 957 el mismo que prescribe en su artículo 67, que el aseguramiento de la escena del delito será llevado a cabo por funcionarios de la policía judicial que cuenten con un conocimiento técnico avanzado en cuanto al manejo de la evidencia digital, debiendo dar inmediata noticia de ello al Fiscal.

Reátegui. (2019), presentó el libro de la editora y distribuidora Ediciones Legales E.I.R.L., titulado "Nuevo Código Procesal Penal comentado Tomo I", donde en su Capítulo VI de la exhibición forzosa y la incautación, articulo 220 diligencia de secuestro o exhibición, numeral 5, menciona que, la Fiscalía de la Nación, a fin de garantizar la autenticidad de lo incautado, dicta el Reglamento correspondiente a fin de normar el diseño y control de la cadena de custodia, así como el procedimiento de seguridad y conservación de los bienes incautados, donde además se formuló el reglamento de la cadena de custodia de elementos materiales, evidencias y administración de bienes incautados.

Sequeiros. (2015), presentó una tesis para optar el título profesional de abogado en la universidad de Huánuco, facultad de derecho y ciencias políticas, titulada "Vacío legales que imposibilitan la sanción de los delitos informáticos en el nuevo código penal peruano", al respecto la tesis sustenta en relación al vacío legal o laguna jurídica en el derecho a la ausencia de reglamentación legislativa en una materia concreta, siendo esta una situación de vacío en la ley que ha sufrido omisión en su texto en cuanto a la regulación concreta de una determinada situación, que no encuentra respuesta legal específica; con ello se obliga a quienes aplican dicha ley (jueces y fiscales) emplear técnicas sustitutivas del vacío, con las cuales puedan obtener respuesta eficaz a tal ausencia.

El presente trabajo de investigación, cuenta con el siguiente marco teoría, precisando que si bien es cierto no son fuentes que hablen específicamente del tema a tratar, empero desarrollan información que ayuda al desarrollo de la misma.

El Delito informático, es la acción dolosa que presenta un individuo, provocando un perjuicio a personas o entidades, que usan una plataforma virtual o tecnológica, que dicho acto no necesariamente conlleve a un beneficio directo o indirecto del autor del delito, y aun cuando no lleve a un perjuicio de forma grave o leve a la víctima, empleando en este

delito acciones habituales, que solo generan molestias de la misma, sin embargo, esta última siente que se ha vulnerado o dañado algunos de sus derechos. (Loredo, 2017, p.15).

Al respecto se tiene que, un hecho constituye delito cuando es relevante jurídicamente, el cual implica que un hecho cualquiera para que sea delito debe estar regulado penalmente; entonces se podrá decir que el hecho encuadra en un tipo penal, es a ésta la que se le conoce como principio de legalidad, y el juez tiene la prohibición de sancionar otras conductas que no estén estrictamente tipificadas en la ley penal. (Lamperti, 2017, p. 85).

Los delitos informáticos o también llamados ciberdelitos son cualquier crimen donde la tecnología de la información y la comunicación es: 1) utilizado como una herramienta en la comisión de un delito; 2) el objetivo de un delito; 3) un dispositivo de almacenamiento en la comisión de un delito. (Levin y Ilkina, 2013, p. 14).

Así mismo, se entiende por criminalidad informática o ciberdelincuencia a aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso, conductas típicas que únicamente pueden ser cometidas a través de la tecnología. (Villavicencio, 2014, p. 86).

En cuanto a las modalidades que se utiliza para cometer estos hechos delictivos, comúnmente se realiza los siguientes: los ataques contra sistemas y datos informáticos, es un intento por perjudicar o dañar un sistema informático o de red. El problema que surge con la propagación de virus informáticos puede ser considerable teniendo en cuenta que puede dañar o eliminar datos de los equipos e incluso puede ocupar el programa de correo electrónico para difundirse a otros equipos, llegando a incluso borrar todo el contenido existente en el disco duro. (Hosthame, 2017, pp. 33-35).

Por lo anteriormente expuesto a modo de ejemplo se tiene que, los Botnets son redes de equipos infectados controlados por un atacante de forma remota donde generalmente, un hacker o un grupo de ellos crea un botnet usando un malware que infecta a una gran cantidad de máquinas. (kaspersky, 2013, p. 22).

De igual manera, al igual que existen una gran cantidad de delitos informáticos, también existen una amplia gama de delincuentes informáticos, en la informática se les conoce a los expertos en seguridad informática con el término de “hacker”, que hace referencia, como se señaló, a la persona que usa su habilidad para obtener acceso sin autorización a los archivos informáticos o redes, esta definición, de hecho, es asociada como una conducta delictiva. (López y Yedra, 2017, pp.35-36).

También se tiene que, los delitos informáticos son aquellos que dolosamente interceptan un medio de índole informática, con la finalidad de afectar, obstaculizar, viciar, divulgar, eliminar información de carácter público o particular halladas en ordenadores, sin embargo, actualmente existe una clasificación de los hackers, la primera es el hacker de sobrero blanco y el segundo es el hacker de sombrero negro. (Mamani, 2017, p.34).

Los Black Hat Hacker que son los hackers de sombrero negro, son individuos con amplios conocimientos informáticos que buscan romper la seguridad de un sistema buscando una ganancia, ya sea a fin de obtener bases de datos para su posterior venta en el mercado negro, venta de “xploits” (vulnerabilidades de seguridad), robo de identidad, cuentas bancarias, etc., además que, otro tipo de estas modalidades son aquellos que hacen uso del anonimato en internet con el fin de realizar los hechos delictivos como el cyberbullying, estafas, pornografía infantil, turismo sexual, etc. (López, López y Jerónimo, 2017, p. 17).

Encontrándose además los más comunes como son los phishing, donde normalmente se lleva a cabo por la suplantación de correo electrónico o de mensajería instantánea y que a menudo dirige a los usuarios a entrar en detalles en una página web falsa cuyo aspecto y el tacto son casi idéntica a la legítima donde se solicita información confidencial a través de internet de manera fraudulenta con el fin de obtener números de tarjetas de crédito, contraseñas u otros datos personales. (Aggarwal, Arora, Ghai y Poonam, 2014, p. 49).

Existen múltiples herramientas que permiten encontrar pistas, descubrir detalles, que sirven como medio de prueba para el descubrimiento de los objetivos a cubrir por un análisis informático, entre los más comunes tenemos a los capturadores de tráfico, que permiten la captura de los paquetes de datos que se transmiten y reciben por equipos informáticos en

una red local, están los sistemas de detección de intrusos (o IDS abreviatura de sus definiciones en inglés Intrusion Detection System) que son aplicativos que permiten detectar cualquier acceso no autorizado a un solo computador o a una red de computadores (Arnedo, 2014, p. 36).

La presente investigación tiene como problema general: Conocer si se logra sancionar los delitos cometidos a través del uso la tecnología, y formulo las siguientes preguntas como problema específico: (1) ¿Se debe regular la implementación de la ley de delitos informáticos Ley N° 30096 en los actos de investigación a nivel preliminar?, como problema específico: (2) ¿Cómo se trasgrede los bienes jurídicos protegidos a causa de los delitos informáticos?, como problema específico. (3) ¿Existe suficientes herramientas tecnológicas para combatir la ciber delincuencia?

Empleando como justificación teórica, la presente investigación no va a modificar aspecto alguno de una teoría existente, por el contrario, nos vamos a servir de teorías existentes para comprender su real dimensión con relación a las nuevas tecnologías de la información, teniéndose que, los delitos informáticos como nuevo hito histórico desafían a las ciencias jurídicas.

La justificación metodológica del presente trabajo se justifica metodológicamente en los instrumentos de la recolección de los datos en cuestionario de preguntas, que nos permitirá enfocarnos en mediar la variable, a fin de que el Estado y la Sociedad tomen conciencia respecto a lo hallado.

En la justificación práctica, con el producto de la investigación no se va a modificar la situación de la población a estudiarse, siempre y cuando, las conclusiones a las que arribamos no sean estudiadas o tomadas en cuenta, para proponer una disposición legislativa. Esta investigación parte de la necesidad de estudiar los delitos informáticos en su relación con las nuevas tecnologías.

Encontrando dentro de lo previamente antes expuesto, esta investigación asume relevancia social, educativa, cultural y sobre todo jurídica, porque en su producto final va a presentar una solución al problema que enfrenta el Estado en relación a la protección al derecho del usuario tecnológico en todas sus dimensiones, además de dar a conocer los delitos

informáticos más comunes y sus modalidades, que permitirá desarrollar una cultura de prevención y uso responsable de la tecnología en el mundo digital, a fin de evitar vulneraciones y/o afectaciones a estos derechos de relevancia constitucional y supraconstitucional.

Como contribución, la presente investigación concede aportes a la solución de un problema latente, como es la vulneración de bienes jurídicos protegidos a través de la ciberdelincuencia. Se trata de un problema que se suscita a diario en nuestras vidas, en un mundo donde la tecnología cada vez más abarca muchos aspectos de nuestro desarrollo como personas frente a la sociedad, donde se hace necesario que la sociedad reconozca sus derechos y es función del Estado cumplir con la debida protección que merecen los mismos.

Como Objetivo General se tiene: Determinar la importancia de la aplicación de la ley de delitos informáticos frente a los delitos informáticos; y como objetivo específico **(**1): Explicar la regulación de la ley de delitos informáticos-Ley Nº. 30096; Objetivo específico (2): Analizar si la aplicación de la ley de delitos informáticos logra sancionar efectivamente los delitos cometidos a través de la tecnología; Objetivo específico (3) Evaluar si el rol de los operadores de derecho es suficiente para lograr combatir y sancionar la ciberdelincuencia.

II. Método

2.1. Tipo y diseño de investigación

El presente trabajo de investigación tiene un enfoque cualitativo, esto es utilizar la recolección de información y el análisis de datos proporcionados en anteriores investigaciones, el uso de la revisión literaria se puede dar en cualquier fase del proceso. El investigado en este enfoque propone un problema, pero no sigue un proceso definido por lo cual sus planteamientos iniciales no son específicos a diferencia del enfoque cuantitativo. Así mismo, se tiene que al momento de analizar más datos, se necesita un mayor número de participantes, las cuales serán utilizadas de manera simultaneas en la presente investigación. (Hernández, 2014, p.8).

El método inductivo que se usa contiene información desde un punto individual a lo general, donde además contiene un proceso sistematizado que a partir de resultado de la información de particulares intenta encontrar particularidades que lo fundamenten a su favor, teniendo en cuenta los grados de fundamentación más cercanos. El cual inicia con la observación del problema en un rango nacional en comparaciones con otros países, a fin de que la conclusión final logre un aporte nuevo en la investigación. (Gómez, 2012, p.14).

La investigación desde el enfoque cualitativa en esta investigación es de tipo interpretativa, centrada en el entendimiento de las acciones de los seres vivos, las instituciones en la propia realidad, pretenden trascender al sujeto social para explicar y comprender hechos o fenómenos sociales más complejos todo ello dentro de la sociedad en que sitúa la investigación de estudio, encontrando sentido a los fenómenos en función de los significados que las personas les otorguen. (Hernández, 2014, p.9).

El diseño usado es la teoría fundamentada, donde el investigador da a conocer una explicación general respecto a un proceso, fenómeno, acción o interacción que se aplicara a un contexto explicado desde la vista de diversos participantes. Esta teoría nueva no debe afectar las normas ya establecidas del tema investigado, esta a su vez tendrá un rango medio a diferencia del rango formal. (Hernández, 2014, p. 472).

2.2. Escenario de estudio

Este presente trabajo de investigación tiene como escenario de estudio, a la División de Investigación de Alta Tecnología – DIVINDAT de Lima, así mismo, también la Primera Fiscalía Provincial Penal de Lima y por último y no menos importante y el Estudio Jurídico "G & C", dado que estos aportes que brindarán dichos participantes serán de suma importancia para la presente investigación.

2.3. Participantes

Los entrevistados serán especialistas en Derecho Penal, como el personal fiscal y asistente, abogado penalista litigante y personal policial, quienes brindarán información relevante desde su perspectiva con referencia al planteamiento de problema del presente trabajo de investigación respecto a los delitos informáticos.

Tabla 1:

Cuadro de características de los participantes:

Nombres Completos	Profesión	Lugar de trabajo	Cargo
Julio Tapia Choy	Abogado	Quinta Fiscalía Superior Penal de Lima.	Asistente en Función Fiscal.
Wilmer Bervel Cabanillas Gallardo	SO2° PNP	División de Investigación de Alta Tecnología.	Investigador de la DIVINDAT PNP.
Dewar Gonzalo Guevara Torres	Abogado	Estudio Jurídico "G&C."	Abogado Litigante Penalista.
Perla Aurora Giudiche Tamayo	Abogada	Primera Fiscalía Provincial Penal de Lima.	Fiscal Adjunta Provincial Provisional

2.4. Técnicas e instrumentos de recolección de datos

La técnica se entiende como los procedimientos, operaciones que realiza el investigador para tener el determinado resulto donde los instrumentos son materiales que permiten la ejecución de la técnica, esto puede ser de acuerdo al enfoque de la investigación como al cuestionario de preguntas. (Niño, 2011, p.93).

El cuestionario de preguntas es un instrumento donde la entrevista es más flexible e íntima que en el enfoque cuantitativo, se define como parte de una reunión en que puede conversar dos personas; entrevistador y entrevistado o entrevistados. Esto a su vez puede estar conformado por una familia o un equipo pequeño de personas, en que a través de la pregunta se logra una comunicación y las construcciones de un tema de investigación. (Hernández, 2014, p.403).

2.5. Procedimiento

El procedimiento de investigación usado en este trabajo será la categorización, este proceso se basará en componer y recomponer la información recolectada en las entrevistas u otro instrumento utilizado para saber los resultados de la investigación, la cantidad de la información se basará de acuerdo a las particiones hechas en las categorías y las sub categorías recogidas en el sistema analítico de la investigación. Esto así mismo, tendrá una carta de presentación a los determinados entrevistados que son parte necesaria en la investigación. (Cortez & Iglesias, 2004, p 45).

2.6. Método de análisis de información

El método que va ser usado en esta investigación es la triangulación, esto se usa cuando hay una mayor cantidad, riqueza y profundidad de datos, siendo la meta no solo corroborar los resultados de otros estudios, sino analizarlo bajo diferentes versiones. Siendo una de sus técnicas más usada en el método cuantitativo y cualitativo el de tener el acceso a la mirada de los problemas desde varios ángulos y posiciones, en la media que se confronta la información sobre un determinado tema y problema y con la producida con la información de diferentes fuentes hechas por los investigadores. (Hernández, 2014, p.418).

Tabla 2:
Cuadro de Categorías

Concepto	**Categoría**	**Sub categoría**
Ley creada para combatir la ciber delincuencia.	LEY Nº 30096	Alcances Limitaciones

		Modificación
Los delitos informáticos son los actos ilícitos que se cometen utilizando la tecnología para perpetrarlos.	DELITOS INFORMÁTICOS	Tipos Modalidades Uso de medios tecnológicos
Son los facultados por Ley en Dirigir y ejecutar los resultados de las diligencias preliminares que se van a realizar para la persecución de un delito.	ACTORES EN LA INVESTIGACIÓN PRELIMINAR	Ministerio Público Policía Nacional del Perú Poder judicial

2.7. Aspectos Éticos

El presente trabajo de investigación se dio de manera autentica y original; citando trabajos previos relacionados al tema: cumpliendo la normativa de la Universidad César Vallejo. Además, en la presente tesis se respetará la confidencialidad y el honor de las personas que participaran como objeto de estudio.

III. Resultados

Pregunta N° 1

¿Qué opina respecto al acelerado avance de las tecnologías informáticas y las modalidades de comisión de delitos con el uso del mismo?

J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
La tecnología permite mejorar el acceso a información variada pero los ciudadanos no mantienen una cultura digital de denuncia. En muchos casos no lo reportan ante las autoridades. Siendo las principales modalidades el fraude electrónico.	Hoy en día el uso de la tecnología es común en la sociedad y también es mal utilizado por los delincuentes que a través de ello cometen distintos actos ilícitos a través de la tecnología.	Lo que puedo ver en mí día a día como abogado litigante es que los delitos informáticos son comunes en el mundo delictivo por lo que la asesoría sobre el mismo es frecuente.	Hoy en día es frecuente el ingreso de los delitos informáticos es muy seguido aperturar investigación preliminarmente por estos tipos de delitos y sus distintas modalidades.

Coincidencia. Acorde a la pregunta anterior, todos los entrevistados manifestaron que la tecnología ha llegado para mejorar muchas cosas en la vida, las facilita y crea nuevas necesidades.

Discrepancia. El entrevistado 1, afirmó que a pesar que la tecnología mejora muchos aspectos en la vida, la falta de una cultura de denuncia de delitos informáticos hace que estos sigan aumentando, además el entrevistado 2 manifestó que la cara negativa de esto trae consecuencias al usuario que entra a internet.

Interpretación. Son múltiples los beneficios y las consecuencias que trae el avance de tecnologías informáticas, puesto que a la vez se incrementan delitos entre ellas, pero pese a ello la ley debe de ir de la mano con las nuevas modalidades de delitos informáticos, para que este avance sirva de mejora al país.

Pregunta N° 2

¿Considera usted que la legislación sobre delitos informáticos -Ley Nº 30096 en el derecho penal peruano es suficiente para sancionar las nuevas formas delictivas con el uso de las tecnologías informáticas? ¿Por qué?

J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
Aún falta mejorar muchos aspectos, porque existen casos en los cuales no se puede probar que tal persona cometió un delito informático.	No es suficiente debido a que la tecnología es utilizada para perpetrar los delitos informáticos por lo que se requiere mayores herramientas tecnológicas a fin de seguir dicho delito.	No, porque muchas veces no se logra una sanción efectiva mayormente los casos se pierden es decir caen, la parte agraviada no llegar a ser resarcida por el delito cometido.	Si, es suficiente porque se tiene también la regulación del código penal peruano en los artículos 207º - A,B, C y D, y con esta ley se complementan de manera eficaz.

Coincidencia. Acorde a la pregunta anterior, el entrevistado 1, 2 y 3 manifestaron que no es suficiente dicha ley, debido a la complejidad del delito informático y las herramientas que se deben utilizar para combatir el mismo.

Discrepancia. El entrevistado 4 afirmó que la ley de delitos informáticos es suficiente, puesto que ya se encuentra regulado en el Código Penal

Interpretación. El delito informático es un delito complejo que requiere de herramientas especiales para investigar y sancionar.

Pregunta N° 3

¿Considera usted que los actos de investigación realizados a nivel preliminar logran una efectiva sanción penal frente a los delitos informáticos? ¿Por qué?

J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
No, necesariamente toda vez que muchas veces las investigaciones preliminares resultan cortas de tiempo para recabar todos los elementos necesarios para arribar a la verdad.	Muchas veces no se logra debido a que no se logra el fin de las diligencias preliminares por lo que la mayoría de los casos no llegan a las instancias judiciales.	Muchas veces no tanto. Ya que la PNP y la fiscalía no logran sancionar estos delitos, los actos de investigación son deficientes y no logran los objetivos que es recabar los medios probatorios para que posteriormente se sancione.	Si, porque a través de ello se tiene suficientes elementos probatorios para posteriormente se sustente cargos ante el órgano jurisdiccional.

Coincidencia. Acorde a la pregunta anterior, el entrevistado 1, 2 y 3 afirmaron que a través de los actos de investigación no se logra una sanción efectiva puesto que no se llega a recabar los elementos probatorios.

Discrepancia. El entrevistado 4 manifiesta su diferencia con los demás puesto que refiere si se tiene suficientes elementos probatorios para sustentar cargos.

Interpretación. Los actos de investigación a nivel preliminar muchas veces no logran su objetivo la cual es conseguir una sanción penal frente a los delitos informáticos.

Pregunta N° 4

Explique ¿Cuáles son los actos de investigación que se utilizan para investigar un delito informático?

J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
Principalmente el ingreso a los sistemas informativos que navegan en el ciberespacio tales como el ingreso al IP de una computadora, en otros casos rastreo de celulares y intervención telefónica.	Entre los más comunes es el ingreso a los IP de los usuarios cibernéticos donde este tiene la similitud de una credencial de identificación por lo que a través de la geocalización se ubica a los mismos.	Desde el ámbito donde me desempeño proponemos que se realice diligencias tales como: se identifique y se individualice al autor o autores, se recabe videocámaras, capturas de pantallas de la computadoras o celulares y similares.	Frecuentemente se dispone la investigación por parte de la fiscalía al personal policial de la DIVINDAT PNP por ser el personal capacitado.

Coincidencia. Acorde a la pregunta anterior, el entrevistado 1, 2, 3 y 4, coincidieron en mencionar los distintos actos de investigación que se realizan en las diligencias de investigación.

Discrepancia. Los entrevistados 1,2,3 y 4 no discreparon en cuanta las diligencias a efectuarse en el delito informático.

Interpretación. Son distintas los actos de investigación que se realizan en investigación por el delito informático, donde se puede resaltar de lo antes mencionados, que se requiere de diversas diligencias para perseguir e investigar estos tipos de delitos.

Pregunta N° 5

¿Desde una perspectiva jurídica qué opinión le merece la vigente ley de delitos informáticos -Ley Nº 30096?

J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
Con esta Ley se busca sancionar y reducir los índices de comisión de delitos informáticos; sin embargo, deberán ser reajustada en mérito a la experiencia y a la cantidad de casos que se presentan.	La Ley Nº 30096 es buena, sin embargo, requiere que se ponga mayor énfasis en su aplicación y también en la capacitación tecnológica de los Operadores de Derecho.	La ley es buena gracias a este se ha reforzado lo tipificado en el Código Penal y las modalidades que se utilizan para cometer estos actos ilícitos porque son debidamente tipificados.	Que es eficaz debido a que se identifica de manera expresa las distintas modalidades para cometer actos ilícitos. Sin embargo, es importante que su aplicación sea eficiente y se logre el fin de toda ley.

Coincidencia. Acorde a la pregunta anterior, el entrevistado 3 y 4 afirmaron que dicha ley es buena y eficaz, que reforzado el código penal y expresa las diversas modalidades que se comenten con el uso de la tecnología. .

Discrepancia. El entrevistado 1 y 2 en cambio manifestaron que para la efectiva aplicación de la ley Nº 30096 se debe de capacitar a los Operadores de Derecho, debido a la cantidad de qué casos que se presentan día a día.

Interpretación. La ley es buena, sin embargo, debe darse mayor énfasis a su aplicación en cuanto a la capacitación de personal para que este sea efectiva.

Pregunta N° 6

¿De acuerdo a su experiencia laboral se logra identificar al autor (es) de la comisión del delito informático? ¿Por qué?			
J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
Si, ello en razón que en la máxima experiencia que logra desbaratar bandas criminales, así como a personas inescrupulosas que se dedican a esta ilícita labor ello de distintos partes del país.	Muchas veces no, porque es difícil conseguir el usuario tecnológico ya que estos tipos de delitos suelen cometerse en países y no necesariamente en el territorio peruano.	Muchas veces perdemos los casos para justamente a que no se logra la identificación del actor de estos actos ilícitos y siendo que el artículo 77º del Código de Procedimientos Penales menciona que este es un requisito de procedibilidad para primera acción penal entonces se archiva.	No, porque es difícil ubicar a la persona que está detrás de un Operativo Tecnológico, sin embargo, en conjunto PNP y fiscalía se trata de combatir ello.

Coincidencia. Acorde a la pregunta anterior, el entrevistado 2, 3 y 4 afirmaron que muchas veces no se tiene la identificaron del autor (es) de estos actos ilícitos, por lo que se tiene que archivar las denuncias.

Discrepancia. El entrevistado 1 manifiesta que debido a su experiencia se ha logrado individualizar a los autores de los delitos informáticos.

Interpretación. En la mayoría de casos no se logra individualizar al autor (es) de los actos delictivos cometidos a través de la tecnología, puesto a que estos se encuentran detrás de una pantalla de computadora o talvez fuera del territorio peruano.

Pregunta N° 7

¿Cuál cree usted que es el mayor límite para que se consiga una efectiva sanción penal en contra del autor(es) de los delitos informáticos? ¿Por qué?

J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
Ello se da cuando los Operadores de Justicia no han logrado identificar al autor o presuntos autores del presente ilícito lo que deviene en el archivo de la denuncia y como consecuencia que quede impune el hecho delictivo.	El mayor límite es la falta de capacitación de los Operadores de Derecho, ya que, en este tipo de delitos se usa muchos términos tecnológicos que talvez no se podría comprender.	Justamente que no se llega a identificar a los autores de estos actos ilícitos, por ello primigeniamente se interpone denuncia penal contra los que resulten responsables.	Tal vez el desconocimiento tecnológico del personal policial se otras dependencias y también del personal fiscal y judicial

Coincidencia. Acorde a la pregunta anterior, el entrevistado 1, 2, 3 y 4 afirmaron que el desconocimiento de los términos tecnológicos por parte de los Operadores de Derecho son el mayor límite para que no se logre una efectiva sanción penal frente a un delito informático.

Discrepancia. En este caso todos los entrevistados demostraron estar conforme a la pregunta formulada.

Interpretación. El desconocimiento de la tecnología y demás complejidades por parte de los Operadores de Derecho es el mayor límite para que no se logre una efectiva sanción penal frente a un delito informático.

Pregunta N° 8

¿Considera usted que debería de crearse una fiscalía especializada en delitos informáticos para lograr una efectiva aplicación de la ley de delitos informáticos -Ley Nº 30096 en el derecho penal peruano? ¿Por qué?

J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
Si para que tenga autonomía y dedicación exclusiva este tipo de delitos y a la vez el personal se encuentre más capacitado sobre los términos, herramientas y demás tecnología que se utilizada para perseguir este delito.	Definitivamente si así como existe la DINDAT donde el personal policial está capacitado para realizar investigaciones altamente tecnológicos también se debería hace una fiscalía especializada y capacitada de la misma manera.	Por supuesto que si es necesario por la alta complejidad de este tipo de delito.	Si, considero que la creación de ello, haría que se sancione de manera efectiva los delitos informáticos y sus distintas modalidades para perpetrarlos ya que estos ingresan con los demás delitos comunes.

Coincidencia. Acorde a la pregunta anterior, el entrevistado 1, 2, 3 y 4 afirmaron que debería crease una fiscalía especializa en delitos informáticos.

Discrepancia. En este caso todos los entrevistados demostraron estar conforme a la pregunta formulada

Interpretación. Es de importancia que se dé la creación de las fiscalías especializadas en delitos informáticos debido a su complejidad y la diferencia entre otros delitos comunes.

Pregunta N° 9

¿Cree usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?

J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
Como toda ley busca prevenir la comisión de delitos, sin embargo, siempre habrá personas que actuarán al margen de la Ley; además de que falta mayor educación preventiva en la sociedad frente a los delitos informáticos.	Sí, pero aún falta mayor promoción de dicha ley, ya que, el Estado debe promover la prevención frente a los mismos en la sociedad y sobre todo en las poblaciones vulnerables de donde se desconoce el uso y demás de la tecnología.	Si, sin embargo, falta mayor promoción de la ley para que la sociedad tendrá conocimiento de que derecho gozan y cuáles son los bienes jurídicos que la ley protege.	Si, ahora está en los ciudadanos a pie que, así como se capacitan en el uso de las redes sociales. También deberán hacerlo con los peligros que acarrea el uso de la tecnología.

Coincidencia. Acorde a la pregunta anterior, el entrevistado 1, 2, 3 y 4 coincidieron en afirmar que la ley de delitos informáticos contribuye a la prevención de los mismos, y que está en los ciudadanos capacitarse en conocer las distintas modalidades que comenten el autor(es) de este tipo de delitos.

Discrepancia. En este caso todos los entrevistados demostraron estar conforme a la pregunta formulada

Interpretación. Es de importancia que se dé la creación de las fiscalías especializadas en delitos informáticos debido a su complejidad y la diferencia entre otros delitos comunes.

IV. Discusión

Debido a la existencia de casos en los cuales no se puede probar que la persona cometió un delito, hay ciertas falencias tales como la investigación a realizarse a nivel preliminar, ello respecto a la individualización del autor o autores de los delitos informáticos y que por lo tanto a ser este tipo penal complejo requiere de una investigación a nivel fiscal de igual manera compleja, es así, como los expertos en la materia dieron a conocer las deficiencias y falta de precisiones en su aplicación normativa. De acuerdo con los resultados se reconoce que la Ley Nº 30096 es ineficaz e insuficiente para que de manera efectiva se sancione penalmente y se logre el resarcimiento del daño causado hacia el agraviado (a), donde se evidencia sus deficiencias, y por más que se plantearon diversas modificaciones a la ley, adecuándolo al documento internacional que se creó antes del Convenio de Budapest. Hubo la intención de adaptar la norma contra los delitos informáticos a los estándares que la comunidad europea exige para poder ser parte del Convenio. Una demostración del reconocimiento de las inconsistencias de la ley Nº 30096 es que a tan solo seis meses de su entrada en vigencia fue modificada a través de la Ley Nº 30171 en el año 2013.

Apoyándome en lo anteriormente expuesto Espinoza. (2016), en el artículo científico "La tecnología de la información como herramienta construccionista para el autor financiero híbrido", publicado en la revista Fides Et Radtio, volumen 11, mencionó que es importante tener claramente cuáles son los hechos delictivos, teniendo en cuenta que estos hechos siempre son repetitivos, es ahí donde es sumamente necesario el empleo de instrumentos y sistemas para poder reconocer claramente dichos indicios y de esta forma tipificar de forma correcta el delito y evitar que este se quede en esta epata o sea archivado por la autoridad.

Por su parte Justo, (2017). mencionó en su investigación el trabajo *"Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal"*, correspondiente al proyecto financiado por Ford Foundation. Dicha investigación enfatiza la importancia y facultades en el ámbito procesal penal que deben de tener los investigadores en las diferentes modalidades del Cibercrimen tales como procesos, servicios, actividades o manejo de información que se realizan en línea, considerándose que un mismo ilícito se puede realizar en diferentes jurisdicciones (países), por la naturaleza del internet.

De igual manera, Mayer. (2018), en la revista Ius et Praxis, publicó el artículo "Elementos Criminológicos para el análisis jurídico – penal de los delitos informáticos", en el cual mencionó que este delito constituye una materia que se viene presentando en tiempos recientes por el crecimiento de la tecnología, concentrando a la criminología en estos ámbitos también, es decir que a medida que evoluciona la tecnología también está evolucionando la delincuencia, razón por la cual las normas también tiene que abarcar esos ámbitos y de igual forma generar sistemas en los que se apoyen para poder controlar el incremento de dicho delito.

Ojeda, Arias, Rincón y Daza. (2010), en el artículo "Delitos informáticos y entorno jurídico vigente en Colombia", en la revista Cuad. Contab, volumen 11, número 28, indicó que es necesario e importante poder conocer el contexto que presenta este delito, dado que está orientado a posibles acciones y respuestas que se enfocan a prevenir y dar el tratamiento debido, haciendo una revisión de las normas que han sido implementadas para controlar el mismo, contrastando la ley con los recursos que se tienen para la aplicación de la misma, llegando a la conclusión que una no funciona sin la otra.

Por su parte Lasso. (2017), tipifica delitos informáticos presentes en la ley 30096, los cuales son: el fraude informático, la pornografía infantil, estafa informática, suplantación de identidad, acceso ilícito, atentado a la integridad de datos informáticos, tráfico ilegal de datos e interceptación de datos informáticos, debido a la necesidad de contar con un ordenamiento jurídico que sancione de forma adecuada y particular a la cibercriminalidad, no solo desde la identificación de los delitos cometidos y el establecimiento de penas sino también desde el procedimiento penal para dar solución a las investigaciones.

Se obtuvo que las herramientas actuales son mayormente digitales tales como software, los capturadores de tráfico; los sistemas de detección de intrusos, emuladores, herramientas de borrado de archivos, de recuperación de contraseñas, de datos o archivos y de análisis de discos montaje y recuperación, software de clonación entre otras.

Esto acorde con Jiménez. (2018), quien afirma que una aplicación de uso didáctico para comunicación segura de datos a través de la red verifica la integridad de los datos y mensajes.

La información obtenida del presente trabajo de investigación, da a conocer que los entrevistados en relación a la primera pregunta ¿Qué opina respecto al acelerado avance de las tecnologías informáticas y las modalidades de comisión de delitos con el uso del mismo?; los entrevistados C.G.W, D.G.T y P.A.G.T. coincidieron en manifestar que la tecnología ha llegado para mejorar muchas cosas en la vida, las facilita y crea nuevas necesidades, sin embargo, uno de mis entrevistados J.T.C, opinó que a pesar que la tecnología mejora muchos aspectos en la vida, la falta de una cultura de denuncia de delitos informáticos hace que estos sigan aumentando, además el entrevistado 2 manifestó que la cara negativa de esto trae consecuencias al usuario que entra a internet.

En relación a la segunda pregunta formulada ¿Considera usted que la legislación sobre delitos informáticos -Ley Nº 30096 en el derecho penal peruano es suficiente para sancionar las nuevas formas delictivas con el uso de las tecnologías informáticas? ¿Por qué?; los entrevistado J. T. C., C. G. W. y D. G. T manifestaron que no es suficiente dicha ley, debido a la complejidad del delito informático y las herramientas que se deben utilizar para combatir el mismo, no obstante, el entrevistado P.A.G.T. afirmó que la ley de delitos informáticos es sueficiente, puesto que ya se encuentra regulado en del Código Penal.

En relación a la tercera pregunta formulada ¿Considera usted que los actos de investigación realizados a nivel preliminar logran una efectiva sanción penal frente a los delitos informáticos? ¿Por qué?; los entrevistados J. T. C., C. G. W. y D. G. T afirmaron que a través de los actos de investigación no se logra una sanción efectiva puesto que no se llega a recabar los elementos probatorios, sin embargo, el entrevistado P.A.G.T. manifiesta su diferencia con los demás puesto que refiere si se tiene suficientes elementos probatorios para sustentar cargos.

En relación a la cuarta pregunta formulada Explique ¿Cuáles son los actos de investigación que se utilizan para investigar un delito informático? ¿Por qué?; los entrevistados J.T.C, C.G.W, D.G.T. y P.A.G.T. coincidieron en mencionar los distintos actos de investigación que se realizan en las diligencias de investigación. Los entrevistados J.T.C, C.G.W, D.G.T. y P.A.G.T. no discreparon y coincidieron en cuanto a las diligencias a efectuarse en el delito informático.

En relación a la quinta pregunta formulada ¿Considera Usted que la regulación en el derecho penal peruano de la ley de delitos informáticos -Ley N.º 30096 es suficiente para sancionar las distintas modalidades de delitos informáticos? ¿Por qué?; los entrevistados D.G.T y P.A.G.T. afirmaron que a través de los actos de investigación no se logra una sanción efectiva puesto que no se llega a recabar los elementos probatorios, sin embargo, los entrevistados J.T.C y C.G.W manifiesta su diferencia con los demás puesto que refiere si se tiene suficientes elementos probatorios para sustentar cargos.

En relación a la sexta pregunta formulada ¿De acuerdo a su experiencia laboral se logra identificar al autor (es) de la comisión del delito informático? ¿Por qué?; los entrevistados C.G.W, D.G.T y P.A.G.T. afirmaron que muchas veces no se tiene la identificaron del autor (es) de estos actos ilícitos, por lo que se tiene que archivar las denuncias, sin embargo, el entrevistado J.T.C manifiesta que debido a su experiencia se ha logrado individualizar a los autores de los delitos informáticos.

En relación a la séptima pregunta formulada ¿Considera Usted que debería crearse una fiscalía especializada en delitos informáticos para lograr una efectiva aplicación de la ley de delitos informáticos -Ley N.º 30096 en el derecho penal peruano? ¿Por qué?; los entrevistados J.T.C, C.G.W, D.G.T. y P.A.G.T. afirmaron que el desconocimiento de los términos tecnológicos por parte de los Operadores de Derecho son el mayor límite para que no se logre una efectiva sanción penal frente a un delito informático.

En relación a la octava pregunta formulada ¿Considera Usted que debería de crearse unas fiscalías especializadas en delitos informáticos para lograr una efectiva aplicación de la ley de delitos informáticos -Ley N.º 30096 en el derecho penal peruano? ¿Por qué?; los entrevistados J.T.C, C.G.W, D.G.T. y P.A.G.T. coincidieron en que, debido a la complejidad de los delitos informáticos, se debería crear una fiscalía especializa en delitos informáticos.

En relación a la novena pregunta formulada ¿Considera Usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?; los entrevistados J.T.C, C.G.W, D.G.T. y P.A.G.T. coincidieron que debería de crease una fiscalía especializa en delitos informáticos, debido a la alta complejidad de los mismos.

V. Conclusiones

La regulación de la ley de delitos informáticos- ley Nº 30096, describe las conductas ilícitas que afectan los sistemas y datas informáticos, secreto de comunicaciones, contra el patrimonio, la fe pública y la libertad sexual cometidos mediante la utilización de la tecnología.

La aplicación de la Ley Nº 30096 -ley de delitos informáticos no logra sancionar de manera efectiva aquellos ilícitos cometidos a través de la tecnología, ello por la falta de identificación e individualización del autor (es) del delito informático y la alta complejidad que contrae el mismo en las investigaciones preliminares.

El rol de los operadores de derecho no es suficiente para que se sancione efectivamente los también llamados ciberdelitos puesto que los mismos no se encuentran capacitados de manera sólida y constante para conocer y combatir este tipo penal ello debido a su alta complejidad tecnológica.

VI. Recomendaciones

Se debe continuar con la revisión de la ley N° 30096, para evitar vacíos y ambigüedades que pudieran conspirar con las sentencias fallidas que terminan dejando en libertad a los ciber delincuentes.

Se recomienda que los entes gubernamentales deben regular de forma adecuada los distintos tipos de delitos para establecer una política contra la criminalidad efectiva ya que la ley resulta insuficiente.

Es necesario que se utilicen de forma permanente herramientas que permitan el rápido y eficaz desarrollo del proceso que asegure una sanción de los delitos informáticos, se requiere entonces que se capacite y actualice a todos los actores involucrados en la prevención y penalización de los mismos.

Referencias

Alarcón, D. & Barrera, J. (2017). Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016. Universidad Privada Norbert Wiener. Recuperado el 20 de marzo de 2019, de http://repositorio.uwiener.edu.pe/bitstream/handle/123456789/1630/MAESTRO%20-%20%20Barrera%20Bar%C3%B3n%2C%20Javier%20Antonio.pdf?sequence=1&isAllowed=y

Arocena, G. (2012). La regulación de los delitos informáticos en el código penal argentino. Introducción a la ley nacional núm. 26.388. México: Boletín Mexicano de Derecho Comparado. Recuperado el 15 de marzo de 2019, de http://www.scielo.org.mx/scielo.php?pid=S004186332012000300002&script=sci

Bramont-Arias, T. (2007). El Delito Informático en el Código Penal Peruano. Lima: Fondo Editorial de la PUCP.

Council of Europe, (2001). Convenio de Cibercriminalidad de Budapest. Recuperado el 20 de marzo de 2019 de: http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.pdf

Di lorio, A. & Castallote, M. (2016). El rastro digital del delito. Aspectos técnicos, legales y estratégicos de la Informática Forense. Fasta: Mar de Plata. Recuperado el 20 de marzo de 2019, de https://bit.ly/2SqOKw8

Hancco, E. (2017). La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096. Recuperado el 20 de marzo de 2019, de http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/6436/DEhazaey.pdf?sequence=1&isAllowed=y

Hernández, S. (2018). Metodología de la investigación. Lima: MC Graw Hill Education.

Ilkina, D. (2013). Comparación internacional del crimen cibernético. Toronto: Ryerson University.

Jiménez, J. (2017). Manual de Derecho Penal Informático. Lima: Jurista Editores.

Jaramillo, J. A., Valarezo, G. y Astudillo, O. (2014). Rigurosidad versus flexibilidad en la investigación cualitativa. Revista Panorama Médico. Quito. 8 (1), 06-13.

Justo, M. (2017). Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal. Recuperado el 20 de marzo de 2019, de https://bit.ly/2RumV9F

Lamperti, S. B. (2017). Aspectos Legales. Los Delitos Informáticos. El rastro digital del delito: aspectos técnicos, legales y estratégicos de la Informática Forense. Mar de Plata: Universidad FASTA.

Lasso, V. (2017). Estado del peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia. Recuperado el 20 de marzo de 2019, de https://bit.ly/2RzcxgQ

López, L. & Jerónimo, G. (2017). Factores que contribuyen a la prevención de los delitos informáticos en el Estado de Tabasco. Revista Género & Direito, 6(3). 1-17.

Loredo, A. (2017). El bien jurídico protegido en los Delitos informáticos. Revista chilena de derecho. Versión On-line ISSN 0718-3437. Recuperado el 20 de marzo de 2019, de https://scielo.conicyt.cl/scielo.php?script=sci_abstract&pid=S071834372017000100011&lng=es&nrm=iso

Libertador, M. y Roussos, A. (2008). Lo cualitativo, un modelo para la comprensión de los métodos de investigación. Buenos Aires: Universidad de Belgrano.

Mayer, L. (2017). El bien jurídico protegido en los delitos informáticos. revista Chilena de Derecho. Volumen (44) numeral 1.

Mayer, I. (2018). Elementos Criminológicos para el análisis jurídico – penal de los delitos informáticos, ISBN: 978-956-9959-36-3. Editorial: Der Ediciones.

Montes de Oca, G.A. (2004). Derecho de Internet. Buenos Aires: Heliasta.

Morachimo, M. (2013). Reconstruyendo la Ley de Delitos Informáticos. Gaceta Constitucional. No. 71.

MP, (2017). Boletín Estadístico del Ministerio Público. Lima: Ministerio Público.

Mininter, (2016). Ministerio del Interior. Plataforma digital única del Estado Peruano. Recuperado el 20 de marzo de 2019, de https://www.gob.pe/mininter

Nessi, M. (2017). Manual de Evidencia Digital: Proyecto de apoyo al sector justicia. Recuperado el 20 de marzo de 2019, de https://img.legis.pe/wp-content/uploads/2018/03/Manual-de-evidencia-digital-Legis.pe_.pdf

Rico, M. (2013). Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos. Revista IUS, 7(31), 207-222.

Rincón, L. M., Taborda, D. A., y Roldan, L. (2017). Clonación de tarjetas de crédito. Medellín: Institución Tecnológico de Antioquia.

Rincón, R. J. (2015). El delito en la ciber sociedad y la justicia penal internacional. Madrid: Universidad Complutense.

Rueda, M. (2009). Cuestiones político – criminales sobre las conductas de hacking. En Derecho Penal Contemporáneo - Revista Internacional No. 28.

Sánchez, J. (2017). Adopción de estrategias de Ciberseguridad en la protección de la información en la Oficina de Economía del Ejército. Lima: Instituto Científico Tecnológico del Ejército.

Sequeiros, I. (2015). Vacíos legales que imposibilitan la sanción de los delitos informáticos en el Nuevo Código Penal Peruano. Recuperado el 20 de marzo de 2019, de http://repositorio.udh.edu.pe/bitstream/handle/123456789/286/ivett%20claritza%20sequeiros%20calderon.pdf?sequence=1&isAllowed=y

Temperine, M. (2014). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. (2ed.). Argentina: 14º Simposio Argentino de Informática y Derecho.

Anexos

Anexo N° 1: Tabla de Categorización

"La aplicación de la ley Nº. 30096 - Ley de delitos informáticos respecto a su regulación en el derecho penal peruano"

PROBLEMAS	OBJECTIVOS	CATEGORÍAS	SUB CATEGORIAS
Problema General: ¿Saber si se logra sancionar los delitos cometidos a través del uso la tecnología? **Problemas Específicos:** (1) ¿Se debe regular la implementación de la ley de delitos informáticos Ley N° 30096 en los actos de investigación a nivel preliminar?, como problema específico: (2) ¿Cómo se trasgrede los bienes jurídicos protegidos a causa de los delitos informáticos?, como problema específico. (3) ¿Existe suficientes herramientas tecnológicas para combatir la ciber delincuencia?	**Objetivo General** tiene: Determinar la importancia de la aplicación de la ley de delitos informáticos frente a los delitos informáticos. **Objetivo Específico (1):** Explicar la regulación de la ley de delitos informáticos- Ley Nº. 30096; **(2):** Analizar si la aplicación de la ley de delitos informáticos logra sancionar efectivamente los delitos cometidos a través de la tecnología; **(3):** Evaluar si el rol de los operadores de justicia es suficiente para lograr combatir y sancionar la ciberdelincuencia.	**LEY Nº 30096** **DELITOS INFORMÁTICOS** **ACTORES EN LA INVESTIGACIÓN PRELIMINAR**	Alcances Limitaciones Modificación Tipos Modalidades Uso de medios tecnológicos Ministerio Público Policía Nacional del Perú Poder judicial

Anexo N° 2: Artículo Científico

La aplicación de la ley Nº. 30096 - Ley de delitos informáticos respecto a su regulación en el derecho penal peruano

(The application of the law Nº. 30096 - Law on cybercrime regarding its regulation in Peruvian criminal law)

Cinthya Díaz

Universidad Cesar Vallejo

RESUMEN

La presente investigación tiene como objetivo general el determinar la eficacia de la ley Nº. 30096 - Ley de delitos informáticos respecto a su regulación en el derecho penal peruano. Para el cual se utilizó una serie de métodos de investigación, propias de la investigación cualitativa, de nivel descriptivo. Se utilizó como técnica la entrevista con su respectivo instrumento de recolección de datos, la guía de entrevista, con el cual se recopiló información de los expertos sobre el tema, llegándose a conclusiones precisas. En tal sentido, el tratamiento jurídico penal de los delitos informáticos es ineficaz, toda vez que no existe una fiscalía especializada que se avoque a aquel tipo penal por el cual genera inseguridad jurídica ya que existe una ineficiente investigación a nivel preliminar por lo que no se logra una sanción efectiva de los delitos informáticos contra los bienes jurídicos protegidos en la ley especial- Ley Nº. 30096

***Palabra clave*:** Delito informático, investigación preliminar, bienes jurídicos.

ABSTRACT

The present investigation has as general objective to determine the effectiveness of the law Nº. 30096 - Law on cybercrime regarding its regulation in Peruvian criminal law. For which a series of research methods, typical of qualitative research, of descriptive level was used. The interview with its respective data collection instrument, the interview guide, was used as a technique, with which information was collected from the experts on the subject, reaching precise conclusions. In this sense, the criminal legal treatment of cybercrime is ineffective, since there is no specialized prosecutor's

office in that criminal type for which it generates insecurity in the investigation at the preliminary level so that an effective sanction of the crimes is not achieved IT against legal assets protected in the special law - Law Nº. 30096

Keyword: Computer crime, preliminary investigation, legal assets.

1. Introducción

Respecto al análisis que se le realiza a los delitos informáticos, se puede apreciar que son diversos los elementos que vigorizan la necesidad e importancia de implementar y considerar sistemas informáticos que brinden resultados rápidos y precisos a la hora de identificar este delito con todas sus características, además de permitir que las autoridades efectúen sanciones efectivas, empero es preciso mencionar que la informática es un área del conocimiento que se caracteriza por una alta especificación y complejidad técnica, viéndose refleja en el uso de una terminología y de diversos códigos distintos unos de otros, ya que prácticamente componen un idioma propio, poniendo de esta forma una dificultad tremante a los operadores de derecho a la hora de buscar la sanción correspondiente.

El delito informático, o también llamado ciberdelito, es un tipo de problema que vienen enfrentado distintos países, siendo esta una acción antijurídica que realiza una determinada persona a través de la plataforma internet, es decir de un espacio digital, toda vez que este tipo de delito nace por el avance tecnológico de la época, por el crecimiento en el uso de esta ventana virtual, por lo que se ha generado que los delincuentes amplíen su campo de acción, amenazando la seguridad de las personas en las mismas, bajo ese mismo concepto, se refleja que países como España donde ya está regulado este tipo de delitos no solo basta la implementación de la norma, sino que ellos han visto necesarios implementar mecanismos o medidas, para la correcta aplicación de la misma, llegando a controlar el avance de este delito, dado que el uso de estas medidas ayudan a que las acciones tomadas para identificar el delito, faciliten la tipificación de las mismas, brindando de esta forma una efectiva tutela jurisdiccional, derecho constitucional que le asiste a la víctima.

En este mismo contexto, es preciso mencionar que, en México, entre los años 2013 al 2017 se vio un incremento en este delito, motivo por cual se implementó las herramientas y sistemas necesarios para el control de la misma, ya que por ejemplo uno de los principales problemas para tipificar este delito

era la identificación del autor o autores del mismo, resolviendo así la mayoría de estos problemas que se presentaban, siendo una traba al momento de castigar a los responsables por dicha acción.

Por otra parte, en el Perú este tipo de delito ha ido aumentando rápidamente a medida que aumenta la tecnología, generando un problema grave en la actualidad, ya que involucra la utilización de apoyo teórico – virtual, toda vez que para los operadores de justicia que actúan y luchan de forma incansable contra los delitos informáticos, los mismos tienen una tarea importante y difícil de solucionar, asumiendo esta importante misión la Policía Nacional del Perú, la Fiscalía y el Poder Judicial, estando estos comprometidos a afrontar la ya mencionada problemática.

En la misma línea, es importante aclarar que la mayor limitación que se presenta para acabar con este delito es la falta de implementación de herramientas que ayude y facilite la sanción del mismo, dado que muchas de las denuncias presentadas por este delito no han podido ser acusadas por el fiscal, ya que no ha sido una tarea fácil identificar e individualizar al o a los sujetos autores del mismo, teniendo que archivarlos por el motivo indicado anteriormente, siendo esto el resultado de la falta de distintas herramientas que aquel tipo penal requiere.

En el Perú la ley de delitos informáticos, N.º 30096, ha sido creada a fin de legislar y garantizar la lucha eficaz contra el ciberdelito. Siendo preciso mencionar que ocurrió una modificación de la ley antes mencionada por la ley 30171, modificando los artículos 2, 3, 4, 5, 7, 8 y 10. Este delito cibernético tiene como bien jurídico dañado: el patrimonio, la confidencialidad, integridad, disponibilidad de la información, entre otros, toda vez, que las víctimas de este caso ven violado su información personal, generando vulneración a los derechos antes ya mencionados, siendo preciso e importante que el autor del daño tenga la intención de causar un perjuicio a su víctima, por lo que es un delito doloso. Así mismo, en la actualidad se ha implementado una división integrada por el personal policial especializado, siendo este la División de Investigación de Alta Tecnología de la PNP (DIVINDAT) quienes a disposición y en trabajo conjunto con el Ministerio Público, están encargados de realizar los actos de investigación a nivel preliminar, basándose en la tecnología para la realización de los mismos, sin embargo se han encontrado con un limitante que afecta el combate que tienen con este tipo de delito, siendo esta traba la propia tecnología con la que cuenta el Perú para combatir dicho problema, consiguiendo que estas divisiones se encuentren sobre recargada de trabajo añadiendo a esto que las fiscalías no cuenten con un área especializada en tratar con crímenes

informáticos, lo que acarrea que al momento de realizarse la correspondiente sustentación de cargos ante el Órganos Jurisdiccional no se cuente con suficientes elementos de convicción que logren una sanción penal efectiva.

En el plano Internacional como antecedente se tiene a Arocena. (2012), en su artículo "La regulación de los delitos informáticos en el código penal argentino. Introducción a la ley nacional núm. 26.388", en la revista Boletín Mexicano de Derecho Comparado, mencionó que en este delito es importante el poder generar técnicas que faciliten la aplicación de las normas, en razón de que para la solución de este tipo de problema no vasta la normativa sino generar una forma correcta, verídica y certera, que muestre la información que necesita el fiscal para poder formalizar su denuncia y de esta forma plantear su acusación.

Di lorio. (2017), manifestó en su libro de la Universidad fasta Ediciones, Mar del Plata, Argentina titulado "El rastro digital del delito, aspecto técnico, legales y estratégicos de la Informática Forense", que durante una investigación penal pueden presentarse escenarios donde la información se encuentre ubicada fuera de la República Argentina, planteándose en ese momento dificultades que representan desafíos para los investigadores. Existen convenios bilaterales y tratados de asistencia recíproca entre algunos países en lo que respecta a medidas de investigación y de prueba. La normatividad internacional que se avoca a esta dificultad es la Convención de Cibercriminalidad de la Unión Europea- Convenio de Budapest.

Espinoza. (2016), en el artículo científico "La tecnología de la información como herramienta construccionista para el autor financiero híbrido", publicado en la revista Fides Et Radtio, volumen 11, mencionó que es importante tener claramente cuáles son los hechos delictivos, teniendo en cuenta que estos hechos siempre son repetitivos, es ahí donde es sumamente necesario el empleo de instrumentos y sistemas para poder reconocer claramente dichos indicios y de esta forma tipificar de forma correcta el delito y evitar que este se quede en esta etapa o sea archivado por la autoridad.

Hernández. (2009), "El delito informático", mencionó que una de las ramas del derecho creada por la evolución tecnológica, que se encarga exclusivamente de regular y estudiar estos tipos de delitos, teniendo un conocimiento amplio acerca de la digitalización y e nuevo mundo que esta generado el mismo, dándole control a dichas plataformas y evitando que se vulnere o viole derechos de los usuarios de la misma.

Jiménez. (2018), en su tesis titulada “Desarrollo de una aplicación de uso didáctico para comunicación segura de datos a través de la red”, sustentada en la Escuela Politécnica Nacional de Quito; mencionó que en los servicios de integridad la función que cumple el algoritmo “Un algoritmo Hash es una función que toma una cadena o mensaje de longitud variable y produce un valor hash de longitud fija, también llamado resumen de mensaje, que se emplea para verificar la integridad de los datos y mensaje, que se emplea para verificar la integridad de los datos y mensajes, se representa como una cadena corta de letras aleatorias y números, es como una huella digital de un mensajes, es un proceso unidireccional, pues no es posible crear el texto original utilizando cualquier función del hash inverso.

Justo, (2017). mencionó en su investigación el trabajo “Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal”, correspondiente al proyecto financiado por Ford Foundation. Dicha investigación enfatiza la importancia y facultades en el ámbito procesal penal que deben de tener los investigadores en las diferentes modalidades del Cibercrimen tales como procesos, servicios, actividades o manejo de información que se realizan en línea, considerándose que un mismo ilícito se puede realizar en diferentes jurisdicciones (países), por la naturaleza del internet.

Lamperti, (2017). señala que, existe consenso en reconocer una clasificación de los delitos informáticos que guarda sentido con la definición más útil, es así que se define a los delitos informáticos como conductas que a) ataca a las propias tecnologías de la computación y las comunicaciones; b) incluyen la utilización de tecnologías digitales en la comisión del delito; o c) incluyen la utilización incidental de las tecnologías en la comisión de otros delitos y, siendo que la computadora viene a ser una de las fuentes digitales probatorios.

Lasso, (2017). presentó una mono grafía para optar al título de Especialista en Seguridad Informática de la Universidad Nacional abierta y a distancia, UNAD Escuela de Ciencias Básicas Tecnología e Ingeniería Especialización en Seguridad Informática Palmira, titulada “Estado del peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia”, al respecto precisa que el estudio del fenómeno, denominado comúnmente delincuencia o criminalidad informática, y la motivación de contar con una capacidad de respuesta legal adecuada, ha permitido que se dé solución jurídica a muchos de los aspectos concernientes al cibercrimen tanto desde el Derecho Penal como desde el Derecho Procesal Penal.

Loredo. (2017), dijo que los delitos informáticos, es la acción dolosa que presenta un individuo, provocando un perjuicio a personas o entidades, que usan una plataforma virtual o tecnológica, que dicho acto no necesariamente conlleve a un beneficio directo o indirecto del autor del delito, y aun cuando no lleve a un perjuicio de forma grave o leve a la víctima, empleando es este delito acciones habituales, que solo generan molestias de la misma, es decir que esta última se sienta vulnerado o dañado algunos de sus derechos.

Manjarrés, (2012). "Caracterización de los delitos informáticos en Colombia", en la revista Pensamiento Americano, describió que la incesante evolución de la criminalidad informática y la salida al mercado de nuevas tecnologías, produciendo esta que tanto los métodos utilizados como la aplicación de la misma, generen posibles víctimas, considerando que dichas acciones pueden generar un perjuicio importante para la misma, toda vez que este delito puede dar los ámbitos personales que presenta la persona, tales como la intimidad, en lo económico y hasta en lo patrimonial, pudiendo además traer un perjuicio a su seguridad.

Mayer. (2017), en el artículo " El bien jurídico protegido en los delitos informáticos", en la revista Chilena de Derecho, volumen 44, numeral 1, indicó que los delitos informáticos comprenden dos tipos de teorías, distintas entre ellas, empero sumamente vinculadas siendo esta la norma descrita , siendo ella la forma escrita que limita esta conducta delictuosa y la otra es las herramientas y/o instrumentos que es la parte operativa que identifica el delito y ayuda a la aplicación de la primera; siempre preciso mencionar que una no podría llegar a sus objetivos sin la otra, toda vez que el trabajo en conjuntos de las ya mencionas generan resultados favorecedores y adecuados para la sanción del autor que provoco dicho delito.

Mayer. (2018), en la revista Ius et Praxis, publicó el artículo "Elementos Criminológicos para el análisis jurídico – penal de los delitos informáticos", en el cual mencionó que este delito constituye una materia que se viene presentando en tiempos recientes por el crecimiento de la tecnología, concentrando a la criminología en estos ámbitos también, es decir que a medida que evoluciona la tecnología también está evolucionando la delincuencia, razón por la cual las normas también tiene que abarcar esos ámbitos y de igual forma generar sistemas en los que se apoyen para poder controlar el incremento de dicho delito.

Ojeda, Arias, Rincón y Daza. (2010), en el artículo “Delitos informáticos y entorno jurídico vigente en Colombia”, en la revista Cuad. Contab, volumen 11, número 28, indicó que es necesario e importante poder conocer el contexto que presenta este delito, dado que está orientado a posibles acciones y respuestas que se enfocan a prevenir y dar el tratamiento debido, haciendo una revisión de las normas que han sido implementadas para controlar el mismo, contrastando la ley con los recursos que se tienen para la aplicación de la misma, llegando a la conclusión que una no funciona sin la otra.

Ramírez (2018) realizó un Informe final de proyecto aplicado para optar el título de Especialista en Seguridad Informática que trato del “Análisis de la Evidencia Digital en Colombia como soporte judicial de Delitos Informáticos mediante cadena de custodia”, correspondiente a la Universidad Nacional abierta y a distancia UNAD Escuela de Ciencias Básicas e Ingeniería especialización en Seguridad Informática Villavicencio, Colombia. El informe define la finalidad de la cadena de custodia indicando que en esencia es mantener y preservar la integridad física, así como lógica de una posible prueba o evidencia. Esta preservación debe realizarse desde el mismo instante de la recopilación o registro, su almacenamiento, transporte y análisis hasta finalizar con su entrega a la autoridad judicial.

Rico. (2012), en la revista IUS, artículo titulado “Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos”, indicó que este es un infracción que se encuentra dentro de los delitos informáticos, siendo que el pago electrónico, generado por el avance electrónico a propiciado que personas inescrupulosas tengan conductas que dañen los derechos de la otra parte, siendo que en estos casos a través de esos sistemas se pueden rastrear que daño es el ocasionado, cuanto es la gravedad que presenta, quien la cometió o quienes la cometieron, para la toma de acciones inmediata y que el daño no alcance la gravedad límite.

Como antecedente nacional, se tiene a Jiménez (2017), quien presentó el libro de ediciones Jurista editores E.I.R.L Perú titulado “Manual de Derecho Penal Informático”, al respecto hace referencia sobre los lineamientos generales de la criminalidad informática y sugiere el modelo europeo como mejor alternativa a seguir para una actuación globalizada contra la ciberdelincuencia transnacional, por las nuevas formas de colaboración entre estados europeos, quienes con una visión integradora, parten del deseo común de llegar a conclusiones semejantes, sobre cuál debe ser el tratamiento adecuado de determinados fenómenos en aras de una mayor eficacia.

Nessi. (2017), presentó el proyecto de apoyo al sector Justicia American Bar Association Rule of lawInitiative aba roli Perú, Ministerio Publico y Policía Nacional del Perú, titulada "Manual de Evidencia Digital", al respecto precisa que debe tenerse en cuenta que quienes participen en los diferentes actos, ya sean estos, estrictamente de aseguramiento o análisis de la evidencia o de conducción de la investigación penal, lo harán bajo las prescripciones del Nuevo Código Procesal Penal Decreto Legislativo N° 957 el mismo que prescribe en su artículo 67, el aseguramiento de la escena del delito será llevado a cabo por funcionarios de la Policía Judicial que cuenten con un conocimiento técnico avanzado en cuanto al manejo de la evidencia digital, debiendo dar inmediata noticia de ello al Fiscal.

Reátegui (2019), presentó el libro de la editora y distribuidora Ediciones Legales E.I.R.L Perú titulado "Nuevo Código Procesal Penal comentado Tomo I", en su Capítulo VI de la Exhibición forzosa y la Incautación, Articulo 220 Diligencia de secuestro o exhibición, numeral 5 que la Fiscalía de la Nación, a fin de garantizar la autenticidad de lo incautado, dictara el Reglamento correspondiente a fin de normar el diseño y control de la cadena de custodia, así como el procedimiento de seguridad y conservación de los bienes incautados. Se formuló el Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados.

Sequeiros (2015), presentó una tesis para optar el título profesional de abogado en la Universidad de Huánuco, facultad de derecho y Ciencias Políticas, titulada "Vacío legales que imposibilitan la sanción de los delitos informáticos en el nuevo Código Penal Peruano", al respecto la tesis sustenta en relación al vacío legal o laguna jurídica en el Derecho a la ausencia de reglamentación legislativa en una materia concreta. Es una situación de vacío en la ley que ha sufrido omisión en su texto la regulación concreta de una determinada situación, que no encuentra respuesta legal específica; con ello se obliga a quienes aplican dicha ley (jueces, abogados, fiscales, y otros) al empleo de técnicas sustitutivas del vacío, con las cuales puedan obtener respuesta eficaz a tal ausencia.

El presente trabajo de investigación, cuenta con el siguiente marco teoría, precisando que si bien es cierto no son fuentes que hablen específicamente del tema a tratar, empero desarrollan información que ayuda al desarrollo de la misma.

El Delito informático, es la acción dolosa que presenta un individuo, provocando un perjuicio a personas o entidades, que usan una plataforma virtual o tecnológica, que dicho acto no

necesariamente conlleve a un beneficio directo o indirecto del autor del delito, y aun cuando no lleve a un perjuicio de forma grave o leve a la víctima, empleando es este delito acciones habituales, que solo generan molestias de la misma, es decir que esta última se sienta vulnerado o dañado algunos de sus derechos (Loredo, 2017, p.15).

Al respecto se tiene que, un hecho constituye delito cuando es relevante jurídicamente, el cual implica que un hecho cualquiera para que sea delito debe estar regulado penalmente; entonces se podrá decir que el hecho encuadra en un tipo penal, es a ésta la que se le conoce como principio de legalidad, y el juez tiene la prohibición de sancionar otras conductas que no estén estrictamente tipificadas en la ley penal. (Lamperti, 2017, p. 85).

El ciberdelito (o delitos informáticos) es cualquier crimen donde la tecnología de la información y la comunicación es: 1) utilizado como una herramienta en la comisión de un delito; 2) el objetivo de un delito; 3) un dispositivo de almacenamiento en la comisión de un delito. (Ilkina, 2013, p. 14).

Así mismo, se entiende por criminalidad informática o ciberdelincuencia a aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas a través de la tecnología. (Villavicencio, 2014, p. 286).

En cuanto a las modalidades que se utiliza para cometer estos hechos delictivos, comúnmente se realiza los siguientes: los ataques contra sistemas y datos informáticos, es un intento por perjudicar o dañar un sistema informático o de red. El problema que surge con la propagación de virus informáticos puede ser considerable teniendo en cuenta que puede dañar o eliminar datos de los equipos e incluso puede ocupar el programa de correo electrónico para difundirse a otros equipos, llegando a –incluso- borrar todo el contenido existente en el disco duro. (Hosthame, 2017, pp. 33-35).

Los Botnets (redes de equipos infectados controlados por usuarios remotos) es cualquier grupo de PC infectados y controlados por un atacante de forma remota. Generalmente, un hacker o un grupo de ellos crea un botnet usando un malware que infecta a una gran cantidad de máquinas. (kaspersky,2013, p. 22)

Así mismo, al igual que existen una gran cantidad de delitos informáticos, también existen una amplia gama de delincuentes informáticos, en la informática se les conoce a los expertos en seguridad informática con el término de "hacker", que hace referencia, como se señaló, a la persona que usa su habilidad para obtener acceso sin autorización a los archivos informáticos o redes, esta definición, de hecho, es asociada a la conducta delictiva. (López y Yedra, 2017, pp.35-36).

Los delitos informáticos son aquellos que dolosamente interceptan un medio de índole informática, con la finalidad de afectar, obstaculizar, viciar, divulgar, eliminar información de carácter público o particular halladas en ordenadores, Sin embargo, actualmente existe una clasificación de los hackers, la primera es el hacker de sobrero blanco y el segundo es el hacker de sombrero negro. (Mamani, 2017, p.34)

Los Black Hat Hacker (Hackers de sombrero negro), son individuos con amplios conocimientos informáticos que buscan romper la seguridad de un sistema buscando una ganancia, ya se obtener bases de datos para su posterior venta en el mercado negro, venta de "xploits" (vulnerabilidades de seguridad), robo de identidad, cuentas bancarias, etc. otro tipo de delincuentes que son aquellos que hacen uso del anonimato en internet con el fin de realizar conductas poco éticas: acoso cyberbullying, estafas, pornografía infantil, turismo sexual, etc. (López, López y Jerónimo, 2017, p. 17).

Encontrándose además los más comunes como son los phishing normalmente se lleva a cabo por la suplantación de correo electrónico o de mensajería instantánea y que a menudo dirige a los usuarios a entrar en detalles en una página web falsa cuyo aspecto y el tacto son casi idéntica a la legítima, se solicita información confidencial a través de Internet de manera fraudulenta con el fin de obtener fraudulentamente números de tarjetas de crédito, contraseñas u otros datos personales. (Aggarwal, Arora, Ghai y Poonam, 2014, p. 49).

Existen múltiples herramientas que permiten encontrar pistas, descubrir detalles, que sirven como medio de prueba para el descubrimiento de los objetivos a cubrir por un análisis informático, entre los más comunes tenemos a los capturadores de tráfico, que permiten la captura de los paquetes de datos que se transmiten y reciben por equipos informáticos en una red local; están los sistemas de detección de intrusos (o IDS abreviatura de sus definiciones en inglés Intrusion Detection System)

que son aplicativos que permiten detectar cualquier acceso no autorizado a un solo computador o a una red de computadores. (Arnedo, 2014, p. 36).

La justificación de esta investigación ha sido elegida debido al pleno desarrollo de las nuevas tecnologías de la información, dentro las cuales se encuentran los delitos informáticos como nuevo concepto equiparable, se hace necesario y es menester de las ciencias jurídicas proteger al ser humano en su total dimensión en sociedad. Ello se puede plasmar en la realidad que, durante la década posterior a la incorporación de los delitos informáticos al Código Penal -CP el número de delitos se incrementó. Así, entre enero de 2000 y diciembre de 2010, se registraron 9075 denuncias por delitos informáticos en 27 distritos judiciales, pero sólo se formalizaron el 32.3% de aquellas. (Ministerio Público. "Persecución estratégica del delito", 2011, p. 8)., por lo que, resulta de importancia descubrir cuales son los factores en contra para que ocurra lo anteriormente expuesto.

La presente investigación concede aportes a la solución de un problema latente, como es la vulneración de bienes jurídicos protegidos a través de la ciberdelincuencia. Se trata de un problema que se suscita a diario en nuestras vidas, en un mundo donde la tecnología cada vez más abarca muchos aspectos de nuestro desarrollo como personas frente a la sociedad, donde se hace necesario como personas conocer nuestros derechos y es función del Estado cumplir con la debida protección que merecen los mismos.

Así mismo, se justifica metodológicamente en los instrumentos de la recolección de los datos (cuestionario de preguntas), que nos permitirá enforcarnos en mediar la variable, a fin de que el Estado y la Sociedad tome conciencia respecto a lo hallado.

2. Resultados

Pregunta N° 1

¿Qué opina respecto al acelerado avance de las tecnologías informáticas y las modalidades de comisión de delitos con el uso del mismo?			
J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
La tecnología	Hoy en día el	Lo que puedo ver en	Claro hoy en día es

permite mejorar el acceso a información variada pero los ciudadanos no mantienen una cultura digital de denuncia. En muchos casos no lo reportan ante las autoridades. Siendo las principales modalidades de la comisión de delitos el fraude electrónico y la pornografía infantil.	uso de la tecnología es común en la sociedad y también es mal utilizado por los delincuentes que a través de ello cometen distintos actos ilícitos a través de la tecnología.	mi día a día como abogado litigante es que los delitos informáticos son comunes en el mundo delictivo por lo que la asesoría sobre el mismo es frecuente.	frecuente el ingreso de los delitos informáticos es muy seguido aperturar investigación preliminarmente por estos tipos de delitos y sus distintas modalidades.

Coincidencia. Acorde a la pregunta anterior, todos los entrevistados manifestaron que la tecnología ha llegado para mejorar muchas cosas en la vida, las facilita y crea nuevas necesidades.

Discrepancia. El entrevistado 1, afirmó que a pesar que la tecnología mejora muchos aspectos en la vida, la falta de una cultura de denuncia de delitos informáticos hace que estos sigan aumentando, además el entrevistado 2 manifestó que la cara negativa de esto trae consecuencias al usuario que entra a internet.

Interpretación. Son múltiples los beneficios y las consecuencias que trae el avance de tecnologías informáticas, puesto que a la vez se incrementan delitos entre ellas, pero

pese a ello la ley debe de ir de la mano con las nuevas modalidades de delitos informáticos, para que este avance sirva de mejora al país.

Pregunta N° 2

¿Considera usted que la legislación sobre delitos informáticos -Ley Nº 30096 en el derecho penal peruano es suficiente para sancionar las nuevas formas delictivas con el uso de las tecnologías informáticas? ¿Por qué?

J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
Aún falta mejorar muchos aspectos, porque existen casos en los cuales no se puede probar que tal persona cometió un delito informático.	No es suficiente debido a que la tecnología es utilizada para perpetrar los delitos informáticos por lo que se requiere mayores herramientas tecnológicas a fin de seguir dicho delito.	No, porque muchas veces no se logra una sanción efectiva mayormente los casos se pierden es decir caen, la parte agraviada no llegar a ser resarcida por el delito cometido.	Si, es suficiente porque se tiene también la regulación el código penal peruano en los artículos 207º - A,B, C y D, y con esta ley se complementan de manera efectiva.

Coincidencia. Acorde a la pregunta anterior, el entrevistado 1, 2 y 3 manifestaron que no es suficiente dicha ley, debido a la complejidad del delito informático y las herramientas que se deben utilizar para combatir el mismo.

Discrepancia. El entrevistado 4 afirmó que la ley de delitos informáticos es suficiente, puesto que ya se encuentra regulado en el Código Penal

Interpretación. El delito informático es un delito complejo que requiere de herramientas especiales para investigar y sancionar.

Pregunta N° 3

¿Considera usted que los actos de investigación realizados a nivel preliminar logran una efectiva sanción penal frente a los delitos informáticos ¿Por qué?

J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
No, necesariamente toda vez que muchas veces las investigaciones preliminares resultan cortas de tiempo para recabar todos los elementos necesarios para arribar a la verdad.	Muchas veces no se logra debido a que no se logra el fin de las diligencias preliminares por lo que la mayoría de los casos no llegan a las instancias judiciales.	Muchas veces no tanto. Ya que la PNP y la fiscalía no logran sancionar estos delitos, los actos de investigación son deficientes y no logran los objetivos que es recabar los medios probatorios para que posteriormente se sancione.	Si, porque a través de ello se tiene suficientes elementos probatorios para posteriormente se sustente cargos ante el órgano jurisdiccional.

Coincidencia. Acorde a la pregunta anterior, el entrevistado 1, 2 y 3 afirmaron que a través de los actos de investigación no se logra una sanción efectiva puesto que no se llega a recabar los elementos probatorios.

Discrepancia. El entrevistado 4 manifiesta su diferencia con los demás puesto que refiere si se tiene suficientes elementos probatorios para sustentar cargos.

Interpretación. Los actos de investigación a nivel preliminar muchas veces no logran su objetivo la cual es conseguir una sanción penal frente a los delitos informáticos.

Pregunta N° 4

Explique ¿Cuáles son los actos de investigación que se utilizan para investigar un delito informático?			
J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
Principalmente el ingreso a los sistemas informativos que navegan en el ciberespacio tales como el ingreso al IP de una computadora, en otros casos rastreo de celulares y intervención telefónica.	Entre los mas comunes es el ingreso a los IP de los usuarios cibernéticos donde este tiene la similitud de una credencial de identificación por lo que a través de la geocalizacion se ubica a los mismos.	Desde el ámbito donde me desempeño proponemos que se realice diligencias tales como: se identifique y se individualice al autor o autores, se recabe videocámaras, capturas de pantallas de la computadoras o celulares y similares, entre otros.	Frecuentemente se dispone la investigación por parte de la fiscalía al personal policial de la DIVINDAT PNP por ser el personal capacitado.

Coincidencia. Acorde a la pregunta anterior, el entrevistado 1, 2, 3 y 4, coincidieron en mencionar los distintos actos de investigación que se realizan en las diligencias de investigación.

Discrepancia. Los entrevistados 1,2,3 y 4 no discreparon en cuanta las diligencias a efectuarse en el delito informático.

Interpretación. Son distintas los actos de investigación que se realizan en investigación por el delito informático, donde se puede resaltar de lo antes mencionados, que se requiere de diversas diligencias para perseguir e investigar estos tipos de delitos.

Pregunta N° 5

Desde una perspectiva jurídica, ¿qué opinión le merece la vigente ley de delitos informáticos -Ley N.º 30096?			
J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
Con este Ley se busca sancionar y reducir los índices de comisión de delitos informáticos; sin embargo, deberán ser reajustada en mérito a la experiencia y a la cantidad de casos que se presentan.	La Ley Nº 30096 es buena, sin embargo, requiere que se ponga mayor énfasis en su aplicación y también en la capacitación tecnológica de los Operadores de Derecho.	La ley es buena gracias a este se ha reforzado lo tipificado en el Código Penal y las modalidades que se utilizan para cometer estos actos ilícitos porque son debidamente tipificados.	Que es eficaz debido a que se identifica de manera expresa las distintas modalidades para cometer actos ilícitos. Sin embargo, es importante que su aplicación tanto en las fiscalías penales como juzgados penales sea eficiente y se logre el fin de toda ley, que es en este caso sancionar los delitos informáticos.

Coincidencia. Acorde a la pregunta anterior, el entrevistado 3 y 4 afirmaron que dicha ley es buena y eficaz, que reforzado el código penal y expresa las diversas modalidades que se comenten con el uso de la tecnología.

Discrepancia. El entrevistado 1 y 2 en cambio manifestaron que para la efectiva aplicación de la ley Nº 30096 se debe de capacitar a los Operadores de Derecho, debido a la cantidad de qué casos que se presentan día a día.

Interpretación. La ley es buena, sin embargo, debe darse mayor énfasis a su aplicación en cuanto a la capacitación de personal para que este sea efectiva.

Pregunta N° 6

¿De acuerdo a su experiencia laboral se logra identificar al autor (es) de la comisión del delito informático? ¿Por qué?			
J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
Si, ello en razón que en la máxima experiencia que logra desbaratar bandas criminales, así como a personas inescrupulosas que se dedican a esta ilícita labor ello de distintos partes del país.	Muchas veces no, porque es difícil conseguir el usuario tecnológico ya que estos tipos de delitos suelen cometerse en países y no necesariamente en el territorio peruano.	Muchas veces perdemos los casos para justamente a que no se logra la identificación del actor de estos actos ilícitos y siendo que el artículo 77º del Código Penal menciona que este es un requisito de procedibilidad para primera acción penal entonces se archiva.	No, porque es difícil ubicar a la persona que está detrás de un Operativo Tecnológico, sin embargo, en conjunto PNP y fiscalía se trata de combatir ello.

Coincidencia. Acorde a la pregunta anterior, el entrevistado 2, 3 y 4 afirmaron que muchas veces no se tiene la identificaron del autor (es) de estos actos ilícitos, por lo que se tiene que archivar las denuncias.

Discrepancia. El entrevistado 1 manifiesta que debido a su experiencia se ha logrado individualizar a los autores de los delitos informáticos.

Interpretación. En la mayoría de casos no se logra individualizar al autor (es) de los actos delictivos cometidos a través de la tecnología, puesto a que estos se encuentran detrás de una pantalla de computadora o talvez fuera del territorio peruano.

Pregunta N° 7

¿Cuál cree usted que es el mayor límite para que se consiga una efectiva sanción penal en contra del autor(es) de los delitos informáticos? ¿Por qué?

J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
Ello se da cuando los Operadores de Justicias no han logrado identificar al autor o presuntos autores del presente ilícito lo que deviene en el archivo de la denuncia y como consecuencia que quede impune el hecho delictivo y que se vea trasgredido el bien jurídico protegido de la víctima.	El mayor limite es la falta de capacitación de los Operadores de Derecho, ya que, en este tipo de delitos se usa muchos términos tecnológicos que talvez no se podría comprender.	Justamente que no se llega a identificar a los autores de estos actos ilícitos, por ello primigeniamente se interpone denuncia penal contra los que resulten responsables.	Talvez el desconocimiento tecnológico del personal policial se otras dependencias y también del personal fiscal y judicial

Coincidencia. Acorde a la pregunta anterior, el entrevistado 1, 2, 3 y 4 afirmaron que el desconocimiento de los términos tecnológicos por parte de los Operadores de Derecho son el mayor límite para que no se logre una efectiva sanción penal frente a un delito informático.

Discrepancia. En este caso todos los entrevistados demostraron estar conforme a la pregunta formulada.

Interpretación. El desconocimiento de la tecnología y demás complejidades por parte de los Operadores de Derecho es el mayor límite para que no se logre una efectiva sanción penal frente a un delito informático.

Pregunta N° 8

¿Considera usted que debería de crearse una fiscalía especializada en delitos informáticos para lograr una efectiva aplicación de la ley de delitos informáticos -Ley Nº 30096 en el derecho penal peruano? ¿Por qué?

J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
Si para que tenga autonomía y dedicación exclusiva este tipo de delitos y a la vez el personal se encuentre más capacitado sobre los términos, herramientas y demás tecnología que se utilizada para perseguir estos tipos de delitos.	Definitivamente si así como existe la DINDAT donde el personal policial está capacitado para realizar investigaciones altamente tecnológicos también se debería hace una fiscalía especializada y capacitada de la misma manera.	Por supuesto que si es necesario por la alta complejidad de este tipo de delito.	Si, considero que la creación de ello, haría que se sancione de manera efectiva los delitos informáticos y sus distintas modalidades para perpetrarlos ya que estos ingresan con los demás delitos comunes.

Coincidencia. Acorde a la pregunta anterior, el entrevistado 1, 2, 3 y 4 afirmaron que debería crease una fiscalía especializa en delitos informáticos.

Discrepancia. En este caso todos los entrevistados demostraron estar conforme a la pregunta formulada

Interpretación. Es de importancia que se dé la creación de las fiscalías especializadas en delitos informáticos debido a su complejidad y la diferencia entre otros delitos comunes.

Pregunta N° 9

¿Cree usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?

J. T. C. (EX-1)	C. G. W. (EX-2)	D. G. T. (EX-3)	P.A.G.T. (EX-4)
Como toda ley buscan prevenir la comisión de delitos, sin embargo, siempre habrá personas que actuarán al margen de la Ley; además de que falta mayor educación preventiva en la sociedad frente a los delitos que se cometen a través de la tecnología.	Si, pero aún falta mayor promoción de dicha ley, ya que, el Estado debe promover la prevención frente a los mismos en la sociedad y sobre todo en las poblaciones vulnerables de donde se desconoce el uso y demás de la tecnología.	Si, sin embargo, falta mayor promoción de la ley para que la sociedad tendrá conocimiento de que derecho gozan y cuáles son los bienes jurídicos que la ley protege.	Si ahora esta en los ciudadanos a pie que, así como se capacitan en el uso de las redes sociales. También deberán hacerlo con los peligros que acarrea el uso de la tecnología.

Coincidencia. Acorde a la pregunta anterior, el entrevistado 1, 2, 3 y 4 coincidieron en afirmar que la ley de delitos informáticos contribuye a la prevención de los mismo, y que está en los ciudadanos capacitarse en conocer las distintas modalidades que comenten el autor(es) de este tipo de delitos.

Discrepancia. En este caso todos los entrevistados demostraron estar conforme a la pregunta formulada

Interpretación. Es de importancia que se dé la creación de las fiscalías especializadas en delitos informáticos debido a su complejidad y la diferencia entre otros delitos comunes.

3. Discusión

Debido a la existencia de casos en los cuales no se puede probar que la persona cometió un delito, hay ciertas falencias tales como la investigación a realizarse a nivel preliminar, ello respecto a la individualización del autor o autores de los delitos informáticos y que por lo tanto a ser este tipo penal complejo requiere de una investigación a nivel fiscal de igual manera compleja, es así, como los expertos en la materia dieron a conocer las deficiencias y falta de precisiones en su aplicación normativa. De acuerdo con los resultados se reconoce que la Ley Nº 30096 es ineficaz e insuficiente para que de manera efectiva se sancione penalmente y se logre el resarcimiento del daño causado hacia el agraviado (a), donde se evidencia sus deficiencias, y por más que se plantearon diversas modificaciones a la ley, adecuándolo al documento internacional que se creó antes del Convenio de Budapest. Una demostración del reconocimiento de las inconsistencias de la ley Nº 30096 es que a tan solo seis meses de su entrada en vigencia fue modificada a través de la Ley Nº 30171 en el año 2013.

Apoyándome en lo anteriormente expuesto, Espinoza. (2016), en el artículo científico "La tecnología de la información como herramienta construccionista para el autor financiero hibrido", publicado en la revista Fides Et Radtio, volumen 11, mencionó que es importante tener claramente cuáles son los hechos delictivos, teniendo en cuenta que estos hechos siempre son repetitivos, es ahí donde es sumamente necesario el empleo de instrumentos y sistemas para poder reconocer claramente dichos indicios y de esta forma tipificar de forma correcta el delito y evitar que este se quede en esta epata o sea archivado por la autoridad.

Por su parte Justo, (2017). mencionó en su investigación el trabajo "Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal", correspondiente al proyecto financiado por Ford Foundation. Dicha investigación enfatiza la importancia y facultades en el ámbito procesal penal que deben de tener los investigadores en las diferentes modalidades del Cibercrimen tales como procesos, servicios, actividades o manejo de información que se realizan en línea, considerándose que un mismo ilícito se puede realizar en diferentes jurisdicciones (países), por la naturaleza del internet.

De igual manera, Mayer. (2018), en la revista Ius et Praxis, publicó el artículo "Elementos Criminológicos para el análisis jurídico – penal de los delitos informáticos", en el cual mencionó que este delito constituye una materia que se viene presentando en tiempos recientes por el crecimiento de la tecnología, concentrando a la criminología en estos ámbitos también, es decir que

a medida que evoluciona la tecnología también está evolucionando la delincuencia, razón por la cual las normas también tiene que abarcar esos ámbitos y de igual forma generar sistemas en los que se apoyen para poder controlar el incremento de dicho delito.

Ojeda, Arias, Rincón y Daza. (2010), en el artículo "Delitos informáticos y entorno jurídico vigente en Colombia", en la revista Cuad. Contab, volumen 11, número 28, indicó que es necesario e importante poder conocer el contexto que presenta este delito, dado que está orientado a posibles acciones y respuestas que se enfocan a prevenir y dar el tratamiento debido, haciendo una revisión de las normas que han sido implementadas para controlar el mismo, contrastando la ley con los recursos que se tienen para la aplicación de la misma, llegando a la conclusión que una no funciona sin la otra.

Por su parte Lasso (2017), tipifica delitos informáticos presentes en la ley 30096, los cuales son: el fraude informático, la pornografía infantil, estafa informática, suplantación de identidad, acceso ilícito, atentado a la integridad de datos informáticos, tráfico ilegal de datos e interceptación de datos informáticos, debido a la necesidad de contar con un ordenamiento jurídico que sancione de forma adecuada y particular a la cibercriminalidad, no solo desde la identificación de los delitos cometidos y el establecimiento de penas sino también desde el procedimiento penal para dar solución a las investigaciones.

Se obtuvo que las herramientas actuales son mayormente digitales tales como software, los capturadores de tráfico; los sistemas de detección de intrusos, emuladores, herramientas de borrado de archivos, de recuperación de contraseñas, de datos o archivos y de análisis de discos montaje y recuperación, software de clonación entre otras.

Esto acorde con Jiménez (2018), quien afirma que una aplicación de uso didáctico para comunicación segura de datos a través de la red verifica la integridad de los datos y mensajes.

La información obtenida del presente trabajo de investigación, da a conocer que los entrevistados en relación a la primera pregunta ¿Qué opina respecto al acelerado avance de las tecnologías informáticas y las modalidades de comisión de delitos con el uso del mismo?; los entrevistados C.G.W, D.G.T y P.A.G.T. coincidieron en manifestar que la tecnología ha llegado para mejorar muchas cosas en la vida, las facilita y crea nuevas necesidades, sin embargo, uno de mis entrevistados J.T.C, opinó que a pesar que la tecnología mejora muchos aspectos en la vida, la falta

de una cultura de denuncia de delitos informáticos hace que estos sigan aumentando, además el entrevistado 2 manifestó que la cara negativa de esto trae consecuencias al usuario que entra a internet.

En relación a la segunda pregunta formulada ¿Considera usted que la legislación sobre delitos informáticos -Ley Nº 30096 en el derecho penal peruano es suficiente para sancionar las nuevas formas delictivas con el uso de las tecnologías informáticas? ¿Por qué?; los entrevistado J. T. C., C. G. W. y D. G. T manifestaron que no es suficiente dicha ley, debido a la complejidad del delito informático y las herramientas que se deben utilizar para combatir el mismo, no obstante, el entrevistado P.A.G.T. afirmó que la ley de delitos informáticos es sueficiente, puesto que ya se encuentra regulado lo del Código Penal.

En relación a la tercera pregunta formulada ¿Considera usted que los actos de investigación realizados a nivel preliminar logran una efectiva sanción penal frente a los delitos informáticos? ¿Por qué?; los entrevistados J. T. C., C. G. W. y D. G. T afirmaron que a través de los actos de investigación no se logra una sanción efectiva puesto que no se llega a recabar los elementos probatorios, sin embargo, el entrevistado P.A.G.T. manifiesta su diferencia con los demás puesto que refiere si se tiene suficientes elementos probatorios para sustentar cargos.

En relación a la cuarta pregunta formulada Explique ¿Cuáles son los actos de investigación que se utilizan para investigar un delito informático? ¿Por qué?; los entrevistados J.T.C, C.G.W, D.G.T. y M.R.J. coincidieron en mencionar los distintos actos de investigación que se realizan en las diligencias de investigación. Los entrevistados J.T.C, C.G.W, D.G.T. y P.A.G.T. no discreparon y coincidieron en cuanto a las diligencias a efectuarse en el delito informático.

En relación a la quinta pregunta formulada ¿considera Usted que la regulación en el derecho penal peruano de la ley de delitos informáticos -Ley N.º 30096 es suficiente para sancionar las distintas modalidades de delitos informáticos? ¿Por qué?; los entrevistados D.G.T y P.A.G.T. afirmaron que a través de los actos de investigación no se logra una sanción efectiva puesto que no se llega a recabar los elementos probatorios, sin embargo, los entrevistados J.T.C y C.G.W manifiesta su diferencia con los demás puesto que refiere si se tiene suficientes elementos probatorios para sustentar cargos.

En relación a la sexta pregunta formulada ¿De acuerdo a su experiencia laboral se logra identificar al autor (es) de la comisión del delito informático? ¿Por qué?; los entrevistados C.G.W, D.G.T y

P.A.G.T. afirmaron que muchas veces no se tiene la identificaron del autor (es) de estos actos ilícitos, por lo que se tiene que archivar las denuncias, sin embargo, el entrevistado J.T.C manifiesta que debido a su experiencia se ha logrado individualizar a los autores de los delitos informáticos.

En relación a la séptima pregunta formulada ¿considera Usted que debería crearse una fiscalía especializada en delitos informáticos para lograr una efectiva aplicación de la ley de delitos informáticos -Ley N.º 30096 en el derecho penal peruano? ¿Por qué?; los entrevistados J.T.C, C.G.W, D.G.T. y P.A.G.T. afirmaron que el desconocimiento de los términos tecnológicos por parte de los Operadores de Derecho son el mayor límite para que no se logre una efectiva sanción penal frente a un delito informático.

En relación a la octava pregunta formulada ¿considera Usted que debería de crearse unas fiscalías especializadas en delitos informáticos para lograr una efectiva aplicación de la ley de delitos informáticos -Ley N.º 30096 en el derecho penal peruano? ¿Por qué?; los entrevistados J.T.C, C.G.W, D.G.T. y P.A.G.T. coincidieron en que, debido a la complejidad de los delitos informáticos, se debería crear una fiscalía especializa en delitos informáticos.

En relación a la novena pregunta formulada ¿considera Usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?; ¿Por qué?; los entrevistados J.T.C, C.G.W, D.G.T. y P.A.G.T. coincidieron que debería crease una fiscalía especializa en delitos informáticos.

4. Conclusiones

La regulación de la ley de delitos informáticos- ley Nº 30096, describe las conductas ilícitas que afectan los sistemas y datas informáticos, secreto de comunicaciones, contra el patrimonio, la fe pública y la libertad sexual cometidos mediante la utilización de la tecnología.

La aplicación de la Ley Nº 30096 -ley de delitos informáticos no logra sancionar de manera efectiva aquellos ilícitos cometidos a través de la tecnología, ello por la falta de identificación e individualización del autor (es) del delito informático y la alta complejidad que contrae el mismo en las investigaciones preliminares.

El rol de los Operadores de Derecho no es suficiente para sancionar los también llamados ciberdelitos puesto que los mismos no se encuentran capacitados para conocer este tipo penal, debido a su alta complejidad tecnológica.

5. Agradecimiento

A mi asesora Lutgarda Palomino G., por sus enseñanzas y dedicación para poder realizar y culminar el presente trabajo de investigación, y a la vida por ofrecer diariamente un nuevo comienzo para el logro de objetivos.

Referencias

Bramont-Arias, T.L. (2007). El Delito Informático en el Código Penal Peruano. Lima: Fondo Editorial de la PUCP.

Council of Europe, (2001). Convenio de Cibercriminalidad de Budapest. Budapest. Recuperado el 20 de marzo de 2019, de: http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.PDF

Di lorio, A. y Castallote, M. (2016). El rastro digital del delito. Aspectos técnicos, legales y estratégicos de la Informática Forense. Fasta: Mar de Plata. Recuperado el 20 de marzo de 2019, de https://bit.ly/2SqOKw8

Hancco, E. (2017). La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley30096. Recuperado el 20 de marzo de 2019, de http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/6436/DEhazaey.pdf?sequence=1&isAllowed=y

Hernández, S. (2018). Metodología de la investigación. Lima, Perú: MC Graw Hill Education.

Jiménez, J. (2017). Manual de Derecho Penal Informático. Perú: Jurista Editores.

Jaramillo, J. A., Valarezo, G. y Astudillo, O. B. (2014). Rigurosidad versus flexibilidad en la investigación cualitativa. Revista Panorama Médico. Quito. 8 (1), 06-13.

Justo, M. (2017). Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal. Recuperado el 20 de marzo de 2019, de https://bit.ly/2RumV9F

Lamperti, S. B. (2017). Aspectos Legales. Los Delitos Informáticos. El rastro digital del delito: aspectos técnicos, legales y estratégicos de la Informática Forense. Mar de Plata: Universidad FASTA.

Lasso, V. (2017). Estado del peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia. Recuperado el 20 de marzo de 2019, de https://bit.ly/2RzcxgQ

Loredo, A. (2017). El bien jurídico protegido en los Delitos informáticos. Revista chilena de derecho. Versión On-line ISSN 0718-3437. Recuperado el 20 de marzo de 2019, de https://scielo.conicyt.cl/scielo.php?script=sci_abstract&pid=S071834372017000100011&lng=es&nrm=iso

Libertador, M. y Roussos, A. (2008). Lo cualitativo, un modelo para la comprensión de los métodos de investigación. Buenos Aires: Universidad de Belgrano.

Anexo Nº 3: Validación de Entrevista

Nº	CATEGORÍAS/ Ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Categoría: Tratamiento Jurídico Penal	Si	No	Si	No	Si	No	
1	¿Qué opina respecto al acelerado avance de las tecnologías informáticas y las modalidades de comisión de delitos con el uso del mismo?	X		X		X		
2	¿Desde una perspectiva jurídica qué opinión le merece la vigente ley de delitos informáticos -Ley N° 30096?	X		X		X		
	Categoría: Capacitación del personal	Si	No	Si	No	Si	No	
3	¿Considera Usted que los actos de investigación realizados a nivel preliminar logran una efectiva sanción penal frente a los delitos informáticos? ¿Por qué?	X		X		X		
4	Explique ¿Cuáles son los actos de investigación que se utilizan para investigar un delito informático?	X		X		X		
	Categoría: Aplicación de la ley							
5	¿Considera Usted que la regulación en el derecho penal	Si	No	Si	No	Si	No	

	peruano de la ley de delitos informáticos -Ley N° 30096 es suficiente para sancionar las distintas modalidades de delitos informáticos? ¿Por qué?	X		X		X		
6	¿De acuerdo a su experiencia laboral se logra identificar al autor (es) de la comisión del delito informático ? ¿Por qué?	X		X		X		

7	¿Considera Usted que debería de crearse una fiscalía especializada en delitos informáticos para lograr una efectiva aplicación de la ley de delitos informáticos –Ley N° 30096 en el derecho penal peruano? ¿Por qué?	X		X		X		
8	¿Considera usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?	X		X		X		
9	¿Cuál cree Usted que es el mayor límite para que se consiga una efectiva sanción penal en contra del autor(es) de los delitos informáticos? ¿Por qué?	X		X		X		

Observaciones (precisar si hay suficiencia): SUFICIENCIA

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y Nombres del experto validador. Dr. / Mg: ELKE SUSY SALAZAR ARNAS **DNI:** CAL 64280

Especialidad del validador: Magister en Derecho Procesal Penal

29 de SEPTIEMBRE del 2019

Leyenda:

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.

[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR DE JUICIO DE EXPERTOS

Nº	CATEGORÍAS/ Ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Categoría: Tratamiento Jurídico Penal	Si	No	Si	No	Si	No	
1	¿Qué opina respecto al acelerado avance de las tecnologías informáticas y las modalidades de comisión de delitos con el uso del mismo?	X		X		X		
2	¿Desde una perspectiva jurídica qué opinión le merece la vigente ley de delitos informáticos -Ley N° 30096?	X		X		X		
	Categoría: Capacitación del personal	Si	No	Si	No	Si	No	
3	¿Considera Usted que los actos de investigación realizados a nivel preliminar logran una efectiva sanción penal frente a los delitos informáticos? ¿Por qué?	X		X		X		
4	Explique ¿Cuáles son los actos de investigación que se utilizan para investigar un delito informático?	X		X		X		
	Categoría: Aplicación de la ley							
5	¿Considera Usted que la regulación en el derecho penal	Si	No	Si	No	Si	No	

	peruano de la ley de delitos informáticos -Ley N° 30096 es suficiente para sancionar las distintas modalidades de delitos informáticos? ¿Por qué?	X		X		X		
6	¿De acuerdo a su experiencia laboral se logra identificar al autor (es) de la comisión del delito informático ? ¿Por qué?	X		X		X		

7	¿Considera Usted que debería de crearse una fiscalía especializada en delitos informáticos para lograr una efectiva aplicación de la ley de delitos informáticos –Ley N° 30096 en el derecho penal peruano? ¿Por qué?	X		X		X		
8	¿Considera usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?	X		X		X		
9	¿Cuál cree Usted que es el mayor límite para que se consiga una efectiva sanción penal en contra del autor(es) de los delitos informáticos? ¿Por qué?	X		X		X		

Observaciones (precisar si hay suficiencia): SUFICIENCIA

Opinión de aplicabilidad: **Aplicable** [X] **Aplicable después de corregir** [ ] **No aplicable** [ ]

Apellidos y Nombres del experto validador. Dr. / Mg: _____ **DNI:** CAL 70850

Especialidad del validador: Maestro Derecho Penal

JIMMY GONZALES MENDOZA
CAL N° 70850

23 de SEPTIEMBRE del 2019

Leyenda:

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.

[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR DE JUICIO DE EXPERTOS

Nº	CATEGORÍAS/ Ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Categoría: Tratamiento Jurídico Penal	Si	No	Si	No	Si	No	
1	¿Qué opina respecto al acelerado avance de las tecnologías informáticas y las modalidades de comisión de delitos con el uso del mismo?	X		X		X		
2	¿Desde una perspectiva jurídica qué opinión le merece la vigente ley de delitos informáticos -Ley N° 30096?	X		X		X		
	Categoría: Capacitación del personal	Si	No	Si	No	Si	No	
3	¿Considera Usted que los actos de investigación realizados a nivel preliminar logran una efectiva sanción penal frente a los delitos informáticos? ¿Por qué?	X		X		X		
4	Explique ¿Cuáles son los actos de investigación que se utilizan para investigar un delito informático?	X		X		X		
	Categoría: Aplicación de la ley							
5	¿Considera Usted que la regulación en el derecho penal	Si	No	Si	No	Si	No	

	peruano de la ley de delitos informáticos -Ley N° 30096 es suficiente para sancionar las distintas modalidades de delitos informáticos? ¿Por qué?	X		X		X		
6	¿De acuerdo a su experiencia laboral se logra identificar al autor (es) de la comisión del delito informático ? ¿Por qué?	X		X		X		

7	¿Considera Usted que debería de crearse una fiscalía especializada en delitos informáticos para lograr una efectiva aplicación de la ley de delitos informáticos –Ley N° 30096 en el derecho penal peruano? ¿Por qué?	X		X		X		
8	¿Considera usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?	X		X		X		
9	¿Cuál cree Usted que es el mayor límite para que se consiga una efectiva sanción penal en contra del autor(es) de los delitos informáticos? ¿Por qué?	X		X		X		

Observaciones (precisar si hay suficiencia): Suficiencia

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y Nombres del experto validador. Dr. / Mg: Katherine Luque Padras DNI: 10017827

Especialidad del validador: Derecho Penal

. CAL 37559

23 de Septiembre del 2019

Leyenda:

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.

[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR DE JUICIO DE EXPERTOS

Nº	CATEGORÍAS/ Ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Categoría: Tratamiento Jurídico Penal	Si	No	Si	No	Si	No	
1	¿Qué opina respecto al acelerado avance de las tecnologías informáticas y las modalidades de comisión de delitos con el uso del mismo?	X		X		X		
2	¿Desde una perspectiva jurídica qué opinión le merece la vigente ley de delitos informáticos -Ley N° 30096?	X		X		X		
	Categoría: Capacitación del personal	Si	No	Si	No	Si	No	
3	¿Considera Usted que los actos de investigación realizados a nivel preliminar logran una efectiva sanción penal frente a los delitos informáticos? ¿Por qué?	X		X		X		
4	Explique ¿Cuáles son los actos de investigación que se utilizan para investigar un delito informático?	X		X		X		
	Categoría: Aplicación de la ley							
5	¿Considera Usted que la regulación en el derecho penal	Si	No	Si	No	Si	No	

	peruano de la ley de delitos informáticos -Ley N° 30096 es suficiente para sancionar las distintas modalidades de delitos informáticos? ¿Por qué?	X		X		X		
6	¿De acuerdo a su experiencia laboral se logra identificar al autor (es) de la comisión del delito informático ? ¿Por qué?	X		X		X		

7	¿Considera Usted que debería de crearse una fiscalía especializada en delitos informáticos para lograr una efectiva aplicación de la ley de delitos informáticos –Ley N° 30096 en el derecho penal peruano? ¿Por qué?	X		X		X		
8	¿Considera usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?	X		X		X		
9	¿Cuál cree Usted que es el mayor límite para que se consiga una efectiva sanción penal en contra del autor(es) de los delitos informáticos? ¿Por qué?	X		X		X		

ones (precisar si hay suficiencia): Suficiencia

e aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

y Nombres del experto validador. Dr. / ~~Mg~~: Derecho Penal DNI: CAL 20873

lad del validador: Magister Manuel M. Valdivia Cotrina

23 de Septiembre d

Leyenda:

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.

[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR DE JUICIO DE EXPERTOS

Nº	CATEGORÍAS/ Ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Categoría: Tratamiento Jurídico Penal	Si	No	Si	No	Si	No	
1	¿Qué opina respecto al acelerado avance de las tecnologías informáticas y las modalidades de comisión de delitos con el uso del mismo?	X		X		X		
2	¿Desde una perspectiva jurídica qué opinión le merece la vigente ley de delitos informáticos -Ley N° 30096?	X		X		X		
	Categoría: Capacitación del personal	Si	No	Si	No	Si	No	
3	¿Considera Usted que los actos de investigación realizados a nivel preliminar logran una efectiva sanción penal frente a los delitos informáticos? ¿Por qué?	X		X		X		
4	Explique ¿Cuáles son los actos de investigación que se utilizan para investigar un delito informático?	X		X		X		
	Categoría: Aplicación de la ley							
5	¿Considera Usted que la regulación en el derecho penal	Si	No	Si	No	Si	No	

	peruano de la ley de delitos informáticos -Ley N° 30096 es suficiente para sancionar las distintas modalidades de delitos informáticos? ¿Por qué?	X		X		X		
6	¿De acuerdo a su experiencia laboral se logra identificar al autor (es) de la comisión del delito informático ? ¿Por qué?	X		X		X		

7	¿Considera Usted que debería de crearse una fiscalía especializada en delitos informáticos para lograr una efectiva aplicación de la ley de delitos informáticos –Ley N° 30096 en el derecho penal peruano? ¿Por qué?	X		X		X		
8	¿Considera usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?	X		X		X		
9	¿Cuál cree Usted que es el mayor límite para que se consiga una efectiva sanción penal en contra del autor(es) de los delitos informáticos? ¿Por qué?	X		X		X		

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y Nombres del experto validador. Dr. / Mg: Cortez Pineda, Jorge Luis **DNI:** CAL 10029

Especialidad del validador: Penalista

23 de Septiembre del 2019

Leyenda:

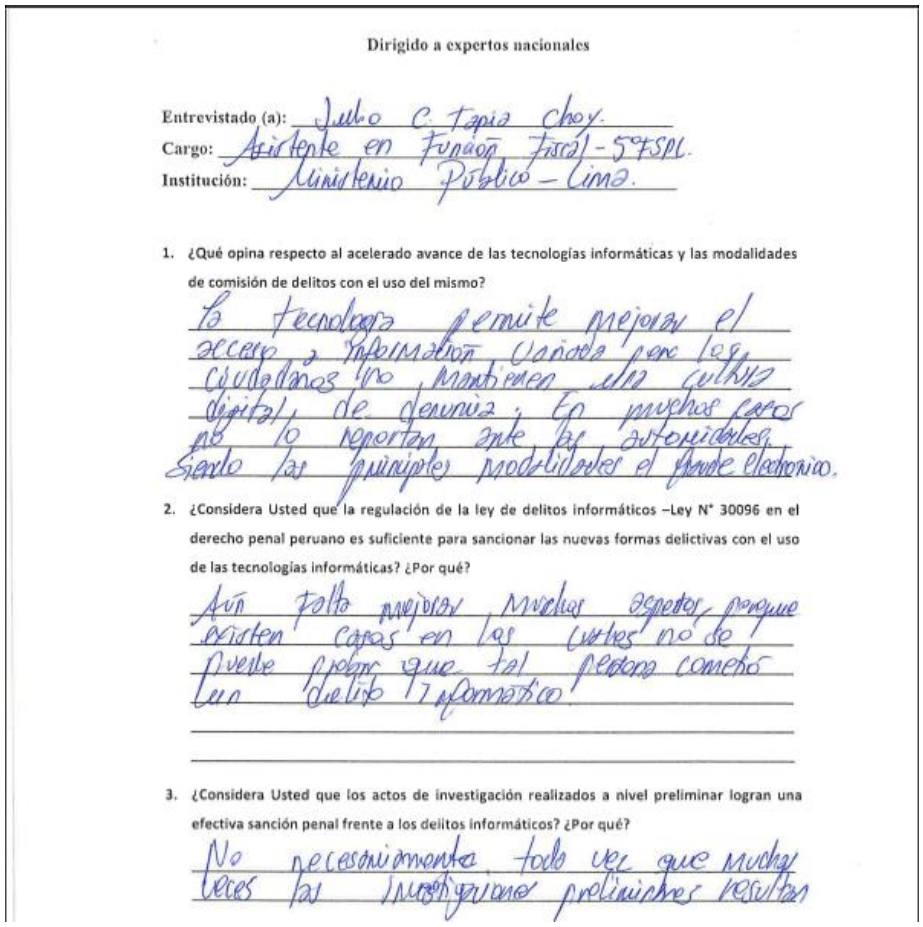
[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.

[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Anexo Nº 4: Entrevistas Resueltas



Dirigido a expertos nacionales

Entrevistado (a): Julio C. Tapia Choy.
Cargo: Asistente en Función Fiscal - 5ºFSPL.
Institución: Ministerio Público – Lima.

1. ¿Qué opina respecto al acelerado avance de las tecnologías informáticas y las modalidades de comisión de delitos con el uso del mismo?

La tecnología permite mejorar el acceso a información valiosa pero los ciudadanos no mantienen una cultura digital de denuncia. En muchos casos no lo reportan ante las autoridades siendo las principales modalidades el fraude electrónico.

2. ¿Considera Usted que la regulación de la ley de delitos informáticos –Ley N° 30096 en el derecho penal peruano es suficiente para sancionar las nuevas formas delictivas con el uso de las tecnologías informáticas? ¿Por qué?

Aún falta mejorar. Muchos aspectos porque existen casos en los cuales no se puede probar que tal persona cometió un delito informático.

3. ¿Considera Usted que los actos de investigación realizados a nivel preliminar logran una efectiva sanción penal frente a los delitos informáticos? ¿Por qué?

No necesariamente, todo vez que muchas veces las investigaciones preliminares resultan

4. Explique ¿Cuáles son los actos de investigación que se utilizan para investigar un delito informático?

Principalmente el ingreso a los sistemas informáticos que navegan en el cibor espacio total como el ingreso a la de una computadora, en otras pueden a pertenecer de celulares y intervención telefónica.

5. ¿Desde una perspectiva jurídica qué opinión le merece la vigente ley de delitos informáticos -Ley N° 30096?

Con esta ley se busca sancionar y reducir los índices de comisión de delitos informáticos, sin embargo, deberán ser reajustadas en mérito a la experiencia y a la cantidad de casos que se presentan.

6. ¿De acuerdo a su experiencia laboral se logra identificar al autor (es) de la comisión del delito informático ? ¿Por qué?

Si ello en razón que en la mayoría se logra desbaratar bandas personas inescrupulosas que se dedican a esta ilícita labor ello de distintas partes del país.

7. ¿Cuál cree Usted que es el mayor límite para que se consiga una efectiva sanción penal en contra del autor(es) de los delitos informáticos? ¿Por qué?

Idoneidad y como consecuencia que quede impune el hecho delictivo.

8. ¿Considera Usted que debería de crearse una fiscalía especializada en delitos informáticos para lograr una efectiva aplicación de la ley de delitos informáticos –Ley N° 30096 en el derecho penal peruano? ¿Por qué?

Si, para que tenga autonomía y dedicación exclusiva este tipo de delitos y a la vez el personal se encuentre más capacitado sobre los términos, herramientas y demás tecnologías que se utiliza para perpetuar este delito.

9. ¿Considera usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?

Como toda ley buscan prevenir la comisión de delitos, sin embargo siempre habrá personas que, debido al mayor de la ley, además de que falta mayor educación concientizar en la sociedad frente a los delitos informáticos.

Muchas gracias por su valiosa opinión

Justin C. Tapia Cruz
Asistente Función Fiscal.
CAL. 38050

Dirigido a expertos nacionales

Entrevistado (a): Wilmer Bernal Gabarrillas Gallardo
Cargo: PNP - DIVINDAT - CAP: 31680237
Institución: DIVINDAT - CIFMA.

1. ¿Qué opina respecto al acelerado avance de las tecnologías informáticas y las modalidades de comisión de delitos con el uso del mismo?

Hoy en día el uso de la tecnología se convirtió en la sociedad y también es mal utilizado por los delincuentes que a través de ello cometen diversos actos ilícitos a través de la tecnología

2. ¿Considera Usted que la regulación de la ley de delitos informáticos –Ley N° 30096 en el derecho penal peruano es suficiente para sancionar las nuevas formas delictivas con el uso de las tecnologías informáticas? ¿Por qué?

No es suficiente, debido a que la tecnología es utilizado para perpetrar los delitos informáticos, por lo que se requiere mayores herramientas tecnológicas al fin del seguir dicho delito.

3. ¿Considera Usted que los actos de investigación realizados a nivel preliminar logran una efectiva sanción penal frente a los delitos informáticos? ¿Por qué?

Muchas veces no se logra debido a que no se logra el fin de las diligencias

4. Explique ¿Cuáles son los actos de investigación que se utilizan para investigar un delito informático?

Entre los más comunes es el ingreso a IP de los usuarios cibernéticos donde este tiene la dificultad de una posible identificación por lo que a través de la geocalización se ubica a los mismos.

5. ¿Desde una perspectiva jurídica qué opinión le merece la vigente ley de delitos informáticos -Ley N° 30096?

La Ley Nº 30096 es buena, sin embargo requiere que se ponga mayor énfasis en su difusión y también en la capacitación tecnológica de los Operadores de Derecho.

6. ¿De acuerdo a su experiencia laboral se logra identificar al autor (es) de la comisión del delito informático ? ¿Por qué?

Muchas veces no, porque es difícil conseguir el usuario tecnológico ya que estos tipos de delitos suelen cometerse en países y no necesariamente en el territorio peruano.

7. ¿Cuál cree Usted que es el mayor límite para que se consiga una efectiva sanción penal en contra del autor(es) de los delitos informáticos? ¿Por qué?

8. ¿Considera Usted que debería de crearse una fiscalía especializada en delitos informáticos para lograr una efectiva aplicación de la ley de delitos informáticos –Ley N° 30096 en el derecho penal peruano? ¿Por qué?

Definitivamente sí así como, existe la DIVINDAT donde el personal policial está altamente capacitado para realizar investigaciones tecnológicas también se debería crear una fiscalía especializada y capacitada de la misma manera.

9. ¿Considera usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?

Sí, pero aún falta mayor promoción de dicha ley, ya que, el Estado debe promover la prevención frente a los mismos en la sociedad y sobre todo en las poblaciones vulnerables de donde se desconoce el uso y demás de la tecnología.

Muchas gracias por su valiosa opinión

CIP 31680237

Dirigido a expertos nacionales

Entrevistado (a): Dewar Gonzalo Quevedo Torres
Cargo: Abogado Penalista Litigante.
Institución: Estudio Jurídico "E & E"

1. ¿Qué opina respecto al acelerado avance de las tecnologías informáticas y las modalidades de comisión de delitos con el uso del mismo?

Lo que puedo ver en mi día a día como abogado litigante es que los delitos informáticos son comunes en el mundo delictivo por lo que la norma sobre el mismo es relevante.

2. ¿Considera Usted que la regulación de la ley de delitos informáticos –Ley N° 30096 en el derecho penal peruano es suficiente para sancionar las nuevas formas delictivas con el uso de las tecnologías informáticas? ¿Por qué?

No porque muchas veces no se logra una sanción efectiva propiamente los casos se pierden es decir esen, la parte afectada no llega a ser resarcida por el delito cometido.

3. ¿Considera Usted que los actos de investigación realizados a nivel preliminar logran una efectiva sanción penal frente a los delitos informáticos? ¿Por qué?

Muchas veces no tanto. Ya que la DNP y la fiscalía no logran

[illegible] los objetivos que es recabar los medios probatorios para que posteriormente se sancione.

4. Explique ¿Cuáles son los actos de investigación que se utilizan para investigar un delito informático?

Desde el ámbito donde me desempeño opinaremos que se realice diligencias tales como: se identifique y se individualice al autor o autores, se recabe videocámaras, capturas de pantallas de los computadores o celulares y similares.

5. ¿Desde una perspectiva jurídica qué opinión le merece la vigente ley de delitos informáticos -Ley N° 30096?

La ley es buena gracias a ello ha regulado lo tipificado en el Código Penal y las modalidades que se utilizan para cometer estos actos ilícitos porque son debidamente tipificados.

6. ¿De acuerdo a su experiencia laboral se logra identificar al autor (es) de la comisión del delito informático ? ¿Por qué?

Muchas veces perdemos los casos, porque lamentablemente no se logra identificar al autor de estos actos ilícitos y siendo que el Art. 77° del Código de Procedimientos Penales menciona que este es un requisito de procedibilidad para promover acción penal entonces se archiva.

7. ¿Cuál cree Usted que es el mayor límite para que se consiga una efectiva sanción penal en contra del autor(es) de los delitos informáticos? ¿Por qué?

responsable?

8. ¿Considera Usted que debería de crearse una fiscalía especializada en delitos informáticos para lograr una efectiva aplicación de la ley de delitos informáticos –Ley N° 30096 en el derecho penal peruano? ¿Por qué?

Por supuesto que sí es necesario por la alta complejidad de este tipo de delito.

9. ¿Considera usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?

Si sin embargo, falta mayor promoción de la ley para que la sociedad tenga conocimiento de qué derecho gozan y cuáles son los bienes jurídicos que la ley protege.

Muchas gracias por su valiosa opinión

CAL. 32498

Dirigido a expertos nacionales

Entrevistado (a): Perla Aurora Gudiche Tambuyo
Cargo: Fiscal Adjunta Provincial Provisional-Lima
Institución: Ministerio Público - Lima - 1°FPP

1. ¿Qué opina respecto al acelerado avance de las tecnologías informáticas y las modalidades de comisión de delitos con el uso del mismo?

Hoy en dia es frecuente el ingreso de los delitos informáticos es muy seguido apertura y investigación preliminar mente por estos tipos de delitos y sus distintas modalidades.

2. ¿Considera Usted que la regulación de la ley de delitos informáticos –Ley N° 30096 en el derecho penal peruano es suficiente para sancionar las nuevas formas delictivas con el uso de las tecnologías informáticas? ¿Por qué?

Si, es suficiente porque se tiene también la regulación del Código Penal Peruano en los artículos 207°-A, B, C y D, y con esta ley se complementan de manera eficaz.

3. ¿Considera Usted que los actos de investigación realizados a nivel preliminar logran una efectiva sanción penal frente a los delitos informáticos? ¿Por qué?

Si porque a través de ello se tiene suficientes elementos probatorios

Cuerpos del Delito (como).

4. Explique ¿Cuáles son los actos de investigación que se utilizan para investigar un delito informático?

Frecuentemente se dispone la intervención por parte de la Fiscalía el personal policial de la DIVINDAT PNP, por ser el personal capacitado.

5. ¿Desde una perspectiva jurídica qué opinión le merece la vigente ley de delitos informáticos -Ley N° 30096?

Que es eficaz debido a que se identifica de manera expresa las distintas modalidades para cometer actos ilícitos; Sin embargo, es importante que su aplicación sea eficiente y se logre el fin de toda ley.

6. ¿De acuerdo a su experiencia laboral se logra identificar al autor (es) de la comisión del delito informático ? ¿Por qué?

No, porque es difícil ubicar a la persona que esta detrás de un operativo tecnologico, sin embargo, en conjunto la PNP y Fiscalía trata de combatir ello.

7. ¿Cuál cree Usted que es el mayor límite para que se consiga una efectiva sanción penal en contra del autor(es) de los delitos informáticos? ¿Por qué?

8. ¿Considera Usted que debería de crearse una fiscalía especializada en delitos informáticos para lograr una efectiva aplicación de la ley de delitos informáticos –Ley N° 30096 en el derecho penal peruano? ¿Por qué?

Talvez el desconocimiento, considero que sí, la creación de ello, haría que se sancione de manera efectiva los delitos informáticos y sus distintas modalidades para perpetrarlos ya que estos ingresan como comunes.

9. ¿Considera usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?

Sí, ahora está en los ciudadanos a pie que, así como se capacitan en el uso de las redes sociales. También deberían hacerlo con los peligros que conlleva el uso de la tecnología!

Muchas gracias por su valiosa opinión

56

DNI: 09797472