UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

TESIS

MODIFICACIÓN LEGISLATIVA DE LA LEY 30096 DE DELITOS INFORMÁTICOS PARA SU EFICACIA CONTRA LA CIBERDELINCUENCIA EN LA CIUDAD DE CHICLAYO

PARA OPTAR TÍTULO PROFESIONAL DE ABOGADO

Autor:

Bach. Roman Cruz Eucario Hector

ORCID: https://orcid.org/0000-0001-8457-2409

Asesor:

Dr. Failoc Piscoya Dante Roberto

ORCID: https://orcid.org/0000-0001-5428-5476

Línea de Investigación:

Ciencias jurídicas

Pimentel – Perú 2020

MODIFICACIÓN LEGISLATIVA DE LA LEY 30096 DE DELITOS INFORMÁTICOS PARA SU EFICACIA CONTRA LA CIBERDELINCUENCIA EN LA CIUDAD DE CHICLAYO

APROBACIÓN DE LA TESIS

_____

Dra. Cabrera Cabrera Xiomara

Asesora Metodológica

_____

Dr. Robinson Barrio de Mendoza Vasquez

Presidente del jurado de tesis

_____	_____
Dra. Xiomara Cabrera Cabrera	Mg. Wilmer César Enrique Cueva Ruesta
Secretaria del jurado de tesis	**Vocal del jurado de tesis**

DECLARACIÓN JURADA DE ORIGINALIDAD

Quien suscribe la **DECLARACIÓN JURADA**, soy **egresado (s)** del Programa de Estudios de **escuela profesional de derecho** de la Universidad Señor de Sipán S.A.C, declaro bajo juramento que soy autor del trabajo titulado:

Modificación legislativa de la ley 30096 de delitos informáticos para su eficacia contra la ciberdelincuencia en la cuidad de Chiclayo.

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

En virtud de lo antes mencionado, firman:

Roman Cruz, Eucario Hector	DNI: 21140252	

Pimentel, 25 de enero del 2023.

Dedicatoria

A Dios por su infinita misericordia y amor, por bendecirme con sabiduría e inteligencia para que este camino sea mucho más fácil.

A mi familia, por ser las personas leales, quienes con amor y comprensión superior entender cada una de mis ausencias en momentos especiales, quienes siempre están para mí, en los buenos y malos momentos.

Agradecimiento

A todas aquellas personas quienes han estado a mi lado, mi familia y amigos.

A los docentes y asesora metodológica, Dra. Xiomara Cabrera, quien siempre estuvo pendiente y con responsabilidad asesoró mi investigación.

Resumen

La investigación definió la realidad problemática, caracterizando los antecedentes del problema. Su objetivo propone una modificación legislativa de la ley 30096 de delitos informáticos para lograr su eficacia contra la ciberdelincuencia. Se fundamentó teóricamente en doctrina sobre delitos informáticos; diagnosticándose el estado actual de la ciberdelincuencia. El estudio tiene un enfoque mixto, el instrumento de recolección de datos fue el cuestionario, aplicado a 20 Abogados especialistas en Derecho Penal. Los resultados mostraron que son diversos los delitos que se vienen cometiendo, y que no se encuentran correctamente regulados jurídicamente. Se llegó a concluir que, delitos informáticos son aquellas actividades ilícitas que son cometidas haciendo uso de una computadora u cualquier aparato electrónico conectado a una red de conexión, los cuales para el derecho se comprenden como elementos físicos. Estos delitos se caracterizan por tratarse de conductas que son realizadas en tiempo récord y de una forma muy fácil, cuyo único medio para poder ejecutarlas son los medios informáticos y que no necesariamente el delincuente está en el lugar donde se encuentra la persona o la entidad afectada, sino que no es necesaria la presencia física dicho, así estos delitos buscan florifera la identificación y la persecución de los mismos. Finalmente, se ha registrado que, la norma vigente presenta vacíos legales donde los ciberdelincuentes cometen actos ilícitos, los cuales quedan en muchas ocasiones impunes, siendo necesario que los delitos de daños informáticos puedan reformularse desde nuevos principios integradores.

Palabras clave: Delitos informáticos, ciberdelincuencia, delitos computacionales, principios.

Abstract

The investigation defined the problematic reality, characterizing the antecedents of the problem. Its objective proposes a legislative modification of Law 30096 on computer crimes to achieve its effectiveness against cybercrime. It was theoretically based on computer crime doctrine; diagnosing the current state of cybercrime. The study has a mixed approach, the data collection instrument was the questionnaire, applied to 20 lawyers specializing in Criminal Law. The results showed that there are various crimes that have been committed, and that they are not properly regulated by law. It was concluded that computer crimes are those illegal activities that are committed using a computer or any electronic device connected to a connection network, which by law are understood as physical elements. These crimes are characterized by being conducts that are carried out in record time and in a very easy way, whose only means to execute them are computer media and that the offender is not necessarily in the place where the person or entity affected is, but said physical presence is not necessary, so these crimes seek to identify and prosecute them. Finally, it has been recorded that the current regulation presents legal loopholes where cybercriminals commit illicit acts, which often go unpunished, making it necessary for the crimes of computer damage to be reformulated from new integrating principles.

Keywords: computer crimes, cybercrime, computer crimes, principles.

Índice

I. INTRODUCCIÓN

El mundo ha evolucionado de manera vertiginosa en todos los ámbitos. El avance de la tecnología ha traído muchos beneficios en esta evolución del mundo en el que vivimos; esta permite la interconectividad con la humanidad entera y sin fronteras, generando el desarrollo profesional, intelectual e industrial a gran escala y sin detenimiento a futuro. Para Flores et al. (2017) esta evolución es parte la globalización y ha influenciado en diferentes ámbitos originando nuevas formas de desarrollo social.

Dentro de este avance ha sobresalido las TIC (Tecnologías de la información y Comunicación), que sin complicaciones ha alterado el orden de la vida humana. Hizo del hombre una vida más fácil para la intercomunicación con sus similares del planeta Tierra. Alimentó de manera sobrecargada la información y sin límites en todos los campos del conocimiento, siendo un elemento importantísimo para la investigación. En Latinoamérica, Quiroga et al. (2019) las TIC tienen beneficios potenciales incluyendo habilidades motoras y que representan el aprendizaje de calidad.

Sin embargo; acompañando a las ventajas contrajo consigo una serie de desventajas para la humanidad, como las TIC que han sido empleadas para actos delictivos, empleando como herramientas para los delitos cibernéticos, las redes de internet. Para Fernández y Vargas (2018) en el Perú, los delitos informáticos son una ocurrencia y problemática reciente que conlleva a cometer ciberdelitos y aprovechado la desventaja de la Policía que no cuentan con habilidades para contrarrestarlos.

Los ciberdelincuentes emplean diversos métodos mediante la red de internet como el phishing, es decir, robar contraseñas o números de tarjetas usando correos electrónicos falsos de organizaciones reales y oficiales. También existe el ciberbulling o acoso escolar y el grooming o ciberacoso sexual a menores.

Pero ¿Qué se entiende por ciberdelincuencia? Se podría decir que es la actividad que tiene como objetivo atentar contra la seguridad e integridad de las personas o entidades privadas o públicas, obteniendo datos e información personal y privada para cometer actos de fraude mediante el uso de las redes de internet. También se

puede considerar ciberdelincuencia a los actos de delitos informáticos como la suplantación de identidad, el acoso sexual, el fraude o estafa. Para esto, por ejemplo, utilizan los malware o virus cibernéticos para infectar o instalarse en los ordenadores y extraer información o en el peor de los casos, dañar el ordenador. Para Fernández y Vargas (2018) el malware, en el Perú es uno de los delitos más comunes y, señala como ejemplo que mediante un phishing que supuestamente provenía del Banco de Crédito del Perú para robar información de los usuarios.
Estos delitos informáticos en el Perú son condenados desde el 22 de octubre de 2013 con la promulgación de la Ley 30096 “Ley de delitos informáticos”.

En Chiclayo existe un alto índice de delitos cometidos a través del uso de las tecnologías de información y comunicación. Y muchas de ellas quedan impunes, hasta la actualidad son pocas las conductas de este tipo que son sancionadas penalmente.

En el Estado Peruano no existe una norma jurídica que especifique los tipos penales que definen dichos delitos, estos son más frecuentes en las redes sociales donde actúan una serie de modalidades que afectan a la sociedad en general. La norma vigente presenta vacíos legales, los cuales quedan en muchas ocasiones impunes, siendo necesario que los delitos de daños informáticos puedan reformularse desde nuevos principios integradores.

1.1. Realidad Problemática

La aparición de las TIC (Tecnologías de la Información y Comunicación) ha generado diversos cambios en la comunidad nacional e internacional que ha generado la creación y aparición de diversas redes de comunicación, las cuales se encuentran conectados en los diversos países por lo que las personas pueden comunicarse entre sí dos de ese modo se dice que las nuevas tecnologías han facilitado difundir la cultura y la forma y estilo de vida de las personas. Además de esto, la tecnología ha contribuido, en gran medida, a la transformación y modernización de la industria y de las instituciones, alterando, casi por completo, nuestra forma de entender la vida, haciéndonos, en el proceso, dependientes de ella. Sin embargo, aunque la evolución de la sociedad a las nuevas tecnologías ha sido algo positivo, son muchas las incógnitas e incertidumbres que ésta suscita, sobre todo tras la aparición de internet, donde el ciberespacio se ha convertido el escenario perfecto para una nueva forma de criminalidad; la ciberdelincuencia.

La ciberdelincuencia está presente en todas las manifestaciones de la vida cotidiana, tanto en el ámbito público como en el privado. Según su desarrollo, se comprende que ha ido ampliando en las diversidades formas de ejecutar los crímenes es así que la naturaleza de estos se ha perpetuado a través de la red donde se destacan principalmente la ejecución de delitos de índole sexual, de naturaleza económica, política, resaltando así el ciberacoso o el bullying entre otros ilícitos. Este tipo de delitos que se cometen en este espacio no conocen fronteras, y es un delito que lo encontramos vigentes en todos los países, en algunos con una tasa mayor que en otros.

Por ejemplo, en España, según el Observatorio de Delitos Informáticos en el año 2019 se suscitaron cerca de 218302 ciberdelitos, entre los que más se destacan se encuentran, el fraude informático con 192375, las amenazas y coacciones con 12782 casos, la falsificación informática con 4275, acceso e interpretación ilícita con 4004, y en menor medida aquellos que afectan el honor, la libertad sexual y otros. Pero agrega que existen otras conductas que se vienen

produciendo a través de este, al que no debemos perder de vista, por el daño que vienen causando.

En el caso de Colombia el Tictac en su informe trimestral de ciberseguridad del 2020, sostiene que frente a la coyuntura nacional del COVID-19 se ha presentado un aumento de hasta un 37% de ciberataques. De hecho, los servicios y trámites del gobierno electrónico se han visto fuertemente afectados, ya que han sido usados por organizaciones criminales, para propagar malware (software malicioso) a través de diferentes medios. Las entidades gubernamentales más suplantadas son la DIAN 57%, Fiscalía General de la Nación 12%, organismos de tránsito 10%, Policía Nacional 9% y Ministerio de Salud 7%.

Por otro lado, la Fiscalía General de la Nación ha reportado cerca de 67 casos nuevos de delitos informáticos. Frente a esto, la Policía Nacional, confirmó que, en el primer trimestre del 2020, a pesar de presentar una disminución del 13% frente a 2019, el hurto por medios informáticos fue el ciberdelito más denunciado con 2.314 casos.

Seguido a esto, dada la contingencia, la suplantación de sitios web (Phishing) fue el segundo delito de mayor incremento, reportando 1.016 casos frente al 2019 (307 casos), es decir, un incremento de 240%. En tercer lugar, La violación de datos personales con 958 casos denunciados, reportando un incremento del 9% frente al 2019.

Al problema que se viene exponiendo no es ajeno el Perú, según la División de Investigación de Delitos de Alta Tecnología (Divindat) de la Policía registró 3,012 denuncias de fraudes electrónicos, pornografía infantil, suplantación de identidad y otros delitos informáticos durante el 2019. Así la mayor cantidad de denuncias se concentra en el delito contra el patrimonio a través de los fraudes informáticos y sus subtipos alcanzaron 2,097 denuncias durante el 2019. Esta cifra se elevó en más de 8% con respecto al 2018, que cerró con 1928 casos. Según las estadísticas presentadas Se comprende que el mayor índice de denuncias ha

recaído en aquellas acciones que se cometen en contra del patrimonio las cuales se Ejecutan a través del fraude informático y los diferentes subtipos delitos que se cometen al respecto tal es así que la afectación al patrimonio alcanzó alrededor de 2,097 denuncias realizadas en el año 2019, mientras que para el año anterior se había identificado un 8% lo que quiere decir que conforme va avanzando los años las denuncias continúan incrementándose Pues en el 2018 se identificó 1928 casos de estos delitos.

De esta manera, se comprende que de la totalidad de 1641 denuncias, las cuales se habían registrado el tipo de acciones que se cometían eran las transacciones bancarias las cuales no eran autorizadas pues está se realizaban haciendo uso de las redes de internet. Además de que particularmente hubo 431 casos, cuya acción resaltante fue la compra fraudulenta y 25 quienes denunciaron sobre la clonación de tarjetas de crédito o de débito. Es de esa manera que las denuncias no han disminuido, sino que al contrario estos han continuado incrementándose y que además de ello las medidas o estrategias que utilizan los ciberdelincuentes continúan mejorando, es decir emplean nuevas herramientas digitales, tales como el software y otras plataformas que les permite poder delinquir en línea y tanto que de este último la categoría al respecto aumentó a 268 denuncias para el año 2019 mientras que un año anterior sólo se registraron 362.

Particularmente, el acoso sexual las estafas que se ejecutan en línea las diversas amenazas que son realizadas a través de mensajes de texto o redes sociales, llámese también extorsión son parte de las conductas que se ejecutan con gran frecuencia. Entendiéndose que, la suplantación de identidad se ha convertido actualmente en una amenaza digital muy frecuente en la realidad peruana. Pues registró en el año 2019 247 casos mientras que otros ilícitos, tales como las proposiciones a los niños, niñas y adolescentes cuyos fines son sexuales lo vienen realizando de manera digital haciendo uso precisamente de las redes y resalta la pornografía infantil sobre estos últimos se han registrado alrededor de 237 casos durante el mismo año.

En el caso de Chiclayo el problema es similar, existe un alto índice de delitos cometidos a través del uso de las tecnologías de información y comunicación. Y muchas de ellas quedan impunes, hasta la actualidad son pocas las conductas de este tipo que se sancionadas penalmente. Frente a ello conviene modificar la Ley 30096 de delitos informáticos para lograr su eficacia contra la ciberdelincuencia.

1.2. Trabajos Previos

Internacionales

Espinosa (2019) desarrolló una investigación denominada “Ciberdelincuencia. Aproximación criminológica de los delitos en la red”, para cual utilizó un enfoque cualitativo, y tuvo como objetivo estudiar el avance las TIC y las consecuencias que esto ha generado en la seguridad jurídica. En los resultados del estudio se identificó que la ciberdelincuencia es un fenómeno que amenaza a la sociedad, puesto que la tecnología se ha convertido en un medio principal para la creación de dispositivos o mecanismos que permiten la transmisión de datos personales por los mismos ataques de origen informático. En las conclusiones ha manifestado que la tecnología ha contribuido en la comunicación de las personas sin importar la ubicación donde se encuentren, pero ello también ha contribuido al surgimiento de una serie de nuevas formas de criminalidad, lo que se conoce como ciberdelincuencia, ello debido a las deficiencias normativas que existen sobre la protección de los datos en las actividades de la red.

Fernández, Muñoz y Cuevas (2019) realizó un artículo denominado “Perfil psicosociológico en el ciberdelincuente”, el cual tuvo como objetivo el procurar una clarificación de los términos como ciberdelincuencia, cibercrimen, ciberdelito y ciberterrorismo, así como exponer las cualidades psicológicas más sobresalientes de estos fenómenos y las posibles clases de delincuentes según sus categorías correspondiente, para lo cual se empleó una metodología de búsqueda bibliográfica general hasta la fecha actual 2019, incluyéndose en el proceso palabras claves.

En las conclusiones del estudio se ha podido identificar que el internet se ha convertido en un espacio perfecto para la implantación de la ciberdelincuencia y el ciberterrorismo debido a que estos dos tipos de modalidades no se encontrarían regulas por ningún tipo de leyes bien definidas. En otras palabras, hasta la actualidad resulta complejo detallar el perfil preciso de los ciberdelincuentes y los ciberterroristas debido a que la información encontrada por el investigador solo ayuda para brindar una simple descripción de características generales e imprecisas, lo cual es insuficiente para controlar o impedir la actividad de estas personas en el internet.

Moragas y Pascual (2019) ha desarrollado una investigación titulada “Las tecnologías de internet, un riesgo para empresas y ciudadanos”, mediante el cual buscó analizar cada uno de los sucesos y sus consecuencias con el fin de poder establecer una clasificación y, a partir de ello, encontrar posibles soluciones comunes o maneras de evitar todos los riesgos de la ciberdelincuencia por el uso de las tecnologías de Internet conlleva, debido a que cualquier acción realizada en la red se transformaría automáticamente en pública siendo necesario prestar atención a todo lo que se publica en internet a quienes damos el ingreso a acceder a nuestra información.

En los resultados de información de la investigación se obtuvo que la Directiva de la Unión Europea tiene como objetivo principal el combatir la ciberdelincuencia fomentando la seguridad de la información mediante leyes nacionales más estrictas, penas más severas que las existentes y una cooperación entre autoridades que son responsables de investigar estos delitos. A pesar de que existen algunas medidas de seguridad estas no cubrirían del todo los riesgos existentes en el mundo, más aún si se vincula con la delincuencia informática pues como se sabe este tipo de delincuencia día a día encuentra alguna modalidad nueva de actuar.

Cruz, Jirón y Miranda (2018) realizó una investigación denominada “La ciberdelincuencia y su regulación jurídica en Centroamérica con énfasis en Costa Rica, el Salvador y Nicaragua”, a través del cual se buscó representar el interés

por Desarrollar más acerca del fenómeno social y jurídico, el cual envuelve a la ciberdelincuencia puesto que en la actualidad se hayan diversidad de vacíos jurídicos dentro de las legislaciones precisamente sobre el derecho informático en la investigación el objetivo planteado consistió en analizar de manera general a la ciberdelincuencia pero precisamente o particularmente está nadie se realizó en las legislaciones de los países de Centroamérica, empleando un método Comparativo/ Inductivo – Deductivo.

En las conclusiones ha manifestado que el delito informático es una tendencia criminal ejecutada en diversos países de Centroamérica, se trata de comportamientos que de manera frecuente se van desarrollando con mejores técnicas y habilidades esto se presenta con mayor frecuencia en países donde precisamente existen vacíos normativos y todo esto afecta de manera grave a los derechos de naturaleza constitucional de aquellas personas que han sido Víctimas de los ciberdelincuentes pues no existe ninguna normativa clara que la sancionen. Asimismo, en las conclusiones el autor señala que, el desarrollo y avances de la tecnología traen consigo la ejecución y mejora de nuevas formas de ejecutar los delitos.

Anguita (2018) desarrolló un artículo denominado “Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea”, con el objetivo de analizar las primeras gestiones realizadas por la UE en la lucha contra el cibercrimen y además se procederá a un seguimiento de las principales actuaciones y mecanismos que la Unión Europea ha ido desarrollando para combatir y proteger a sus ciudadanos y las empresas, si bien el internet a desatado una revolución tecnológica también ha desatado un problema para la represión de los delitos bajo la modalidad de la web que aun en la normativa no especifican claramente las sanciones para este tipo de delitos.

En las conclusiones indican que el trabajo de los estados miembros y la Unión Europea han sido muy significativos para frenar la delincuencia informática debido a que mediante sus instrumentos normativos, política o proyectos ha ayudado para que se frene el ciberdelito; sin embargo con todo el logro obtenido

este no sería suficiente para frenar la ciberdelincuencia puesto que aún existe mucho trabajo que realizarse mencionando que una de las dificultades principales reside en el funcionamiento de los sistemas informáticos y la estructura del internet pues de momento existe una generalizada libertad normativa la otra que el estado no ha precisado la normativa para ese delito cibernético.

Ávila (2018) ha desarrollado un artículo titulado “Los menores víctimas de la ciberdelincuencia. Medidas preventivas en el artículo internacional”, cuyo objetivo estuvo dirigido a la protección de menores de edad quienes han sido víctimas de ciberdelitos. Teniendo como objetivo el buscar determinar cuáles han sido las medidas de carácter preventivo que ha utilizado o que viene adoptando la organización de Naciones Unidas, entre otras organizaciones internacionales y principalmente los mismos estados con la finalidad de poder disminuir o al menos prevenir la ejecución de estos delitos que son ejecutados a través de las redes entendiéndose que en donde encontramos. Pues a los menores de edad como aquellas víctimas principales de estos delitos y que al respecto los estados deben de mejorar sus herramientas para lograr prevenir este tipo de acciones ilícitas.

En conclusión, se manifiesta que los niños niñas y adolescentes menores de edad son las principales víctimas, en tanto representan la población más vulnerable ante situaciones donde se ejecutan ese tipo de delitos a través de las redes, pues estos navegarían mucho más tiempo en internet, por lo deberían ser los padres quienes deberían controla el uso de las TIC en menores de edad, quienes debido a su falta de madurez física como mental suelen ser los primeros en caer en la ciberdelincuencia. Siendo necesario que se agreguen instrumentos internacionales centrados en respuestas y sanciones a un sistema más funcional para proteger a los menores de edad de estos delitos para el cuidado de uno de los valores más importante que tenemos como sociedades globales.

Trávez (2018) desarrolló un estudio denominado “La vulneración de los derechos constitucionales por la falta de tipificación de las nuevas conductas delictivas a

través de las tecnologías de informática y comunicación (TICS)", mediante el cual se buscó realizar una propuesta de reforma académica de ley al COIP sobre los delitos informáticos, que permita una mejor interpretación de los mismos independizándolos de manera singular con sus respectivas características, y la posterior incorporación de nuevas conductas. El objetivo planteado fue determinar la vulneración de derechos constitucionales por la falta de tipificación de las nuevas conductas delictivas a través de las TICs; empleando un enfoque cuantitativo con una metodología científico, deductivo, analítico sintético, jurídico e histórico.

En conclusión el autor menciona, es necesario una regulación y control de la información personal por el estado pues es, este, quien deberá velar por la seguridad siendo necesario supervisar y regular las instituciones nacionales como extranjeras; además que por la falta de políticas más estricta hacen que los medios de comunicación a través del internet, sea más fácil acceder a ella, de tal modo que los ciberdelincuentes se aprovechan de la facilidad de acceder a esta y realizar su delito de acoso, violación u otro delito como lo es el Grooming que una manera ilícita de actuar del delincuente para la cual no existe el control de la legalidad para poderlos penalizar como indicaría la ley.

Nacionales

Mori (2019) desarrolló un estudio denominado "Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de Lima, periodo 2008 al 2012", el cual tuvo como objetivo conocer las diferentes causas que han influido en la inexactitud del trabajo de los operadores de Justicia, quienes vienen realizando en las diversas investigaciones y en el juzgamiento de estos ilícitos penales en el modo de proteger penalmente ello. La investigación es de tipo descriptivo explicativo con un diseño no experimental; obteniéndose como resultados del estudio que los ciberdelincuentes poseen comportamientos denominados delitos de cuello blanco.

En conclusión se obtuvo que para una buena labor y trabajo de parte de los operadores de Justicia durante la investigación y el modo de ejecución del

juzgamiento de estos ilícitos penales y las medidas de cómo se protege penalmente la intimidad, es que el personal deber ser capacitado pues existe mucho desconocimiento de la tecnología, siendo necesario que las capacitaciones para los operadores del delito cibernético tiene que ser constante teniendo el conocimiento que la tecnología crece a pasos agigantados por lo que las modalidades de cometer delitos por internet también se reinventan día a día, pues debe existir competitividad en la investigación juzgamiento en los delitos informáticos en la protección penal de la intimidad.

Zorrilla (2018) en su estudio denominado “Inconsistencias y ambigüedades en la ley de delitos informáticos ley n° 30096 y su modificatoria ley 20171, que imposibilita su eficaz cumplimiento”, tuvo como objetivo determinar cuáles son las inconsistencias y las ambigüedades que existen en la ley de delitos informáticos, a fin de poder determinar las razones por las cuales se incumple. Es una investigación de naturaleza dogmática, de diseño no experimental, de corte transversal. En los resultados ha identificado que la informática contiene una serie de características, las cuales lo convierten en una herramienta idónea para el progreso de la humanidad.

Sin embargo, en la realidad está también contiene o representa un medio que facilita la ejecución de conductas ilícitas, las cuales atentan principalmente contra el patrimonio de las personas quienes son víctimas de este ilícito. Actualmente, la sociedad vive expuesta a una serie de atentados ilícitos debido a que la tecnología avanza precisamente la tecnología de comunicación y de información, es tanto que su información privada atiende muchas veces hacer violentada.

En las conclusiones, se ha establecido que en el Estado Peruano no existe una norma jurídica que especifique los tipos penales que definen en dichos delitos, pues estos son más frecuentes en las redes sociales donde actúan una serie de modalidades que afectan a la sociedad en general. La naturaleza de los delitos informáticos es virtual, en tanto la tipificación de los ilícitos suele ser confusa, ya que a nivel general existe poco conocimiento al respecto, así también se observa

en la realidad una serie de ausencia. En cuanto la cultura informática y al impacto que generan los delitos informáticos, además de que hay una responsabilidad del manejo de las tecnologías de la información. De esa manera, es que considera la necesidad de realizar una reformulación a la ley de delitos informáticos vigente, toda vez que existen diversas conductas que no son sancionadas por acogerse a los vacíos legales que presenta la misma norma. Además, que, esta modificatoria es necesaria teniendo en cuenta que la ciberdelincuencia es un delito muy moderno que se actualiza día a día.

Vilca (2018) ha desarrollado una investigación denominada “Los hackers: delito informático frente al código penal peruano”, el cual tuvo como propósito determinar Cuáles han sido los vacíos legales en la legislación penal peruano, precisamente en la comunicación electrónica comercial que se viene ejecutando hoy en día por las empresas y las cuales han sido Víctimas de los diferentes delitos informáticos en los últimos tiempos. Asimismo, la investigación empleada fue de tipo descriptivo con un diseño metodológico No experimental. Si bien la figura hacker se encuentra relacionada a la actividad ilícita de la ciberdelincuencia entendiéndose que como un autor de esta infracción o afectación que se le realiza a la privacidad o a la intimidad de una persona o inclusive de instituciones con la finalidad de poder realizar algún hecho ilícito de datos, dado a ello es necesario se proponga una regulación precisa para esta actividad que se realiza vía internet a fin de regular y proteger su actuación dentro del ordenamiento legal.

En conclusión, la falta de una información precisa sobre los límites de la tecnología informática es un factor crítico en el impacto de los delitos informáticos y la ciberdelincuencia en la sociedad por lo que es necesario realizar un análisis comparativo de legislación con otros países, debido a que en el Perú existirían vacíos legales frente a esta modalidad. Además, la generalidad de los delitos informáticos provoca únicamente la ignorancia de la sociedad sobre este tema a que es imperativa la existencia normas que especifiquen los hechos o actos que se realizan por un computador.

Tenorio (2018) ha desarrollado un estudio denominado “Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la ciberdelincuencia”, el cual tuvo como objetivo brindar el conocimiento de la importancia de la adhesión por parte del Gobierno Peruano al Convenio de Budapest sobre la ciberdelincuencia y las oportunidades que se deben explotar. Según menciona el autor en el Perú se ha registrado casos de ciberdelitos contra empresas, instituciones y personas que generaron considerables pérdidas económicas. Por ello la importancia de que el gobierno forme parte del convenio de Budapest ya que a través de este se pueda combatir el mal usos de las TICs ello bajo el esquema de esfuerzos y colaboración internacional.

En conclusión, tanto los ciberdelitos y las modalidades como se realizarían estas se encontrarían en una constante evolución desde la masificación del internet a inicios de la década de los 90; siendo necesario que adicionen la cooperación internacional en materia judicial. La cooperación es importante debido a que el sujeto activo no necesitaría estar físicamente en un determinado lugar en donde estará el afectado, pues la presencia de este no es física ya que emplearía la TICs. En otras palabras, lo que busca esta cooperación internacional es el brindar herramientas de derecho penal sustantivo y procesal, así como mejorar capacidades de cada Estado.

Herrera (2018) desarrolla una investigación denominada “Eficacia de la ley de delitos informáticos en el Distrito Judicial de Huánuco 2017”, cuyo objetivo consistió en demostrar el nivel de la eficacia de la ley de los delitos informáticos en el distrito judicial, con una investigación de enfoque cualitativo y cuantitativo con un alcance descriptivo. En el país a medida que crece y se conoce más sobre la informática en similitud avanza el uso de manera incorrecta de esta tecnología llegando a existir los denominados delincuentes informáticos quienes en varias ocasiones han podido librarse de la ley y burlarse de esta sin dejar rastro algo que los pueda comprometer, a pesar de que existe una ley que sanciona no sería suficiente eficaz, pues los delitos no cesan cuestionándose la eficacia de la ley cibernética.

En conclusión, estos nuevos delincuentes con conocimientos específicos tendrían que ser investigados con mayor inteligencia y a su vez el personal encargado deberá ser capacitado correctamente ya que por la falta de conocimiento deja de sancionar delitos cibernéticos. Además, en la misma normativa se hallan vacíos legales que no especificarían claramente los distintos delitos mediante esta modalidad, aprovechándose los ciberdelincuentes pues sus actos quedarían impunes, siendo necesario que los delitos de daños informáticos puedan reformularse desde nuevos principios integradores.

Mesa (2017) desarrolló una tesis sobre “La ciberdelincuencia y sus consecuencias jurídicas”, cuyo objetivo consistió en conocer las implicancias sociales respecto al uso frecuente de las TIC, siendo que este es uno de los factores utilizados por los delincuentes y en la rapidez en cómo estos vienen ejecutando las conductas ilícitas. En las conclusiones del estudio se ha identificado que existe deficiencias en su normatividad, ello porque existe mayores protocolos o reglamentación que regularice alianzas entre las fronteras y las facilidades para que puedan ejecutarse medidas de prevención y de ataque ante las conductas ilícitas. En otras palabras, la ciberdelincuencia se ha mostrado muy difícil de combatir, ello también porque la tecnología que usa la policía nacional no cuenta con la tecnología moderna que se requiere, ni los instrumentos jurídicos correctos y eficientes.

Sequeiros (2016) en su investigación titulada “Vacíos legales que imposibilitan la sanción de los delitos informáticos en el Nuevo Código Penal Peruano – 2015”, tuvo como propósito identificar los vacíos legales que existen en la normatividad penal vigente para conocer las razones que conllevan a la inaplicación de los delitos informáticos. Es una investigación de nivel básica, de diseño no experimental y desarrollado bajo un enfoque cualitativo. En los resultados se ha encontrado que la tecnología de información y comunicación ha aumentado y es un fenómeno creciente, pero a su vez la ciberdelincuencia continúa avanzando y a medida que la tecnología avance, las modalidades de la delincuencia también se ven mejoradas, lo que conlleva a que resulten poco difíciles de ser sancionadas.

Finalmente, en las conclusiones manifiesta que la falta de informaciones sobre los límites que pueda contener la tecnología, así es que en realidad se tiene el comercio electrónico a través del cual muchas personas han sido víctimas de robos, para lo cual el sujeto activo invierte una serie de formas para la ejecución de los actos ilícitos. Siendo que estamos ante una realidad jurídica muy deficiente para este de tipo de conductas, cuyas modalidades son modernas y tienden a ser cambiantes frecuentemente, surge la necesidad de modificar la normatividad vigente, ello para evitar la impunidad en este tipo de delitos, donde los bienes jurídicos que se afectan son diversos.

1.3. Teorías relacionadas al tema

1.3.1. Fundamentación teórica de los delitos informáticos

1.3.1.1. Delitos informáticos

La sociedad contemporánea se ha adaptado rápidamente a la informática, lo cual es de gran ayuda en el desarrollo de las actividades del ser humano. Según su naturaleza jurídica, este se comprende como falsificaciones informáticas, las cuales se ejecutan mediante la introducción y supresión de datos informático. Se conceptualiza como el fraude informático que introduce, altera o borra datos, sea por interferencia en los sistemas informáticos. Sin embargo, en la realidad se ha observado que, la delincuencia informática se desarrolla al mismo tiempo que las TIC avanzan, puesto que los delincuentes cibernéticos lo ven como un beneficio a su favor, ya que a través de ello alcanzan estrategia, capacidades y habilidades para poder cometer sus ilícitos.

Las palabras “delitos informáticos” está relacionada directamente con el internet y sus beneficios que aporta a la humanidad, de modo que estos se refieren a las actividades ilícitas que son cometidas haciendo uso de una computadora u cualquier aparato electrónico conectado a una red de conexión, los cuales para el derecho se comprenden como elementos físicos (…) Este tipo de conductas

tienen alcances a delitos como fraudes, robos, chantajes, falsificación y malversación de fondos públicos (Alcívar, Domenech y Ortiz, 2015).

Dicho de otra manera, el constante avance tecnológico que enfrenta la sociedad constituye una forma de evolucionar medios y herramientas para la ejecución de conductas ilícitas que utilizan como medio principal la tecnología. Este tipo penal recoge una serie de actividades, así es que el Convenio de Ciberdelincuencia del Consejo de Europa lo ha definido como uno de los delitos o una forma de especificar diferentes actos que tienen como finalidad atacar la privacidad, la integridad y la disponibilidad que presentan los sistemas informáticos, las redes de conexión y todos aquellos datos informáticos, ya que a través de las actividades ilícitas es que se comete una serie de abusos de derechos.

Entre las características principales de esta figura es que se trata de delitos que son muy difícil de demostrar, de modo que las pruebas o medios probatorios resultan inalcanzables, además, se caracterizan por tratarse de conductas que son realizadas en tiempo récord y de una forma muy fácil, cuyo único medio para poder ejecutarlas son los medios informáticos y que no necesariamente el delincuente está en el lugar donde se encuentra la persona o la entidad afectada, sino que no es necesaria la presencia física dicho, así estos delitos buscan florifera la identificación y la persecución de los mismos.

Es conocido también según su actividad informática como un Sabotaje informático entendiéndose que todas las acciones que se cometen tienen como finalidad ejecutar fines que persigue su actividad generando daños en el Hardware o en el software de un sistema. Los daños que puede generar son múltiples entendiéndose que sus herramientas o estrategias de aplicación son cada día más modernas. Si bien es cierto no necesita que la gente activo este en el lugar físico a quién se está afectando sino más bien puede hacerlo de manera virtual por su único medio que requiere para la ejecución de las conductas ilícitas es una computadora y una red de conexión sin embargo las conductas que este realiza si generan daños físicos Asimismo genera daños lógicos valga sé decir aquellos que derivan del resultado de la pérdida de la

ocultación O la alteración que han sufrido los datos informáticos de un determinado ordenador (Herrera, 2018).

Son diversas las manifestaciones de este tipo penal es así que por ejemplo se encuentran los delitos informáticos contra la privacidad e intimidad de la persona los cuales están dirigidos precisamente a dañar ese aspecto del ser humano lo que significa que se hace uso indebido de información es de carácter confidencial o de contenidos netamente personales o familiares y este tipo de conductas tiende a agravarse cuando la víctima es un menor de edad.

Según la finalidad de los delitos informáticos se sobreentiende que se trata de un instrumento o un medio donde se cometen acciones criminales haciendo uso de la computadora y de una red de conexión tales como la adulteración de cheques tarjetas de crédito el desvío de activos y pasivos en empresas privadas o públicas del mismo modo se cómo te cometen actividades Cómo es la premeditación o la simulación de delitos frecuentes como el fraude se sustrae o se altera informaciones que forman parte del plano íntimo del ser humano así también se Ase adulteración de informaciones de entrada como de salida se hace uso de programas que no se encuentran autorizados o que no tienen licencias y es de esa manera que se pueden cometer una serie de actividades con sólo utilizar como herramienta una computadora y tener acceso a una conexión de internet (Calderón, 2010).

Todas esas conductas se van actualizando y las herramientas o estrategias del sujeto activo también son frecuentes A Cambio toda vez que el avance de la tecnología trae también la adecuación de nuevas modalidades de ejecución de este tipo de ilícitos penales.

1.3.1.2. Sujeto activo

El sujeto activo en los delitos informáticos es aquella persona que se encarga de realizar las conductas que se encuentran descritas en el tipo penal en este caso puede ser cualquier persona que comete un tipo de delito y que, además, se caracteriza por poseer conocimientos especializados en el manejo de sistemas

informáticos. De manera que, no estamos ante la presencia de un delincuente común, sino ante la presencia de un delincuente especialista. Las personas que cometen este tipo de delitos hacen uso de las nuevas tecnologías y son expertos en actividades ilícitas relacionadas a las redes informáticas

Las características que posee el sujeto activo son netamente especiales que no se encuentran dentro del perfil de un delincuente común, pues este sujeto activo posee capacidades y habilidades actuando con total conocimiento y experiencia ante el manejo de los sistemas informáticos y actúa desde lugares estratégicos. Este tiene opciones para poder realizar mejoras ensayos sobre las próximas actividades que quiera realizar, es así que va mejorando sus estrategias y modalidades de ejecución y no se ve expuesto ante alguna amenaza física, toda vez que no hay ninguna relación física con su víctima, pues éste se caracteriza por actuar bajo el anonimato (Trávez, 2018).

1.3.1.3. Sujeto pasivo

En los delitos informáticos el sujeto pasivo está compuesto por aquellas personas que han sido Víctimas de una conducta delictiva, la cual utilizó como medio la computadora y las redes de conexión o cualquier otro equipo de cómputo. El sujeto pasivo puede ser una persona natural o una persona jurídica, incluso puede ser privada o pública. Las víctimas de este tipo de ilícitos o actos criminales pueden estar a larga distancia de los sujetos activos, toda vez que el sujeto pasivo no tiene o no es expuesto ante el actuar del sujeto activo; es decir, este último no puede someterlo a ningún tipo de violencia física o amenaza, sino que la víctima qué es el sujeto pasivo tiende a conocer sobre los hechos ocurridos que han atentado contra su patrimonio o según el bien jurídico afectado tiempo después de realizado este.

La doctrina lo define al sujeto pasivo como aquella víctima del delito quien es perjudicado directamente por la ejecución de las actividades criminales que realizan los sujetos activos. En la convención americana de Derechos Humanos en su Artículo 25 ha establecido que el Estado tiene la obligación de garantizar una protección judicial a aquellas Víctimas de delitos informáticos, valga decir

qué el e sujeto pasivo como víctima tiene el deber de exigir protección del Estado. De ese modo, queda claro que el sujeto pasivo es la víctima del delito informático (Bayardo, 2019).

Dicho de otra manera, se trata de aquel sujeto sobre el cual recae la conducta sea de acción u omisión que ha realizado el sujeto activo, como se indicaba en líneas arriba está puede ser personas naturales, instituciones bancarias, instituciones de naturaleza militar, gobiernos locales, gobiernos regionales, gobiernos nacionales e incluso gobiernos internacionales.

Como responsable o titular del bien jurídico es que posee de todas las facultades jurídicas para poder exigir la protección judicial ante la comisión de este tipo de actividades y precisamente el sujeto pasivo se caracteriza por descubrir la comisión ilícita cuando está ya ha ocurrido y ello es en su frecuencia por el desconocimiento del modus operandi de los sujetos activos es de ese modo que el sujeto pasivo no puede realizar actividades preventivas para evitar la afectación de sus bienes jurídicos.

1.3.1.4. Tipos de Delitos Informáticos

Existe una gran gama de tipo de delitos informáticos, problema que es una consecuencia de lo difícil que resultan ser detectados, al que se a une las legislaciones deficientes para poner un alto a este tipo de conductas, dejando así que estos delitos se creen y se cometan por la capacidad técnica e imaginativa de quien busca hacer de la informática un instrumento para delinquir, es difícil e imposible alcanzar a describir concreta mente los tipos de delitos informáticos, ya que conforme avanza la tecnología informática ellos también se vienen creando, por lo que solamente nos queda a mencionar en líneas generales.

Los fraudes informáticos, el sabotaje informático, el espionaje informático, el robo o hurto de software, el robo de servicios, el acceso no autorizado a servicios informáticos, entre otros delitos, pero para esta investigación solo importan estos, ya que mayormente se enfocan a disminuir el patrimonio de los afectados.

El tipo de delito informático se configura de acuerdo a la finalidad y forma que usa el ciberdelincuente para lograr su cometido, aunque la gran mayoría parte de la interceptación de datos y afectación del software con la que opera una persona o entidad durante su actividad cibernética.

Cada uno de estos delitos descritos en líneas anteriores ha sido objeto de tipificación por nuestros legisladores mediante la ley 30096 (Ley de delitos informáticos), aunque se denota que hay ciertas deficiencias que pueden causar una mala aplicación de la norma, problema que no es más que reflejo de la falta de capacidad y orientación técnica para hacer frente a estos delitos. Entonces, esta norma presenta un erróneo uso de capacidad técnicas en informática a favor de la delincuencia, problema que se puede agravar al ver que en la realidad no es el que posee la capacidad técnica el comete el delito, sino más bien pone su servicio a favor de u tercero.

1.3.2. Fundamentos teóricos de la ciberdelincuencia

1.3.2.1. La Ciberdelincuencia

La ciberdelincuencia está relacionada con la criminalidad que se comete haciendo uso de las computadoras en tanto estamos ante un fenómeno exclusivo de la sociedad industrial parte de la globalización el cual surge en la era de la informática. La evolución de las TIC ha conllevado a que se ejecuten una serie de conductas delictivas. En tanto, la ciberdelincuencia consiste en la delincuencia informática que bien puede tratarse de diferentes tipos penales de conductas que resultan ser un peligro para los bienes o el patrimonio o el aspecto íntimo de una persona.

El convenio sobre ciberdelincuencia del Consejo de Europa del año 2001 ha establecido dentro de sus fundamentos que aquellos actos o acciones que estén dirigidas a tentar la confidencialidad la integridad y la disponibilidad de un sistema informático de redes y o datos informáticos así también se consideran a aquellos abusos y atentados que se cometen en contra de estos. Precisamente el artículo dos de este mismo convenio regula estos bienes jurídicos

entendiéndose aquí aquellas conductas como es el acceso la interceptación y la interferencia. Mientras que el artículo 9 considera a todos los delitos que se encuentran relacionados con el contenido valgas e indicar a aquellos que atentan contra la intimidad de la persona así por ejemplo la pornografía infantil y también otras conductas de apología del racismo y xenofobia la cual es realizada a través de las redes sociales.

Doctrinariamente se le conoce como un conjunto de actividades que tienen como propósito el perjuicio a los sistemas informáticos, datos y redes de conexión, dañando así a personas naturales, personas jurídicas, privadas y públicas. Sin embargo, se dice que las conductas que ocurren son acciones criminales tradicionales, pero sus modalidades son modernas, ya que están a la vanguardia del avance de la tecnología. Entre sus características, se encuentran que son conductas que únicamente se cometen en el ciberespacio, para lo cual se utilizan los medios informáticos como principal herramienta para su ejecución. Esta problemática ha continuado creciendo de forma muy continua, significando este un riesgo eminente para la sociedad, inclusive las diferencias conductas que se cometen son consideradas como delitos de segundo milenio.

Estas actividades ilegales tienen como fin el acceso a sistemas públicos y privados. El Perú ha firmado el convenio de Budapest, cuyo origen fue en los países de Europa. Es así que, en el año 2019, la resolución legislativa 3913 regula ciertos parámetros en relación a este convenio. Sin embargo, es preciso mencionar que el código penal vigente en su Artículo 186 ya regula sobre aquellas conductas ilícitas, las cuales son realizadas haciendo el uso de transferencias electrónicas de fondos o la violación de cualquier clave secreta.

1.3.2.2. Bien jurídico en la ciberdelincuencia

Los bienes jurídicos de manera general tratan sobre la producción de cuidar y proteger los intereses que resultan vitales para el buen desarrollo de los individuos que forman parte de una sociedad es de esa manera que sus intereses cobran un reconocimiento jurídico esto en conformidad con la legislación penal, donde se ha precisado que la ejecución de un delito afecta

directamente a un bien jurídico por lo que de ningún modo resulta entendible que los delitos no lesión en bienes jurídicos puesto que la afectación se observa de manera directa. Además de que en los delitos de daño en compañía con la cosa que ha sido dañada o destruida se afectan también a la propiedad lo cual vendría a ser uno de los bienes jurídicos protegidos por la misma ejecución punible de los hechos (Reyes, 2015).

Según su naturaleza ocupan un lugar donde funcionan como límites y garantías dentro del derecho penal puesto que no debe olvidarse que estos bienes contienen o se caracterizan por funcionar como condiciones necesarias para el accionar del ser humano. Dicho de otro modo, esto trata de valores que la sociedad asume como principios importantes para poder asegurar su sistema de convivencia social particularmente, a esto se refiere derechos tales como la vida, el honor, la intimidad personal la libertad, entre otros derechos, llámese también bienes jurídicos, los cuales se encuentran protegidos para poder asegurarse que la afectación sobre estos no se ejecuten.

En este tipo de delitos de carácter informático el bien jurídico se concibe de forma conjunta y relacionada en primer lugar se encuentra las informaciones de manera general aquellas informaciones almacenadas tratadas y transmitidas a través de los diferentes sistemas de tratamiento automatizado de datos y en segundo lugar se encuentran todos aquellos bienes jurídicos que han sido afectados mediante este tipo de delitos tales como la indemnidad sexual la intimidad entre otros delitos (Villavicencio, 2014).

Es entendido también como como un conjunto de aquellas bases de datos o también entiendo ese como el producto final de aquel proceso informático automatizado por lo que dicho de otro modo, se constituiría como un bien autónomo, el cual constituye un valor económico y que tiene importancia, precisamente por ese valor de todas las informaciones lo cual lo ha hecho que se incorporen como bienes jurídicos tutelados.

Estos delitos tienen o poseen un patrón el cual consiste en el uso de los diversos medios electrónicos o cualquier otro dispositivo que sirvan para el uso en el ciberespacio es decir en las redes pues afectan bienes jurídicos de una forma más variada.

1.3.2.3. Delitos computacionales

El delito computacional se entiende como una conducta delictiva tradicional, la cual se ejecuta con diferentes elementos, los cuales se encuentran regulados en la legislación penal, pues se utiliza principalmente o se caracteriza precisamente por el uso de los medios informáticos, como las principales herramientas que facilitan la comisión de estos ilícitos penales, entre ellos funcionan con mayor frecuencia los delitos, tales como la estafa, los robos y los hurtos que se ejecutan a través del uso de la computadora, la cual se encuentra o se caracteriza por estar conectada a una red bancaria, ya que principalmente estos son los casos donde se tutela bienes jurídicos tradicionales, como es el patrimonio al igual que la arbitraria violación que se comete sobre los correos que atacan principalmente la identidad de la persona.

Se caracterizan porque persiguen un fin distinto a los delitos informáticos, por el modo el uso de la computadora, así como el sistema operativo que utilizan como medio principal para la ejecución de estos ilícitos penales tradicionales tales como los que se han citado anteriormente el robo y hurto la estafa entre

1.3.2.4. Delitos informáticos

Un delito informático Se comprende como una conducta delictiva donde la afectación va directamente a los bienes informáticos afectando, así de forma directa el software, ya que se introduce el virus, los cuales van a permitir acceder sin autorización a la computadora o es decir al software. Dicho de otra manera, todas las herramientas que son utilizadas por las cuales se utiliza las redes como uno de los fines principales para poder ingresar y acceder a las informaciones o bases de datos de dónde se va a obtener beneficios ilícitos afectando a su titular. Se trata de conductas criminógenas de cuello blanco (white collar crimes), ya que los sujetos activos son personas con especializados en la informática para

poder ejecutarlas, de modo que se entiende como acciones que son ejecutadas por oportunidad, ello por qué se realiza un aprovechamiento de las ocasiones, las cuales son creadas o que han sido identificadas dentro del panorama función y organización de los sistemas tecnológicos y económicos.

La finalidad que persiguen está enfocada a la introducción de los sistemas operativos, lo cual se realiza con la finalidad de alcanzar informaciones de estos soportes magnéticos para utilizarlos en beneficio de los ciberdelincuentes afectando a sus titulares, es decir este beneficio va directamente o lo recibe directamente el sujeto activo o los terceros ajenos a las empresas usuarias de los sistemas operativos. El objetivo de esto consiste en la afectación de bienes jurídicos lo cual se realiza a través de una introducción de forma ilícita a un sistema operativo.

1.3.3. Diferencia entre delitos informáticos y delitos computacionales

Los delitos informáticos se comprenden como aquellas conductas, a través de las cuales se ataca bienes informáticos, estos atacan directamente al software mediante la introducción de determinados virus sin que se permita la autorización del ingreso a la computadora. Mientras que, los delitos computacionales son conductas tradicionales, las cuales utilizan medios informáticos para poder ejecutar delitos como es el caso de robo, hurto, estafa, entre otros, pues se caracterizan por hacer uso de la computadora.

La diferencia entre estos delitos consiste en la finalidad de los mismos y medios que utilizan. Los delitos informáticos son conocidos también como crimen electrónico, pues utilizan el internet como un medio principal para poder dañar el ordenador, medios electrónicos y redes de Internet. Básicamente, en este tipo de delitos se trabaja con una programación haciendo uso del Internet es indispensable para el ejecución de estás conducta.

Mientras que, los delitos computacionales utilizan a los medios electrónicos, siendo que los bienes jurídicos afectados son aquellos tradicionales cómo es el

patrimonio y por consecuencia, la intimidad de las personas. Estos han sido utilizados como el medio de conductas, las cuales atacan directamente a la privacidad de la comunicación de las personas generando daños al patrimonio de las mismas. Este tipo de conductas son ejecutadas por organizaciones dedicadas a la delincuencia organizada. Los delitos informáticos se entienden como un acción típica, anti jurídica y culpable, convirtiéndose en un abuso informático parte de la criminalidad informática.

1.3.4. La prohibición de la analogía penal

El término analogía según Rivas (2019) consiste en la aplicación de una determinada norma a un supuesto que no se encuentra legalmente recogido por la norma. Sin embargo, presenta semejanzas a los supuestos que dicha norma comprende. (…) se trata de una figura que consiste en aplicar a un caso no regulado por la ley, pero con características semejantes a los que ella contempla, una norma extraída y existente en la propia ley o inclusive del propio ordenamiento jurídico en su conjunto (analogía iuris).

Esta figura está prohibida en las normas penales, es pues en esta área solo se permite la sanción de aquellas conductas que coincidan con el tipo penal previamente establecido y no otras parecidas, así tengan características de dos o más figuras delictivas, ya que al no estar reguladas carecerán de relevancia jurídica para el Derecho Penal. Esta prohibición es consecuencia necesaria del principio de legalidad, que se sustenta en la expresión latina: “nullum crimen sine praevia lege poenale” (No hay delito sin ley penal anterior).

Dicho de otra manera, la prohibición de la analogía se fundamenta más que todo en que le corresponde única y exclusivamente al legislador, por disposición constitucional, la función de crear delitos y penas. Por su naturaleza, se refiere a un proceso de comparación de dos cosas que, por la magnitud de la semejanza en sus características, resultan idóneas para ser calificadas como análogas. Pero en el ámbito jurídico esta guarda relación con los procedimientos argumentativos, los cuales permiten o facilitan el traslado de las soluciones que han sido previstas para determinados casos a otros diferentes que además no

están o no se encuentran regulados por la legislación jurídica, pero que sí presentan similitudes al primero puesto que comparten con igual o iguales características principales. Sin embargo, esta figura está claramente prohibida ara los casos penales (Montiel, 2013).

1.3.5. El Principio de Legalidad en el Derecho Penal

Al referirnos al principio de legalidad en el ámbito penal, nos estamos refiriendo a su vez a la idea de una correcta y debida investigación, juicio o procedimiento, pues claramente se establece que nadie será sometido a investigación, juicio o procedimiento, si previamente no han sido determinados y reglados por la ley; además siempre se debe tener en cuenta conservar y cumplir los derechos y garantías del imputado.

El principio de legalidad se constituye en la idea de que nadie de ninguna manera deberá ser sometido a un proceso imputándosele una conducta que previamente no ha sido descrito o prohibido por la ley penal; así también implica la legalidad de la sanción penal, lo que significa que no se podrá imponer al imputado una pena que no corresponde a la determinada por el legislador. En tanto que para el Derecho Penal el principio de legalidad establece que no existirá o no se calificara una conducta como delictuosa si previamente no hay un tipo penal que lo regule y por consiguiente tampoco habrá pena que pueda ser impuesta (Pérez, 2014).

Las sanciones que pueden ser aplicadas a un administrado también deben ser establecidas por una norma con rango de ley.

El Tribunal Constitucional ha citado en el Expediente Nº 6301- 2006-PA/TC que el principio de legalidad se contempla en ser una auténtica garantía constitucional de los derechos fundamentales de las personas, del mismo modo figura como un criterio rector en el ejercicio del poder punitivo del Estado de Derecho. De tal manera que este principio exige que la ley establezca que conductas son deberán ser consideradas como delictivas, pero además también requiere que las conductas prohibidas sean redactadas de manera clara y

concreta por la ley, no admitiéndose de ninguna forma la aplicación por analogía y el uso de cláusulas generales e indeterminadas en la tipificación de las prohibiciones.

Del mismo modo el Tribunal también se pronunció en el Expediente Nº 1182-2005-PA/ TC, seguido por Carol Luz Sáenz Contreras contra SENATI por la indebida aplicación de sanciones disciplinarias, mediante el cual ha este principio en materia sancionadora es el que impide que se pueda a una determinada persona atribuir la comisión de una falta, si esta no está previamente prohibida por la ley, a su vez impide que se le pueda aplicar una pena diferente a la establecida por la ley.

De tal modo que como lo ha expresado el Tribunal constitucional, el principio de legalidad impone el desarrollo de tres exigencias, primero, la existencia de una ley (lex scripta), segundo, la anterioridad de dicha ley al hecho sancionado (lex praevia), y tercero, la descripción en la ley de un supuesto de hecho estrictamente determinado (lex certa).

1.3.6. Marco legal

La ley vigente de delitos informáticos en su capítulo 2 al señalado a los delitos contra los datos y sistemas informáticos, precisamente en su Artículo 3 menciona sobre el atentado que se comete en contra de la integridad de los datos informáticos, básicamente es cuando el sujeto activo hace uso de las tecnologías de información para poder introducir borrar deteriorar o alterar datos informáticos.

En el capítulo 3 de la citada norma se regula sobre aquellos delitos que son cometidos contra la integridad y la libertad sexual, su artículo 5 regula sobre las diferentes proposiciones que suelen hacerse a los niños y adolescentes con fines sexuales, haciendo el uso de media la tecnología, así como la pornografía actividades sexuales bajo este medio.

En el capítulo cuarto se menciona los delitos que se cometen en contra de la intimidad y el secreto de comunicaciones, así también ahí se considera el tráfico ilícito ilegal de datos, la interceptación de los datos informáticos Y en el capítulo 5 se considera aquellos delitos informáticos que atentan contra el patrimonio, válgase decir, el fraude informático y en el capítulo 6 aquellos delitos contra la fe pública, básicamente en la suplantación de identidad.

La ley de los delitos informáticos no es precisamente aquella que se caracteriza por ser la más eficaz jurídicamente, ya que con el avanzar de la tecnología la ciber delincuencia sigue incrementándose. Es preciso añadir que la legislación penal no escapa de los problemas de improvisación y deficiencias de técnica legislativa de los que adolecen nuestros representantes en el Congreso de la República.

Pues, la tecnología de información y principalmente las telecomunicaciones han ido adquiriendo roles esenciales en la vida del ser humano, únicamente no en el ámbito personal, sino que también en el comercial, así como también en todas aquellas actividades propias de la Administración pública, por lo que también la delincuencia ha tomado las medidas para afectar los bienes jurídicos pero esto debido a que la Ley Nº 30096 tiene discrepancias con otras normas, toda vez que hay bienes jurídicos que se encuentran protegidos por otras figuras penales (Northcote, 2013).

En ese sentido, es precio mencionar que el Legislador con la finalidad de evitar la inaplicación de las normas penales, padecen de dos problemáticas, la primera se debe a un exceso de la regulación jurídica y otro es por defecto. Lo primero que se menciona tiene que ver con los tipos penales, los cuales contienen excesivos elementos para la configuración de estos y todo es todo esto ha generado que en la práctica la sanción resulte difícil, puesto que no se puede identificar de qué manera es que culmina el delito. En cuanto a la segunda sobre por defecto, esta regulación se denomina así porque genera situaciones cuando los tipos penales son demasiado generales sobre los cuales existe vacíos de modo que en la práctica el tipo penal no guarda relación con las conductas que

se realizan hoy las conductas ilícitas que son cometidos, de modo que muchas actividades ilícitas no han podido ser sancionadas por la misma ausencia o presencia de vacíos legales o dicho así porque los tipos penales son muy generales. En la práctica todo esto ha generado que muchos ilícitos no sean sancionados, ya que resulta difícil demostrar con certeza la ejecución de un ilícito penal.

Es preciso comentar o qué el artículo tercero de la norma antes indicada precisa que todas las personas que utilizan una tecnología de información o de comunicaciones que ha introducido borrado deteriorado alterado suprimido o ha hecho inaccesible datos de datos informáticos, así como también la norma regula esto se olvida o el legislador no ha considerado la parte donde debe establecer acerca del titular de las informaciones que han sido vulneradas o violentadas por lo que significa que existe un sujeto activo que ha borrado esa base de datos, en tanto estaría este incurriendo en un tipo de delito, a pesar que no exista ningún perjuicio pues se trata de su propia información.

Entonces vale aclarar que la problemática que enfrentan los tipos penales no solicitan la acreditación de los perjuicios con los cuales las personas ingresan sus datos en las diferentes bases ya sean bases propias o ajenas sino que estos también incurren en el delito ello muy a pesar de que puedan tener una autorización para realizar dicha conducta o que estos no causan ningún perjuicio con Estas actividades. Por lo que se comprende que muchas personas podrían suponer que la finalidad de la norma buscaría sancionar a las personas que borran modifican los datos de otras personas generando daños y perjuicios a otros es entonces que no es esto lo excepcional que expresa el tipo penal y como ya se ha precisado en párrafos anteriores la normatividad penal debe de ser aplicada de forma precisa sin ningún tipo de analogía ni interpretación excesiva o extensiva.

1.4. Formulación del Problema

¿Cuáles son las deficiencias de la ley 30096 de los delitos informáticos para su eficacia contra la ciberdelincuencia?

1.5. Justificación e importancia del estudio

La importancia de la investigación radica en que en este país aún no se han promovido políticas que contribuyan a solución el problema de la ciberdelincuencia. Esta investigación fue necesaria porque permitió revisar y analizar el marco legal sobre los delitos informáticos, a fin de analizar la eficacia y eficiencia del conjunto de acciones, programas y estrategias que hasta hoy se han implementado en el país y cómo están contribuyendo para frenar la ciberdelincuencia.

Esta investigación sirvió para brindar los mecanismos necesarios al sistema de justicia peruano para regular este tipo de delitos. Así como sirve para evitar que haya más víctimas de este delito, siendo la seguridad jurídica de la sociedad el principal beneficio de esta investigación.

Metodológicamente se desarrollaron nuevas teorías, las cuales aportarán a la investigación científica, es por ello que, con este estudio se desarrolló una propuesta legislativa que consistirá en una modificatoria a la legación penal, de tal manera que se pretendió adoptar nuevos delitos a fin de prevenir y combatir el cibercrimen, aunado a ella, se pretendió homogenizar la legislación conforme a los preceptos penales de otros países en delitos de la materia investigada.

Socialmente, contribuye con una solución práctica, la cual se reflejará con la disminución del índice de los diversos delitos que se cometen con el uso de las tecnologías de información y comunicación. En tanto, esta solución permitirá sancionar estas conductas contribuyendo a que no queden impunes.

1.6. Hipótesis

Si se modifica legislativamente la ley 30096 de delitos informáticos se logrará su eficacia contra la ciberdelincuencia.

1.7. Objetivos

1.7.1. Objetivo General

Proponer una modificación legislativa de la ley 30096 de delitos informáticos para lograr su eficacia contra la ciberdelincuencia en la ciudad de Chiclayo.

1.7.2. Objetivos Específicos

1. Fundamentar teóricamente los delitos informáticos en la doctrina.
2. Caracterizar los antecedentes del problema.
3. Diagnosticar el estado actual de la ciberdelincuencia en la ciudad de Chiclayo
4. Elaborar la propuesta de modificación legislativa.
5. Corroborar mediante consulta de expertos la modificación legislativa de la ley 30096 de delitos informáticos para lograr su eficacia contra la ciberdelincuencia en la ciudad de Chiclayo.

II. MATERIAL Y METODO

2.1. Tipo y diseño de la investigación

La presente investigación ha sido desarrollada bajo el enfoque mixto cualitativo-cuantitativo, entendiéndose que una investigación cuantitativa permite generalizar los resultados de forma más amplia y responde a un enfoque cualitativo, toda vez que se analizó marco legal y jurisprudencia. A través de este tipo de estudio se permite alcanzar un control sobre el fenómeno de investigación, puesto que se utiliza datos estadísticos que permitirán determinar el conteo y la magnitud del objeto de estudio. Hernández (2014) ha mencionado que, a través del enfoque cuantitativo el planteamiento del problema a estudiar ha sido específico y delimitado desde un inicio, así es que se puede entender como una investigación objetiva que tiene un patrón estructurado, para lo cual se realizó la construcción de teorías relacionadas a la investigación, además se utilizó el método deductivo.

Es de tipo Aplicada, propositiva por cuanto busca generar nuevos conocimientos o nuevas teorías, que en este caso se desarrollará una propuesta legislativa, la cual contiene una posible solución a la problemática identificada. Una investigación propositiva consiste en un proceso dialéctico que tiene como herramientas las técnicas y los procedimientos para poder realizar un diagnóstico y por consecuencia resolver un problema, para lo cual se va a generar nuevas teorías o normativas. Permite el desarrollo y además fortalecer las políticas vigentes.

Su diseño es no experimental descriptivo, toda vez que no se ha realizado ninguna manipulación de las variables, sino que se ha hecho uso del estudio de la problemática en su estado natural, la cual fue analizada a través de la observación empírica del propio investigador.

2.2. Población y muestra

La población es aquel conjunto de participantes pueden ser objetos fenómenos sucesos o comunidades sobre los cuales se va a recolectar datos, que para el caso la población está compuesta por Abogados especialistas en Derecho Penal del Ilustre Colegio de Abogados de Lambayeque. Mientras que la muestra es el sub

conjunto de la población. A través de esta se delimita la población y en la presente investigación se utilizó un método de selección, precisamente el no probabilístico intencional, mediante el cual se ha podido precisar el tamaño de la muestra aplicando ciertos criterios, como es la accesibilidad y la experiencia de los informantes. En tal sentido, la muestra en este estudio ha estado compuesta por 20 Policías de la División de Investigaciones de Delitos de Alta Tecnología (DIVINTAD) de la DIRINCRI – PNP.

2.3. Variables, Operacionalización

La presente investigación estudio las siguientes variables:

Variable independiente: Modificación legislativa de la ley 30096 de delitos informáticos, cuyas dimensiones fueron la exposición de motivos, la fórmula legal y los costos y beneficios, el efecto de la norma. De dimensiones lo que se estudió fueron los fundamentos de la norma, la modificación de la misma, los costos generados al Estado y los beneficios que contribuyeron a la sociedad.

Variable dependiente: la ciberdelincuencia, cuyas dimensiones fueron los delitos computacionales y los delitos informáticos. De tales indicadores se estudiaron el uso de los medios informáticos y el ataque a los bienes informáticos.

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

Métodos científicos

-Histórico –Jurídico
-Análisis –síntesis
-Jurídico –doctrinario
-Jurídico-comparativo
-Jurídico-descriptivo
-Jurídico-propositivo

Técnicas e instrumentos de recolección de datos

Las técnicas e instrumentos de recolección de datos en este estudio han resultado esenciales para poder alcanzar los objetivos de la misma, en tanto se han utilizado los siguientes:

Observación: Se utilizó en la realidad problemática desde donde se definió el problema de investigación

Técnica de campo: aquella a través de la cual se buscó obtener los datos estadísticos que posteriormente fueron analizados y presentados con sus respectivas descripciones. El instrumento utilizado fue el cuestionario, el cual estuvo compuesta por un número determinado de ítems, los cuales fueron elaborados para cada una de las variables.

Técnica documental: aquella a través de la cual se buscó obtener información para lograr la fundamentación del marco teórico y del marco metodológico. Para el caso fue necesario hacer uso del fichaje, precisamente el fichaje de resumen, comentario, textuales y las bibliográficas.

2.4.1. Validez y confiabilidad

La validez se refiere a aquel instrumento o herramienta que permite determinar el grado que mide una variable. Se trata más que todo de una situación compleja, puesto que debe alcanzarse en un instrumento la medición, el cual es aplicable representando así un medio o evidencia en la investigación.

En este caso se ha utilizado la validez de expertos, a través del cual se va a medir el grado del instrumento de las variables través de opiniones expertos sobre profesionales expertos en la materia lo cual va hacer una evidencia irrefutable, tal es así que Hernández (2014) mencionó que la validez de expertos es el principal instrumento de revisión expertos académicos.

Mientras que la confiabilidad se refiere al instrumento que este tiene que ser confiable, a fin de que pueda representar un estudio objetivo y de calidad. Entonces,

el nivel de la confiabilidad va depender del número de ítems que contiene el cuestionario.

2.5. Procedimiento de análisis de datos

El procedimiento de análisis de datos en esta investigación se inició con la codificación de los datos que fueron obtenidos con la aplicación del cuestionario, datos que son procesados en un programa estadístico (SPSS). Dichos datos se analizarán y presentarán sus descripciones correspondientes por cada una de las variables.

2.6. Criterios éticos

Los criterios éticos son aquellos principios que están relacionados con la ´ética que debe estar presente en toda investigación, y que es muy necesario más aún en investigaciones cuantitativas, como es el caso de la presente. A continuación, se señala los criterios utilizados:

*Consentimiento informado***:** es aquel mediante el cual se buscó el informar sobre sus derechos y deberes de las personas que participaron como muestra en el estudio.

*Confidencialidad**:*** aquel principio mediante el cual se le garantiza a los informantes la reserva y anonimato de sus datos personales, los cuales no serán expuestos, ello con la finalidad de poder lograr datos basados en la veracidad.

2.7. Criterios de rigor científico

Los criterios de rigor científicos son aquellos que tienen como propósito lograr la coherencia y correcta estructuración de una investigación. En el presente caso se han utilizado los siguientes:

Neutralidad: mediante este criterio lo que se pretende es asegurar que los resultados de la investigación, a fin de que estos no se inclinen hacia los intereses del investigador, sino que sean objetivos al propósito del estudio.

Valor de la verdad: mediante este criterio, lo que se busca es demostrar únicamente la veracidad de aquellos datos obtenidos con la aplicación del cuestionario, presentándolos a través del análisis de los mimos en comparación con la realidad problemática.

III. RESULTADOS

3.1. Resultados en Tablas y Figuras

Se aplicó un cuestionario a 20 Policías de la División de Investigaciones de Delitos de Alta Tecnología (DIVINTAD) de la DIRINCRI – PNP, con la finalidad de recolectar informaciones precisas que permitieran un mayor análisis sobre las deficiencias que enfrenta la ley 30096 de delitos informáticos para su eficacia contra la ciberdelincuencia.

El cuestionario estuvo compuesto por nueve (09) ítems, los cuales fueron elaborados para cada una de las variables.

Tabla 1

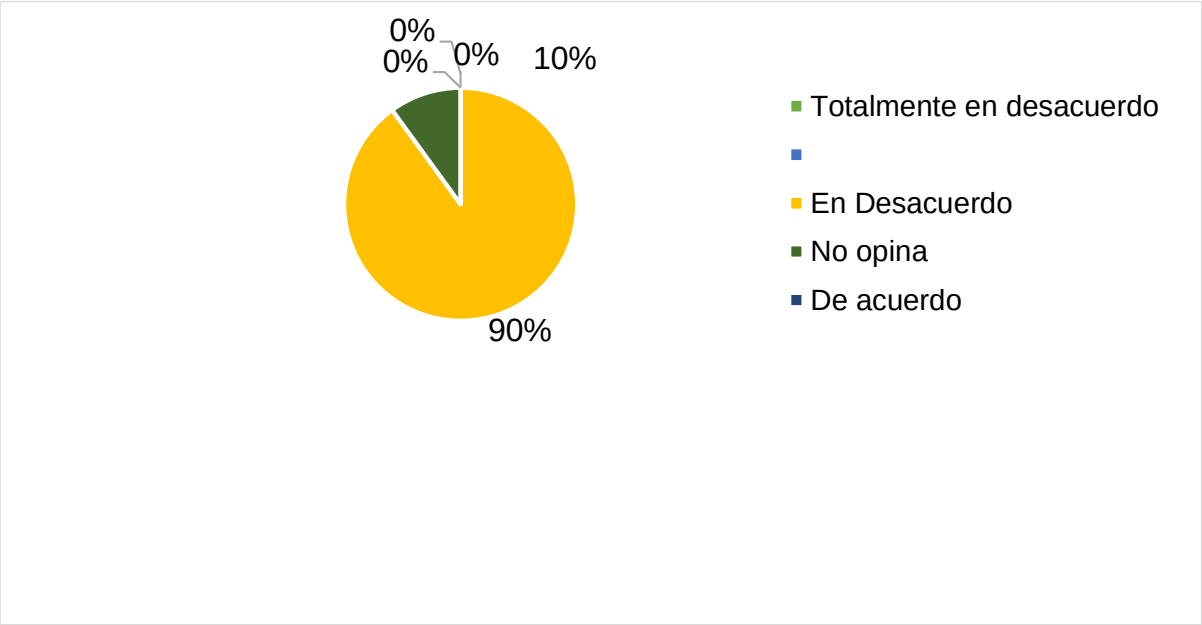
Tipificación del delito de acceso ilícito

Item	Cantidad	%
Totalmente en desacuerdo	**15**	**75**
Totalmente de acuerdo	1	5
En Desacuerdo	4	20
No opina	0	0
De acuerdo	0	0
Total	20	100

Nota: Fuente: Cuestionario 1 elaborado por el autor

Figura 1

Tipificación del delito de Acceso ilícito



Nota: En la figura se registra un 75% de respuestas que han manifestado estar totalmente en desacuerdo con que el delito de Acceso ilícito recogido en la ley de delitos informáticos Ley 30096 no se encuentra correctamente tipificado la conducta criminal, seguido de un 20% quienes indicaron que están en desacuerdo y un 5% de los encuestados ha señalado estar totalmente de acuerdo.

Tabla 2

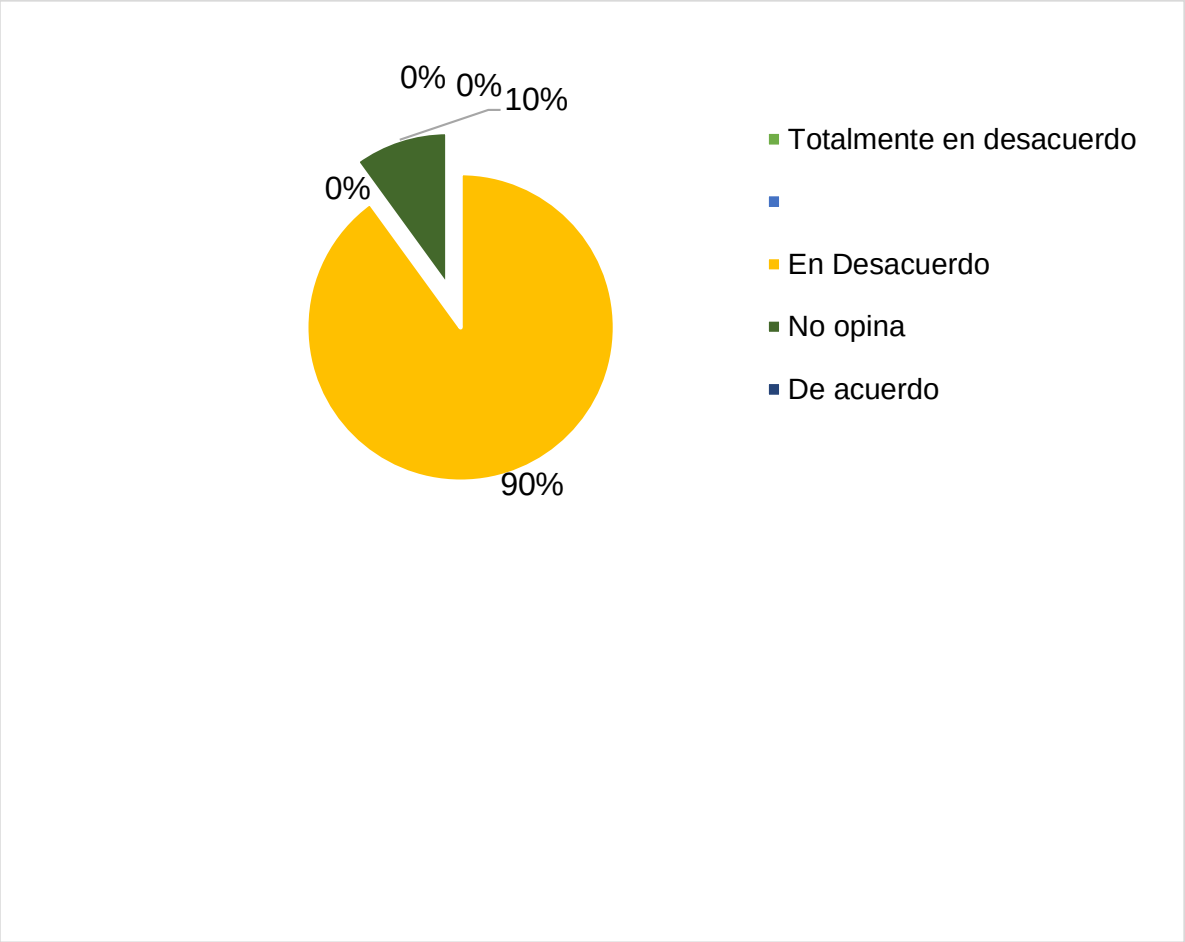
Tipificación del delito de Atentado a la integridad de datos informáticos

Item	Cantidad	%
Totalmente en desacuerdo	**1**	**5**
Totalmente de acuerdo	1	5
En Desacuerdo	13	65
No opina	4	20
De acuerdo	1	5
Total	20	100

Nota: Fuente: cuestionario 1 elaborado por el autor

Figura 2

Tipificación del delito de Atentado a la integridad de datos informáticos



Nota: Las respuestas muestran un 65% quienes han señalado que están en desacuerdo con que el delito de Atentado a la integridad de datos informáticos recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal, un 20% de ellos no ha opinado, un 5% señaló que está totalmente en desacuerdo y un 5% indicó estar de acuerdo.

Tabla 3

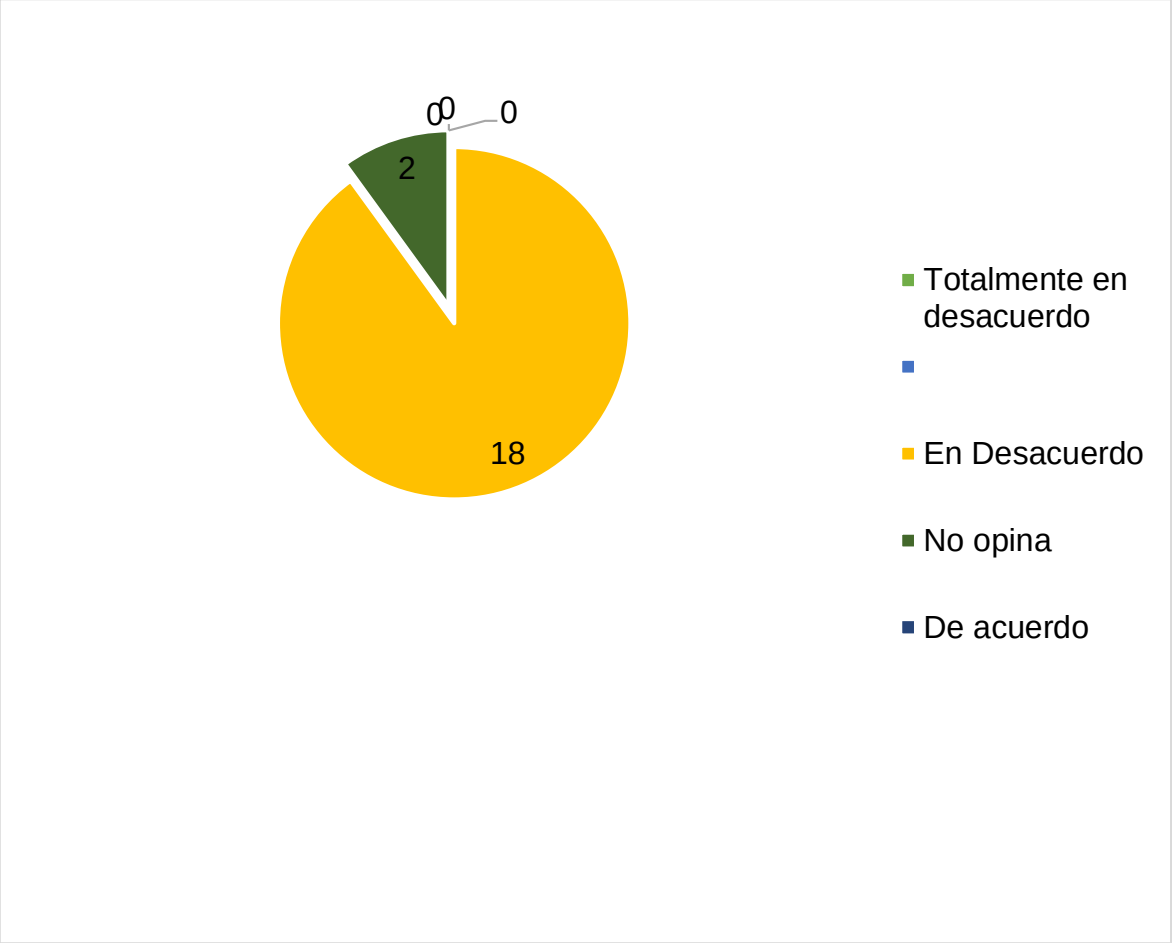
Tipificación del delito del delito de Atentado a la integridad de sistemas informáticos

Item	Cantidad	%
Totalmente en desacuerdo	**12**	**60**
Totalmente de acuerdo	0	0
En Desacuerdo	8	40
No opina	0	0
De acuerdo	0	0
Total	20	100

Nota: Fuente: cuestionario 1 elaborado por el autor

Figura 3

Tipificación del delito del delito de Atentado a la integridad de sistemas informáticos



Nota: Las respuestas muestran un 60% de los informantes quienes han señalado que el delito de Atentado a la integridad de sistemas informáticos recogido en la ley

de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal, seguido de un 40% quienes han manifestado que estan en desacuerdo.

Tabla 4

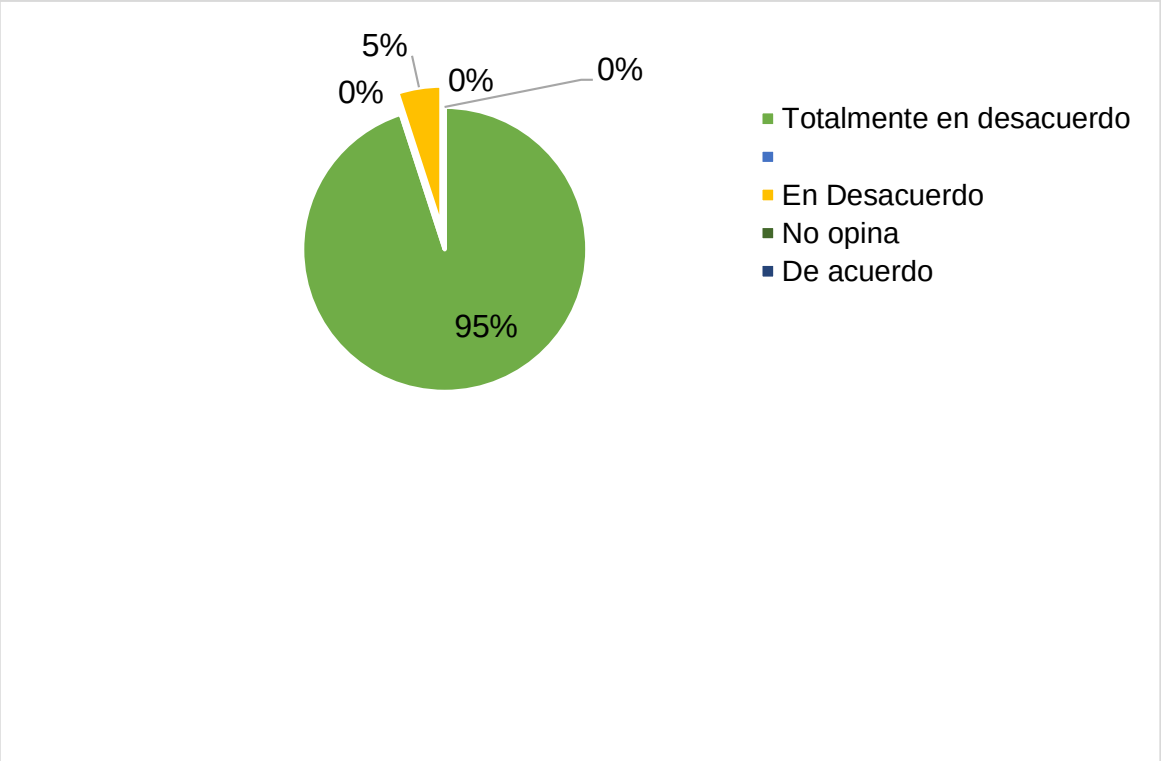
Tipificación del delito de Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos recogido en la ley de delitos informáticos

Item	Cantidad	%
Totalmente en desacuerdo	**19**	**95**
Totalmente de acuerdo	0	0
En Desacuerdo	1	5
No opina	0	0
De acuerdo	0	0
Total	20	100

Nota: Fuente: cuestionario 1 elaborado por el autor

Figura 4

Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos recogido en la ley de delitos informáticos



Nota: Las respuestas muestran a un 95% de los informantes quienes precisan que están totalmente en desacuerdo con que Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos recogido en la ley de delitos informáticos Ley 30096, se encuentren correctamente tipificado la conducta criminal y un 5% señaló que están en desacuerdo.

Tabla 5

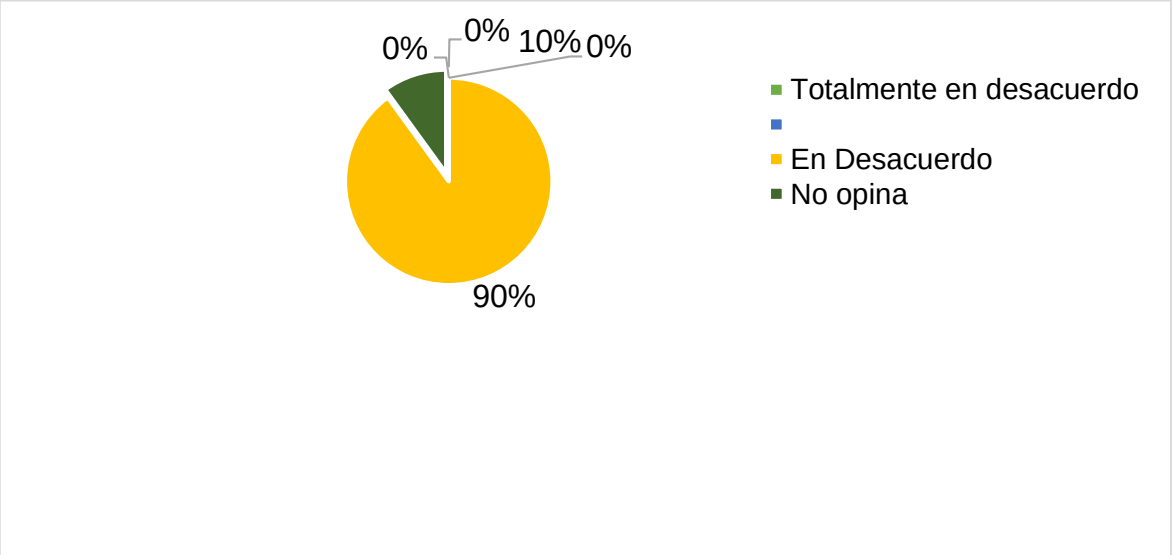
Tipificación del delito de Tráfico ilegal de datos

Item	Cantidad	%
Totalmente en desacuerdo	**14**	**70**
Totalmente de acuerdo	0	0
En Desacuerdo	3	15
No opina	3	15
De acuerdo	0	0
Total	20	100

Nota: Fuente: cuestionario 1 elaborado por el autor

Figura 5

Tráfico ilegal de datos



Nota: Las respuestas muestran a un 70% de los informantes quienes han indicado que el delito de Tráfico ilegal de datos recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal, seguido de un

15% los cuales señalaron estar en desacuerdo y otro 15% quienes no opinaron sobre la premisa consultada.

Tabla 6

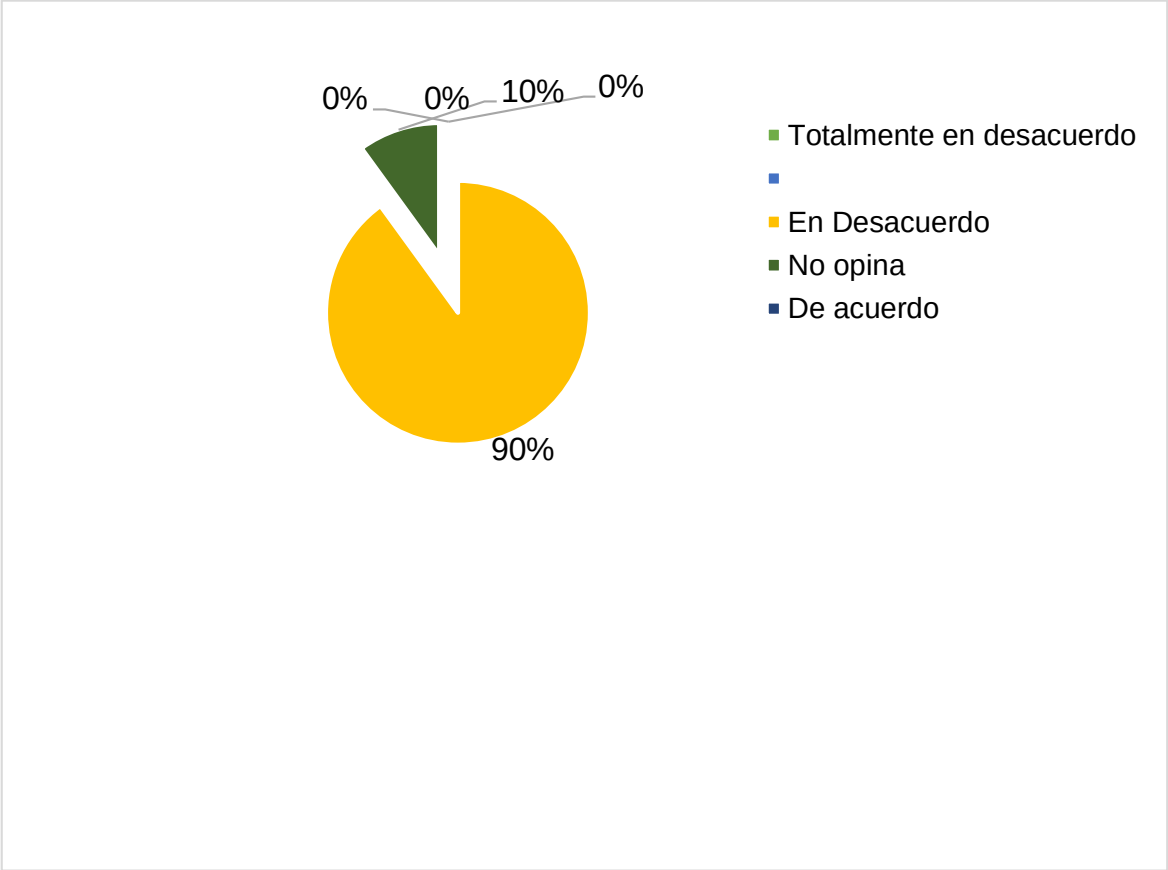
Tipificación del delito de Interceptación de datos informáticos

Item	Cantidad	%
Totalmente en desacuerdo	**2**	**10**
Totalmente de acuerdo	0	0
En Desacuerdo	18	90
No opina	0	0
De acuerdo	0	0
Total	20	100

Nota: Fuente: cuestionario 1 elaborado por el autor

Figura 6

Tipificación del delito de Interceptación de datos informáticos



Nota: Las respuestas muestran un 90% quienes han manifestado estar en desacuerdo con que el delito de Interceptación de datos informáticos recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal, seguido de un 10% quien indicó estar totalmente en desacuerdo.

Tabla 7

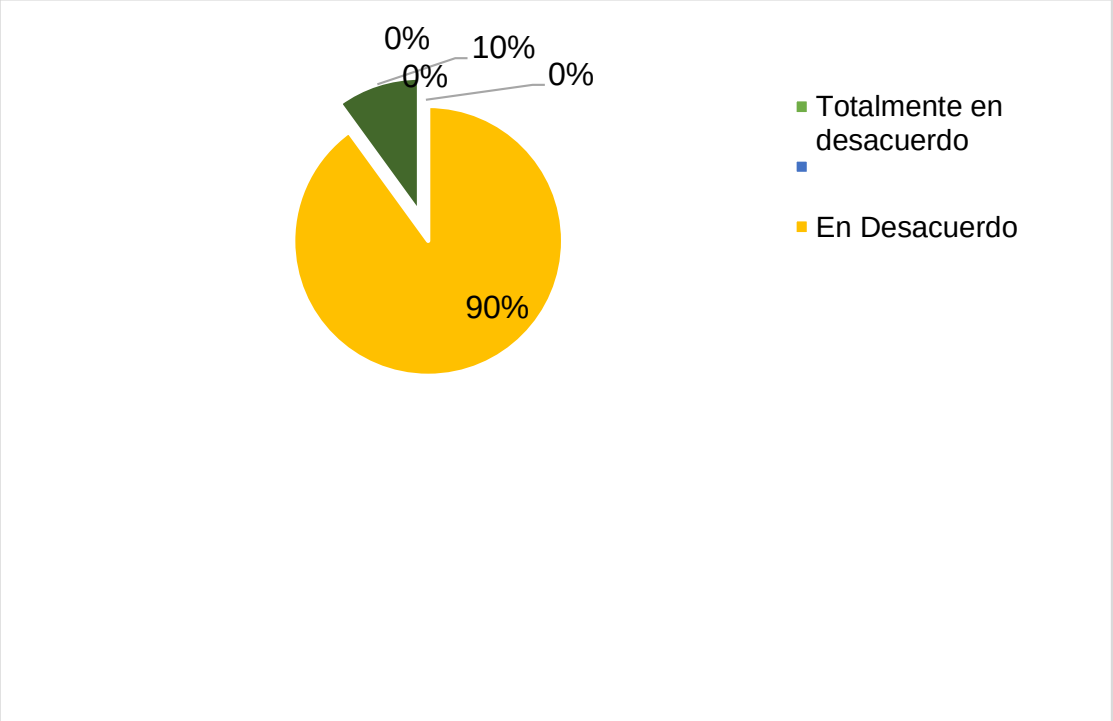
Tipificación del delito de Fraude informático

Item	Cantidad	%
Totalmente en desacuerdo	**2**	**10**
Totalmente de acuerdo	0	0
En Desacuerdo	14	70
No opina	3	15
De acuerdo	1	5
Total	20	100

Nota: Fuente: cuestionario 1 elaborado por el autor

Figura 7

Tipificación del delito de Fraude informático



Nota: Las respuestas muestran a un 70% de los informantes quienes han manifestado que están en desacuerdo con que el delito de Fraude informático recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal, seguido de un 10% quienes indicaron que están totalmente en desacuerdo, un 15% precisó estar de acuerdo y un 5% que no ha opinado sobre la consulta realizada.

Tabla 8

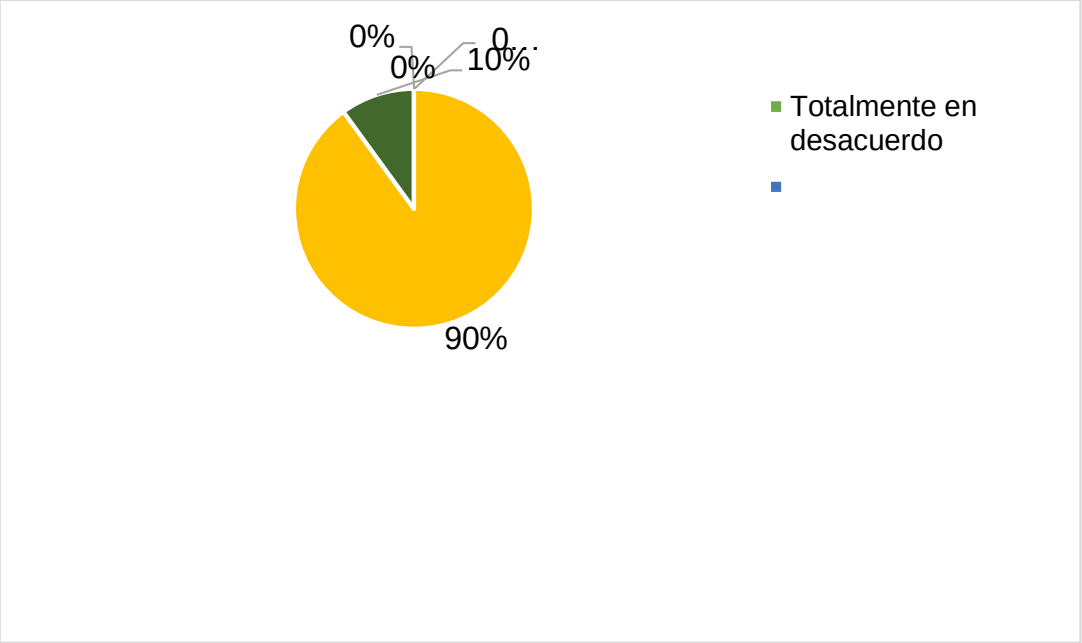
Tipificación del delito de Suplantación de identidad

Item	Cantidad	%
Totalmente en desacuerdo	**0**	**0**
Totalmente de acuerdo	0	0
En Desacuerdo	20	100
No opina	0	0
De acuerdo	0	0
Total	20	100

Nota: Fuente: cuestionario 1 elaborado por el autor

Figura 8

Tipificación del delito de Suplantación de identidad



Nota: Las respuestas muestran que un 100% de los informantes ha señalado que el delito de Suplantación de identidad recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal.

Tabla 9

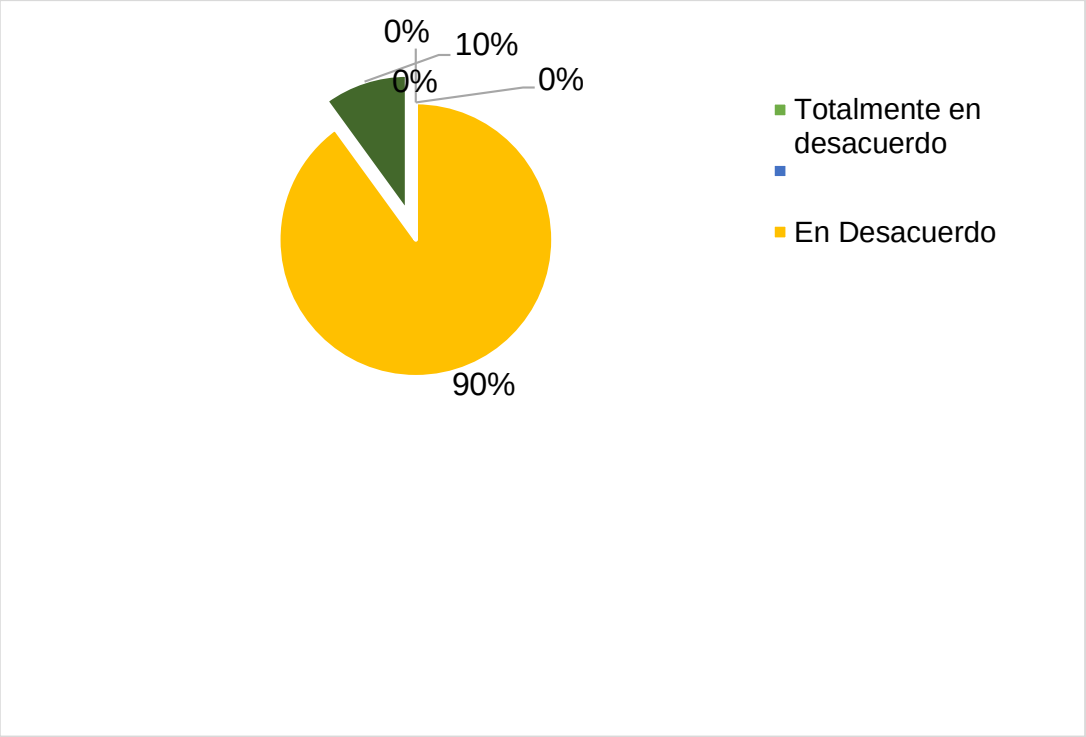
Tipificación del delito de Abuso de mecanismos y dispositivos informáticos

Item	Cantidad	%
Totalmente en desacuerdo	**0**	**0**
Totalmente de acuerdo	0	0
En Desacuerdo	18	90
No opina	2	10
De acuerdo	0	0
Total	20	100

Nota: Fuente: cuestionario 1 elaborado por el autor

Figura 9

Tipificación del delito de Abuso de mecanismos y dispositivos informáticos



Nota: *Las respuestas muestran un 90% quienes han indicado estar en desacuerdo con que el delito de Abuso de mecanismos y dispositivos informáticos recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal y un 10% quienes indicaron no opinaron sobre la consulta realizada.*

3.2. Discusión de resultados

Fue un objetivo del estudio fundamentar teóricamente los delitos informáticos en la doctrina, ante ello se encontró diferentes estudios, tales como Cruz, Jirón y Miranda (2018) en su tesis "La ciberdelincuencia y su regulación jurídica en Centroamérica con énfasis en Costa Rica, el Salvador y Nicaragua" resaltó que el delito informático es una tendencia criminal ejecutada en diversos países de Centroamérica, se trata de comportamientos que de manera frecuente se van desarrollando con mejores técnicas y habilidades esto se presenta con mayor frecuencia en países donde precisamente existen vacíos normativos y todo esto afecta de manera grave a los derechos de naturaleza constitucional de aquellas personas que han sido Víctimas de los ciberdelincuentes pues no existe ninguna normativa clara que la sancionen. Asimismo, en las conclusiones el autor señala que, el desarrollo y avances de la tecnología traen consigo la ejecución y mejora de nuevas formas de ejecutar los delitos.

Así también, Zorrilla (2018) en su estudio denominado "Inconsistencias y ambigüedades en la ley de delitos informáticos ley n° 30096 y su modificatoria ley 20171, que imposibilita su eficaz cumplimiento" señaló que la informática contiene una serie de características, las cuales lo convierten en una herramienta idónea para el progreso de la humanidad. En la realidad está también contiene o representa un medio que facilita la ejecución de conductas ilícitas, las cuales atentan principalmente contra el patrimonio de las personas quienes son víctimas de este ilícito.

Actualmente, la sociedad vive expuesta a una serie de atentados ilícitos debido a que la tecnología avanza precisamente la tecnología de comunicación y de información, es tanto que su información privada atiende muchas veces hacer violentada. En el Estado Peruano no existe una norma jurídica que especifique los

tipos penales que definen en dichos delitos, pues estos son más frecuentes en las redes sociales donde actúan una serie de modalidades que afectan a la sociedad en general. La naturaleza de los delitos informáticos es virtual, en tanto la tipificación de los ilícitos suele ser confusa, ya que a nivel general existe poco conocimiento al respecto, así también se observa en la realidad una serie de ausencia.

En cuanto la cultura informática y al impacto que generan los delitos informáticos, además de que hay una responsabilidad del manejo de las tecnologías de la información. De esa manera, es que considera la necesidad de realizar una reformulación a la ley de delitos informáticos vigente, toda vez que existen diversas conductas que no son sancionadas por acogerse a los vacíos legales que presenta la misma norma. Además, que, esta modificatoria es necesaria teniendo en cuenta que la ciberdelincuencia es un delito muy moderno que se actualiza día a día. Los resultados del estudio, precisamente del cuestionario mostraron que un 75% de los informantes está totalmente en desacuerdo con que el delito de Acceso ilícito recogido en la ley de delitos informáticos Ley 30096 no se encuentra correctamente tipificado la conducta criminal, seguida de un 20% quienes indicaron que están en desacuerdo.

El segundo objetivo del estudio consistió en Diagnosticar el estado actual de la ciberdelincuencia, ante ello se encontró una investigación de Espinosa (2019) en su trabajo “Ciberdelincuencia. Aproximación criminológica de los delitos en la red” precisó que la ciberdelincuencia es un fenómeno que amenaza a la sociedad, puesto que la tecnología se ha convertido en un medio principal para la creación de dispositivos o mecanismos que permiten la transmisión de datos personales por los mismos ataques de origen informático.

En las conclusiones ha manifestado que la tecnología ha contribuido en la comunicación de las personas sin importar la ubicación donde se encuentren, pero ello también ha contribuido al surgimiento de una serie de nuevas formas de criminalidad, lo que se conoce como ciberdelincuencia, ello debido a las deficiencias normativas que existen sobre la protección de los datos en las

actividades de la red. Bajo esa misma idea, Anguita (2018) en su artículo denominado “Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea” agregó que el trabajo de los estados miembros y la Unión Europea han sido muy significativos para frenar la delincuencia informática debido a que mediante sus instrumentos normativos, política o proyectos ha ayudado para que se frene el ciberdelito; sin embargo con todo el logro obtenido este no sería suficiente para frenar la ciberdelincuencia puesto que aún existe mucho trabajo que realizarse mencionando que una de las dificultades principales reside en el funcionamiento de los sistemas informáticos y la estructura del internet pues de momento existe una generalizada libertad normativa la otra que el estado no ha precisado la normativa para ese delito cibernético. También se encontró en los resultados que, un 90% quienes han indicado estar en desacuerdo con que el delito de Abuso de mecanismos y dispositivos informáticos recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal y un 10% quienes indicaron no opinaron sobre la consulta realizada.

Otro de los objetivos fue Evaluar la modificación legislativa de la ley 30096 de delitos informáticos para lograr su eficacia contra la ciberdelincuencia, en tanto se registró un estudio de Través (2018) “La vulneración de los derechos constitucionales por la falta de tipificación de las nuevas conductas delictivas a través de las tecnologías de informática y comunicación (TICS)”, a través del cual se encontró que es necesario una regulación y control de la información personal por el estado pues es, este, quien deberá velar por la seguridad siendo necesario supervisar y regular las instituciones nacionales como extranjeras; además que por la falta de políticas más estricta hacen que los medios de comunicación a través del internet, sea más fácil acceder a ella, de tal modo que los ciberdelincuentes se aprovechan de la facilidad de acceder a esta y realizar su delito de acoso, violación u otro delito como lo es el Grooming que una manera ilícita de actuar del delincuente para la cual no existe el control de la legalidad para poderlos penalizar como indicaría la ley.

Así también se ha registrado la investigación de Zorrilla (2018) en su estudio denominado “Inconsistencias y ambigüedades en la ley de delitos informáticos ley

n° 30096 y su modificatoria ley 20171", donde menciona que la la sociedad vive expuesta a una serie de atentados ilícitos debido a que la tecnología avanza precisamente la tecnología de comunicación y de información, es tanto que su información privada atiende muchas veces hacer violentada. Además de que hay una responsabilidad del manejo de las tecnologías de la información. De esa manera, es que considera la necesidad de realizar una reformulación a la ley de delitos informáticos vigente, toda vez que existen diversas conductas que no son sancionadas por acogerse a los vacíos legales que presenta la misma norma. Además, que, esta modificatoria es necesaria teniendo en cuenta que la ciberdelincuencia es un delito muy moderno que se actualiza día a día. De la misma manera, Vilca (2018) ha desarrollado una investigación denominada "Los hackers: delito informático frente al código penal peruano", donde ha señalado que la falta de una información precisa sobre los límites de la tecnología informática es un factor crítico en el impacto de los delitos informáticos y la ciberdelincuencia en la sociedad por lo que es necesario realizar un análisis comparativo de legislación con otros países, debido a que en el Perú existirían vacíos legales frente a esta modalidad. Además, la generalidad de los delitos informáticos provoca únicamente la ignorancia de la sociedad sobre este tema a que es imperativa la existencia normas que especifiquen los hechos o actos que se realizan por un computador. Además indica que, la figura hacker se encuentra relacionada a la actividad ilícita de la ciberdelincuencia entendiéndose que como un autor de esta infracción o afectación que se le realiza a la privacidad o a la intimidad de una persona o inclusive de instituciones con la finalidad de poder realizar algún hecho ilícito de datos, dado a ello es necesario se proponga una regulación precisa para esta actividad que se realiza vía internet a fin de regular y proteger su actuación dentro del ordenamiento legal. Los resultados del estudio mostraron que un 100% de los informantes ha señalado que el delito de Suplantación de identidad recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal.

3.3. Aporte práctico

Propuesta Legislativa:

LEY QUE MODIFICA LA LEY 30096 DE DELITOS INFORMÁTICOS
PROYECTO DE LEY:

Exposición de Motivos

Considerando que, la globalización ha traído grandes cambios a la sociedad, entre ellos, la tecnología, hecho que ocupado el espacio de las personas en sus diferentes contextos, formando así parte de su vida. Teniendo que hoy en día, la computadora, los teléfonos móviles y otros dispositivos se han convertido en instrumentos indispensables para el quehacer diario de las personas y las empresas en ámbito laboral.

Considerando que, existe una alta necesidad de priorizar un tratamiento a este tipo de problemáticas a través de una política criminar cuya finalidad este dirigida a garantizar protección a la sociedad frente a la ciberdelincuencia.

Considerando que, los cambios que han introducido la globalización y la tecnología continúan de las redes informáticas, existe un alto riesgo de que estas redes y la información electrónica continúen siendo utilizadas para la ejecución de estos ilícitos penales, donde las pruebas son almacenadas y transmitidas mediante dichas redes.

Considerando que, la sociedad exige medidas de alcance jurídico efectivo que tienda a garantizar un equilibrio correcto e idóneo entre el interés que persigue la acción penal así como con el absoluto respeto y garantía a los Derechos Humanos

fundamentales inherentes a las personas, ello para poder alcanzar la prevención de todos los actos ilícitos que se dirigen en contra de la confidencialidad la integridad y la disponibilidad de los diversos sistemas informáticos las redes y todos los datos informáticos.

Considerando que, el Estado peruano ha aprobado el Convenio sobre la Ciberdelincuencia de Budapest, mediante la Resolución Legislativa Nº 30913, en el año 2019, es preciso mencionar que esto no ha sido suficiente para mitigar esta problemática, tal es así que, la ley de delitos Informáticos y la unidad policial especializada en la investigación de tales delitos, no es suficiente, puesto que los casos han ido aumentado. Las diversas fallas en la programación de la página web, recepción de mensajes de WhatsApp, mensajes de textos, llamadas con links de supuestas páginas donde se solicita un registro de datos personales para poder acceder a beneficios tentadores donde muchas personas han cometido el error de acceder y por consecuencia ser víctimas de estos delitos. Así como estos, son muchos los factores que contribuyen a la permisibilidad de estos delitos, un caso reciente en la realidad peruana es el robo del Bono Familiar Universal que ha otorgado el Estado Peruano a las personas vulnerables a causa del estado de emergencia a causa de la covid-19.

Considerando que, la norma vigente presenta vacíos legales donde los ciberdelincuentes cometen actos ilícitos, los cuales quedan en muchas ocasiones impunes, siendo necesario que los delitos de daños informáticos puedan reformularse desde nuevos principios integradores. Es obligatorio para nuestro país actualizar y por consecuencia, modificar los tipos penales contenidos en la ley 30096 de delitos informáticos, adecuando de forma correcta los ilícitos, es decir prestando atención a las nuevas formas de criminalidad y los recientes ataques cibernéticos que enfrenta la sociedad y de ese modo se alcance una lucha efectiva contra dichos delitos, facilitando su detección, investigación y sanción.

Considerando que, es necesario una modificación legislativa, la cual permita una adecuación de nuestra legislación a la evolución informática, particularmente, los casos de ataque a la integridad de un sistema informático, el acceso ilícito, la

interceptación ilícita, el ataque a la integridad de los datos informáticos, la falsificación informática, el fraude informático y el abuso de dispositivos, entre otras modalidades que se presentan de forma constante.

Considerando que, es necesario tipificar aquellas conductas donde se sancione la receptación de datos, almacenamiento y/o cualquier otra forma de aquellos datos informáticos que vengan dirigidos a consecuencia de un acceso ilícito, interceptación ilícita y falsificación informática.

FÓRMULA LEGAL:

CAPÍTULO I: FINALIDAD Y OBJETO DE LA LEY

Artículo 1: La presente norma tiene por objeto garantizar la protección integral de los sistemas que utilicen tecnologías de información, la prevención y sanción de los delitos que se cometen contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías.

Capítulo I: Medidas que deberán adoptarse

Artículo 2: "incorpórese el segundo párrafo al artículo 5 de la ley 30096 de delitos informáticos", bajo el siguiente texto:
(…)
Cuando el agente para lograr contactar a una menor de edad a través de internet usa una identidad diferente, será reprimido con una pena privativa de libertad no menor de nueve ni mayor de doce años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal.
(…)

Artículo 3: "Incorpórese el segundo párrafo al artículo 7 de la ley 30096 de delitos informáticos", bajo el siguiente texto:
(…)

Con igual pena será sancionado quien habiendo tomado conocimiento indebido de datos informáticos en transmisiones no públicas, que deba quedar en secreto, y lo revela sin justa causa, o bien lo emplea a beneficio propio o de terceros.
(…)

Artículo 4: "Modifíquese e incorpórese el segundo párrafo al artículo 10 de la ley 30096 de delitos informáticos", bajo el siguiente texto:

El que deliberada e ilegítimamente fabrica, diseña, adapta, desarrolla, posee, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

El que deliberada e ilegítimamente obtiene, reproduce, difunde, comunica o entrega códigos, contraseñas u otros medios idóneos para acceder a un sistema informático o telemático, para la comisión de los delitos previstos en la presente Ley, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

CAPÍTULO II: DISPOSICIONES FINALES

PRIMERA DISPOSICIÓN: La presente investigación será de aplicación a nivel nacional.

SEGUNDA DISPOSICIÓN: La presente investigación entrará en vigencia al día siguiente de su publicación.

PRIMERA DISPOSICIÓN: La presente investigación será publicada en el diario oficial el Peruano.

IV. CONCLUSIONES

Los delitos informáticos son aquellas actividades ilícitas que son cometidas haciendo uso de una computadora o cualquier aparato electrónico conectado a una red de conexión, los cuales para el derecho se comprenden como elementos físicos, se caracterizan por tratarse de conductas que son realizadas en tiempo récord y de una forma muy fácil, cuyo único medio para poder ejecutarlas son los medios informáticos y que no necesariamente el delincuente está en el lugar donde se encuentra la persona o la entidad afectada, sino que no es necesaria la presencia física dicho, así estos delitos buscan florífera la identificación y la persecución de los mismos.

La ciberdelincuencia es un delito de larga trayectoria, consiste en un alto nivel de criminalidad que se comete haciendo uso de las computadoras, siendo este un fenómeno exclusivo de la sociedad industrial parte de la globalización, cuya naturaleza es virtual, por lo que la tipificación de los ilícitos suele ser confusa, ya que a nivel general existe poco conocimiento al respecto, así también se observa en la realidad una serie de ausencia.

En el Estado Peruano no existe una norma jurídica que especifique los tipos penales que definen en dichos delitos, estos son más frecuentes en las redes sociales donde actúan una serie de modalidades que afectan a la sociedad en general. La norma vigente presenta vacíos legales, los cuales quedan en muchas ocasiones impunes, siendo necesario que los delitos de daños informáticos puedan reformularse desde nuevos principios integradores.

Se desarrolló una propuesta legislativa, la cual buscó adoptar nuevos delitos a fin de prevenir y combatir el cibercrimen, aunado a ella, se homogenizó la legislación conforme a los preceptos penales de otros países en delitos de la materia investigada.

Se ha consultado con profesionales expertos sobre la viabilidad de la propuesta legislativa que se presenta, considerando estos que los cambios introducidos

dirigidos a modificar la ley 30096 de delitos informáticos para lograr su eficacia contra la ciberdelincuencia son idóneos, toda vez que contribuyen a penalizar conductas que en los últimos tiempos han gozado de impunidad.

4.1. Recomendaciones

Priorizar un tratamiento jurídico a los alcances de la ciberdelincuencia para garantizar protección a la sociedad frente a la ciberdelincuencia, para lograr el debido equilibrio entre los intereses de la acción penal y el absoluto respeto de los derechos humanos fundamentales, garantizando así la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos.

Ajustar la normatividad vigente, la ley de delitos informáticos al Convenio sobre la Ciberdelincuencia de Budapest, modificando los tipos penales contenidos en la ley 30096 de delitos informáticos atendiendo a las nuevas formas de criminalidad para lograr la lucha efectiva contra dichos delitos, facilitando su detección, investigación y sanción.

Modificar las conductas que busquen asegurar que se sancione conductas que vulneren la integridad de un sistema informático, sancionar el acceso ilícito, la interceptación ilícita, el ataque a la integridad de los datos informáticos, la falsificación informática, el fraude informático y el abuso de dispositivos y todas aquellas conductas que se presenten atentando contra las personas.

Modificar la tipificación penal para las situaciones de receptación de datos, almacenamiento y/o cualquier otra forma de aquellos datos informáticos que vengan dirigidos a consecuencia de un acceso ilícito, interceptación ilícita y falsificación informática.

Que se refuerce la capacitación del personal policial, judicial, peritos y demás que intervengan en la investigación de este tipo de conductas, ello con la finalidad de que se logre eficiencia y eficacia al momento de la identificación, investigación y sanción de este tipo de conductas.

La creación y funcionamiento de Juzgados especializados para la aplicación de la ley de delitos informáticos, a fin de que la unidad policial especializada en la investigación pueda colaborar de forma eficaz y eficiente en la mitigación de los delitos informáticos.

REFERENCIAS

Alcívar, C., Domenech, G., y Ortiz, C. (2015). La seguridad jurídica frente a los delitos informáticos. Avances.

Anguita (2018). Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea. España: Revista de Estudios en Seguridad Internacional.

Ávila, S. J. (2018). Las menores víctimas de la ciberdelincuencia. Medidas preventivas en el artículo internacional. Ecuador: Advocatus.

Bayardo, S. H., y Hermoza, M. M. (2019). Los delitos informáticos y su tipificación en la legislación penal ecuatoriana. Ecuador: Risti.

Calderón, L. (2010). Delitos informáticos y derecho penal. México: Ubijus.

Cruz, Ch. E., Jirón, V. M., y Miranda, G F. (2018). La ciberdelincuencia y su regulación jurídica en Centroamérica con énfasis en Costa Rica, el Salvador y Nicaragua. Nicaragua: Universidad Nacional Autónoma de Nicaragua.

Fernández, R J., Muñoz, M. F., & Cuevas, M. L. (2019). Perfil psicosociológico en el ciberdelincuente. España: RICSH Revista Iberoamericana de las Ciencias Sociales y Humanísticas.

Fernández, W., & Vargas, C. (2018). ¿ Son útiles las TIC para combatir la ciberdelincuencia? La relación entre la denuncia de delitos informáticos y el equipamiento tecnológico de las comisarías. *Revista de Direito, Estado e Telecomunicações*, *10*(2).

Flórez Romero, M., Aguilar Barreto, A. J., Hernández Peña, Y. K., Salazar Torres, J. P., Pinillos Villamizar, J. A., & Pérez Fuentes, C. A. (2017). Sociedad del conocimiento, las TIC y su influencia en la educación.

Herrera, U. L. (2018). Eficacia de la ley de delitos informáticos en el Distrito Judicial de Huánuco 2017. Huánuco: repositorio institucional Universidad de Huánuco.

Montiel, J. P. (2013). Regulaciones de excepción y prohibición de analogía. InDret.

Moragas, J. B., y Pascual, G. C. (2019). Las tecnologías de internet, un riesgo para empresas y ciudadanos. Barcelona: Universitat Politécnica de Catalunya.

Mori, Q. F. (2019). Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de Lima. Lima: Universidad Nacional Federico Villareal.

Pérez, C. L. (2014). Principio de legalidad penal. EUNOMÍA. Revista en Cultura de la Legalidad.

Quiroga, L. P., Jaramillo, S., & Vanegas, O. L. (2019). Ventajas y desventajas de las tic en la educación “Desde la primera infancia hasta la educación superior”. *Revista Educación y Pensamiento*, *26*(26), 77-85.

Reyes, N. M. (2015). Ciberdelincuencia una realidad virtual contada a medias. Colombia: Universidad Piloto de Colombia).

Ribas, E. R. (2019). Interpretación extensiva y analogía en el derecho penal. Revista de derecho penal y criminología.

Tenorio, P. J. (2018). Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la ciberdelincuencia. Lima: Universidad Diplomática del Perú Javier Pérez de Cuéllar.

Trávez, C. N. (2018). La vulneración de los derechos constitucionales por la falta de tipificación de las nuevas conductas delictivas a través de las tecnologías de informática y comunicación (TICS). Quito: Universidad Central del Ecuador.

Vilca, A. G. (2018). Los hackers: delito informático frente al código penal peruano. Huaraz: Universidad Nacional Santiago Antúnez de Mayolo.

Villavicencio, F. (2014). Derecho Penal parte especial. Lima: Grijley.

ANEXOS

Anexo 01: Matriz de consistencia

Variables	Problema	Hipótesis	Objetivos
V. *Independiente:* Modificación legislativa de la ley 30096 de delitos informáticos *V. Dependiente:* La Ciberdelincuencia	¿Cuáles son las deficiencias de la ley 30096 de los delitos informáticos para su eficacia contra la ciberdelincuencia?	Si se modifica legislativamente la ley 30096 de delitos informáticos se logrará su eficacia contra la ciberdelincuencia.	**General:** Proponer una modificación legislativa de la ley 30096 de delitos informáticos para lograr su eficacia contra la ciberdelincuencia en la ciudad de Chiclayo. **Específicos:** Fundamentar teóricamente los delitos informáticos en la doctrina. Caracterizar los antecedentes del problema. Diagnosticar el estado actual de la ciberdelincuencia en la ciudad de Chiclayo Elaborar la propuesta de modificación legislativa. Corroborar mediante consulta de expertos la modificación

			legislativa de la ley 30096 de delitos informáticos para lograr su eficacia contra la ciberdelincuencia en la ciudad de Chiclayo.

Anexo 2: Operacionalización de las variables

Variables	Dimensiones	Indicadores	Técnica
V*. Independiente:* Modificación legislativa de la ley 30096 de delitos informáticos	Exposición de motivos	Fundamentos de la norma	Cuestionario
	Fórmula legal	Modificación de la norma	
	Costos y beneficios	Costos generados al Estado Beneficio hacia la sociedad	
	Efecto de la norma		
V. Dependiente: La Ciberdelincuencia	Delitos computacionales	Uso de medios informáticos	
	Delitos informáticos	Atacan bienes informáticos	

Anexo 03: Instrumentos

UNIVERSIDAD SEÑOR DE SIPÁN

ENCUESTA APLICADA A POLICÍAS DE LA DIVISIÓN DE INVESTIGACIONES DE DELITOS DE ALTA TECNOLOGÍA (DIVINTAD) de la DIRINCRI – PNP

MODIFICACIÓN LEGISLATIVA DE LA LEY 30096 DE DELITOS INFORMÁTICOS PARA SU EFICACIA CONTRA LA CIBERDELINCUENCIA EN LA CIUDAD DE CHICLAYO

- Se le solicita su colaboración para llenar el siguiente cuestionario:

Marque la alternativa correcta, de acuerdo a su conformidad a su criterio y experiencia profesional.

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

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

ITEM	TD	D	NO	A	TA
1.- Cree usted que el delito de *Acceso ilícito recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal*					
2.- Cree usted que el delito de *Atentado a la integridad de datos informáticos recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal*					
3.- Cree usted que el delito de *Atentado a la integridad de sistemas informáticos recogido en la ley de delitos*					

informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal					
4.- Cree usted que el delito de *Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal*					
5.- Cree usted que el delito de *Tráfico ilegal de datos recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal*					
6.- Cree usted que el delito de *Interceptación de datos informáticos recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal*					
7.- Cree usted que el delito de *Fraude informático recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal*					
8.- Cree usted que el delito de *Suplantación de identidad recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal*					
9.- Cree usted que el delito de *Abuso de mecanismos y dispositivos informáticos recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal*					

Anexo 04: Validación de instrumentos por juicio de expertos

UNIVERSIDAD SEÑOR DE SIPÁN

INSTRUMENTO DE VALIDACIÓN POR JUICIO DE EXPERTOS

NOMBRE DEL JUEZ		Mg. Alva Becerra Elmer
	PROFESIÓN	Abogado
	ESPECIALIDAD	Derecho Penal y Procesal Penal
	EXPERIENCIA PROFESIONAL (EN AÑOS)	5
	CARGO	Abogado litigante
MODIFICACION LEGISLATIVA DE LA LEY 30096 DE DELITOS INFORMÁTICOS PARA SU EFICACIA CONTRA LA CIBERDELINCUENCIA EN LA CIUDAD DE CHICLAYO		
DATOS DEL TESISTA		
NOMBRES	Román Cruz Eucario Héctor	
ESPECIALIDAD	ESCUELA DE DERECHO	
INSTRUMENTO EVALUADO	Cuestionario	
OBJETIVOS DE LA INVESTIGACIÓN	**GENERAL** Proponer una modificación legislativa de la ley 30096 de delitos informáticos para lograr su eficacia contra la ciberdelincuencia en la ciudad de Chiclayo.	
	ESPECÍFICOS Fundamentar teóricamente los delitos informáticos en la doctrina. Caracterizar los antecedentes del problema. Diagnosticar el estado actual de la ciberdelincuencia en la ciudad de Chiclayo Elaborar la propuesta de modificación legislativa. Corroborar mediante consulta de expertos la modificación legislativa de la ley 30096 de delitos informáticos para lograr su eficacia contra la ciberdelincuencia en la ciudad de Chiclayo.	
EVALUE CADA ITEM DEL INSTRUMENTO MARCANDO CON UN ASPA EN "*TA*" SI ESTÁ TOTALMENTE DE ACUERDO CON EL ITEM O "TD" SI ESTÁ TOTALMENTE EN DESACUERDO, SI ESTÁ EN DESACUERDO POR FAVOR ESPECIFIQUE SUS SUGERENCIAS		
DETALLE DE LOS ITEMS DEL INSTRUMENTO	El instrumento consta de 9 reactivos y ha sido construido, teniendo en cuenta la revisión de la literatura, luego del juicio de expertos que determinará la validez de contenido será sometido a prueba de piloto para el cálculo de la confiabilidad con el coeficiente de	

	alfa de Cronbach y finalmente será aplicado a las unidades de análisis de esta investigación.
INSTITUCIONES FINANCIERAS	
1.- Cree usted que el delito de Acceso ilícito recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal	TA( ) TD( ) SUGERENCIAS: _____ _____ _____ _____
2.- Cree usted que el delito de Atentado a la integridad de datos informáticos recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal	TA( ) TD( ) SUGERENCIAS: _____ _____ _____ _____
3.- Cree usted que el delito de Atentado a la integridad de sistemas informáticos recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal	TA( ) TD( ) SUGERENCIAS: _____ _____ _____ _____
4.- Cree usted que el delito de Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal	TA( ) TD( ) SUGERENCIAS: _____ _____ _____ _____
5.- Cree usted que el delito de Tráfico ilegal de datos recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal	TA( ) TD( ) SUGERENCIAS: _____ _____ _____ _____
6.- Cree usted que el delito de Interceptación de datos informáticos recogido en la ley de delitos informáticos Ley 30096, se encuentra	TA( ) TD( ) SUGERENCIAS: _____

correctamente tipificado la conducta criminal	_____ _____ _____
7.- Cree usted que el delito de Fraude informático recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal	TA( ) TD( ) SUGERENCIAS: _____ _____ _____ _____
8.- Cree usted que el delito de Suplantación de identidad recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal	TA( ) TD( ) SUGERENCIAS: _____ _____ _____ _____
9.- Cree usted que el delito de Abuso de mecanismos y dispositivos informáticos recogido en la ley de delitos informáticos Ley 30096, se encuentra correctamente tipificado la conducta criminal	TA( ) TD( ) SUGERENCIAS: _____ _____ _____ _____

1. PROMEDIO OBTENIDO:	Nº TA: 9 Nº TD _____
2. COMENTARIO GENERALES: es viable para el propósito del estudio	
3. OBSERVACIONES	

_____
JUEZ - EXPERTO