UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN
FACULTAD DE DERECHO Y CIENCIAS POLITICAS

TESIS

Análisis de la adecuación de la Ley N°30096, al marco del convenio internacional de Budapest 2001, y su incidencia en la reducción de los delitos informáticos. Huaura 2018.

PRESENTADO POR:

Bachiller Cristian José Urpeque Tarazona

PARA OPTAR EL TÍTULO DE ABOGADO

ASESOR

Dr. Félix Antonio Domínguez Ruiz

HUACHO-PERÚ

2019

TITULO

Análisis de la adecuación de la Ley N°30096, al marco del convenio internacional de Budapest 2001, y su incidencia en la reducción de los delitos informáticos. Huaura 2018.

……

Dr. FELÌX ANTONIO DOMINGUEZ RUÌZ

ASESOR

MIEMBROS DEL JURADO

……

DR. CARLOS HUMBERTO CONDE SALINAS

PRESIDENTE

……

M(o) MARAI DEL ROSARIO MEZA AGUIRRE

SECREATARIO

……

M(o) ALDO REMIGIO LA ROSA REGALADO

VOCAL

DEDICATORIA

A mis padres, por su
inquebrantable vida amor.

AGRADECIMIENTOS

A la Universidad Faustino Sánchez Carrión,

A mis docentes, por sus enseñanzas y aliento de superación,

A mi asesor, por la paciencia en sus enseñanzas, y

A mis compañeros de aula, por la alegría en los estudios.

INDICE

PAGINAS PRELIMINARES

RESUMEN

Objetivo: Determinar si la adecuación normativa al convenio de Budapest que regula los delitos de ciberdelincuencia en el Perú resulta eficaz para el control de los delitos informáticos Huaura 2018. **Métodos:** La población ha sido personal de la PNP de la sección DIVINCRI Huacho, son 22 PNP, y 440 abogados litigantes. Muestra, 6 PNP y 40 abogados. Técnica: Encuestas y análisis documental; y Estadística Descriptiva. **Resultados:** La adecuación normativa al convenio de Budapest que regula los delitos de ciberdelincuencia en el Perú no es suficiente para el control de los delitos informáticos Huaura 2018. **Conclusión:** La norma vigente resulta ineficaz para perseguir la ciberdelincuencia; la ciberdelincuencia evoluciona, cambia, aprovechando los recursos de la tecnología y de la ciencia. Se recomienda que el marco normativo debierapermitir diferenciar la tipología que vaya surgiendo en el curso de su evolución; y que se incorpore en el debate legislativo a innovarse la participación de las secciones especializadas del Ministerio Publico y de la PNP; y exigirse que los softwares que operan en los terminales con acceso al internet estén condicionado a la identificación real del usuario; y que la normatividad preventiva debiera vincular la identificación real de usuario con el IP de los terminales con los que se accede al internet.

Palabras claves: Adecuación normativa, Ciberdelincuencia, delitos informáticos.

ABSTRAC

Objective: To determine if the normative adaptation to the Budapest agreement that regulates cybercrime crimes in Peru is effective for the control of Huaura computer crimes 2018. Methods: The population has been staff of the PNP of the DIVINCRI Huacho section, there are 22 PNP, and 440 trial lawyers. Sample, 6 PNP and 40 lawyers. Technique: Surveys and documentary analysis; and Descriptive Statistics. Results: The normative adaptation to the Budapest agreement that regulates cybercrime crimes in Peru is not sufficient for the control of computer crimes Huaura 2018. Conclusion: The current norm is ineffective in pursuing cybercrime; Cybercrime evolves, changes, taking advantage of the resources of technology and science. It is recommended that the regulatory framework should allow differentiating the typology that arises in the course of its evolution; and that the participation of the specialized sections of the Public Ministry and the PNP be incorporated into the legislative debate; and require that software operating in terminals with internet access be conditioned to the user's real identification; and that preventive regulations should link the real user identification with the IP of the terminals with which the internet is accessed.

Keywords: Regulatory adequacy, Cybercrime, computer crimes.

INTRODUCCION

El modo de vida de los ciudadanos se ha visto sorprendida por grandes cambios repentinos en diversos aspectos, alterándose formas convencionales de las relaciones interpersonales, la actividad comercial, las comunicaciones, etc. Una de estas manifestaciones de grandes cambios alcanza a alterar la noción del espacio y el tiempo en las comunicaciones: Por ejemplo, la mensajería instantánea a distancias remotas, otrora solo posibles en la ciencia ficción, hoy es de uso común. Ello es posible a través de la interconexión de terminales (CPU, celulares móviles, etc) cuya información se trasmite por ondas electromagnéticas, habilitadas por unidades de recepción y trasmisión en el espacio (satélites).

Los avances alcanzados por la tecnología en el mejoramiento de la eficiencia de los elementos que intervienen en estas nuevas formas de comunicación son sorprendentes y realmente el común de la gente no alcanzamos a conocer en su verdadera dimensión. Diríase, que la modernidad nos ha tomado por sorpresa a todos y ciertamente también al Derecho mismo que por su naturaleza es reflexiva, y hasta lenta comparativamente. Pues bien, en este ínterin de la modernidad en las tecnologías y parsimonia del derecho viene ocurriendo un nuevo fenómeno vinculado al orden social, el florecimiento de nuevas formas o modalidades de la criminalidad. Se habla ahora de una ciberdelincuencia para referirse a aquella que utiliza los recursos tecnológicos de la informática con fines ilícitos. Esta nueva delincuencia tiene por objetivo aquellos bienes (base de datos, conocimientos, etc. Que utiliza esta tecnología.

Entonces tenemos, medios y recursos tecnológicos utilizados en la informática y contenido en terminales, y de otro lado tenemos, la vía a través del cual se transfiere información (trasmisión

Satelital). Estas dos dimensiones en realidad interactúan y se retroalimentan mutuamente para el avance de ellas mismas. Ambas a su vez son utilizadas en otros medios de la realidad social como la economía, la actividad bancaria, la propiedad, etc. facilitando su registro, acumulación, transferencia, etc. Así, diríase que la actividad humana y de las empresas ahora ocurre a través del internet. De modo que este avance tecnológico facilita las decisiones en geopolítica de los Estados, empresas trasnacionales. Etc. Se utiliza desde lo domestico y cotidiano de los seres humanos en todas partes del mundo.

Por su parte, el Derecho como instrumento normativo de garantía de que la vida social ha de ocurrir en orden y conciliando intereses ha sido expuesta al reto del avance tecnológico que en contraste resulta a todas luces obsoleto. La tesis que ahora se informa, aborda precisamente este aspecto, pero en su vertiente penal. Ha buscado verificar la eficiencia de la normatividad penal en su lucha con aquella criminalidad especializada que accede sin autorización y con fines ilícitos a las bases de datos registrados en los soportes informáticos, a alterar las comunicaciones, “infectar” programas informatizados, etc.

Finalmente, las legislaciones de los Estados tienen como referencia un instrumento jurídico supranacional al que deben ajustar su legislación interna, el “convenio de Budapest”. El Perú se ha adherido a ella y como tal ha debido adecuarse a ella. Ha sido la observación visual del incremento de la ciberdelincuencia lo que nos ha motivado verificar nuestra normatividad se ha adecuado a aquel marco supranacional. Para responder a ello, presentamos el presente informe en los siguientes capítulos.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1.- Descripción de la Realidad Problemática

Con el desarrollo de las tecnologías en los medios informáticos, las telecomunicaciones, el internet, la delincuencia también ha evolucionado. Ahora utiliza este avance tecnológico no solo como ventaja para el logro de delitos comunes, para delitos contra el patrimonio, la libertad o la vida, logrando con la utilización de estos medios eficiencia desde la perspectiva criminal; sino también, por otro lado, ha aparecido otro tipo de delincuencia, especializada aborda la tecnología como fin en sí mismo. En esta variante la delincuencia tiene como objetivo la información contenida en soportes digitales. Aparece entonces lo que se ha denominado la "ciberdelincuencia" que es uno de los principales ilícitos que se comenten en las sociedades que utilizan masivamente las diversas manifestaciones de la tecnología informática.

Ciertamente, el fenómeno trae nuevos riesgos y exige por tanto nuevos retos para el Estado, la necesidad de adecuar sus órganos represores y punitivos para responder a nuevas modalidades de la delincuencia. Como decíamos, un factor importante en el avance de esta criminalidad son los grandes niveles de tecnología alcanzados. Véase, solo por citar como ejemplo simple, que las formas convencionales de seguridad en la correspondencia confidencial otrora en soportes físicos, ahora se materializa a través a

través del internet, red de redes que permite la interconexión de computadoras geográficamente a distancia remotas entre sí.

Dentro de esta delincuencia, han surgido diversas variantes de la especialidad, como aquella cuya especialidad son el acceso a la base de datos almacenados en soportes informáticos que como consecuencia de las transacciones comerciales deben ser registradas. Dichos bancos de datos son demandados para la organización de otras actividades delincuenciales. Así estas bases de datos son obtenidas ilícitamente y comercialización en el mercado informal a la que accede otra actividad también delincuencial subsecuente. Ni se diga cosa distinta de la información clasificada o reservada de las empresas, igualmente vulnerada. Vemos entonces, que globalizada la tecnología de forma similar a la economía resulta la diversificación de la actividad criminal que rebasa las fronteras de competencias y jurisdicciones de determinados Estados.

De modo tal que los esfuerzos regulatorios en la vía penal dentro de un Estado han sido tomados por sorpresa por estas nuevas formas de criminalidad. De modo tal que los marcos normativos locales han dado pase a instrumentos supranacionales. Con lo que los ordenamientos internos necesariamente deben adecuarse. El primer y más importante instrumento normativo supranacional es el Convenio de Budapest. Sin embargo aún este instrumento tiene una data desactualizada al avance alcanzado por la tecnológico informático. En efecto, el convenio de Budapest data de noviembre de 2001 y entro en

vigor en el Perú en julio de 2004. Establece criterios tenerse en cuenta en todas las áreas relevantes de la legislación sobre ciberdelincuencia. Son criterios vinculantes que han de servir de guía para homogenizar las legislaciones nacionales.

Es así que el objetivo de la presente investigación es someter a verificación la eficiencia de la normatividad destinada a tutelar los bienes jurídicos como el patrimonio, la intimidad personal, la titularidad de las bases de datos, las transferencias financieras, etc. Otro aspecto relevante, luego de lograr tal objetivo sería para una siguiente investigación, proponer incorporar a las normas penales y administrativas elementos factuales de modo que sean más acorde al actual estadio de los medios informáticos.

1.2.- Formulación del Problema

1.2.1.- Problema General

¿Cómo la adecuación normativa al convenio de Budapest que regula los delitos de ciberdelincuencia en el Perú resulta eficaz para el control de los delitos informáticos? Huaura 2018

1.2.2.- Problemas Específicos

P.E,1: ¿Cuáles son los aspectos más determinante en relación a la protección de bienes jurídicos para considerar eficaz la normatividad penal que regulan los delitos de ciberdelincuencia en el Perú? Huaura 2018

P.E.2: ¿Cuáles son las conductas en los medios informáticos que afectan bienes jurídicos pero que sin embargo no han sido señalados en la legislación nacional? Huaura 2018

1.3.- Objetivos de la Investigación

1.3.1.- Objetivo General

Determinar cómo la adecuación normativa al convenio de Budapest que regula los delitos de ciberdelincuencia en el Perú resultaría eficaz para el control de los delitos informáticos. Huaura 2018

1.3.2.- Objetivos Específicos

OE!: Determinar cuáles son los aspectos más determinantes en relación a la protección de bienes jurídicos para considerar eficaz la normatividad penal que regulan los delitos de ciberdelincuencia en el Perú. Huaura 2018

OE2: Determinar en qué circunstancias, forma, lugar y tiempo se cometen conductas, comportamientos, hechos a través de los medios informáticos para la comisión de delitos informáticos. Huaura 2018.

1.4.- Justificación de la Investigación

La presente investigación se justifica en la medida que busca determinar los niveles de eficiencia y efectividad de la normatividad legal en relación al incremento de la ciberdelincuencia en el Perú. Hemos definido nuestro espacio de observación de campo en la provincia de Huaura, que debido a su población relativamente pequeña a nivel nacional nos permitirá observar el objetivo con mayor precisión de una realidad nacional. Los resultados que alcancemos con el presente proyecto serán de suma utilidad en el ámbito académico para otras investigaciones de temas conexos, así como para resaltar los aspectos técnicos del uso de los medios informáticos vinculados a la vulneración de bienes jurídicos. Estos delitos, con niveles de incremento masificado a través de

Tecnologías que evolucionan constantemente, con la velocidad distinta a la naturaleza de las normas jurídicas, exponen a estas a niveles ineficaces e incluso obsoletos.

1.5. Delimitación del estudio

Hemos definido nuestro espacio de observación de campo en la provincia de Huaura, que debido a su población relativamente pequeña a nivel nacional nos permitirá observar el objetivo con mayor precisión de una realidad nacional. También es menester informar que en cuanto a la temporalidad a la temática bajo observación tiene como referencia general la vigencia de la ley Nº 30096, octubre del 2013, sin embargo, para los efectos del recojo de evidencia respecto de la eficiencia o efectividad de la aplicación de la misma corresponde al año 2018. Ello, porque al fin de cuentas, la muestra ha sido se recogida en la provincia de Huaura en el año 2018. Sin embargo, los resultados que alcancemos con el presente proyecto serán de suma utilidad en el ámbito académico para otras investigaciones de temas conexos, así como para resaltar los aspectos técnicos del uso de los medios informáticos vinculados a la vulneración de bienes jurídicos. Estos delitos, con niveles de incremento masificado a través de tecnologías que evolucionan constantemente, con la velocidad distinta a la naturaleza de las normas jurídicas, exponen a estas a niveles ineficaces e incluso obsoletos

5.6. Viabilidad de estudio.

Siendo que en la presente investigación se abordará la temática desde un enfoque jurídico racionalista, toda vez que la norma jurídica será analizada en

su dinámica de aplicación emitiendo juicios de valor respecto de la eficiencia de la misma en su contexto social.

Siendo así, ha implicado el manejo de recursos teóricos, para los que nos hemos premunido de una asesoría temática, que ha consistido en diversas consultas a docentes de la especialidad penal de nuestra casa de Estudios. En la parte del recojo de información de campo, conforme al cronograma y presupuesto se contó con el servicio de alumnos de la facultad de ciencias sociales. Debemos precisar, respecto del apoyo metodológico además del formalmente asignado, el Mo Jaime Andrés Rodríguez Carranza, adicionamos en apoyo del Dr. Félix Antonio Domínguez Ruiz, ambos profesores de nuestra Facultad, quienes a nuestro entender se ha tratado de una de las mejores asesorías metodológicas. Finalmente, diremos que hemos recurrido al sistema financiero para cubrir los costos del presupuesto, inicialmente previsto con recursos personales pero que resultaron insuficientes para cubrir los gastos totales del desarrollo de la tesis.

CAPITULO II

MARCO TEORICO

2.1. Antecedentes de la Investigación

2.1.1. A nivel internacional

Iván Mateos Pascual (2013**)** Tesis titulada *Ciberdelincuencia Desarrollo y persecución tecnológica* presentada para la obtención de la licenciatura de Ingeniería Técnica de Telecomunicación en la Universidad Politécnica de Madrid, España. Los objetivos de dicha investigación fueron, DAR a conocer los diferentes aspectos de los que se compone un tema de la magnitud y la infinidad de posibilidades de estudio como es el de la ciberdelincuencia. IDENTIFICAR a los diferentes tipos de cibercriminales según su perfil y modus operandi. Arriba a las siguientes conclusiones: *Los métodos y técnicas empleados por los ciberdelincuentes para alcanzar sus objetivos, se puede definir este análisis según sea la motivación primordial por la que estos se ven guiados. Estos métodos aparecen principalmente en forma de estafas o robos de información y sus principales medios de acceso a las víctimas han pasado de ser el correo electrónico y los sitios web, para ir dejando paso a las omnipresentes redes sociales y los terminales móviles de nueva generación. A continuación, aparecen los denominados ciberdelincuentes sociales, cuyo objetivo no tiene nada que ver con el anterior, sino que se trata de individuos cuyos delitos afectan directamente a las personas, tanto en su integridad física como psicológica.*

El tesista, resalta en su investigación aspectos importantes de los tipos de delitos vinculados al uso de las tecnologías informáticas, y de forma muy interesante expone detalles y diversas formas de actuar delincuencial en un contexto como España donde los niveles de instrucción son superiores al caso peruano, de forma similar podría decirse de los niveles de tecnología alcanzada.

2.1.2. A nivel nacional

Diego Alexander Alarcón Ariza y Javier Antonio Barrera Barón (2017). Tesis titulada *Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016.* Presentada en la Escuela de Posgrado de la Universidad Privada NORBERT WIENER para optar el grado académico de MAESTRO EN INFORMÁTICA EDUCATIVA. El objetivo de dicha tesis fue **Determinar:** La relación del uso del internet con los delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, seccional Sogamoso, 2016. **Hipótesis general**: El uso del internet se relaciona significativamente con los delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, seccional Sogamoso 2016. Conclusiones: el uso del internet mediante las competencias informacionales por habilidad, acceso a la información y aspectos sociales se relacionan con los delitos informáticos de derecho de autor, uso legal de la información y el uso correcto de las redes sociales, es decir que la ocurrencia de los delitos informáticos depende del desarrollo de las competencias informacionales en el uso del internet.

El suscrito ha recogido el aporte en esta tesis por haber estado a relaciona tecnología y delitos, encontrando una estrecha relación entre ambas. Sin embargo, creemos que deja un margen pendiente de investigar relacionado a determinar cuál es la forma de esta relación. Algunos artículos parciales se atreven tímidamente a sostener que las tecnologías brindan facilidades a la actividad delincuencial.

Velarde, José Luis (2014) en su artículo *"Los sistemas informáticos en el Perú"* concluye que: Al entrar en vigencia la novísima ley de delitos informáticos habría que reconocerle el hecho de que reúne en un solo cuerpo normativo todas las conductas delictivas que, según el legislador, pueden ser cometidas por medio de la utilización de sistemas informáticos o tecnológicos (al menos hasta el día de hoy). Resalta que previamente a la promulgación de esta ley ya existían en el Código Penal cuatro artículos (207-A, 207-B, 207-C y 207-D) que regulaban varias de las conductas que son recogidas como punibles en la ley que es ahora materia de comentario y vale decir también que se hacía con una tipificación muy similar a la utilizada en la novísima Ley de Delitos Informáticos, por lo que no deja de sorprender la ola de críticas que la norma ha recibido. Igualmente, de que ya estaban contempladas otras figuras delictivas como la de pornografía infantil, en las cuales la única modificación sustancial que se ha realizado es considerar como agravante el hecho de que la conducta se realice por medio de tecnologías de la información o de la comunicación, lo cual tampoco ha estado exento de críticas, por cierto. Sin embargo, no ha parecido importante que sostenga que la norma en referencia sea inconstitucional, pues podría restringir la libertad de prensa y la libertad de expresión, en determinados supuestos. Se ha tildado a la norma de "ley mordaza", pues se afirma que se busca penar a los medios de comunicación que publiquen información que haya sido escrito en un

párrafo seguido el citado artículo establece que "el agente de infracción culposa es punible en los casos expresamente establecidos por la ley".

Así se hacía notar que si la norma no señalaba si la infracción o conducta es culposa, debía entenderse que esta es de comisión dolosa, pues las infracciones culposas deben estar previstas expresamente (sistema de numerus clausus). De allí que sea posible concluir que las conductas sancionadas en la reciente ley deben ser cometidas, necesariamente, a título doloso. Salvado este punto, la crítica más seria contra. la ley es la que apunta a que la norma sería inconstitucional, pues vulnera la libertad de prensa y de expresión.

Por nuestra parte, hacemos notar que la norma no penaliza de forma precisa la difusión y/o publicación de comunicaciones obtenidas mediante interceptación telefónica o de otros datos obtenida mediante la interceptación telefónica o informática. Se ha dicho también que la tipificación de algunos delitos es tan vaga que puede permitir a jueces y fiscales poder considerar casi cualquier acción como delictiva.

Elías Puelles, Ricardo (2014). En su investigación *Luces y sombras en la lucha contra la delincuencia informática en el Perú,* concluye que con la aparición de Internet y de los delitos informáticos, los criminólogos han comenzado a anunciar que la concepción del delito debe replantearse. Pues estos nuevos crímenes vienen siendo cometidos en lo que en argot criminalístico se denomina en “no lugares”. Lo que ha dado lugar a líneas de estudio en ese sentido. Por ejemplo, mientras que el miedo en el delito tradicional se asociaba a experiencias emocionales, el miedo en el delito informático está vinculado a

un componente cognitivo, ya que el delincuente utiliza el internet y tiene una mejor oportunidad de hacer una valoración racional del riesgo de su conducta en la red.

Nos ha parecido inevitable recoger el aporte de esta tesis porque expone sistemáticamente sus puntos de vistas en relaciona la diferencia que el desarrollo del accionar delincuencial provoca en el agente. Es decir, no es lo mismo, robar de la forma tradicional que "robar" accediendo a una cuenta bancaria por internet. Y finalmente porque la identificación del lugar de los hechos ahora nos trae las dificultades propias de las redes en el internet.

Savaro, Carlos (2014). En su estudio titulado, *Nuevas tecnologías y conductas delictivas* concluyen que las personas que cometen los "delitos informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes. Se trata de personas que tienen habilidades para el manejo de los sistemas informáticos, lo cual los coloca en una situación de ventaja que es rápidamente aprovechada para cometer el ilícito y lograr impunidad. Obviamente, también nos encontramos con un segmento social acomodado que le permite acceder al uso de esta tecnología para los más diversos fines ilícitos.

El autor se esta tesis pone en evidencia las particularidades del sujeto, con alto niveles de conocimiento tecnológico, por tanto, pertenecientes a un estrato social distinto al de la delincuencia común.

Prado Saldarriaga, Víctor (2016), en su artículo, S*obre la Criminalidad Organizada en el Perú* sostiene que el tamaño y la naturaleza de las actividades de cada red criminal varían frecuentemente. Las redes criminales examinadas en el estudio están involucradas principalmente en una sola actividad (a pesar de que este no es siempre el caso) y podrían reorganizarse para dirigir otras actividades. La habilidad de todos los grupos para dirigir una tarea dependía de su habilidad para reclutar a los recursos humanos disponibles y sus habilidades en la red. El grupo *Verhagen* involucrado en el contrabando de cannabis en Europa, por ejemplo, fue muy lejos al intentar reclutar personas con una habilidad particular al anunciarse públicamente en los medios. El uso de la violencia no es estructural en estos grupos; pero si instrumental e incidental ya que su enfoque principal radica en las altas habilidades y facultades de sus miembros".

Expone el reconocido jurista unja de las características principales de toda organización criminal, su especialidad y su capacidad de reorganización. Característica de la especialidad también presente en las organizaciones criminales que utilizan los recursos informáticos.

Lira Arteaga Oscar Manuel (2012), en su artículo *Cibercrimen* sostiene que este ilícito que se encuentra latente en la mesa de debate a nivel mundial ya que genera muy a menudo grandes pérdidas como es el conocido caso de del 11 de septiembre del 2001contra las torres gemelas en la ciudad de new york (EE.UU) el cual fue planteado y ejecutado a través del uso de la tecnología ,además de los últimos reportes de amenaza global de terrorismo digital ,por ende es menester realizar posibles sondeos a nivel gubernamental para frenar este incremento de ilícito penal.

El autor pone de relieve la vulnerabilidad a la que se pueden ver expuestos los mas seguros sistema de seguridad utilizando los recursos informáticos por parte de organizaciones criminales. Ciertamente, el terrorismo internacional, basa el logro de sus objetivos en el nivel de su organización.

2.2.- Bases Teóricas

2.2.1. Origen y Evolución de la legislación penal peruana sobre los delitos informáticos.

Inicialmente, en el Perú el 17 de julio del año 2000 mediante la Ley N° 27309 se incorporaron los Delitos informáticos al Código Penal, ubicándolos dentro del Título V del Libro Segundo, Delitos Contra el Patrimonio.

Sin embargo, como lo señala el propio Convenio de Budapest esta clase de delitos se encuentran orientados a la protección de bienes jurídicos como la información o protección de datos informáticos, o en su defecto la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos.

En ese orden de ideas, autores como Luis Miguel Reyna Alfaro señalan que, si bien el Patrimonio resulta ser el valor genéricamente tutelado, el interés social resguardado de manera específica es “la información contendida en los sistemas de tratamiento automatizados de datos”. Por ello, es evidente que el bien jurídico tutelado conforme a dicha ubicación sistemática resulta inapropiado, ello porque el delito informático ha de comprender todo comportamiento delictivo en el que la computadora es el instrumento

o el objetivo del hecho. En similar sentido se concibe el delito informativo como aquella forma de criminalidad que se encuentra directa o indirectamente en relación con el procesamiento electrónico de datos y se comete con la presencia de un equipo de procesamiento electrónico de datos.

Posteriormente, en octubre del año 2016, se promulgo la Ley de Delitos Informáticos Nº 30096, con el objetivo de reforzar el objetivo de PREVENIR y SANCIONAR las conductas ilícitas que afectan los sistemas y datos informáticos cometidos mediante la utilización de tecnologías de la información o de la comunicación.

Análisis a los principales tipos penales contenidos en la ley en referencia:

DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS

Artículo 2. Acceso ilícito: *El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.*

Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado.

Artículo 3. Atentado contra la integridad de datos informáticos: *El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.*

Consideramos que la redacción del artículo carece de precisión en cuanto a la acción ilícita del sujeto activo: ¿cualquier persona que tenga acceso a los datos informáticos podría ser sujeto activo? Nótese que no hay indicación elementos subjetivos (dolo). Pongamos el supuesto de un técnico que durante su labor incurre en algún supuesto de hecho, pero sin ningún otro fin que no sea su labor de asistencia técnica.

> ***Artículo 4. Atentado contra la integridad de sistemas informáticos:*** *El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.*

Tampoco se especifica el elemento subjetivo del tipo penal.

> ***DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES***
>
> ***Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos:*** *El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.*

> *Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.*

Supongamos que la persona "A" está en Facebook y lista de sugerencia de amigos. Otra persona "B", supuestamente de sexo opuesto y mayor de edad por los datos de su perfil. El primero le solicita su amistad, y el segundo acepta. La plática entre ambos confirma que se trata de una conversación entre personas adultas. Luego "A" le propone a "B" tener relaciones sexuales. Pero "A" desconoce que "B" realmente es menor de edad. Según el sentido literal del presente artículo "A" a incurrido en el tipo penal. Apreciamos que falta precisar el elemento subjetivo. En el ejemplo, podría aplicarse la figura del error en la acción, sin embargo podría mejorarse la redacción. .

DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES

> ***Artículo 6. Tráfico ilegal de datos:*** *El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.*

Este artículo, no se ha definido la base de datos debe ser considerada. Hay bases de datos públicas y privadas.

> ***Artículo 7. Interceptación de datos informáticos:*** *El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.*
>
> *La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.*
>
> *La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.*

El precepto legal se refiere a interceptación datos informáticos sin embargo ha omitido considerar la divulgación de tal información. Nótese que la corrupción en Perú ha sido delatada a través de la constatación de información contenida soportes informáticos.

DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

Artículo 8. Fraude informático: *El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.*

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA

Artículo 9. Suplantación de identidad: *El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.*

DISPOSICIONES COMUNES

Artículo 10. Abuso de mecanismos y dispositivos informáticos: *El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados 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.

Artículo 11. Agravantes: *El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando:*

1. El agente comete el delito en calidad de integrante de una organización criminal.

2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.

4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

Expertos de la Oficina Nacional de Gobierno Electrónico e Informática de la Presidencia del Consejo de Ministros, sostienen que dentro de la legislación se está usando como sinónimos, términos que generan ambigüedad pero son formas de manejar el lenguaje con el mismo objetivo: Respecto al uso de datos o de información a través de medios informáticos: Ilegal, ilícita, indebida y no autorizada.

Por nuestra parte creemos que debió tenerse en cuenta el Convenio sobre la Ciberdelincuencia de Budapest, que es instrumento internacional del año 2001 que establece medidas para tipificar delitos enmarcados en la ciberdelincuencia. Al parecer se ha aprobado un marco legal, en el supuesto que es una ley adecuada al Convenio de Budapest, sin embargo, sostenemos que no lo es así.

Esta Ley organiza se en siete capítulos de la siguiente manera:

a) Delitos contra datos y sistemas informáticos
b) Delitos informáticos contra la indemnidad y libertad sexual
c) Delitos informáticos contra la intimidad y el secreto de las comunicaciones
d) Delitos informáticos contra el patrimonio
e) Delitos informáticos contra la fe pública
f) Disposiciones comunes

2.2.2. Adecuación de la legislación nacional al Convenio de Budapest. Ley Nº30171 que modifica la Ley Nº 30096.

En marzo del 2014 se modifican determinados artículos de la Ley de Delitos informáticos, buscando superar las observaciones ya formuladas a dicha ley, buscando superar las ambigüedades contenidas en la ley original que había dejado espacios libres para los cibercriminales. La finalidad era adecuar el marco legal contenida en la Ley N° 30096 a los estándares legales del Convenio de Budapest. Se incorporar en la redacción típica la exigencia de cometer el delito de forma deliberada e ilegítimamente. Sobre todo, en los tipos penales de acceso ilícito, atentados a la integridad de datos informáticos y a

la integridad de sistemas e interceptación de datos y fraude informáticos. Se especifican los delitos de interceptación de base de datos e interceptación telefónica y a la información clasificada como secreta, reservada o confidencial.

2.2.3. Breve referencia al Convenio de Budapest

Se trata de un instrumento jurídico supranacional adoptado por el Consejo de Europa en el año 2001, cuya finalidad es diseñar una política penal común para luchar contra la "ciberdelincuencia". Actualmente más de 55 países lo han suscrito, y varios países se encuentran debatiendo la posibilidad de suscribirlo, sobre todos países de América Latina y El Caribe. Ha sido elaborado considerando los profundos cambios ocurrido en las relaciones de las personas y empresa como consecuencia de la digitalización de los datos, los avances tecnológicos y la globalización de las redes informáticas. Ha definidos criterios comunes a tenerse en cuenta en el desarrollo de la legislación interna de los Estados que se adhieren, para combatir la *cibercriminalidad.* Lo que nos importa por el momento resaltar del referido instrumento y necesario para la presente investigación es la definición hecha en su Artículo 2, respecto del delito de *Acceso Informático*, como aquella conducta de acceder ***deliberadamente*** e ***ilegítimamente*** a la totalidad o a una parte de un sistema informático. Asimismo, indica que el delito se puede cometer ***infringiendo medidas de seguridad***, con la ***intención*** de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático. Como podrá apreciarse, el convenio hace precisiones o predetermina exigencias (que nosotros hemos resaltado) y constituye en materia de delitos informáticos

un referente de uniformización en el plano internacional. En efecto, se trata del primer y único instrumento internacional existente hasta la fecha en esta materia.

Es bueno hacer referencia que al día de hoy tan sólo treinta Estados han ratificado el Tratado, de un total de cuarenta y seis firmas. Si bien no existen antecedentes normativos directos, ello no obsta para tratar una breve perspectiva histórica previa al Tratado. Rodríguez Bernal sitúa el germen del Convenio de Budapest en 1983, año en el que un grupo de expertos se reúne y recomienda a la Organización para la Cooperación y Desarrollo Económico (OCDE) la necesidad de armonización en los delitos informáticos, lo que finalmente se materializa en un informe tres años después. A partir de entonces el Consejo de Europa toma la iniciativa, y en 1989 publica la Recomendación Nº 89, que luego concluiría en Budapest. Posteriormente, en 1997 se inician las negociaciones, largas y complejas, para la elaboración del Tratado propiamente dicho. El Plan de Acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa con ocasión de su Segunda Cumbre (Estrasburgo, 10 y 11 de octubre de 1997), para buscar respuestas comunes ante el desarrollo de las nuevas tecnologías de la información, influirá decisivamente en el contenido de éste. En el año 2000 se da una reunión en Marsella, de los ministros de Justicia e Interior de la Unión Europea, donde deciden volcarse en la labor del Consejo de Europa, dejando a éste la elaboración final del Tratado. Finalmente, el comité del Consejo encargado de redactar el proyecto alcanza un consenso y se publica el «Proyecto de Convención sobre el Delito Cibernético» el 27 de abril de 2000 éste debería ser finalizado por un grupo de expertos antes de diciembre del mismo año. Sería finalmente aprobado por el Comité de Ministros el 8 de noviembre de 2001, y abierto a la

firma en día 23 del mismo mes. Desde entonces, ha sido de gran influencia en casi todas las legislaciones del mundo.

El Convenio sobre la Cibercriminalidad, consta de 48 artículos y un preámbulo inicial. El primer capítulo tan sólo comprende un precepto, referido a la terminología usada en el texto. El capítulo segundo «Medidas que deberán adoptarse a nivel nacional», incluye elementos tanto de Derecho material (responsabilidad penal, tentativa, complicidad...) como procesal (procedimiento, salvaguardas, datos, registros, jurisdicción…). En cuanto al tercero, se introduce directamente en la cooperación internacional. Abarca cuestiones como la extradición, la asistencia entre Estados, la información, el intercambio de datos y el establecimiento de una red. El último capítulo contiene las disposiciones finales propias de un Tratado internacional: adhesión, entrada en vigor, aplicación territorial, efectos, régimen de reservas, denuncias, notificaciones, etc.

2.2.4. Suscripción de Perú al Convenio de Budapest

No obstante que nuestra legislación ha había recogido los aportes del Convenio, sin embargo, este aún no había sido formalmente suscrito por nuestro país. Recientemente, el 30 de enero de 2019, el Pleno del Congreso del Perú, de forma unánime, aprobó la suscripción del Convenio de Budapest. Dicho tratado busca optimizar la regulación interna en materia de ciberseguridad, con mayor énfasis en materia penal, de tal manera que sus organismos correspondientes puedan tener mayor capacidad para poder perseguir este tipo de delitos especiales como fraude informático, interceptación ilícita, entre otros.

AZAOLA CALDERON, Luis (2010) comenta el Art. 5º del Convenio de Budapest y recoge los siguientes delitos contenidos en el Art. 5º del referido instrumento:

Delito de daño.- Comportamiento consistente en dañar, destruir o inutilizar un bien, el sistema informático, expresa que el delito de daños existirá si usuarios, carentes de autorización, alteran o destruyen archivos o bancos de datos a propósito; la destrucción total de programas y de datos ponen en peligro la estabilidad económica de una empresa. El modus operandi se viene perfeccionando con el tiempo a traves del *"virus"*. Estos actos deben causar un perjuicio patrimonial. **Sabotaje informático**. - consiste, básicamente, en borrar, suprimir o modificar (alterar) sin autorización funciones o datos de las computadoras con intención de obstaculizar el funcionamiento normal del sistema, que se conoce comúnmente como "virus informático". Marchena Gómez señala que el "sabotaje informático es la conducta que consiste en la destrucción o en la producción generalizada de daños". "El sabotaje informático que se dirige a inutilizar los sistemas informáticos causando daños a los programas".

2.2.5. Modalidades Delictivas a través de soportes informáticos

Es oportuno hacer precisiones a las modalidades y formas de las conductas delictivas que básicamente utilizan como medio soporte informático. Por ejemplo, para Ferri: «Son delitos las acciones determinadas por motivos individuales (egoístas) y antisociales,

que turban las condiciones de vida y lesionan la moralidad media de un pueblo dado, en un momento dado»

Hace ya algún tiempo se viene operando en el ambiente tecnológico el concepto de Delito informático, muchos organismos han emitido sus conceptos desde diferentes puntos de vista. Muchos consideran que no es necesario hacer la diferencia con los delitos tradicionales, un ejemplo claro de este concepto se demuestra en el Código Penal de España, en el cual no se compendian los Delitos Informáticos en un grupo específico, los artículos que se emplean a la hora de castigar un Delito Informático se encuentran inmersos en distintos lugares de la normatividad española. Los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos Este tipo de Delitos tiene las siguientes características:

Son delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas.

Son actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.

Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de los mismos, en definitiva, el Delito Informático es todo acto que haga uso de medios informáticos, que sea contrario a

una legislación establecida en un país lo cual acarrea una sanción judicial.

2.2.6. El Acceso ilícito informático según el Convenio de Budapest

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán Pena privativa de libertad mayor a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de prisión preventiva y cincuenta a ciento cincuenta días multa.

Interceptación ilícita: Atentado contra la integridad de los datos: El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con Pena privativa de libertad no menor de tres Ni mayor de seis años y con ochenta a ciento veinte días-multa.

Falsedad informática: El delito de falsedad documental, en general, lleva consigo una serie de consideraciones que hacen referencia tanto a los requisitos imprescindibles para la determinación penal del concepto, como a la definición del documento como base fáctica de cuanto haya de decirse de tal infracción, sobre todo si se tiene en cuenta que su existencia es el auténtico presupuesto del delito.

Fraude o estafa informática: La estafa informática es un fenómeno delictivo que en los últimos años está tomando mayor magnitud y relevancia en el ámbito de la criminalidad informática, siendo éste la base principal del delito informático sobre el que gira la ciberdelincuencia. A pesar de las diferencias que existen a la hora de establecer una definición unitaria del concepto de estafa informática y/o fraude informático, pueden identificarse las siguientes modalidades:

La manipulación informática y artificio semejante,

Transferencia patrimonial no consentida por el titular del mismo,

Ánimo de lucro, y

Perjuicio en tercero

Pornografía infantil: Ingresar a la cultura de la sociedad de la información nos coloca ante el reto de proteger a los menores para evitar los riesgos a que están expuestos cuando se convierten en asiduos usuarios del internet. En esta labor hemos de estar comprometidos la comunidad en general comenzando por los padres de familia, maestros, autoridades y todo aquel que tenga la posibilidad de orientar a los niños y adolescentes de una manera directa y sencilla guiándolos hacia la autoprotección que redunde en su bienestar y seguridad. Conociendo que a través de internet se puede publicar diversidad de temas, esto propicia que la red se transforme en un espacio libre de publicación, lo cual al momento de pensar en un público no adulto usuarios de este medio; ellos pueden ser potenciales víctimas de inescrupulosos que informan y propagan material sobre ideologías totalitarias, erotismo, sexo explícito y pornografía.

2.2.7. Tipología del ciberdelincuente.

El perfil del ciberdelincuente (sujeto activo) en esta modalidad delictual requiere que este posea ciertas habilidades y conocimientos detallados en el manejo del sistema informático. Es en razón a esas cualidades que se les ha calificado a los sujetos activos como delincuentes de cuello blanco, que tienen como características poseer altos conocimientos informáticos y se encuentran ubicados en puestos estratégicos en espacios laborales con acceso a información de carácter sensible. Para Marcelo Manson, los infractores de la ley penal en materia de delitos informáticos no son delincuentes comunes y corrientes, sino que por el contrario, son personas especializadas en la materia informática. Agrega que "las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común, esto es, habilidades para el manejo de los sistemas informáticos y que por su situación laboran en puestos estratégicos donde se maneja información sensible".

Camacho Losa considera que el perfil de estas personas no coincide con el de un delincuente marginal, y caracteriza a los autores de estas infracciones como empleados de confianza de las empresas afectadas.

Vives Antón y Gonzales Cussac afirman que "sujeto activo puede ser tanto las personas legítimamente autorizadas para acceder y operar el sistema (operadores, programadores u otros), como terceros no autorizados que acceden a las terminales públicas o privadas". Gutiérrez Francés y Ruiz Vadillo difieren de estos puntos de vista y sostienen que "el

autor del delito informático puede serlo cualquiera, no precisando el mismo de determinados requisitos personales o conocimientos técnicos cualificados". Por nuestra parte, si bien consideramos que el sujeto activo puede ser cualquier persona (con conocimientos y habilidades en informática), compartimos parcialmente la postura de que el sujeto activo debe ocupar un puesto laboral que le permita acceder a información sensible. Sin embargo, no están excluidos los sujetos que sin ocupar algún cargo estratégico pueden ser sujeto activo por sus habilidades y conocimientos sobre la informática. Por ende, se trata de delitos de dominio.

Las diversas especialidades suelen ser identificada con las denominaciones siguientes:

Hackers, son personas dedicadas, por afición u otro interés, a violar programas y sistemas supuestamente impenetrables. Conocido como delincuente silencioso o tecnológico. Les gusta indagar por todas partes y conocer el funcionamiento de los sistemas informáticos. Realizan esta actividad como reto intelectual, sin producir daño alguno con la única finalidad de descifrar y conocer los sistemas informáticos. Accedensin autorización a un sistema de proceso de datos a través de un proceso de datos a distancia, no cometido con finalidades manipuladoras, fraudulentas, de espionaje, ni sabotaje, sino sencillamente como paseo por placer no autorizado. Morón Lerma, defineal hackers como "personas que acceden o interfieren sin autorización, de forma subrepticia, a un sistema informático o redes de comunicación electrónica de datos y utilizan los mismos sin autorización o más allá de lo autorizado".

Crackers, son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos y, en general, a causar problemas a los sistemas, procesadores o redes informáticas, conocidos como piratas electrónicos. La característica del hacker con los crackers usa programas ya creados que pueden adquirir, normalmente vía internet; mientras que los hackers crean sus propios programas, tienen mucho conocimiento sobre los programas y conocen muy bien los lenguajes informáticos.

Phishing, es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. Resumiendo "todos los datos posibles" para luego ser usados de forma fraudulenta. Se puede resumir de forma fácil, engañando al posible estafado, "suplantando la imagen de una empresa o entidad pública", de esta manera hacen "creer" a la posible víctima que realmente los datos solicitados proceden del sitio "Oficial" cuando en realidad no lo es. El phishing puede producirse de varias formas, desde un simple mensaje a su teléfono móvil, una llamada telefónica, una web que simula una entidad, una ventana emergente, y la más usada y conocida por los internautas, la recepción de un correo electrónico.

Trashing, apuntan a la obtención de información secreta o privada que se logra por la revisión no autorizada de la basura inmaterial botada con el fin de utilizarla por medios informáticos en actividades delictivas. Estas actividades pueden tener como objetivo la realización de espionaje, coerción o simplemente el lucro mediante el uso ilegítimo de

códigos de ingreso a sistemas informáticos que se hayan obtenido en el análisis de la basura recolectada.

2.2.8. Tipicidad de los delitos informáticos.

Tipicidad objetiva.

La **conducta típica** en los delitos informáticos es la vulneración de la seguridad de los sistemas informáticos para el aprovechamiento indebido, ya sea sustrayendo bienes, valores, datos, programes. Igualmente, es típica el uso de las tecnologías informáticas para inducir en error a las personas con fines de aprovechamiento indebido, así como la destrucción, borrado, alteración de bases de datos, bienes, sistemas y cualquier pieza y sistema informático con el fin de perjudicar o reducir la competitividad de una persona o empresa, para provecho propio o de terceros.

El Sujeto activo, cualquier persona con características personales especiales, posee conocimiento avanzado de las tecnologías informáticas. , puesto que es casi imposible que cualquier persona puedacometer el delito, si tener conocimientos suficientes de cómo funcionan los sistemas informáticos, más cuando se trata de vulnerar las medidas deseguridad implementadas contra piratas informáticos. Sujeto pasivo. **El sujeto pasivo**, puede ser personas naturales o instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos.

El Bien jurídico protegido. (Mayer, 2017) en forma general considera que el bien jurídico protegido en los delitos informáticos es la información, es la contenida en un sistema de tratamiento automatizado de la misma, “en cuanto tal”, resulta difícilmente conciliable con una definición del interés protegido que apunte al libre desarrollo de la persona en un Estado democrático de derecho (p. 240). Sin embargo, podemos afirmar que no solo la información contenida en los sistemas informáticos o automatizados son los bienes jurídicos protegidos, sino también diferentes, como es la fe pública, la seguridad de los sistemas, la imagen, libertad personal, privacidad, el patrimonio entre otros. En este orden de ideas, en los delitos informáticos contra el patrimonio, el bien jurídico protegido es propiamente el patrimonio, tales como dinero electrónico, valores, fondos de cuentas, softwares, entre otros, puesto que éstos forman parte del patrimonio del sujeto pasivo. Debe sin embargo advertirse que, que el patrimonio no necesariamente son bienes físicos, sino también los digitales o electrónicos, por ejemplo si a una persona le sustraen de la nube una base de datos de una aplicación que ha estado desarrollando años o meses, para un proyecto grande, donde invirtió tiempo y dinero, pues la sustracción de dicha base de datos constituye patrimonio del sujeto pasivo, el cual es similar que se sustraigan a una fábrica de coches un vehículo de último modelo que acababa de culminar y estuvo para la primera exhibición.

Tipicidad subjetiva.

Los delitos informáticos, por su naturaleza el nivel de conocimiento que requiere, son delitos netamente dolosos. Sin embargo también se podría concretar por culpa o por descuido, en la que no te tenía ninguna intención de la comisión del ilícito, sin embargo vulnera el bien jurídico penalmente protegido.

Móvil. Las motivaciones generalmente son económicos, sin embargo, también hay otros moviles no económico. Los delitos informáticos contra el patrimonio se caracteriza por tener motivaciones económicas para su comisión (Hurto, fraude, sabotaje y estafa), sin embargo el sabotaje podría no ser con fines de aprovechamiento económico directo, por generar pérdidas en el sujeto pasivo más no provecho directo del sujeto activo, pero si el sabotaje es para reducir la competitividad de una empresa de competencia, entonces, tiene carácter patrimonial, puesto que dicho sabotaje se habría cometido para que la otra empresa repunte en el mercado del rubro. Otra de las motivaciones que podemos encontrar en los cibercriminales, como refiere también Han y Dongre (2014), son también por aspectos políticos (motivaciones políticas), donde se busca destruir, alterar o tomar el control de los objetivos, espionaje, o incluso hacer declaraciones políticas, ejercer represalia a grupos y realizar protestas. Otra de las terceras motivaciones que encontramos es nada menos que en aspecto socio culturales (motivación sociocultural), en la que los delitos cibernéticos se cometen con fines filosófico, teológicos, así como por diversión, curiosidad e incluso por mostrar la superioridad o gratificaciones de ego.

2.3. Definiciones Conceptuales.

Base de datos. Conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente. Los datos pueden aparecer en forma de texto, números, gráficos, sonido o vídeo.

Backup. Copia de Respaldo.

Ciber. Prefijo utilizado ampliamente en la comunidad Internet para denominar conceptos relacionados con las redes (cibercultura, ciberespacio, cibernauta, etc.). Su origen proviene del griego "cibernao" que significa "pilotar una nave".

Ciberdelincuencia. Cualquier tipo de actividad ilegal en la que se utilice Internet, una red privada o pública o un sistema informático doméstico.

Data. Unidad mínima entre las que componen una información.

Dirección IP. Identificador de una computadora o dispositivo en una red TCP/IP. Estas redes rutean los mensajes basados en la dirección IP del objetivo. p.ej., 200.32.3.238 es una dirección de IP.

Exploit. Programa o método concreto que saca provecho de una falla o agujero de seguridad de una aplicación o sistema, generalmente para un uso malicioso de dicha vulnerabilidad.

Gigabyte. El gigabyte (GB) equivale a 1.024 millones de bytes, o 1024 Megabytes. Se usa comúnmente para describir el espacio disponible en un medio de almacenamiento. Hay 1024 Gigabytes en un Terabyte.

Hardware. Componentes físicos de una computadora o de una red (a diferencia de los programas o elementos lógicos que los hacen funcionar).

Informática. Es una ciencia que estudia métodos, procesos, técnicas, con el fin de almacenar, procesar y transmitir información y datos en formato digital. La informática se ha desarrollado rápidamente a partir de las tecnologías tales como el circuito integrado, Internet y el teléfono móvil.

Redes sociales. Las redes sociales como Facebook, Twitter, Google Plus, LinkedIn, entre otros, usualmente son sitios web que permiten la fácil interacción entre personas por medios digitales.

Seguridad informática. Es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

Sistema informático. Conjunto de reglas o principios sobre una materia racionalmente enlazados entre sí. Conjunto ordenado de normas y procedimientos que regulan el funcionamiento de un grupo o colectividad.

Sistema Operativo. Programa especial el cual se carga en una computadora al prenderla, y cuya función es gestionar los demás programas, o aplicaciones, que se ejecutarán, como por ejemplo, un procesador de palabras o una hoja de cálculo, un juego o una conexión a Internet. Windows, Linux, Unix, MacOS son todos sistemas operativos.

Software. Es todo programa o aplicación programada para realizar tareas específicas.

SPAM. Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.

Vínculo. Link. Apuntadores hipertexto que sirven para saltar de una información a otra, o de un servidor web a otro, cuando se navega por Internet<--esto es un vínculo

Virus parásito. Se les llama parásitos a los virus que requieren de un portador (o host) para propagarse. Se adjunta a otro programa y se activa cuando ese programa es ejecutado. En el caso de los virus de macro, esta acción se produce porque el virus utiliza como host un módulo en un documento existente, y se activa cuando este módulo es ejecutado (por defecto al cerrar un documento).

WAP. Protocolo de Aplicación Inalámbrica. Permite a los usuarios de celulares el acceso a servidores web especializados, visualizando la información en el visor del teléfono.

WiFi. Red inalámbrica que usa el protocolo inalámbrico de alcance limitado IEEE 802.11b, que transmite datos en banda ancha en el rango espectral de 2.4 GHz.

2.4.- Formulación de Hipótesis

2.4.1.- Hipótesis General

La adecuación normativa de ley Nº 30096 al convenio de Budapest que regula los delitos de ciberdelincuencia en el Perú no es suficiente para el control de los delitos informáticos Huaura 2018.

2.4.2.- Hipótesis Específica

El robo de información confidencial, el hacking y el phishing son accionares

delincuenciales que a la actualidad no han sido contempladas en el marco de la adecuación normativa nacional.

Es incierto determinar en qué circunstancias, forma, lugar y tiempo se cometen estas conductas delictivas, esto se debe a la existencia de una realidad ficticia en un mundo virtual.

CAPÍTULO III

METODOLÓGIA

3.1.. Diseño Metodológico:

3.1.1. Tipo

El tipo de diseño metodológico, y respondiendo a las observaciones del jurado, el tipo del diseño metodológico **Es Aplicada**, en tanto y en cuanto hemos verificado la correspondencia de la norma legal con su aplicación, recogiendo la opiniones de determinados operadores jurídicos.

No obstante ello, el tesista estima no incompatible referir que el tipo de investigación, guiado por la literatura especializada, sobre tipología de investigaciones jurídicas, de Reynaldo Maro Tantalean Odar, y siendo que el objeto de la presente investigación es verificar la correspondencia de la norma nacional con una supranacional, y por otro lado, contrastar su eficiencia o eficacia en términos de aplicación, califica como una investigación de tipo Socio Jurídica, en su variante de relacionar normas positivas y realidad social.

3.1.2. Nivel

De otro lado, la presente investigación reúne las condiciones suficientes para ser calificado de NIVEL Descriptiva, en razón que verificaremos en la muestra en estudio, profesionales de especialidad, miembros de la Policía Nacional y

abogados que laboran en el área penal, todos ellos en la provincia de Huaura, vinculados a la investigación de delitos informáticos. Si la normatividad jurídica, ha comprendido todos los supuestos de hechos que ocasionan perjuicios, donde la delincuencia desarrolla su actividad.

3.1.3. Diseño

Es una investigación No experimental en tanto no se manipulará la muestra, información proporcionada por la PNP será recogida tal cual. Será Transversal en tanto el objeto bajo investigación será recogido en un punto determinado del año 2018 en la provincia de Huaura.

3.1.4. Enfoque

El presente trabajo de investigación, tiene características en su abordaje epistemológico jurídico racionalista, y adopta como estrategia el enfoque cualitativo. Ello, porque la norma jurídica que analizamos creemos inicialmente podría encontrarse obsoleta, pues las formas de ciberdelincuencia han variado desde la promulgación del convenio de Budapest (2001) y la ley N°30096 promulgada en nuestro país en el 2013, lo cual nos lleva a hacer un análisis racionalista.

3.2. Población y muestra

La población de análisis son operadores jurídicos, es decir, personas cualificadas entendidas en la materia, como miembros de la Policía Nacional y abogados que laboran

en el área penal, todos ellos en la provincia de Huaura. Esta característica de la población, de especialidad, ha sido identificada previamente en cuanto a su cantidad y cualidad. La población son el personal de la PNP de la sección DIVINCRI Huacho, destacados de forma permanente y estable en esta área (no incluye al personal de apoyo de secciones especializadas de la ciudad de Lima, que solo vienen como apoyo específico), son 22 PNP. De otro lado, los abogados litigantes, igualmente identificados en razón de la exclusividad del área penal, en la provincia de Huaura, 440 abogados, deducidos del total de los agremiados hábiles que laboran en forma permanente en calidad de abogados litigantes.

Muestra:

Siendo la población a estudiar está conformada por miembros de la policia nacional del peru, abogados en lo penal, la primera muestra a encuestar es de 6 PNP, y la segunda, 40 abogados debidamente colegiados.

3.3.- Operacionalización de variables e indicadores

VARIABLES INDEPENDIENTE	**INDICADORES**	**INSTRUMENTO**
Adecuación normativa nacional sobre Delitos informáticos al Convenio de Budapest	Identificación de coincidencias y diferencias de lanormatividad nacional con el Convenio de Budapest. Tratamiento jurídico penal (Dogmática Penal) Tratamiento legislativo (Legislación)	Encuesta

	Tratamiento de investigación (PNP)	
VARIABLES DEPENDIENTE	Curva del desarrollo de la delincuencia en delitos informáticos Necesidad normativa en el tratamiento en delitos informáticos Estrategia institucional que brinde lineamientos y un enfoque más claro a los operadores de justica Otorgamiento de eficacia a través de la prelación.	Encuesta
Efectividad de la legislaciónnacional respecto de la reducción de delitos informáticos		

3.4.- Técnicas de Recolección De Datos

3.4.1.- Técnicas a Emplear

En la recopilación de datos se utilizaron los medios técnicos adecuados que permitieron captar la real dimensión de la problemática planteada; razón por la cual de entre las técnicas de recopilación de datos tenemos: las encuestas, análisis documental, entrevistas y la Observación científica.

3.4.2.- Descripción de los instrumentos

Los instrumentos a emplear en la presente investigación son los siguientes:

a. Observación: Técnica que nos permite apreciar cómo se desenvuelve el fenómeno estudiado; vale decir, que a través de ella se llega a conocer el grado de aplicación de la institución jurídica en estudio.

b. Encuestas: Se utiliza la técnica indirecta de la aplicación de cuestionarios innominados y obtención de estadísticas que se elaboraran tomando de las informaciones teóricas obtenidas del trabajo de campo a elaborar, conforme al cronograma establecido para la presente.

c. Bibliográficas: Se utiliza para llevar a cabo la revisión y el análisis de la bibliografía relacionada con el tema objeto de estudio, siendo aplicable en todas las fases de la investigación. La información requerida fue obtenida de las Bibliotecas Especializadas de las Facultades de Derecho de las Universidades Locales y nacionales, páginas Web y de la biblioteca personal de la autora.

3.5.- Técnicas para el Procesamiento de la información

Las técnicas que utilizare para el procesamiento de datos será el de la Estadística Descriptiva, pues en base de los resultados obtenidos de las encuestas aplicadas a la población de estudio, se procederá a la tabulación de los resultados utilizan do el programa Excel. Esto permitirá expresar los resultados en porcentajes para la descripción e interpretación de los datos obtenidos.

CAPÍTULO IV
RESULTADOS

4.1.- ANALISIS DE LOS RESULTADOS

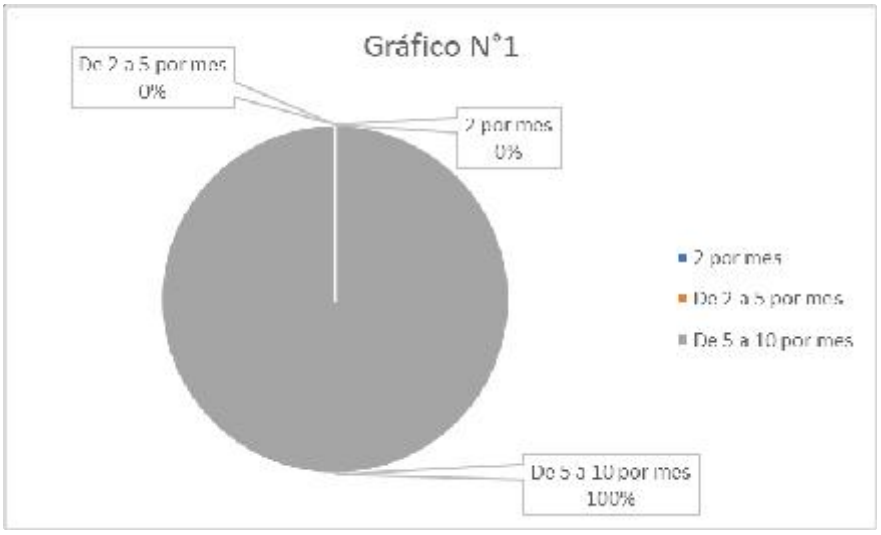
Respecto a la primera pregunta realizada a los 6 efectivos PNP especialistas en el área de delitos informáticos arrojan los siguientes resultados:

Tabla N° 1

Pregunta a los efectivos PNP ¿Con que frecuencia ve usted casos de ciberdelincuencia?

Alternativa	Frecuencia	Porcentaje
2 por mes	0	0%
De 2 a 5 por mes	0	0%
De 5 a 10 por mes	6	100%
TOTAL	6	100%

Fuente: Elaboración propia



De los resultados anteriores se puede observar que los efectivos de la PNP con una mayor incidencia de los casos de ciberdelincuencia, llegan a ver

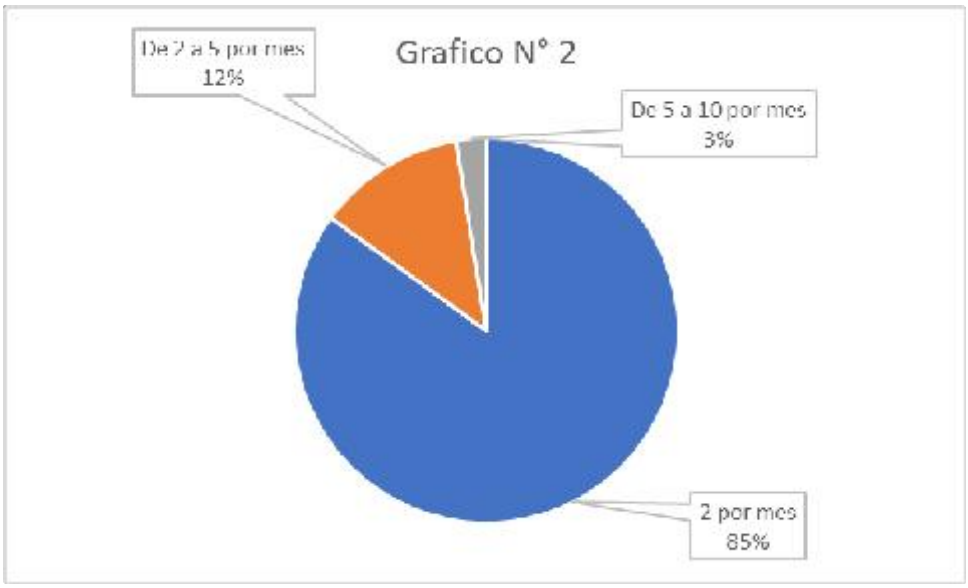
más de 10 casos de ciberdelincuencia al mes, lo cual les permite tener un mayor dominio de la problemática y nos sirve como base para conocer datos verídicos e información relevante para la investigación.

Tabla N° 2

Pregunta a abogados del CAH ¿Con que frecuencia ve usted casos de ciberdelincuencia?

Alternativa	Frecuencia	Porcentaje
2 por mes	34	85%
De 2 a 5 por mes	5	12.5%
De 5 a 10 por mes	1	2.5%
TOTAL	40	100%

Fuente: Elaboración propia



Del análisis de los resultados antes vistos se observa que de los 40 abogados colegiados del C.A.H 34 ven solo un máximo de 2 casos de ciberdelincuencia por mes el 85 %, de la población estudiada; 5 de ellos ven de 2 a 5 casos de ciberdelincuencia por mes, haciendo un total de 12.5% y para concluir solo uno

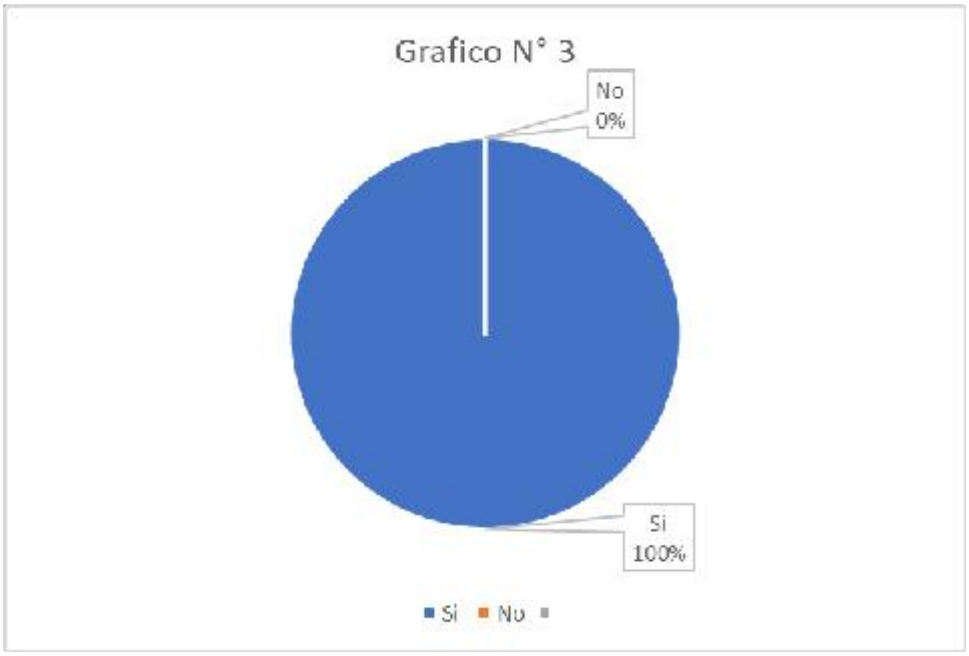
de nuestros encuestados conoce de más de 5 casos al mes, formando parte del 2.5%. Cabe resaltar que ambas poblaciones antes analizadas son conocedores de casos de ciberdelincuencia, con lo cual queda demostrado que dichos operadores de justicia son capaces de determinar con un juicio veraz y concreto sobre el tema de esta investigación, haciéndose su opinión importante para esta investigación.

Tabla N° 3

Pregunta a los efectivos PNP ¿Considera usted que el número de ciberdelitos se ha incrementado?

Alternativa	Frecuencia	Porcentaje
Si	6	100%
No	0	0%
TOTAL	6	100%

Fuente: Elaboracion propia



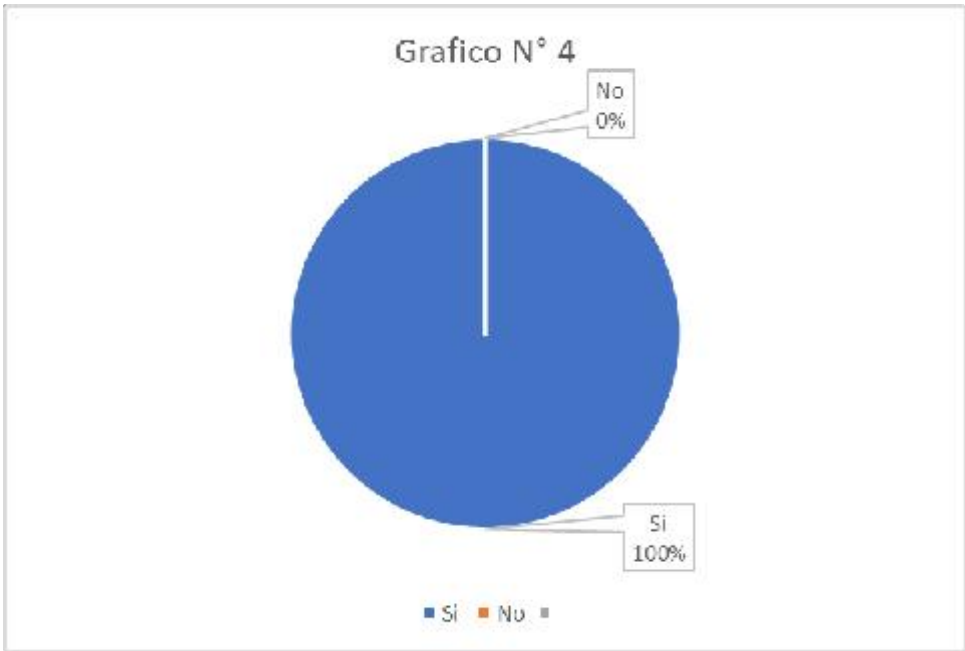
De los resultados anteriores se puede observar que los efectivos PNP consideran que los delitos de ciberdelincuencia se han incrementado.

Tabla N° 4

Pregunta a abogados del CAH ¿Considera usted que el número de ciberdelitos se ha incrementado?

Alternativa	Frecuencia	Porcentaje
Si	40	100%
No	0	0%
TOTAL	40	100%

Fuente: Elaboración propia



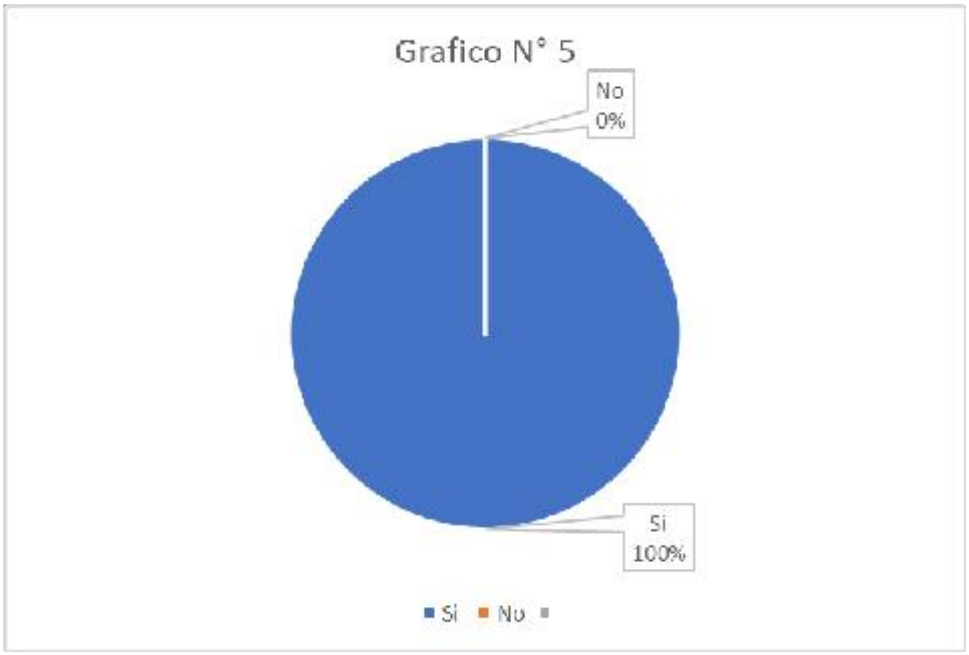
Del análisis de los resultados antes vistos se observa que de los 40 abogados colegiados del C.A.H en su totalidad coincide con que ciberdelincuencia se han incrementado, reflejando una realidad antes mencionada, pues el incremento de estos nuevos casos genera una mayor carga y la creación de nuevos delitos generan un poca o nula eficiencia al momento de aplicar solo los delitos tipificados en el Código penal, dejando la puerta abierta a crear nuevos delitos y que estos no gocen de la tipificación necesaria.

Tabla N° 5

Pregunta a los efectivos PNP ¿Es mayor el número de clientes que buscan su asesoría en casos de violación a la información privada que los casos de fraude bancario?

Alternativa	Frecuencia	Porcentaje
Si	6	100%
No	0	0%
TOTAL	6	100%

Fuente: Elaboración propia



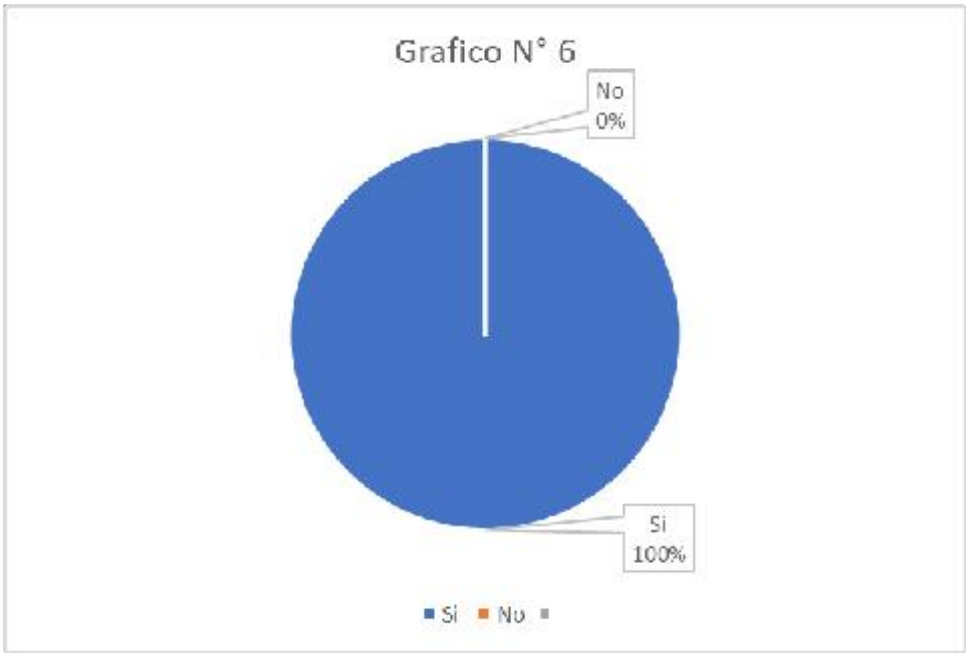
De los resultados anteriores se puede observar que los efectivos PNP cuentan con una mayor incidencia de los casos de ciberdelincuencia, es claro entonces que los afectados de los delitos de fraude bancario buscan en su mayoría la experiencia y pericia de los efectivos PNP.

Tabla N° 6

Pregunta a abogados del CAH ¿Es mayor el número de clientes que buscan su asesoría en casos de violación a la información privada que los casos de fraude bancario?

Alternativa	Frecuencia	Porcentaje
Si	40	100%
No	0	0%
TOTAL	40	100%

Fuente: Elaboracion propia



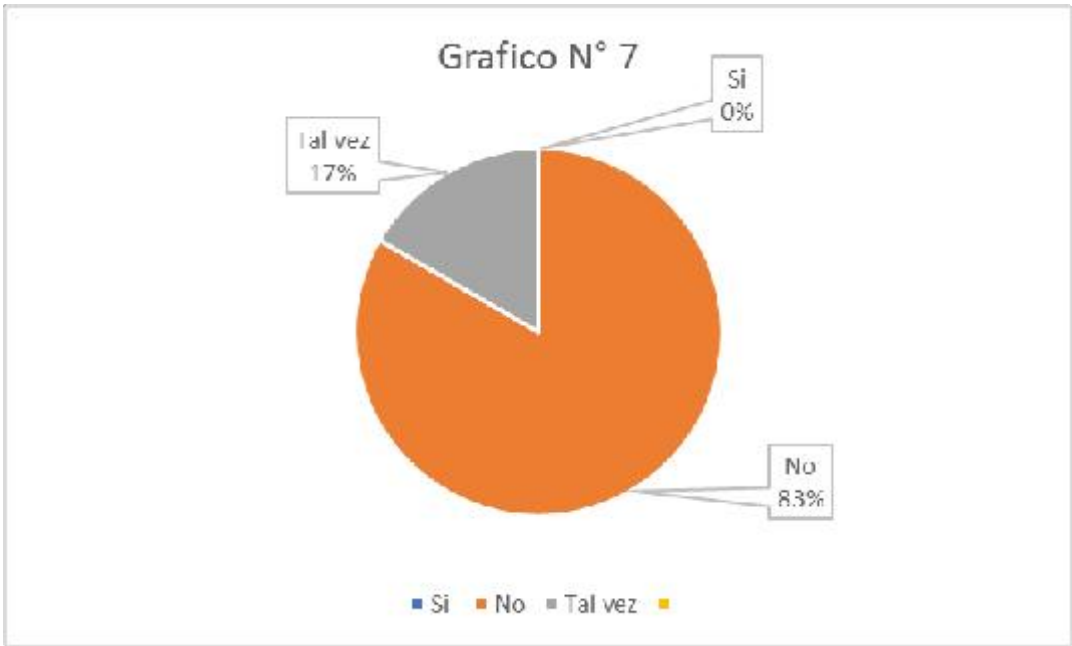
Del análisis de los resultados antes vistos se observa que de los 40 abogados colegiados del C.A.H en su totalidad coincide con que ciberdelincuencia se han incrementado, reflejando una realidad antes mencionada, pues el incremento de estos nuevos casos genera una mayor carga de asesorias, entonces de esta manera se refleja que los delitos de ciberdelincuencia se han incrementado, en un panorama claro y permisivo de la norma penal.

Tabla N° 7

Pregunta a los efectivos PNP A su parecer, ¿la adecuación normativa resulta adecuada para la persecución de delitos informáticos?

Alternativa	Frecuencia	Porcentaje
Si	0	0%
No	5	83.33%
Tal vez	1	16.67%
TOTAL	6	100%

Fuente: Elaboración propia



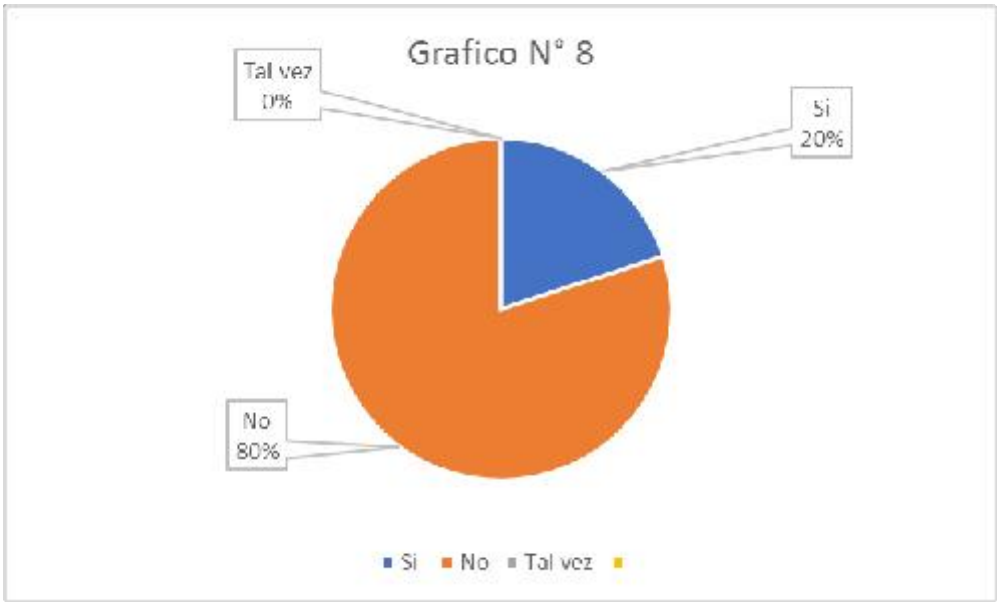
Del cuadro anterior se puede observar que los efectivos PNP quienes cuentan con una mayor incidencia de los casos de ciberdelincuencia, 5 de los 6 efectivos PNP entrevistados consideran que la adecuación normativa vigente no resulta efectiva para perseguir los delitos informáticos, y 1 de ellos considera que tal vez resulte eficiente. Los nuevos delitos informáticos que surgen con la modernidad tecnológica cambiaron bastante desde que la presente ley fue divulgada.

Tabla N° 8

Pregunta a abogados del CAH A su parecer, ¿la adecuación normativa resulta adecuada para la persecución de delitos informáticos?

Alternativa	Frecuencia	Porcentaje
Si	8	20%
No	32	80%
Tal vez	0	0%
TOTAL	40	100%

Fuente: Elaboración propia



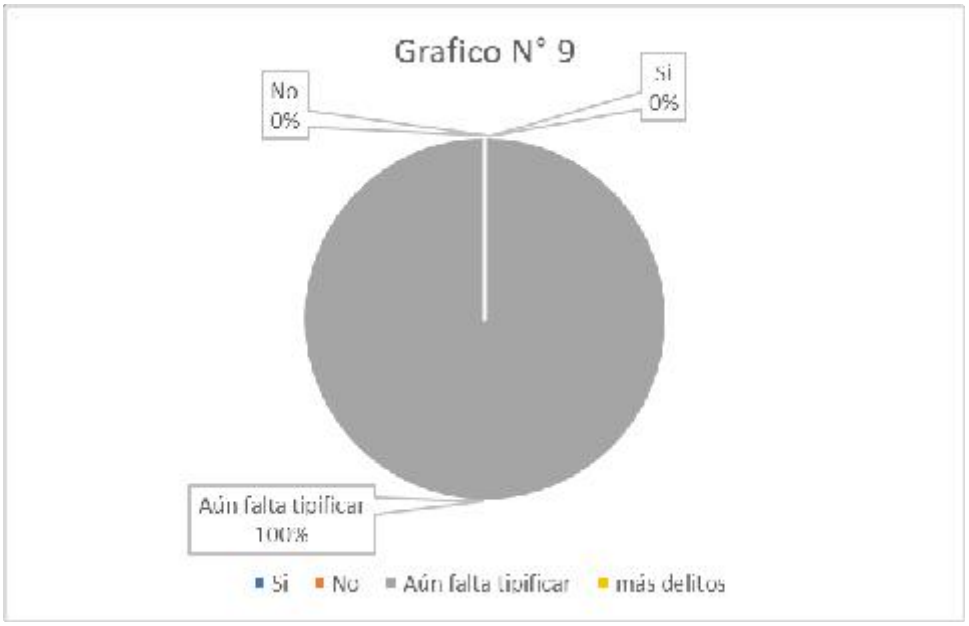
Del anterior cuadro se desprende los siguientes resultados de los 40 entrevistados 8 consideran que si la adecuación normativa vigente resulta adecuada para la persecución de los delitos informáticos y 32 restantes consideran que la adecuación normativa vigente no resulta eficaz al momento de perseguir delitos informáticos, generando una indebida protección del bien jurídico protegido, de este modo se refleja la realidad ya antes desarrollada y esto es porque la norma vigente resulta desfasada para los nuevos delitos que han ido evolucionando conforme con el avance de la tecnología y las diversas plataformas que aseguran ser confiables e inducen a el error generando que se introduzcan datos personales e información bancaria que luego puede ser usada con fines ilícitos.

Tabla N° 9

Pregunta a los efectivos PNP ¿Considera usted que con esta ley los delitos informáticos son plenamente identificados?

Alternativa	Frecuencia	Porcentaje
Si	0	0%
No	0	0%
Aún falta tipificar más delitos	6	100%
TOTAL	6	100%

Fuente: Elaboración propia



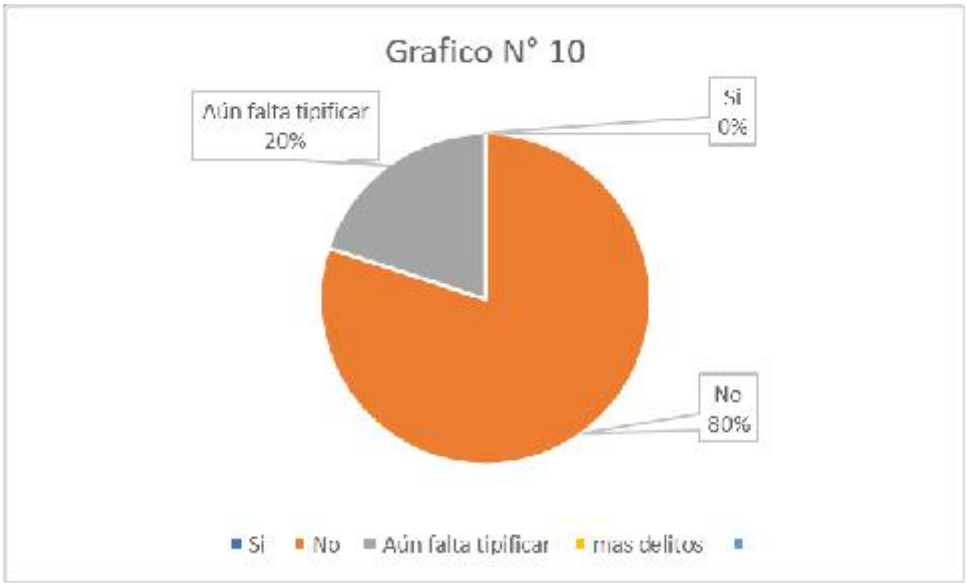
Ante esta pregunta los efectivos PNP en su totalidad respondieron que aun falta tipificar mas delitos, en ese sentido se desarrolla mejor la idea que aun no existe una plena tipificación de los delitos informáticos, es en ese sentido que resulta necesario volver a analizar los nuevos delitos y sus nuevas modalidades pues estos han variado a lo largo de la evolución histórica de la tecnología.

Tabla N° 10

Pregunta a abogados del CAH ¿Considera usted que con esta ley los delitos informáticos son plenamente identificados?

Alternativa	Frecuencia	Porcentaje
Si	0	0%
No	32	80%
Aún falta tipificar más delitos	8	20%
TOTAL	40	100%

Fuente: Elaboración propia



Del anterior cuadro se desprende los siguientes resultados de los 40 entrevistados 8 consideran que aún faltan tipificar más delitos y 32 restantes consideran que la esta ley los delitos informáticos no están plenamente identificados dejando claramente un nuevo tipo de ilícitos que generan una desprotección de las personas y del bien jurídicamente protegido.

Tabla N° 11

Pregunta a los efectivos PNP ¿Considera usted que realizando una ampliación normativa a la ley N° 30096 se lograría reducir el índice de delincuencia informática?

Alternativa	Frecuencia	Porcentaje
Si, así lo considero	6	100%
No, considero que no sería suficiente	0	0%
No se	0	0%
No opino	0	0%
TOTAL	6	100%

Fuente: Elaboración propia

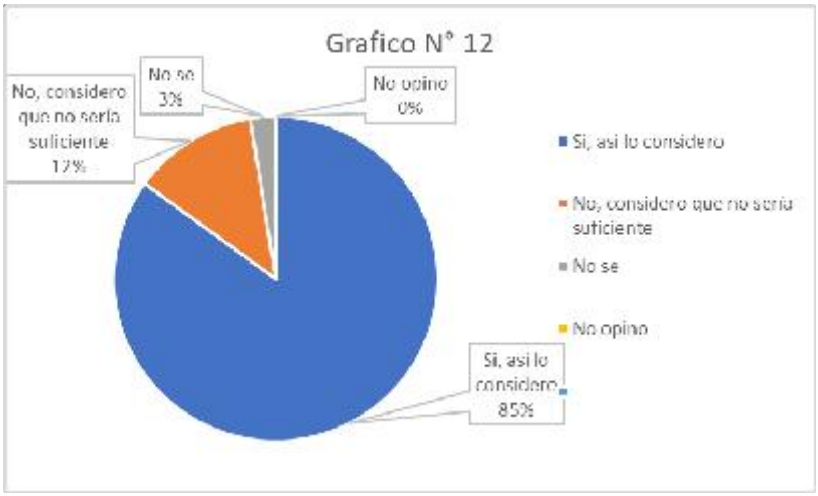
Como respuesta a esta pregunta tenemos los siguientes resultados, en su totalidad los efectivos PNP consideran que realizando una ampliación normativa a la ley N° 30096 se lograría reducir el índice de delincuencia informática, pues con una ampliación normativa se incluirían nuevos ciberdelitos y esto permitiría una mejor persecución de los ilícitos, generando un estado pleno de derecho.

Tabla N° 12

Pregunta a abogados del CAH ¿Considera usted que realizando una ampliación normativa a la ley N° 30096 se lograría reducir el índice de delincuencia informática?

Alternativa	Frecuencia	Porcentaje
Si, así lo considero	34	85%
No, considero que no sería suficiente	5	12.5%
No se	1	2.5%
No opino	0	0%
TOTAL	40	100%

Fuente: Elaboración propia



Del anterior cuadro se desprende los siguientes resultados de los 40 entrevistados 34 consideran que realizando una ampliación normativa a la ley N° 30096 se lograría reducir el índice de delincuencia informática 5 consideran que no seria suficiente una ampliación normativa a la ley N° 30096 se lograría reducir el índice de delincuencia informática y uno no sabe si realizando una ampliación normativa a la ley N° 30096 se lograría reducir el índice de delincuencia informática sin embargo es de común opinión que si se realiza una ampliación normativa a la ley N° 30096 se lograría reducir el índice de delincuencia informática y esto concuerda con nuestra idea principal.

CAPÍTULO V

DISCUCIÓN

5.1.- Discusión de resultados:

Veíamos, por un lado, en el curso del desarrollo de las bases teóricas que en el marco del convenio de Budapest se pretendió perseguir y tipificar los delitos, que para entonces fueron los más vanguardistas posibles. Por otro lado, hemos constatado en el trabajo de campo como los delitos varían, cambian y se transforman en nuevos delitos dando paso a que los ilícitos penales que en un determinado tiempo o espacio fueron debidamente identificados, perseguidos y sancionador han variado en cuanto a los elementos constitutivos, variando de modalidad, diversificándose nuevas en nuevas formas de criminalidad. Así, por ejemplo el hacking ha abierto la puerta a nuevas tendencias del robo de información y resulta nula la estrategia de los diversos órganos de persecución delictiva pues la norma vigente no permite identificar a cabalidad y procesar debidamente estos ilícitos penales, lo que genera entonces que se vulneren derechos de la población.

Pero resulta que aquella dinámica del desarrollo de la delincuencia no se corresponde con la dinámica legislativa. Así, la norma vigente resulta obsoleta y sale a flote la necesidad de cambiar o ampliar dicha norma con el fin de poder perseguir los nuevos delitos informáticos, cabe resaltar a su vez que dichos delitos informáticos seguirán mutando y la necesidad de crear nuevos cuerpos normativos no va a detenerse, sin embargo es necesario que se dé lugar a una ampliación normativa con la opinión de entendidos en el tema.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1.- Conclusiones:

PRIMERA: El marco normativo contenida en la ley N° 30096 es un marco normativo de vigencia actual pero desactualizada en cuanto a que los criterios allí tenidos en cuenta como hechos constitutivos de delitos no responden a los criterios prácticos alcanzados por la tecnología. Ha devenido en desactualizada al no comprender de forma precisa al hacking, el phishing o el robo de información bancaria mediante la clonación de páginas de entidades financieras.

SEGUNDO: Como la delincuencia tradicional, el ciberdelincuente como actividad humana evoluciona, cambia, aprovechando los recursos de la tecnología y de la ciencia. Así, el reto es que el marco normativo debiera permitir diferenciar la tipología que vaya surgiendo en el curso de su evolución. Así por ejemplo, habría que diferenciar la delincuencia cuyo objetivo principal es el de obtener una rentabilidad económica como fruto de sus actos, como las estafas o robos de información y sus principales medios de acceso a las víctimas han pasado de ser el correo electrónico y los sitios web; de los que “infectan” los software y programas contenidos en terminales, a través del acceso al internet. Estos, de forma similar a una contaminación ambiental, afecta a un número indeterminados de personas. Esta tipología correspondería a los denominados delitos de peligro.

6.2.- Recomendaciones:

PRIMERO: Urgente apertura una línea de debate a través del Poder Legislativo que incorpore la participación de las secciones especializadas del Ministerio Publico y de la PNP como entes informantes del detalle de modalidades existentes en el uso de los recursos informáticos vinculadas a perjuicio de los ciudadanos.

SEGUNDO: En la misma línea de la conclusión precedente, debiera exigirse que los softwares que operan en los terminales para acceder al internet estén condicionado a la identificación real del usuario. De modo tal que, el tránsito de un usuario por las redes ocurra realmente identificado.

TERCERO.- La normatividad preventiva debiera vincular la identificación real de usuario con el IP de los terminales con los que se accede al internet.

CAPÍTULO VII

FUENTES DE INFORMACIÓN

5.1.- Fuentes bibliográficas:

Bramont- Arias Torres, Luis A. (Lima:2000). *"Delitos informáticos"*.

Elías Puelles, Ricardo (Lima 2014). *Luces y sombras en la lucha contra la delincuencia informática en el Perú.*

Finckenauer, James O. (Barcelona 2010) *Mafia y crimen organizado*.

Reyna Alfaro, Luis (Lima 2002) *Los Delitos Informáticos Aspectos Criminológicos Dogmáticos y de Política Criminal*.

Savaro Carlos (Argentina 2014). *Nuevas tecnologías y conductas delictivas.*

Velarde, José (Lima 2014*). "Delitos Económicos y Empresariales"*

Zaffaroni, Raúl. (Buenos Aires 2012), *La cuestión Criminal*.

AZAOLA CALDERON, Luis (México 2010). *Delitos informáticos y Derecho penal"*

5.2.- Fuentes hemerográficas:

Ramón Ruiz, Luis. Revista de Ciencias Jurídicas Nº 146 (65-128). Mayo-Agosto 2018. *De la inmigración ilegal y su tratamiento político criminal en los contextos europeo y latinoamericano bajo el enfoque de la seguridad.*

López Martín, S. Revista de Estudios de Juventud. Madrid 2018. *«Jóvenes, Internet y Movimiento Antiglobalización: usos activistas de las Nuevas Tecnologías»*,

Montezuma Panez, Oscar. Revista de la Asociación Peruana de Propiedad

Intelectual. LIMA 2016. *El derecho de las telecomunicaciones, tecnologías de la información y propiedad intelectual.*

5.3. Fuentes documentales:

Boletín jurídico. Freno a la ciberdelincuencia. Noviembre 2013

Convenio sobre la Cibercriminalidad de 23 de noviembre de 2001 del Consejo de Europa

5.4. Fuentes electrónicas

ACURIO DEL PINO, SANTIAGO, Delitos Informáticos: generalidades, publicación en línea, págs. 20 ss.

http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf.

Artículo 2 del Estatuto de la Organización Internacional de la Policía Criminal-Interpol. Véase su página Web oficial: http://www.interpol.int

SALT G. Marcos, Informática y Delito, Publicación en Internet, URL: http://www.derecho.org.ar

WILLIAMS PHIL, Crimen Organizado y Cibernético, sinergias, tendencias y respuestas. Centro de Enseñanza en Seguridad de la Internet de la Universidad Carnegie Mellon. http://www.pitt.edu/~rcss/toc.html

REYNA ALFARO Luis Miguel, Fundamentos para la protección penal de la información Como valor económico de la empresa. Publicación hecha en internet en www.dercho.org.pe.

MERLAT, Máximo, Seguridad Informática: Los Hackers, Buenos Aires Argentina, 1999, Publicación hecha en Internet. www.monografías.com

CUERVO José, Delitos Informáticos y Protección Penal a la Intimidad,

Publicación hecha en Internet URL: www.derecho.org

Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa [en línea]https://www.gdt.guardiacivil.es/webgdt/media/Legislacion/Protocolo_adicional_convencion_cibercrimen.pdf

El Parlamento Europeo investigará el espionaje electrónico de PRISM en los países de la Unión [Artículo]. http://es.engadget.com/2013/07/04/parlamento-europeo-investigara-espionaje-eeuu-prism

ANEXO 1

01. Matriz de Consistencia

PROBLEMA	OBJETIVOS	JUSTIFICACIÓN	HIPOTESIS	VARIABLE
Problema General ¿Cómo la adecuación normativa al convenio de Budapest que regula los delitos de ciberdelincuencia en el Perú resulta eficaz para el control de los delitos informáticos? Huaura 2018 **Problemas Específicos** ¿Cómo la adecuación normativa al Convenio de Budapest que regula los delitos de ciberdelincuencia en el Perú resulta eficaz para el control de los delitos informáticos? Huaura 2018 ¿Cuáles son las conductas en los medios informáticos que afectan bienes jurídicos pero que sin embargo no han sido señalados en la legislación nacional? Huaura 2018	**Objetivo General** Determinar si la adecuación normativa al convenio de Budapest que regula los delitos de ciberdelincuencia en el Perú resulta eficaz para el control de los delitos informáticos Huaura 2018 ¿Determinar cuáles son las conductas en los medios informáticos que Afectan bienes jurídicos pero que sin embargo no han sido señalados en la legislación nacional? Huaura 2018 ¿Determinar en qué circunstancias, forma, lugar y tiempo se cometen conductas, comportamientos, hechos a través de los medios informáticos para la comisión de delitos informáticos? Huaura 2018	La presente investigación se justifica en la medida que busca determinar los niveles de eficiencia y efectividad de la normatividad legal en relación al incremento de la ciberdelincuencia en el Perú. Hemos definido nuestro espacio de observación de campo en la provincia de Huaura, que debido a su población relativamente pequeña a nivel nacional nos permitirá observar el objetivo con mayor precisión de una realidad nacional. Los resultados que alcancemos con el presente proyecto serán de suma utilidad en el ámbito académico para otras investigaciones de temas conexos, así como para resaltar los aspectos técnicos del uso de los medios informáticos vinculados a la vulneración de bienes jurídicos. Estos delitos, con niveles de incremento masificado a través de tecnologías que evolucionan constantemente, con la velocidad distinta a la naturaleza de las normas jurídicas, exponen a estas a niveles ineficaces e incluso obsoletos	**Hipótesis General** La adecuación normativa al convenio de Budapest que regula los delitos de ciberdelincuencia en el Perú no es suficiente para el control de los delitos informáticos Huaura 2018 **Hipótesis Específicas:** **HE1.-**El robo de información confidencial, el hacking y el phishing son accionares delincuenciales que a la actualidad no han sido contempladas en el marco de la adecuación normativa nacional. HE2: Es incierto determinar en qué circunstancias, forma, lugar y tiempo se cometen estas conductas delictivas, esto se debe a la existencia de un realidad ficticia en un mundo virtual.	**Variable de la investigación** Adecuación normativa nacional **Variable Dependiente** Y su efectividad en la reducción de delitos informáticos en Lima 2018 Conductas que dañan bienes jurídicos a través de medios informáticos no contemplados en la legislación

ANEXO N° 2

UNIVERSIDAD NACIONAL "JOSÉ FAUSTINO SÁNCHEZ CARRIÓN"

FACULTAD DE DERECHO Y CIENCIAS POLITICAS

CUESTIONARIO

Buenos Días Estimado (a**)**, espero su colaboración respondiendo con responsabilidad y honestidad, el presente cuestionario. Se agradece no dejar ninguna pregunta sin contestar. El objetivo del presente proyecto, de la encuesta es: ***Determinar si es adecuación normativa al convenio de Budapest que regula los delitos de ciberdelincuencia en el Perú resulta eficaz para el control de los delitos informáticos Huaura 2018.***

La información que nos proporcione será de mucha importancia en la Tesis a mi cargo para la obtención del título de abogado en esta casa de estudios.

Instrucciones: Las preguntas han sido diseñada para una respuesta objetiva (Si o No). Lea cuidadosamente las preguntas y marque con un aspa (x) su respuesta.

INFORMACION GENERAL

Fecha y hora de realización	:	……./...../2019
Ocupación	:	Abogado/PNP
Experiencia profesional	:	Años: …..

PREGUNTAS

1) ¿Con que frecuencia ve usted casos de ciberdelincuencia?
   - 2 por mes
   - De 2 a 5 por mes
   - De 5 a 10 por mes
2) ¿Considera usted que el número de ciberdelitos se ha incrementado?
   - Si
   - No

3) ¿Es mayor el número de clientes que buscan su asesoría en casos de violación a la información privada que los casos de fraude bancario?

Si
No

4) A su parecer, ¿la adecuación normativa resulta adecuada para la persecución de delitos informáticos?

Si
No
A veces

5) ¿Considera usted que con esta ley los delitos informáticos son plenamente identificados?

Si
No
Aun faltan tipificar mas delitos

6) ¿Considera usted que realizando una ampliación normativa a la ley N° 30096 se lograría reducir el índice de delincuencia informática?

Si, así lo considero
No, consideró que no sería suficiente
No se
No opino