UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

El tratamiento jurídico penal por parte del fiscal en los delitos informáticos contra el patrimonio, distrito judicial de Lima Norte 2019

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogado

AUTOR:

Gómez Vásquez, Jean Carlos (ORCID: 0000-0001-5258-7163)

ASESOR:

Mg. Aceto, Luca (ORCID: 0000-0001-8554-6907)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal, Procesal Penal, Sistema de Penas, Causas y Formas del Fenómeno Penal

LIMA – PERÚ

2020

DEDICATORIA

El presente trabajo está dedicado a mi familia por haber sido mi apoyo a lo largo de toda mi carrera universitaria y a lo largo de mi vida. A todas las personas especiales que me acompañaron en esta etapa, aportando a mi formación tanto profesional y como ser humano.

AGRADECIMIENTO

El presente trabajo agradezco a Dios por ser mi guía y acompañarme en el transcurso de mi vida, brindándome paciencia y sabiduría para culminar con éxito mis metas propuestas. A mi familia, por haberme dado la oportunidad de formarme en esta prestigiosa universidad y haber sido mi apoyo durante todo este tiempo.

ÍNDICE

Índice de tablas

RESUMEN

La presente investigación lleva por título “El Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, Distrito Judicial de Lima Norte 2019”, el cual tuvo como objetivo general Determinar de qué manera se da el Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019. Para poder llevar a cabo la investigación se utilizaron diferentes herramientas propias de la investigación cualitativa, de nivel descriptivo, también se empleó la guía de entrevista, con la cual se recopiló información brindada por fiscales del distrito judicial de Lima-Norte, así como también la guía de análisis de fuente documental en la que se analizaron diferentes artículos científicos nacionales y extranjeros.

De tal manera que se concluyó que, Debido a la naturaleza de los delitos informáticos contra el patrimonio, el tratamiento jurídico penal por parte del fiscal se da de una manera deficiente ya que el marco legal sobre los delitos informáticos contra el patrimonio solo se encuentra enmarcados dentro del delito de fraude informático lo cual resulta insuficiente para las distintas modalidades que se presentan lo que no permite tener un marco de referencia adecuado para combatir estas situaciones, toda vez que la normativa sobre delitos informáticos en el país se da de manera muy generalizada.

Finalmente se recomienda que el Ministerio Público debería crear fiscalías especializadas en delitos informáticos para que así se pueda dar un adecuado tratamiento jurídico penal por parte del Fiscal en esta clase de delitos, así mismo se podrían tener las herramientas adecuadas para realizar las investigaciones preliminares y no tener que derivarlas en sede policial; por ende, no se tendrían investigaciones fuera de plazo en el despacho Fiscal.

Palabras clave: *Delitos informáticos, criminales informáticos, fraude informático, patrimonio e informática.*

ABSTRACT

The present investigation is entitled "The Criminal Legal Treatment by the Prosecutor in Computer Crimes against Heritage, Judicial District of Lima Norte 2019", which had the general objective of Determining how the Criminal Legal Treatment is given by the Prosecutor in Computer Crimes against Heritage, in the Judicial District of Lima Norte 2019. In order to carry out the investigation, different tools typical of qualitative research, at a descriptive level, will be used, the interview guide was also used, with which will gather information provided by prosecutors from the Lima-Norte judicial district, as well as the documentary source analysis guide in which different national and foreign scientific articles will be analyzed.

In such a way that it was concluded that, due to the nature of computer crimes against patrimony, the criminal legal treatment by the prosecutor is given in a deficient way since the legal framework on computer crimes against patrimony is only framed within the crime of computer fraud, which is insufficient for the different modalities that are presented, which does not allow having an adequate frame of reference to combat these situations, since the regulations on computer crimes in the country are very generalized.

Finally, it is recommended that the Public Ministry should create specialized prosecutors in computer crimes so that an adequate criminal legal treatment can be given by the Prosecutor in this type of crime, as well as having the appropriate tools to carry out preliminary investigations and not having to refer them to the police headquarters; therefore, there would be no late investigations in the Fiscal office.

Keywords: *Computer crime, computer criminals, computer fraud, Heritage and computer science.*

I.Introducción

Respecto a la aproximación temática**,** el presente proyecto de investigación tuvo como propósito determinar de qué manera se da el tratamiento jurídico penal por parte del fiscal en los delitos informáticos contra el patrimonio en el distrito judicial de Lima Norte, ya que Durante estas últimas décadas hemos sido testigos que el avance tecnológico se ha desarrollado de una manera exponencial, tanto es así, que podríamos considerarlo como un miembro más de la familia, esto debido a que la globalización está presente en nuestro día a día, en nuestros hogares, en el entorno social, laboral, jurídico, político, religioso, en la investigación científica, entre otras tantas actividades que involucran el desarrollo personal del ser humano. Es así que nos encontramos ante una situación en que el avance tecnológico aporta de manera productiva a la persona humana, pero como toda situación favorable también pueden presentarse acciones que pueden perjudicar a todos los que nos beneficiamos con la tecnología y causar así perjuicios a nuestro patrimonio o incluso acceder a datos personales que uno puede tener en sistemas de entidades públicas o privadas.

De esta manera nos encontramos con el principal problema que en la actualidad afronta el avance de la tecnología, que es la ciberdelincuencia, este problema ha ido creciendo en la actualidad, ya que estos ciberdelincuentes están en constante cambio con relación a la manera en que operan, desplazando de esta manera lo que el legislador pudo prever al momento de redactar las acciones que podrían configurarse como delitos informáticos, pero esto no solo se da en Perú, ya que el derecho penal en muchos países ha quedado en el tiempo, pese a que en nuestro país se han realizado modificatorias a la última ley especial de delitos informáticos en el año 2014. A diferencia de la legislación peruana, con respecto a los delitos informáticos, la ciberdelincuencia se ha encontrado en constante evolución, de tal manera que en la actualidad existen diferentes formas en las cuales estos ciberdelincuentes pueden acceder y vulnerar los datos de las personas para obtener algún tipo de provecho sobre el patrimonio de terceros, pero no solo afectar el patrimonio intangible en el sistema informático, sino también el acceder a información personal que puede ser comercializada como base de datos a extraños con cualquier finalidad ilícita, generando así que la persona usuaria de estos

servicios informáticos se encuentre en constante estado de vulneración de estos ciberdelincuentes y en gran parte de los casos sin que la víctima se percate de estos hechos hasta que ya se vea afectado.

Pese a existir diferentes vulneraciones que se pueden presentar ante los delitos informáticos, en esta investigación se va hacer un claro énfasis en los delitos informáticos específicamente contra el patrimonio, ya que en la legislación actual solo nos habla de fraude informático como único delito informático contra el patrimonio, toda vez que los sujetos pasivos de este acto ilícito pueden ser tanto persona natural como jurídica. A esta falencia que existe en la norma, le debemos sumar la capacidad de estos ciberdelincuentes para poder realizar estos hechos generando así una gran dificultad en la persecución punitiva que se le puede aplicar ante estos hechos. Por otro lado, el derecho penal, ha variado sus formas y ámbitos de intervención en ciertas conductas punibles para salvaguardar la sociedad, pero los tiempos han cambiado, de tal manera que el ciberdelincuente que realiza este tipo de acciones ilícitas puede estar cometiendo este acto en un continente, pero afectando a un tercero en otro continente generando así una sensación de inseguridad constante en la persona que no tiene conocimiento en qué momento puede ser vulnerado. Esta situación ha generado que las denuncias se incrementen en estos últimos años en las distintas fiscalías a nivel nacional, pero por su particularidad de ser delito informático, el tratamiento jurídico penal que se le da por parte de los fiscales es muy limitado ya que no se tiene una legislación adecuada para que se configure el delito, ya que no solo existe el fraude informático como delito informático contra el patrimonio, sino que tenemos hurto, estafa y sabotaje informático, así que no podemos encajar todas estas conductas en un solo delito como el de fraude informático.

Ahora, sobre la formulación del problema, Debido al avance tecnológico que existe en la actualidad. Pons (2017) refirió que existe una total dependencia de los sistemas informáticos por parte de la sociedad, por lo que se abrieron espacios para nuevos comportamientos en los delincuentes; por lo que es necesario tener una adecuada seguridad informática, como lo señalaron Candelario y Rodríguez (2015) abordando el tema de seguridad informática teniendo como labor principal resguardar la información de los usuarios desde su confidencialidad, integridad y

disponibilidad para evitar que se suplante información y brindar una garantía a las personas. Así mismo la justificación de nuestro estudio, se centró en el análisis de la recolección de datos, que permitió determinar si en la práctica a nivel fiscal se da un adecuado tratamiento jurídico penal a los delitos informáticos contra el patrimonio, toda vez que la normativa especial contra estos delitos no es suficiente para realizar una adecuada etapa de investigación preliminar, ya que gran parte de estos hechos termina archivándose en su mayoría por falta de interés de la persona, así como también al no tener una individualización concreta de la persona que cometió el hecho delictivo. Sobre el Objetivo General, este fue Determinar de qué manera se da el Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019. Para ello se planteó dos Objetivos específicos, siendo el primero de ellos determinar cómo el abuso informático influye en el acceso no autorizado a servicios informáticos, y el segundo establecer que tan efectivo es el reconocimiento del bien jurídico protegido en los delitos informáticos, ante el fraude informático. Se ha planteado como Supuesto Jurídico General, que los delitos informáticos contra el patrimonio se vienen cometiendo con mayor frecuencia en el país, esto debido a que existe una errónea tipificación de la norma penal con relación a esta clase de delitos, ya que en la Ley 30096 solo se considera al Fraude Informático, cuando en realidad existen diferentes conductas que no se configuran en el tipo penal del Fraude Informático, además como Supuesto Jurídico Específico 1, Los criterios en la calificación en los delitos informáticos contra el patrimonio, específicamente en el de fraude informático son ambiguos, toda vez que existen diferentes modalidades y que no necesariamente tienen que ser cometidos desde el país, ya que por los alcances de la tecnología pueden cometerse desde otro continente, como Supuesto Jurídico Específico 2, tenemos que en la Legislación Peruana existe una sanción por incurrir en la conducta de Fraude Informático, pero este suele ser insuficiente ya que en la mayoría de casos, los afectados solo realizan su denuncia con la finalidad de recuperar su dinero, y así una vez cumplido ese objetivo ya no continúan con la investigación generando así que gran parte de esos casos se archive por falta de interés de los afectados.

II. Marco Teórico

Sobre el marco teórico, comenzamos con los trabajos previos a nivel Internacional, siendo la primera, la tesis titulada “Investigación y Prueba del Ciberdelito”, elaborada por Quevedo (2017) para optar por el grado de Doctor por el Departamento de Derecho y Ciencias Políticas de la Universidad de Barcelona, donde se concluyó que pese a las medidas que se puedan tomar para la investigación de estos ciberdelitos, estas no pueden exceder los límites establecidos dentro de los derechos constitucionales. Aunado a ello, cabe mencionar la tesis que tiene como título *“La Ciberdelincuencia y su Regulación Jurídica en Centroamérica con Énfasis en Costa Rica, El Salvador y Nicaragua”,* realizada por De la Cruz, Jirón y Miranda (2016), para optar por el grado de Licenciados en Derecho por la Facultad de Ciencias Jurídicas y Sociales de la Universidad Autónoma de Nicaragua (UNAN), en donde se concluyó que con el avance tecnológico, se está presentando diferentes formas, generando así que la legislación actual en Centroamérica sea insuficiente, por lo cual es necesario que se involucren los demás estados.

Además, se debe mencionar que la tesis que tiene como título “*La Odisea Procesal de la Criminalidad Informática*”, elaborado por Arocena (2016), para obtener el grado en derecho de la Facultad de Derecho de La Universidad del País Vasco/ Euskal Herriko Unibertsitatea, donde se concluyó que para la calificación de delitos informáticos se requiere un plus adicional a comparación con los delitos tradicionales, sin embargo el punto más sobresaliente es a nivel de fiscalía, ya que se dio la creación de la Fiscalía de Criminalidad Informática. Por otro lado, cabe mencionar la tesis elaborada por Devia (2017) que tiene como título *“Delito Informático: Estafa Informática del artículo 248.2 del Código Penal”,* para obtener el Grado de Doctor en Derecho, que sustentó en la Facultad de Derecho de la Universidad de Sevilla, en donde se concluyó que para dar una adecuada explicación a la relación que existe entre el delito y la informática, se debe tratar desde la perspectiva de los delitos tradicionales ya que gran parte de los bienes jurídicos que se afectan ya están reconocidos en la norma solo que en esta clase de delitos se utiliza como medio de comisión la tecnología informática.

Sobre los antecedentes a nivel nacional, tenemos, la tesis que lleva como título *"La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096, Perú-2017",* elaborada por Hancco (2017), para obtener el Título Profesional de Abogado que sustentó en la Facultad de Derecho de la Universidad Nacional de San Agustín, donde se concluyó que el tipo penal informático, resulta totalmente innecesario, toda vez que los bienes jurídicos que se busca proteger en la ley antes mencionada ya se encuentran protegidos en un tipo penal más amplio. Además de ello, cabe mencionar la tesis que tiene como título *"Los Factores Principales que Impiden la Aplicación de la Ley N°30171-Lima Norte en el Año 2016",* elaborada por Cotrina (2018) para obtener el Título Profesional de Abogado por la Facultad de Derecho de la Universidad César Vallejo, donde se concluyó que uno de los factores determinantes para la correcta aplicación de la Ley N°30171, es la falta de capacitación de los magistrados, fiscales y efectivos de la P.N.P en esta clase de ciberdelitos.

Por otro lado, es menester acotar la tesis titulada *"Los Hackers: "Delito Informático frente al Código Penal Peruano",* elaborada por Vilca (2018) para obtener el título de profesional de abogado la Facultad de Derecho de la Universidad Nacional Santiago Antúnez de Mayolo, donde finalmente se concluyó que la falta de información en esta clase de delitos, no permite tener un marco de referencia adecuado para combatir estas situaciones, toda vez que la normativa sobre delitos informáticos en el país se da de manera muy generalizada. Otro trabajo de investigación es la tesis que se titula *"Proyecto Legal para un Esquema Nacional de Ciber Seguridad",* elaborada por Parra (2016) para obtener el Título Profesional de abogado por la Facultad de Derecho de la Universidad San Martín de Porres, de acuerdo a la conclusión planteada por el investigador, hace una apreciación un poco más extensiva, comparando al Estado Peruano en relación con los demás países, toda vez que el Perú no ha sufrido un ciber ataque a mayor escala, pero que por esa razón no debe ser expectante de la realidad problemática que se presentan en diferentes países, por lo cual es necesaria una adecuada proyección por parte del Estado con otros órganos estatales para estar alertas ante futuros ciber ataques.

Referente al marco teórico, comenzamos con el tratamiento jurídico penal por parte del fiscal definiendo el bien jurídico protegido que se tiene que resguardar en esta clase de delitos, también el abuso informático con respecto al incremento de nuevas tecnologías que favorecen a la criminalidad informática; así como también las diferentes modalidades más comunes utilizadas por los ciberdelincuentes para cometer ciberdelitos.

Sobre el tratamiento jurídico penal por parte del fiscal, se busca es poder tratar de identificar, como se da el desarrollo de la investigación preliminar por parte del fiscal. De acuerdo a Rodríguez y Pino (2015) señaló que la norma procesal otorga herramientas legales para que el RMP pueda llevar a cabo las investigaciones, dejando a su discrecionalidad continuar o no con las investigaciones, ello relacionado con el criterio que se tiene para poder calificar las denuncias ya sea basado en el análisis doctrinario, jurisprudencial y normativo relacionado a los delitos informáticos contra el patrimonio, para así poder determinar las diferentes modalidades que se presentan en torno al fraude informático. Con respecto a la etapa previa de la investigación Peralta, Gutiérrez y Lara (2017) refirieron que es primordial integrar en la disposición de apertura fiscal una precisa y coherente base jurídica para que así se pueda materializar de una manera adecuada el hecho imputado para así evitar inconvenientes ante una futura judicialización de la investigación fiscal. Siguiendo con las principales funciones del titular de la acción penal, Matusan (2013) acotó que la acción del Fiscal es de suma importancia para poder asegurar las evidencias o medios probatorios idóneos que puedan soportar su teoría del caso y de ser necesario precluir la investigación llegando a un acuerdo con la defensa del imputado, lamentablemente en esta clase de delitos es muy difícil llegar a tener un imputado totalmente individualizado por la complejidad misma de esta clase de delitos. Siguiendo con el tratamiento jurídico penal por parte del Fiscal, es elemental señalar a Núñez y Correa (2017) quienes refirieron que la labor investigativa no se desarrolla en un mundo abstracto, sino por el contrario, ya que se ejecuta en una sociedad donde existen diferentes relaciones interpersonales que son titulares de derechos por lo cual se tiene que establecer claramente los limites en los cuales se llevará a cabo la investigación para no vulnerar derechos constitucionales de terceros.

Con relación al bien jurídico protegido se está dando una nueva postura en la cual hacen claro énfasis en la afectación a la funcionalidad informática como interés colectivo, como bien jurídico no convencional a proteger, es así que Mayer (2017) mencionó que, La funcionalidad informática sirve al conjunto de las personas y es, a partir de esta figura que se presenta como un bien jurídico colectivo. Por ende, se presenta de forma que el uso y disfrute no es propio ni excluyente de persona alguna, ni puede distribuirse entre algunos individuos. Se presenta, asimismo, de un interés social relevante para el individuo, que está vinculado, de una u otra forma, con la labor habitual de todos quienes integran un determinado sistema. Esta transgresión al funcionamiento informático afecta al libre desarrollo de las personas que usan algún dispositivo electrónico con acceso a una interconexión, como lo es el internet. Es así que tenemos que la funcionalidad informática está a disposición de otros bienes jurídicos, pero al verse afectados estos bienes jurídicos por una afectación al correcto funcionamiento del sistema informático, nace la necesidad de resguardar y conservar un adecuado funcionamiento de dichos sistemas. De igual manera Prado y Durán (2017) refirieron que para la protección penal de bienes jurídicos supraindividuales se deben dar en base a intereses difusos que conllevarían a proteger nuevos intereses colectivos a través del sistema jurídico por medio de nuevos medios y no por la tradicional categoría del bien jurídico tradicional. Es así que Roxin (2013) señaló que la estabilización de la norma penal no tiene un fin en sí mismo sino por lo contrario, ya que está destinada a que no se produzcan lesiones reales, individuales o sociales con respecto a los bienes jurídicos protegidos.

Sobre el abuso y criminalidad informática, en la actualidad nos encontramos en un auge de nuevas tecnologías con relación a la era informática, por lo cual es necesario establecer las pautas previas para determinar la criminalidad informática, toda vez que la informática es un fenómeno ilimitado y que aún falta mucho por descubrir, por lo cual debemos adecuarnos al contexto moderno en materia de criminalidad informática. Según Arocena (2012) mencionó que, nos encontramos en una realidad en la cual la delincuencia dolosa tradicional, ha adoptado nuevas técnicas con el progreso tecnológico permitiendo así que se produzcan resultados lesivos y generando así el surgimiento de nuevas modalidades delictivas. De la misma manera en la que se están incrementando estos actos ilícitos, también se

está dando una amplia aparición de ciberdelincuentes, que no necesariamente son personas adultas, pero sí con conocimientos en informática.

Por su parte Hernández (2017) señala que nos encontramos en un nuevo escenario en el cual la información va adquiriendo vital importancia en la sociedad, ya que es difícil imaginar que por lo menos exista alguna empresa que no use computadoras para almacenar, procesar o transmitir una gran cantidad de datos, desafortunadamente la tecnología no es usada solo para situaciones provechosas, sino que también para cometer conductas antisociales, siendo su principal característica el uso de un sistema o red informática llegando a establecer a la computadora como un método, medio o fin de determinada conducta delictiva. En ese mismo sentido Picotti (2013) refirió que ante la aparición y desarrollo de estos nuevos delitos es necesario para la incriminación, que el legislador, dentro de los elementos constitutivos, el imprescindible uso de tecnología y productos informáticos o por lo menos la producción de efectos sobre ellos. Con respecto a las características de los individuos vinculados a esta clase de delitos Montiel (2016) señaló que se da un círculo vicioso entre los cibercriminales, las ciber víctimas y los investigadores, esto debido a la lentitud que existe en los avances legales, así como también inexperiencia y falta de recursos de los cuerpos policiales debido a la complejidad de las investigaciones, dándose así una facilidad a que se continúen cometiendo estas conductas ilícitas; debido a ella es que se da una baja tasa de denuncias relacionadas a los ciberdelitos. Dentro del desarrollo de la actividad social Pifarré (2013) refirió que el desplazamiento de la vida cotidiana a la red ha conllevado también a que los comportamientos delictivos se trasladen a ella generándose lesiones a bienes jurídicos tradicionales y no tradicionales. Al llevar estos delitos a otro contexto como es la red informática genera nuevos comportamientos, Sánchez (2012) delimitó al cibercrimen desde el delito económico, como el fraude informático, el robo, la falsificación, el computer hacking, el espionaje informático, el sabotaje, la extorsión informática, la piratería comercial y otros crímenes, aduciendo que los cibercriminales se valen del ciberespacio para poder realizar esta clase de comportamientos sin dejar muchos rastros.

Por otro lado, Campos (2016) realizó una clasificación más general señalando que los delitos informáticos se clasificaban dos grupos; el primero el que usa la

tecnología como medio para la conducta ilícita y un segundo grupo en el cual se utiliza la tecnología como fin para el comportamiento lesivo. Pese a la variada doctrina que se viene desarrollando sobre el tema, los casos en los países van ir variando, ya que como señaló Mayer (2018) la criminalidad informática se centra principalmente en descripciones típicas que no siempre van a coincidir en el contexto nacional al que se desea aplicar y si a eso le sumamos que gran parte de estos actos no se realizan desde el mismo país, sino que puede provenir del extranjero. Por otro lado nuestra ley vigente sobre delitos informáticos contra el patrimonio solo prevé al fraude informático como modalidad para afectar el patrimonio, es así que Acurio (2017) señala que el carácter informático alude solo al medio con el cual se efectuó la defraudación, ya sea el aprovechamiento, utilización, o abuso de las funcionalidades de los sistemas informáticos para lo cual el autor acota que para que primero se presente una defraudación informática primero tiene que ser una defraudación simple. Lamentablemente no es la única manera en la que puedan vulnerar nuestra información personal, así lo postuló Celorio (2016) quien refirió que cada vez que navegamos en internet, a través de cookies y web bugs, terceros pueden obtener información de nuestras búsquedas, segmentándonos hacia un sector empresarial determinado, está clara vulneración no nos va perjudicar siempre y cuando nuestra información no caiga en manos erróneas y que a la larga nos traiga un perjuicio; tratando de prevenir diferentes conductas lesivas gracias a la tecnología, las Naciones Unidas a través de la comisión de Prevención del Delito y Justicia Penal, establecieron el Convenio de Budapest (2004), siendo su principal objetivo una adecuada política penal con una adecuada legislación siendo su mayor aporte la cooperación internacional de los países adheridos a este convenio (Arguelles, 2016).

III.Metodología

El enfoque que se empleó en el presente proyecto de tesis, es de enfoque Cualitativo, en el cual se ha comenzado examinando los hechos y en el proceso se va desarrollando una teoría coherente para poder representar lo que se observa, es así que Cadena, Rendón, Aguilar, Salinas, De la Cruz y Sangerman (2017) refirieron que lo que se busca en este enfoque es poder determinar la naturaleza de la realidad que se está investigando a través de una muestra para obtener mayor información y comprensión de los resultados obtenidos.

3.1 Tipo y Diseño de Investigación:

Sobre el tipo de investigación**,** es necesario precisar que es del tipo aplicada, como refirieron Coria, Pastor y Torres (2013) ya que tiene como propósito aplicar nuevos conocimientos y comprensión de determinados fenómenos sociales en la práctica. Con relación al diseño de investigación se aplicó el de teoría fundamentada, es así que Páramo (2015) señaló que el principal objetivo de este diseño es el de producir interpretaciones de los actores sociales acerca de las conductas sometidas al estudio, lo que conlleva al investigador a contrastar las entrevistas y la observación de conceptos teóricos para reconocer los temas fundamentales. El nivel de estudio utilizado en el presente proyecto de tesis, fue de nivel de investigación descriptiva, para lo cual Carrasco (2006) refirió que en este nivel de investigación nos va especificar sobre las características, cualidades externas e internas, propiedades y rasgos esenciales de los hechos y fenómenos de la realidad en un momento de tiempo histórico y concreto determinado. En pocas palabras es descriptiva porque se va realizar la descripción de cómo se da el fenómeno presentado en determinada realidad problemática.

3.2 Categorías, Subcategorías y Matriz de Categorización:

En el presente apartado, se determinó las categorías y subcategorías empleadas en esta investigación, siendo la primera categoría El Tratamiento Jurídico Penal por parte del Fiscal y la segunda categoría Delitos Informáticos contra el Patrimonio.

Categoría	Definición Conceptual	Definición Operacional	Subcategorías
El Tratamiento Jurídico Penal por parte del Fiscal	La afectación de la funcionalidad informática incide en el libre desarrollo de todas las personas por lo que resulta importante establecer un adecuado tratamiento jurídico penal por parte del Fiscal	Sobre el tratamiento jurídico penal por parte del fiscal, se busca es poder tratar de identificar, como se da el desarrollo de la investigación preliminar por parte del Fiscal.	Bien jurídico protegido en los Delitos Informáticos
			Criminalidad Informática
Delitos Informáticos contra el Patrimonio.	El delito de fraude informático se encuentra previsto en nuestra legislación en el artículo 8 de la Ley N° 30096, como ya podemos suponerlo lo que se busca en este delito es poder sancionar las conductas delictivas que tiene como fin atentar contra el patrimonio.	El delito de fraude informático comprende algunas acciones en su tipificación como, la de diseño, introducción, alteración, borrado, supresión, como alguna de las acciones que se pueden cometer en el fraude informático. (Villavicencio, 2015, p.29)	Fraude Informático
			El Acceso no Autorizado a Servicios Informáticos

Tabla 01: Matriz de Categorización

3.3 Escenario de Estudio:

El escenario de estudio, corresponde al lugar en el cual se va realizar la investigación de la realidad problemática presentada, con la finalidad de obtener los datos necesarios para poder absolver las interrogantes planteadas en esta investigación, siendo el escenario de la presente investigación el distrito judicial de Lima-Norte, en el cual se realizan las investigaciones preliminares relacionadas con los delitos informáticos contra el patrimonio.

3.4 Participantes:

Con relación a la caracterización de los sujetos, Hernández et al., (2014) señaló que, en algunas investigaciones cualitativas, es necesaria la opinión de expertos en un tema para así poder generar una recolección de datos más precisas. En la presente investigación, los sujetos a quienes se entrevistarán son:

Entrevistados	Cargo	Institución
Ruth Yojany Chinguel Guerrero	Fiscal Adjunto Provincial-2do Despacho 1FPPC	Ministerio Público – Lima Norte
Ruth Evelyn Zubieta Quineche	Fiscal Adjunta Provincial Provisional Transitoria	Ministerio Público – Lima Norte
Marlene Anyela Falcón Ore	Fiscal Adjunto Provincial-1er Despacho 2FPPC	Ministerio Público – Lima Norte
Dimas Hugo Lázaro Rivas	Fiscal Provincial-2do Despacho 1FPPC	Ministerio Público – Lima Norte
Marian Isabel Menacho Zamora	Fiscal Adjunto Provincial-7ma. FPPC	Ministerio Público – Lima Norte

Tabla 02: Participantes y Categorización de los entrevistados.

3.5 Técnicas e instrumentos de recolección de datos:

Las técnicas que se aplicaron en esta investigación son la entrevista y el análisis documental, de la misma forma los instrumentos utilizados son la guía de entrevista y la guía de análisis documental. Ramírez (2012) acotó que la técnica de la entrevista es un proceso comunicativo en el cual el investigador extrae información de su entrevistado, dicha información resulta ser relevante para obtener datos referentes a su investigación. Por su parte Norma (2018) señaló que el análisis de documentos se realiza con anterioridad e independientemente de la investigación ya que son percepciones de autores sobre un hecho determinado por lo cual serán contrastados con los datos que arroje la investigación para llegar a conclusiones que podrían diferir con los autores consultados.

3.6 Procedimiento:

En esta investigación se enfocó en la obtención de teorías a través de nuevos conocimientos, así lo señaló Vegas (2013), que luego de la obtención de información para la investigación esta debe convertirse datos útiles para la misma, por lo que se exige una postura clara para abordar correctamente la realidad investigada. El procedimiento comenzó con la elaboración de la matriz de

consistencia en las cuales contenía las categorías de la investigación, el problema general y los problemas específicos, además de la inclusión de los objetivos; para luego continuar con la recolección de los antecedentes nacionales e internacionales que sirvieron como base para la presente investigación. Continuando con el procedimiento para la elaboración de la tesis, se consultó los diferentes aportes teóricos jurídicos de especialistas con la finalidad de abordar los temas necesarios en la presente investigación, de igual manera se realizó una guía de entrevista con 9 preguntas relacionadas a la problemática planteada con la finalidad de abordar los objetivos planteados. Como paso final se procedió a entrevistar a 05 fiscales del distrito judicial de Lima Norte, para luego recopilar los resultados recogidos en las entrevistas y recabar las discusiones, conclusiones y recomendaciones sobre el tema abordado.

3.7 Rigor Científico:

Para Hernández et al. (2014), lo que se busca en una investigación cualitativa es poder realizar es un trabajo de calidad y que a su vez cumpla con el rigor de la metodología de la investigación, teniendo siempre en cuenta los criterios como la dependencia, credibilidad o validez, entre otros. Con la finalidad de otorgar el rigor científico se ha recurrido a tres asesores, quienes han otorgado validación del instrumento de Guía de entrevista, los cuales se detallan a continuación:

VALIDACIÓN DE INSTRUMENTOS (Guía de Entrevista)		
Datos generales	**Cargo**	**Porcentaje**
Dr. Ángel Fernando La Torre Guerrero	Docente de Proyecto de investigación en la Universidad Cesar Vallejo	95%
Dr. Hugo Miguel Romero Bendezú	Docente de la Universidad Cesar Vallejo	95%
Dra. Edith Corina Sebastian López	Docente de la Universidad Cesar Vallejo	95%
PROMEDIO	**95 %**	

Tabla 3: Validación de la Guía de entrevista.

3.8 Método de Análisis de la Información:

Según Hernández et al. (2014), en la investigación cualitativa, a diferencia del proceso cuantitativo, la recolección y análisis de datos se dan prácticamente en paralelo, por lo cual es más flexible, ya que recibimos datos no estructurados a los cuales nosotros les proporcionamos una estructura en la investigación, por lo cual cada estudiante o investigador podrá acoplarlo a las circunstancias y naturaleza de su estudio en particular. En el análisis de datos cualitativos que recibimos se dan de manera muy variada, de tal manera que el propósito central es primero explorar los datos para establecer una adecuada estructura y coherencia, para luego describir la experiencia de los entrevistados de acuerdo a su óptica, lenguaje y propias expresiones; es así que procedemos a darle sentido e interpretar los datos en función del planteamiento de la problemática y de la misma manera vincular los resultados recogidos a través de la entrevista con el conocimiento disponible para así poder generar una adecuada teoría fundamentada en base a los datos.

Por último, una vez aplicados los instrumentos de investigación y obtenido los datos, se realizó el desarrollo de la investigación, con la finalidad de poder abordar correctamente los supuestos jurídicos planteados en la presente investigación; de tal manera que se analizaran los datos para llegar al resultado y poder formular conclusiones y recomendaciones propias de esta investigación.

3.9 Aspectos Éticos:

El presente proyecto de investigación ha sido realizado citando a diferentes autores de libros y revistas indexadas de acuerdo al manual APA, además se han citado diferentes tesis y el Convenio Internacional de Budapest para poder complementar nuestro proyecto; así como también se han respetado los derechos de autor haciendo las referencias bibliográficas correspondientes.

IV.Resultados y Discusión

En este apartado se describió los resultados recolectados en los instrumentos de recolección de datos de la guía de entrevista y la guía de análisis documental, teniendo en cuenta los objetivos de investigación señalados previamente, en primer lugar, describimos los resultados recolectados en el instrumento de recolección de datos de la guía de entrevista, iniciando primero con el objetivó general que fue Determinar de qué manera se da el Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019. Para lograr este objetivo se formularon las siguientes interrogantes:

Con relación a la primera pregunta, ¿Considera Ud. que se tienen las adecuadas herramientas y colaboración policial para un correcto Tratamiento Jurídico Penal por parte del Fiscal contra los Delitos Informáticos contra el Patrimonio?, los entrevistados Menacho, Falcón y Lázaro (2020) señalaron que, dentro del Ministerio Público no existen las herramientas adecuadas para poder realizar la investigación ni recabar los elementos suficientes para esta clase de delitos debido a su particularidad de intangibilidad; por lo que estas investigaciones deben ser derivadas a la División de Investigación de Alta Tecnología de la Policía Nacional del Perú (DIVINDAT), ya que ellos cuentan con las herramientas idóneas para poder realizar las investigaciones ordenadas por el Fiscal.

Por otro lado, Zubieta y Chinguel (2020), también coincidieron con los demás entrevistados con respecto a la derivación de la investigación a la policía especializada en esta clase de delitos, pero además añadieron que esta derivación conllevaría a que el plazo de la investigación se ampliara más de lo permitido en el Sistema de Gestión Fiscal (SGF).

Así mismo en la segunda pregunta formulada, ¿Qué opina sobre la adhesión de Perú al Convenio de Budapest, considera que se han visto cambios significativos en la lucha en contra de los delitos informáticos contra el patrimonio?**,** los entrevistados Menacho, Falcón, Lázaro, Zubieta y Chinguel (2020) consideraron que si bien el Convenio de Budapest significa un gran avance en la lucha contra los delitos informáticos de manera general, este no ha presentado cambios significativos en la investigación y persecución de los delitos informáticos contra el

patrimonio; sin embargo el punto fuerte en la adhesión del Perú a este convenio ha permitido la cooperación internacional para la identificación de los delincuentes informáticos dentro de los países adscritos a este Convenido Internacional.

Continuando con la tercera pregunta, ¿Considera Ud. que exista una limitación jurídica o algún otro factor que impida la formulación de cargos e imputaciones en la comisión de delitos informáticos contra el patrimonio?, los entrevistados tuvieron diferentes posturas, por lo que Menacho (2020), señaló que no existen limitaciones jurídicas para formular cargos como tal, pero que si existen limitaciones extrajurídicas que no permiten determinar al sujeto activo, como sucede en el caso del uso del WhatsApp que se realiza a través de un código encriptado que resulta tedioso descifrar para recuperar la conversación, pero para ello se tiene que solicitar primero al juez que conceda el levantamiento del secreto de las comunicaciones y contactar con dicha resolución concesoria a la empresa que gestiona dicha base de datos para que remitan la conversación completa que posiblemente favorecería en una investigación. En esta misma línea Falcón (2020), refirió que una de las más grandes complicaciones se da entorno a la identificación del imputado ya que la misma tecnología permite ocultar rastros en la red informática. Otro punto resaltante y conflictivo se da en los criterios establecidos por el NCPP, como por ejemplo en la competencia territorial, ya que en esta clase de delitos no se puede determinar un lugar físico y exacto donde se comete la vulneración. De igual manera Lázaro (2020), indicó que no existe una limitación jurídica; sino que radica en el interés que tiene el agraviado de proseguir con la investigación ya que gran parte de las denuncias realizadas son solo exigencias que la entidad bancaria le solicita al agraviado para atender su reclamo. Chinguel (2020)**,** por su parte refiere que la principal limitación que se da en las investigaciones esta netamente relacionado con la naturaleza de estos delitos, como lo es en el caso de las evidencias que debido a su intangibilidad estas pueden desaparecer o ser alteradas rápidamente. Por su parte Zubieta (2020), refirió que la limitación más grande sería el hecho que cada ley que existe en nuestro país no se encuentra reglamentada, situación por lo cual existen vacíos.

Con Respecto al Primer objetivo específico se planteó determinar cómo la criminalidad informática influye en el acceso no autorizado a servicios informáticos, en el Distrito Judicial de Lima Norte 2019, se obtuvieron las siguientes respuestas:

Con relación a la cuarta pregunta, ¿Dentro de su consideración, cree Ud. que las nuevas modalidades de criminalidad informática influyen en el acceso no autorizado a servicios informáticos? ¿sí o no? ¿Por qué?**,** los entrevistados Menacho, Falcón, Lázaro, Zubieta y Chinguel (2020), coincidieron que efectivamente la criminalidad informática ha venido influyendo en el acceso no autorizado a servicios informáticos, más aún hoy en día debido a la coyuntura por la que está atravesando el país, por lo que la adquisición de productos se hace a través de diferentes tecnologías ocasionando así que se incrementen las modalidades para evitar las medidas de seguridad interpuestas por comercios y entidades bancarias.

Así mismo en la quinta pregunta se consultó si, ¿Bajo su experiencia, considera Ud. que son las personas naturales son las más vulnerables ante la comisión de fraude informático, en comparación con las personas jurídicas en la sociedad? ¿Por qué?, a lo que los entrevistados, Falcón, Lázaro, Zubieta y Chinguel (2020), refirieron que tanto personas naturales como personas jurídicas pueden ser víctimas de los criminales informáticos; pero lo que se aprecia en la práctica es que la mayoría de víctimas suelen ser personas naturales; esto debido a la facilidad que se tiene para acceder a sus datos personales, situación que no sucede con las empresas ya que gran parte de ellas cuentan con una seguridad informática lo que conlleva que el ataque que se pueda efectuar sea más complejo.

Continuando con la sexta pregunta se preguntó si, ¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos contra el patrimonio?**,** los entrevistados tuvieron diferentes posturas, es así que Menacho (2020), señaló que hasta la fecha no todos los medios electrónicos relacionados al internet cuentan con sistemas de prevención para evitar que se cometan delitos informáticos con el patrimonio. De igual manera Zubieta (2020), refirió que no existen estrategias adecuadas en prevención de delitos informáticos contra el patrimonio dado que para rastrear el IP donde salió la información es solo accesible a personas que cuentan con los medios necesarios.

En tal sentido, no existe forma de prevención a menos que no sea por cuenta propia y no por parte del estado y mucho menos sanción en caso de incurrir en ello. Para Lázaro (2020), también señaló que es muy complicado estrategia de prevención esto debido a la facilidad con la que se puede ocultar los rastros dentro de la navegación a través de internet, a lo mucho se podría seguir informando al público en general no brindar datos personales vinculados a su registro bancario, pero de todas maneras para realizar compras a través de internet te siguen pidiendo datos como dígitos de la tarjeta, la fecha de vencimiento, el CVV, etc. Con respecto a las sanciones estas ya se encuentran establecidas dentro de la norma penal (Ley N° 30096).

Por otro lado, Falcón (2020), refirió que las estrategias que se deben tomar en cuenta para la prevención de estos delitos no deben venir solo por parte del derecho, sino en trabajo conjunto con las entidades bancarias para que los usuarios no se encuentren expuestos a estos ataques sin poner trabas burocráticas al momento de la investigación y con respecto a las sanciones estas ya se encuentran establecidos dentro de la norma. Así mismo Chinguel (2020) indicó que, si bien la norma prevé una sanción por este tipo de conductas, la complejidad al momento de recabar información para individualizar al sujeto activo sigue siendo una lucha constante a través de los medios informáticos; es ahí donde radica la importancia de una colaboración eficiente entre la fiscalía y las entidades financieras que tengan conocimiento ante afectación de sus usuarios.

Con respecto al segundo objetivo específico: Establecer que tan efectivo es el reconocimiento del bien jurídico protegido en los delitos informáticos, ante el fraude informático en el Distrito Judicial de Lima Norte 2019, se obtuvo las siguientes respuestas:

Con relación a la séptima pregunta se consultó, ¿Qué tan efectivo es el reconocimiento del bien jurídico protegido en los delitos informáticos, especialmente en el delito de fraude informático?**,** los entrevistados Lázaro, Falcón y Chinguel (2020), sostuvieron que la Ley de delitos informáticos (Ley N° 30096) son muy generales y que, si bien resguardan al patrimonio como bien jurídico tutelado, esta norma solo ha seguido los preceptos generales establecidos por el

Convenio de Budapest sin tener en consideración que se pueden ir incrementando las diferentes modalidades en afectación al patrimonio; lo que genera que no sea muy efectiva la norma al ser muy general.

Por otro lado, Menacho (2020), señaló que El reconocimiento del bien jurídico es esencial para todas las investigaciones, dado que si no existe el bien jurídico afectado no podemos revelar el delito cometido, y sería una afectación el principio de legalidad si no se establece cual es el delito y el bien jurídico afectado. Otra postura distinta fue la de Zubieta (2020), en la que refirió que se configuran diferentes tipos de delitos por separados como el fraude, el cual debe estar vinculado a la informática, por ello vuelvo a reiterar que si bien se reconoce el bien jurídico en un delito informático este no se encuentra reglamentado, ósea bajo qué medidas, circunstancias, etc.

Así mismo en la octava pregunta, ¿Qué opina Ud. sobre establecer como bien jurídico protegido, no solo al patrimonio sino también a bienes jurídicos no tradicionales, como el correcto funcionamiento del sistema informático, en los delitos de fraude informático?**,** los entrevistados Menacho, Falcón y Chinguel (2020), coincidieron que podría ser viable tomar al correcto funcionamiento del sistema informático como un agravante dentro de los delitos informáticos contra el patrimonio y no como un bien jurídico no tradicional, ya que la posible afectación influiría en el patrimonio del sujeto pasivo.

De acuerdo a Zubieta (2020), señaló que debe hacerse una diferenciación y reiteró toda ley necesita su reglamento para que no ocurra este tipo de situación, que no sean genéricas sino específicas, para que no se tenga, a menos que no sea necesario de usar una ley general para cada tipo de caso. Por otro lado, Lázaro (2020), refirió que es importante resaltar que en los delitos informáticos dentro de la Ley N°30096 se tiene al sistema informático en el capítulo II como una afectación a la base de datos según las alteraciones que se hagan en este, pero no se toma en cuenta que el sistema informático también es parte del patrimonio, toda vez que cualquier tipo de vulneración o daño de este, puede menguar en el patrimonio del titular del sistema informático.

Por último, en la novena pregunta, ¿Considera Ud. idóneo que solo se encuentre tipificado el delito de Fraude Informático para tratar de contemplar las diferentes acciones ilícitas que se llevan a cabo en los delitos informáticos contra el patrimonio? los entrevistados Lázaro y Chinguel (2020), coincidieron que no es idóneo contemplar las diferentes modalidades de delitos informáticos contra el patrimonio, dentro del delito de fraude informático ya que existen diferentes conductas que se han ido implementando por los criminales informáticos que la norma no prevé. De igual manera Falcón (2020), señaló que no basta con tener un solo artículo que refiera sobre afectaciones al patrimonio, toda vez que la criminalidad informática cada vez encuentra diferentes modalidades para lucrar a través de la tecnología, pero por el momento puede ser suficiente ya que gran parte de las denuncias realizadas son por fraudes o pagos realizados sin consentimiento.

Por otro lado, Menacho (2020), sostuvo que la idea es que el delito informático como cualquier otro tengas sus agravantes para no considerarlo como un delito simple, dado que existen diversas herramientas que develan la alevosía de la actuación de los delincuentes informáticos. De igual manera Zubieta (2020), sostuvo que se deberían considerar las diferentes modalidades que no estén contempladas, pero estableciendo bajo qué circunstancias se configuran estas nuevas conductas**.**

En este apartado **redactamos los resultados de la guía de análisis de fuente documental** obtenidos en los instrumentos de recolección de datos, que son siete articulo científicos internacionales, un artículo científico nacional y la Ley de delitos informáticos que guardan relación con la presente investigación.

Respecto al Objetivo general que es: Determinar de qué manera se da el Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019, se analizó el artículo científico titulado "*Deterrence and Dissuasion in Cyberspace*", en el que se determinó que al ser la tecnología una herramienta indispensable en el día a día de la convivencia en la sociedad, debemos tener en cuenta que, si bien te facilita realizar diferentes acciones desde la comodidad de tu casa, también es una puerta de acceso para que personas realicen actos ilícitos perjudicando a terceros, teniendo como

principal aliado al anonimato que brinda realizar este tipo de acciones en el ciber espacio. De igual manera se analizó el artículo científico titulado *"Understanding policing of cybercrime in South Africa: The phenomena, challenges and effective responses"*, en la que se expresó que debido a la particularidad de los delitos informáticos contra el patrimonio, es que se debe dar una adecuada calificación del delito por parte del fiscal, ya que como señala el autor son pocas las pistas que se dejan en esta clase de actos, más sin embargo si se tiene una dirección IP asociado el acto debería ser elemento suficiente para tratar de individualizar al sujeto que habría cometido el delito. Por último, también se analizó La Ley de Delitos informáticos, específicamente el articulo 8 sobre fraude informático, en el que se determinó que, pese a que el legislador desde hace varios años trato de resguardar los diferentes bienes jurídicos que pueden ser vulnerados a través de la tecnología, en la realidad la aplicación de la investigación fiscal no es la más adecuada para esta clase de delitos, debido a que no se le da el interés adecuado por parte de los afectados.

Respecto al objetivo específico 1 que es: Determinar cómo la criminalidad informática influye en el acceso no autorizado a servicios informáticos, en el Distrito Judicial de Lima Norte 2019, se analizó el artículo científico titulado "Ciberterrorismo: amenaza fulminante. Resumen de la tesis *"El delito de terrorismo informático como figura jurídica en el código penal vigente. Propuesta para su inclusión en la Ley sobre Delitos Informáticos en el Perú"*, en el que se concluyó que cuando nos referimos a criminales informáticos debemos entenderlo como aquella persona que tiene poco o abundante conocimiento sobre informática con la finalidad de acceder y obtener algún beneficio por lo que no solo se necesita de un equipo tecnológico sino también de alguien que lo manipule. Así mismo se analizó el artículo científico titulado "*The Meaning of the Cyber Revolution"*, que refirió que generalmente cuando el acto delictivo es cometido por varios sujetos, en la calificación de la disposición fiscal se van a clasificar como imputados, que a lo largo de la investigación se dará con el grado de participación de cada uno, sin embargo, en los delitos informáticos, la pluralidad de sujetos tan solo dificultaría la labor de investigación ya que no necesariamente todos los sujetos están en el mismo lugar, sino que están en distintos lugares generando así diferentes direcciones

electrónicas, que no necesariamente revelará la identidad de la persona que cometió los ilícitos. De igual manera se desarrolló el artículo científico titulado *"Investigation on Cyber Crime, Cyber Law and Cyber Security. International Journal of Computer Science and Information Security"*, en el que se refirió que el anonimato que se da en el ciberespacio es el principal aliado para estos ciberdelincuentes, ya sea que se use a la tecnología como medio o fin para acometerlos, siempre tendrán la ventaja debido a que no tiene contacto con un objeto tangible. Por otro lado, dependiendo de la acción que realicen es posible poder obtener pistas sobre los atacantes, por ejemplo, en el caso de fraude electrónico lo que se busca es el lucro, por lo cual siempre se va tener un registro de la persona beneficiada en el sistema, por lo cual la investigación puede partir desde ese punto, sin embargo, en el caso que la finalidad solo era atacar una página web los rastros que se pueden obtener son mínimos.

Respecto al objetivo específico 2 que es: Establecer que tan efectivo es el reconocimiento del bien jurídico protegido en el fraude informático en el Distrito Judicial de Lima Norte 2019, se analizó el artículo científico titulado *"Cybercrime and Cybercriminals: A Comprehensive Study"*, en la que se mencionó que debido a la gran variedad de métodos para engañar a las personas y capturar sus datos, es que nos encontramos ante un creciente fenómeno delincuencial, que en la mayoría de sus acciones afectan al patrimonio, sin embargo, es en la variedad de métodos para cometer estos delitos que podemos apreciar que ya sea la tecnología como medio o fin siempre va a ir de la mano con la afectación al patrimonio. De igual manera se analizó el artículo científico titulado *"El bien jurídico protegido en los delitos informáticos"*, en el que refirió que lo que se trata de resguardar en estos supuestos es proteger los bienes jurídicos tradicionales, como el patrimonio, a través de bienes jurídicos no tradicionales, como el correcto funcionamiento del sistema informático, por lo cual al momento de aperturar una investigación fiscal debería consignarse de esa manera para darle un adecuado tratamiento jurídico penal. Así mismo se desarrolló el artículo científico titulado *"Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration"*, en el que se determinó que las consecuencias de los delitos informáticos contra el patrimonio, no siempre van a ser lucrativas ya que

dependiendo de cuál era la finalidad del acto ilícito, el fiscal deberá proceder con la apertura de la investigación, debemos tener en claro que dentro de la ley de delitos informáticos existen otros delitos los cuales se pueden encuadrar en la protección de datos informáticos y no el de patrimonio.

En esta sección realizamos la discusión de resultados obtenidos en los instrumentos de recolección de datos con los resultados de las investigaciones de los trabajos previos tanto nacional e internacional citados en el marco teórico, así como también las teorías relacionadas al presente estudio de investigación.

Con relación al objetivo general: Determinar de qué manera se da el Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019. Se determinó que de los hallazgos encontrados en los instrumentos de recolección de datos, la mayoría de Fiscales entrevistados coincidieron que dentro del Ministerio Público no existen las herramientas adecuadas para poder realizar la investigación ni recabar los elementos suficientes para esta clase de delitos debido a su particularidad de intangibilidad; además algunos de los Fiscales entrevistados añadieron que este tipo de derivaciones en sede policial conllevaría a un exceso en el plazo de la investigación. Si bien es cierto que la adhesión al Convenio de Budapest significó un gran avance en la lucha contra los delitos informáticos, este no ha presentado cambios significativos en la investigación y persecución de los delitos informáticos contra el patrimonio; sin embargo, el punto fuerte en la adhesión del Perú a este convenio ha permitido la cooperación internacional para la identificación de los delincuentes informáticos dentro de los países adscritos a este Convenido Internacional. Del mismo modo se señaló que no existen limitaciones jurídicas como tal para formular cargos en la investigación, pero que si existen otros factores relacionado a la naturaleza de esta clase de delitos que repercutirían al momento de hacer la investigación. Por otro lado, también se realizó el análisis de artículos científicos internacionales, en el que se determinó que una de las principales ventajas que se tiene a través de la tecnología es el anonimato motivo por el cual se debe dar una adecuada calificación del delito por parte del fiscal, ya que son pocas las pistas que se dejan en esta clase de actos, más sin embargo si se tiene una dirección IP asociado el acto debería ser elemento suficiente para tratar de

individualizar al sujeto que habría cometido el delito. pese a que el legislador desde hace varios años trato de resguardar los diferentes bienes jurídicos que pueden ser vulnerados a través de la tecnología, en la realidad la aplicación de la investigación fiscal no es la más adecuada para esta clase de delitos, debido a que no se le da el interés adecuado por parte de los afectados.

Del mismo modo, para Vilca (2018) en la tesis titulada “Los Hackers: “Delito Informático frente al Código Penal Peruano”, concluyó que la falta de información en esta clase de delitos, no permite tener un marco de referencia adecuado para combatir estas situaciones, toda vez que la normativa sobre delitos informáticos en el país se da de manera muy generalizada. Así mismo Matusan (2013) señaló que, la acción del Fiscal es de suma importancia para poder asegurar las evidencias o medios probatorios idóneos que puedan soportar su teoría del caso y de ser necesario precluir la investigación llegando a un acuerdo con la defensa del imputado, lamentablemente en esta clase de delitos es muy difícil llegar a tener un imputado totalmente individualizado por la complejidad misma de esta clase de delitos.

Respecto al objetivo específico 1: Determinar cómo la criminalidad informática influye en el acceso no autorizado a servicios informáticos, en el Distrito Judicial de Lima Norte 2019. Se determinó que de los resultados de la investigación obtenidos en el instrumento de recolección de datos de la guía de entrevista, los entrevistados coincidieron que la criminalidad informática ha venido influyendo en el acceso no autorizado a servicios informáticos, más aún hoy en día debido a la coyuntura por la que está atravesando el país, por lo que la adquisición de productos se hace a través de diferentes tecnologías ocasionando así que se incrementen las modalidades para evitar las medidas de seguridad interpuestas por comercios y entidades bancarias. Así mismo se determinó que tanto las personas naturales como las jurídicas pueden ser potenciales víctimas de los criminales informáticos sin embargo la mayoría de estos casos se dan en personas naturales debido a que un ciberataque a una empresa que tiene seguridad informática sería más complejo. Otro factor importante radica en la prevención en esta clase de delitos; sin embargo, los entrevistados señalaron que no se dan adecuadas estrategias para la prevención en esta clase de delitos pero que sería un gran aporte que la protección

y prevención en esta clase de delitos no venga solo por parte del derecho, sino también por la colaboración de las entidades cuyos usuarios sufrieron las afectaciones; con respecto a las sanciones estas ya se encuentran establecidos dentro de la norma. Por otro lado, también se analizó artículos científicos nacionales e internacionales en el que se refirió que cuando nos referimos a criminales informáticos debemos entenderlo como aquella persona que tiene poco o abundante conocimiento sobre informática con la finalidad de acceder y obtener algún beneficio por lo que no solo se necesita de un equipo tecnológico sino también de alguien que lo manipule; por lo que si este acto delictivo es cometido por varios sujetos, en la calificación de la disposición fiscal se van a clasificar como imputados, que a lo largo de la investigación se dará con el grado de participación de cada uno, sin embargo, en los delitos informáticos, la pluralidad de sujetos tan solo dificultaría la labor de investigación ya que no necesariamente todos los sujetos están en el mismo lugar, sino que están en distintos lugares generando así diferentes direcciones electrónicas, que no necesariamente revelará la identidad de la persona que cometió los ilícitos, es así que la principal herramienta para el avance de la criminalidad informática es el anonimato que se da en el ciberespacio, ya sea que se use a la tecnología como medio o fin para acometerlos, siempre tendrán la ventaja debido a que no tiene contacto con un objeto tangible.

Aunado a ello Parra (2016) en la tesis titulada “Proyecto Legal para un Esquema Nacional de Ciber Seguridad”, concluyó que Estado Peruano en comparación con los demás países, no había sufrido un ciber ataque a mayor escala, pero que por esa razón no debe ser expectante de la realidad problemática que se presentan en diferentes países, por lo cual es necesaria una adecuada proyección por parte del Estado con otros órganos estatales para estar alertas ante futuros ciber ataques. Así también lo señaló Hernández (2017) quien refirió que nos encontramos en un nuevo escenario en el cual la información va adquiriendo vital importancia en la sociedad, ya que es difícil imaginar que por lo menos exista alguna empresa que no use computadoras para almacenar, procesar o transmitir una gran cantidad de datos, desafortunadamente la tecnología no es usada solo para situaciones provechosas, sino que también para cometer conductas antisociales, siendo su

principal característica el uso de un sistema o red informática llegando a establecer a la computadora como un método, medio o fin de determinada conducta delictiva.

Respecto al objetivo específico 2: Establecer que tan efectivo es el reconocimiento del bien jurídico protegido en los delitos informáticos, ante el fraude informático en el Distrito Judicial de Lima Norte 2019. Se determinó que de los resultados de la investigación obtenidos en el instrumento de recolección de datos de la guía de entrevista, la mayoría de los entrevistados coincidieron que la norma relacionada a los delitos informáticos contra el patrimonio se da de manera general y que si bien resguardan al patrimonio como bien jurídico tutelado, esta norma solo ha seguido los preceptos generales establecidos por el Convenio de Budapest sin tener en consideración que se pueden ir incrementando las diferentes modalidades en afectación al patrimonio además se añadió que si bien se reconoce el bien jurídico en un delito informático este no se encuentra reglamentado, ósea bajo qué medidas, circunstancias, etc. De igual manera la mayoría d ellos entrevistados son de la postura que podría ser viable tomar al correcto funcionamiento del sistema informático como un agravante dentro de los delitos informáticos contra el patrimonio y no como un bien jurídico no tradicional, ya que la posible afectación influiría en el patrimonio del sujeto pasivo. Así mismo se coincidió en las entrevistas que no es idóneo contemplar las diferentes modalidades de delitos informáticos contra el patrimonio, dentro del delito de fraude informático ya que existen diferentes conductas que se han ido implementando por los criminales informáticos que la norma no prevé pero que por el momento puede ser suficiente ya que gran parte de las denuncias realizadas son por fraudes o pagos realizados sin consentimiento; de esta manera se deberían considerar las diferentes modalidades que no estén contempladas, pero estableciendo bajo qué circunstancias se configuran estas nuevas conductas**.**

Bajo el mismo contexto Devia (2017) en la tesis titulada “Delito Informático: Estafa Informática del artículo 248.2 del Código Penal”, concluyó que para dar una adecuada explicación a la relación que existe entre el delito y la informática, se debe tratar desde la perspectiva de los delitos tradicionales ya que gran parte de los bienes jurídicos que se afectan ya están reconocidos en la norma solo que en esta clase de delitos se utiliza como medio de comisión la tecnología informática.

Por otro lado, se está dando una nueva postura en la cual hacen claro énfasis en la afectación a la funcionalidad informática como interés colectivo, como bien jurídico no convencional a proteger, es así que Mayer (2017) mencionó que, La funcionalidad informática sirve al conjunto de las personas y es, a partir de esta figura que se presenta como un bien jurídico colectivo. Por ende, se presenta de forma que el uso y disfrute no es propio ni excluyente de persona alguna, ni puede distribuirse entre algunos individuos. Se presenta, asimismo, de un interés social relevante para el individuo, que está vinculado, de una u otra forma, con la labor habitual de todos quienes integran un determinado sistema. Esta transgresión al funcionamiento informático afecta al libre desarrollo de las personas que usan algún dispositivo electrónico con acceso a una interconexión, como lo es el internet. Es así que tenemos que la funcionalidad informática está a disposición de otros bienes jurídicos, pero al verse afectados estos bienes jurídicos por una afectación al correcto funcionamiento del sistema informático, nace la necesidad de resguardar y conservar un adecuado funcionamiento de dichos sistemas.

V.Conclusiones

Primera: Debido a la naturaleza de los delitos informáticos contra el patrimonio, el tratamiento jurídico penal por parte del fiscal se da de una manera deficiente ya que el marco legal sobre los delitos informáticos contra el patrimonio solo se encuentra enmarcados dentro del delito de fraude informático lo cual resulta insuficiente para las distintas modalidades que se presentan lo que no permite tener un marco de referencia adecuado para combatir estas situaciones, toda vez que la normativa sobre delitos informáticos en el país se da de manera muy generalizada.

Segunda: En la actualidad se aprecia un crecimiento de la criminalidad informática que ha venido influyendo en el acceso no autorizado a servicios informáticos, esto debido a la coyuntura social que vivimos por la pandemia, lo que ha llevado a las personas a recurrir al comercio electrónico para adquirir productos evitando el contacto físico, pero exponiéndose a ser posibles víctimas de diferentes modalidades de delitos informáticos contra el patrimonio y no solo de fraude informático.

Tercera: Pese a que la Ley de delitos informáticos (Ley N° 30096) resguarda al patrimonio como bien jurídico protegido en el delito de fraude informático, esta se da de manera muy general; por lo que no es muy efectiva ya que se trata de resguardar al patrimonio conteniendo diferentes acciones en un solo artículo de la norma penal, constituyendo una norma legal deficiente e inidónea.

VI.Recomendaciones

Primera: Se debería crear fiscalías especializadas en delitos informáticos para que así se pueda dar un adecuado tratamiento jurídico penal por parte del Fiscal en esta clase de delitos, así mismo se podrían tener las herramientas adecuadas para realizar las investigaciones preliminares y no tener que derivarlas en sede policial; por ende, no se tendrían investigaciones fuera de plazo en el despacho Fiscal.

Segunda: Se debería plantear un nuevo proyecto de ley en el Congreso para realizar con mayor detalle la modificación de los delitos informáticos contra el patrimonio establecidos en la ley especial N°30096, de esta manera poder ampliar y abarcar las diferentes modalidades que se han ido presentando por parte de los criminales informáticos y no tan solo tener al fraude informático como único delito informático contra el patrimonio desde un enfoque general sino que debe darse una protección singular debido a la complejidad de investigar este tipo de delitos.

Tercera: Se deberían implementar las capacitaciones adecuadas de las instituciones públicas involucradas en la prevención y represión de los delitos informáticos, así como está establecido en las disposiciones complementarias de la Ley N° 30096, más aún cuando en el año 2019 el Estado Peruano se ha adscrito al Convenio de Budapest. Lo que se busca con estas capacitaciones es poder establecer con uniformidad los conocimientos acerca de los delitos informáticos no solo como medio para cometer este tipo de actos sino también como finalidad.

Referencias Bibliográficas

- Argüelles Arellano, M. C. (2016). Retos de la legislación informática en México. *Computación y Sistemas, 20(4)*,827-831. ISSN: 1405-5546. http://www.scielo.org.mx/pdf/cys/v20n4/1405-5546-cys-20-04-00827.pdf

- Arocena, G. A. (2012). La regulación de los delitos informáticos en el Código Penal Argentino. Introducción a la Ley Nacional Núm. 26.388. *Boletín Mexicano de Derecho Comparado, 45(135)*,945-988. ISSN: 2448-4873. http://www.scielo.org.mx/pdf/bmdc/v45n135/v45n135a2.pdf

- Arocena, L. (2016). *La Odisea Procesal de la Criminalidad Informática.* (Tesis para obtener el grado en Derecho). Universidad del País Vasco / Euskal Herriko Unibertsitatea, España.

- Cadena Iñiguez, P., Rendón Medel, R., Aguilar Ávila, J., Salinas Cruz, E., de la Cruz Morales, F. R., y Sangerman Jarquín, D. M. (2017). Métodos cuantitativos, métodos cualitativos o su combinación en la investigación: un acercamiento en las ciencias sociales. *Revista Mexicana de Ciencias Agrícolas, 8(7)*,1603-1617. ISSN: 2007-0934. https://www.redalyc.org/pdf/2631/263153520009.pdf

- Campos Xool, P. I. (2016). Delitos informáticos en México y sus formas de prevención. *Revista Visión Criminológica-Criminalística. (29)*,30-47. ISSN: 2007-5804. http://revista.cleu.edu.mx/new/descargas/1604/articulos/Articulo09_Delitos_informaticos_en_Mexico_y_sus_formas_de_prevencion.pdf

- Candelario Samper, J. J., y Rodríguez Bolaño, M. (2015). Seguridad informática en el Siglo XX: una perspectiva jurídica tecnológica enfocada hacia las organizaciones nacionales y mundiales. *Publicaciones E Investigación, (9)*, 153 - 162. ISSN: 1900-6608. https://doi.org/10.22490/25394088.1441

- Carrasco, S. (2006). *"Metodología de investigación científica: Pautas metodológicas para diseñar y elaborar el proyecto de investigación"*. Lima: Editorial San Marcos.

- Celorio, M. (2016). Derechos Humanos en internet en México: Violación y Desposesión*. Revista de la realidad Mexicana Actual, El Cotidiano. (200)*, 293-305.ISSN:0186-1840. https://biblat.unam.mx/hevila/ElCotidiano/2016/no200/21.pdf

- Chaisse, J. y Bauer, C. (2019). Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration. *Vanderbilt Journal of Entertainment & Technology Law, 21(3)*, 549-589. ISSN: 1536-3872. https://ssrn.com/abstract=3382749

- Coria Páez, A. L., Pastor Román, I., y Torres Hernández, Z. (2013). Propuesta de metodología para elaborar una investigación científica en el área de Administración de Negocios. *Pensamiento & Gestión, (35)*,1-24. ISSN: 1657-6276. https://www.redalyc.org/pdf/646/64629832002.pdf

- Cotrina, S. (2018). *Los Factores Principales que Impiden la Aplicación de la Ley N°30171-Lima Norte en el Año 2016*. (Tesis para obtener el Título Profesional de Abogado). Universidad César Vallejo, Perú.

- De la Cruz, E., Jirón, M., Miranda, F. (2016). *La Ciberdelincuencia y su Regulación Jurídica en Centroamérica con Énfasis en Costa Rica, El Salvador y Nicaragua.* (Tesis para optar por el grado de Licenciados en Derecho). Universidad Nacional Autónoma de Nicaragua.

- Devia, E. (2017). *Delito Informático: Estafa Informática del Artículo 248.2 del Código Penal*. (Tesis para obtener el Grado de Doctor en Derecho). Universidad de Sevilla, España.

- Dlamini, S., y Mbambo, C. (2019). Understanding policing of cybercrime in South Africa: The phenomena, challenges and effective responses. *Cogent Social Sciences, 5(1)*, 1-13. ISSN: 2331-1886. https://doi.org/10.1080/23311886.2019.1675404

- Fassio, A. (2018). Reflexiones acerca de la metodología cualitativa para el estudio de las organizaciones. *Revista Digital Ciencias Administrativas, (12)*,73-84. ISSN 2314-3738. https://doi.org/10.24215/23143738e028

- Hancco, E. (2017). *La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096, Perú-2017.* (Tesis para obtener el Título Profesional de Abogado). Universidad Nacional de San Agustín, Perú.

- Hernández Martínez, R. (2017). Prolegómeno de la informática en la actividad del criminólogo y el criminalista. *Revista Visión Criminológica-Criminalística 5(17)*,18-27. ISSN: 2007-5804. http://revista.cleu.edu.mx/new/descargas/1701/revista/Revista%2017%20Digital.pdf

- Hernández, R; Fernández, C. y Baptista, P. (2014). Metodología de la Investigación. (6.a ed.) México: Mg. Graw-Hill Interamericana.

- Kello, L. (2013), The Meaning of the Cyber Revolution. *International Security, 38(2), 7-40*. ISSN: 1531-4804. https://doi.org/10.1162/ISEC_a_00138

- Matusan Acuña, C. (2013). La Acción Penal Privada y la afectación de derechos fundamentales. *Revista VIA IURIS, (14)*,187-197. ISSN: 1909-5759. https://www.redalyc.org/pdf/2739/273929754011.pdf

- Mayer Lux, L. (2017). El bien jurídico protegido en los delitos informáticos. *Revista Chilena de Derecho, 44(1)*, 261-285. ISSN: 0718-3437. http://dx.doi.org/10.4067/S0718-34372017000100011

- Mayer Lux, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Revista Ius et Praxis. 24(1)*, 159-206. ISSN: 0718-0012. https://dx.doi.org/10.4067/S0718-00122018000100159

- Montiel Juan, I. (2016). Cibercriminalidad social juvenil: la cifra negra. *IDP. Revista de Internet, Derecho y Política, (22)*,108-120. ISSN:1699-8154. https://www.redalyc.org/pdf/788/78846481008.pdf

- Núñez Ojeda, R. y Correa Zacarías C. (2017). La prueba ilícita en las diligencias limitativas de derechos fundamentales en el proceso penal chileno. Algunos problemas. *Revista Ius et Praxis, 23(1)*, 195-246. ISSN: 0718-0012.

http://dx.doi.org/10.4067/S0718-00122017000100007

- Nye Jr., J. S. (2017). Deterrence and Dissuasion in Cyberspace*. International Security, 41(3)*, 44-71. ISSN: 1531-4804. https://doi.org/10.1162/ISEC_a_00266

- Páramo Morales, D. (2015). La teoría fundamentada (Grounded Theory), metodología cualitativa de investigación científica. *Pensamiento & Gestión, (39)*,7-13. ISSN: 1657-6276. https://www.redalyc.org/pdf/646/64644480001.pdf

- Parra, R. (2016). *Proyecto Legal para un Esquema Nacional de Ciber Seguridad.* (Tesis para obtener el Título Profesional de Abogado). Universidad San Martin de Porres, Perú

- Peralta Escobar, L. A., Gutiérrez Garza, E., y Carmona Lara, M. C. (2017). el diseño del modelo institucional de la procuraduría general de la república en la eficiencia de la denuncia ambiental. *Boletín Mexicano de Derecho Comparado. 50(150)*,1083-1114. ISSN: 2448-4873. http://dx.doi.org/10.22201/iij.24484873e.2017.150.11834

- Picotti, L (2013). Los Derechos Fundamentales en el uso y abuso de las redes sociales en Italia: Aspectos Penales. *IDP. Revista de Internet, Derecho y Política, (16)*,76-90. ISSN: 1699-8154. https://dialnet.unirioja.es/servlet/articulo?codigo=4477376

- Pifarré, M. J. (2013). «Internet y redes sociales: un nuevo contexto para el delito». *IDP. Revista de Internet, Derecho y Política, (16)*,40-43. ISSN: 1699-8154. https://www.redalyc.org/pdf/788/78828864004.pdf

- Pino, S. (2015). Derecho Penal Informático. Quito, Ecuador: Corporación de Estudios y Publicaciones (CEP.). ISBN: 978-9942-10-262-1

- Pons Gamon, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO Revista Latinoamericana De Estudios De Seguridad, (20)*, 80-93. ISSN: 1390-4299. https://doi.org/10.17141/urvio.20.2017.2563

- Prado Prado, G. y Durán Migliardi, M. (2017). Sobre la evolución de la protección penal de los bienes jurídicos supraindividuales. Precisiones y limitaciones previas para una propuesta de protección penal del orden público económico enchile. *Revista de Derecho - Universidad Católica del Norte, 24(1)*,263-295. ISSN: 0718-9753. http://dx.doi.org/10.4067/S0718-97532017000100263

- Quevedo, J. (2017). *Investigación y Prueba del Ciberdelito.* (Tesis para optar por el grado de Doctor en Derecho y Ciencias Políticas). Universidad de Barcelona, España.

- Ramírez Atehortúa, F. y Zwerg Villegas, A. M. (2012). Metodología de la investigación más que una receta. *AD-Minister, (20)*, 91-111. ISSN 1692-0279. https://www.redalyc.org/articulo.oa?id=322327350004

- Ranganayaki, T. y Venkatachalam, M. (2015). Investigation on Cyber Crime, Cyber Law and Cyber Security. *International Journal of Computer Science and Information Security*, 68-71. ISSN 1947-5500. http://sites.google.com/site/ijcsis/

- Rodríguez Vega, M. y Pino Reyes, O. (2015). Análisis de la (in)eficacia del principio de obligatoriedad en el ejercicio de la acción penal en la etapa preliminar del proceso penal chileno. *Revista de Derecho - Universidad Católica del Norte, 22(1)*,351-399. ISSN: 0718-9753. http://dx.doi.org/10.4067/S0718-97532015000100009

- Roxin, C. (2013). El concepto de bien jurídico como instrumento de crítica legislativa sometido a examen. *Revista Electrónica de Ciencia Penal y Criminología, 15(1)*, 1-27. ISSN: 1695-0194. http://criminet.ugr.es/recpc/15/recpc15-01.pdf

- Sabillon, R., Cano, J., Cavaller Reyes V. y Serra Ruiz, J. (2016). Cybercrime and Cybercriminals: A Comprehensive Study. *International Journal of Computer Networks and Communications Security, 4(6)*, 165-176. ISSN: 2410-0595. http://hdl.handle.net/10609/78507

- Sánchez Medero, G. (2012). Ciberespacio y el crimen organizado. los nuevos

desafíos del Siglo XXI. *Revista Enfoques: Ciencia Política y Administración Pública, 10(16)*,71-87. ISSN: 0718-0241. https://www.redalyc.org/pdf/960/96024266004.pdf

- Santivañez, D. (2015). Ciberterrorismo: amenaza fulminante. Resumen de la tesis “El delito de terrorismo informático como figura jurídica en el código penal vigente. Propuesta para su inclusión en la Ley sobre Delitos Informáticos en el Perú”. *Ius et Praxis, Revista de la Facultad de Derecho, (46)*, 225-240. ISSN: 1027-8168. http://revistas.ulima.edu.pe/index.php/Ius_et_Praxis/article/view/673/649

- Vegas Meléndez, H. (2013). Investigación cualitativa para el abordaje de la gestión pública local. *Observatorio Laboral Revista Venezolana, 6(11)*,79-95. ISSN: 1856-9099. https://www.redalyc.org/pdf/2190/219030140006.pdf

- Vilca, G. (2018). *Los Hackers: Delito Informático frente al Código Penal Peruano.* (Tesis para obtener el Título Profesional de Abogado). Universidad Nacional Santiago Antúnez de Mayolo, Perú.

- Villavicencio, F. (2015). *Comentarios a la Ley N° 30096, Ley de delitos Informáticos.* Perú, Chiclayo: Ediciones Prometeo Desencadenado.

ANEXO 3.- MATRIZ DE CATEGORIZACIÓN APRIORÍSTICA.

OBJETIVOS DE INVESTIGACION	CATEGORIAS	CONCEPTUALIZACIÓN	SUBCATEGORIAS	FUENTE	TÉCNICAS E INTRUMENTOS DE RECOLECCIÓN DE DATOS
Objetivo General: Determinar de qué manera se da el Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019. **Objetivos específicos:** 1.- Determinar cómo la criminalidad informática influye en el acceso no autorizado a servicios informáticos, en el Distrito Judicial de Lima Norte 2019. 2.- Establecer que tan efectivo es el reconocimiento del bien jurídico protegido en el fraude informático en el Distrito Judicial de Lima Norte 2019.	El Tratamiento Jurídico Penal por parte del Fiscal	Sobre el tratamiento jurídico penal por parte del fiscal, se busca es poder tratar de identificar, como se da el desarrollo de la investigación preliminar por parte del Fiscal en esta clase de delitos.	Bien jurídico protegido	Distrito Fiscal de Lima Norte	**TÉCNICAS:** -Entrevistas. -Análisis Documental
			Criminalidad Informática		
	Delitos Informáticos contra el Patrimonio.	El delito de fraude informático comprende algunas acciones en su tipificación como, la de diseño, introducción, alteración, borrado, supresión, como alguna de las acciones que se pueden cometer en el fraude informático.	Fraude Informático		**INSTRUMENTOS:** -Guía de Entrevista. -Guía de Análisis Documental
			El Acceso no Autorizado a Servicios Informáticos		

ANEXO 4.- GUÍA DE ENTREVISTAS.

FICHA DE ENTREVISTA

(FISCALES)

El Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, Distrito Judicial de Lima Norte 2019

Entrevistado/a:

Cargo/profesión/grado académico:

Institución:

Objetivo general

Determinar de qué manera se da el Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019.

1.- ¿Considera Ud. que se tienen las adecuadas herramientas y colaboración policial para un correcto Tratamiento Jurídico Penal por parte del Fiscal contra los Delitos Informáticos contra el Patrimonio?

……
……
……
……

2.- ¿Qué opina sobre la adhesión de Perú al Convenio de Budapest, considera que se han visto cambios significativos en la lucha en contra de los delitos informáticos contra el patrimonio?

……
……
……
……

3.- ¿Considera Ud. que exista una limitación jurídica o algún otro factor que impida la formulación de cargos e imputaciones en la comisión de delitos informáticos contra el patrimonio?

……
……

……
……

Objetivo específico 1

Determinar cómo la criminalidad informática influye en el acceso no autorizado a servicios informáticos, en el Distrito Judicial de Lima Norte 2019.

4.- ¿Dentro de su consideración, cree Ud. que las nuevas modalidades de criminalidad informática influyen en el acceso no autorizado a servicios informáticos? ¿sí o no? ¿Por qué?

……
……
……
……

5- ¿Bajo su experiencia, considera Ud. que son las personas naturales son las más vulnerables ante la comisión de fraude informático, en comparación con las personas jurídicas en la sociedad? ¿Por qué?

……
……
……
……

6.- ¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos contra el patrimonio?

……
……

……
……

Objetivo específico 2

Establecer que tan efectivo es el reconocimiento del bien jurídico protegido en los delitos informáticos, ante el fraude informático en el Distrito Judicial de Lima Norte 2019.

7.- Bajo su percepción, ¿Qué tan efectivo es el reconocimiento del bien jurídico protegido en los delitos informáticos, especialmente en el delito de fraude informático?

……
……
……
……

8.- ¿Qué opina Ud. sobre establecer como bien jurídico protegido, no solo al patrimonio sino también a bienes jurídicos no tradicionales, como el correcto funcionamiento del sistema informático, en los delitos de fraude informático?

……
……
……
……
……
……

9.- ¿Considera Ud. idóneo que solo se encuentre tipificado el delito de Fraude Informático para tratar de contemplar las diferentes acciones ilícitas que se llevan a cabo en los delitos informáticos contra el patrimonio?

……
……
……
……
……

ANEXO 5.- VALIDACIONES DEL INSTRUMENTO.

UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: Sebastian Lopez Edith Corina
1.2. Cargo e institución donde labora: Docente ucv
1.3. Nombre del instrumento motivo de evaluación: Guia de entrevista
1.4. Autor(A) de Instrumento: Yomy Vásquez Juan Carlos

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.												✓	
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.												✓	
3. ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.												✓	
4. ORGANIZACIÓN	Existe una organización lógica.												✓	
5. SUFICIENCIA	Toma en cuanta los aspectos metodológicos esenciales												✓	
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.												✓	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												✓	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos												✓	
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.												✓	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												✓	

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación — Si
- El Instrumento no cumple con Los requisitos para su aplicación

IV. PROMEDIO DE VALORACIÓN : 95 %

Lima, 22 noviembre del 2019

FIRMA DEL EXPERTO INFORMANTE

DNI No 09484937 Telf.:

UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: ROMERO BENDEZU HUGO MIGUEL
1.2. Cargo e institución donde labora: DOCENTE UCV
1.3. Nombre del instrumento motivo de evaluación: GUIA DE ENTREVISTA
1.4. Autor(A) de Instrumento: Jóny Vásquez Juan Carlos

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.												✓	
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.												✓	
3. ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.												✓	
4. ORGANIZACIÓN	Existe una organización lógica.												✓	
5. SUFICIENCIA	Toma en cuanta los aspectos metodológicos esenciales												✓	
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.												✓	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												✓	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos												✓	
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.												✓	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												✓	

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación — SI
- El Instrumento no cumple con Los requisitos para su aplicación

IV. PROMEDIO DE VALORACIÓN :

95 %

Lima, 19 - NOV. del 2019

FIRMA DEL EXPERTO INFORMANTE

DNI No. 40445301 Telf. 969910337

UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: LA TORRE GUERRERO ANGEL FERNANDO

1.2. Cargo e institución donde labora: DOCENTE A TIEMPO COMPLETO UCV

1.3. Nombre del instrumento motivo de evaluación: GUÍA DE ENTREVISTA

1.4. Autor(A) de Instrumento: Jenny Vásquez Jean Carlos

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.												V	
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.												V	
3. ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.												V	
4. ORGANIZACIÓN	Existe una organización lógica.												V	
5. SUFICIENCIA	Toma en cuanta los aspectos metodológicos esenciales												V	
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.												V	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												V	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos												V	
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.												V	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												V	

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación
- El Instrumento no cumple con Los requisitos para su aplicación

Si

IV. PROMEDIO DE VALORACIÓN :

95 %

Lima, 14 De NOVIEMBRE del 2019

FIRMA DEL EXPERTO INFORMANTE

DNI No. 09968447 Telf. 980758844

ANEXO 6.- MATRIZ DE CONSISTENCIA.

MATRIZ DE CONSISTENCIA PARA ELABORACIÓN INFORME DE INVESTIGACIÓN

NOMBRE DEL ESTUDIANTE: Jean Carlos Gómez Vásquez

FACULTAD/ESCUELA: DERECHO

TÍTULO	
"El Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, Distrito Judicial de Lima Norte 2019."	
PROBLEMAS	
Problema General	¿Cómo se relaciona el Tratamiento Jurídico Penal por parte del fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019?
Problema Específico 1	¿De qué manera la criminalidad Informática influye en el acceso no autorizado a servicios informáticos, en el Distrito Judicial de Lima Norte 2019?
Problema Específico 2	¿Cuál es la efectividad del bien jurídico protegido en los delitos de fraudes informáticos, en el Distrito Judicial de Lima Norte 2019?
OBJETIVOS	
Objetivo General	Determinar de qué manera se da el Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019.
Objetivo Específico 1	Determinar cómo la criminalidad informática influye en el acceso no autorizado a servicios informáticos, en el Distrito Judicial de Lima Norte 2019.
Objetivo Específico 2	Establecer que tan efectivo es el reconocimiento del bien jurídico protegido en el fraude informático en el Distrito Judicial de Lima Norte 2019.

SUPUESTOS JURÍDICOS	
Supuesto General	Los delitos informáticos contra el patrimonio se vienen cometiendo con mayor frecuencia en el país, esto debido a que existe una errónea tipificación de la norma penal con relación a esta clase de delitos, ya que en la Ley N° 30096 solo se considera al Fraude Informático, cuando en realidad existen diferentes conductas que no se configuran en el tipo penal del Fraude Informático.
Supuesto Específico 1	Si bien en la Legislación Peruana existe una sanción por incurrir en la conducta de Fraude Informático, este suele ser insuficiente ya que en la mayoría de casos, los afectados solo realizan su denuncia con la finalidad de recuperar su dinero, y así una vez cumplido ese objetivo ya no continúan con la investigación generando así que gran parte de esos casos se archive por falta de interés.
Supuesto Específico 2	Los criterios en la calificación en los delitos informáticos contra el patrimonio, específicamente en el de fraude informático son ambiguos, toda vez que existen diferentes modalidades y que no necesariamente tienen que ser cometidos desde el país, ya que por los alcances de la tecnología pueden cometerse desde otro continente.
Categorización	Categoría 1: El Tratamiento Jurídico Penal por parte del Fiscal Subcategoría 1: Bien jurídico protegido Subcategoría 2: Criminalidad Informática Categoría 2: Delitos Informáticos contra el Patrimonio Subcategoría 1: Fraude Informático Subcategoría 2: El acceso no autorizado a servicios informáticos

MÉTODO	
Diseño de investigación	- **Enfoque:** Cualitativo - **Diseño:** Teoría Fundamentada - **Tipo de investigación**: Aplicada - **Nivel de la investigación:** Descriptivo
Método de muestreo	- **Población:** Fiscales - **Muestra:** 05 Fiscales
Plan de análisis y trayectoria metodológica	- **Técnica e instrumento de recolección de datos** ✓ **Técnica:** Entrevista y Análisis Documental ✓ **Instrumento:** Guía de entrevista y guía de análisis documental
Análisis cualitativo de datos	Hermenéutico, analítico, comparativo, inductivo y sintético

ANEXO 7.- GUÍA DE ANÁLISIS DOCUMENTAL.

GUÍA DE ANÁLISIS DE FUENTE DOCUMENTAL

Título: "El Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, Distrito Judicial de Lima Norte 2019."

Objetivo General: Determinar de qué manera se da el Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019.

AUTOR (A): Jean Carlos Gómez Vásquez

FECHA : 05-06-2020

FUENTE DOCUMENTAL	CONTENIDO DE LA FUENTE A ANALIZAR	ANÁLISIS DEL CONTENIDO	CONCLUSIÓN
Nye Jr., J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security, 41(3)*, 44-71. ISSN: 1531-4804. https://doi.org/10.1162/ISEC_a_00266	Si los atacantes usan Internet, pueden enmascarar el punto de origen detrás de las banderas de varios servidores remotos, que se pueden ubicar en una variedad de jurisdicciones. Pueden usar actores no estatales como representantes y crear banderas falsas. A pesar de que los análisis forenses que rastrean el intercambio de mensajes entre máquinas pueden detectar muchos "saltos" entre servidores, a menudo lleva tiempo, y cuantos más saltos, mayor es la incertidumbre, Además, conocer la verdadera ubicación de una máquina no es lo mismo que conocer al último instigador de un ataque.	Una de las mayores desventajas de tener acceso al internet es el anonimato con el cual se puede navegar en diferentes páginas de la red, por lo cual genera uno de los mayores inconvenientes al momento de investigar para poder rastrear a aquellas personas que cometen este tipo de actos ilícitos, refugiándose en el anonimato que le brinda el ciberespacio.	Al ser la tecnología una herramienta indispensable en el día a día de la convivencia en la sociedad, debemos tener en cuenta que, si bien te facilita realizar diferentes acciones desde la comodidad de tu casa, también es una puerta de acceso para que personas realicen actos ilícitos perjudicando a terceros, teniendo como principal aliado al anonimato que brinda realizar este tipo de acciones en el ciber espacio.

GUÍA DE ANÁLISIS DE FUENTE DOCUMENTAL

Título: "El Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, Distrito Judicial de Lima Norte 2019."

Objetivo General: Determinar de qué manera se da el Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019.

AUTOR (A): Jean Carlos Gómez Vásquez

FECHA : 05-06-2020

FUENTE DOCUMENTAL	CONTENIDO DE LA FUENTE A ANALIZAR	ANÁLISIS DEL CONTENIDO	CONCLUSIÓN
la Ley de Delitos Informáticos N° 30096, que luego fue modificada por la Ley N° 30171	"Artículo 8. Fraude informático. El que deliberada e ilegítimamente 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."	Esta norma se encuentra vigente desde el año 2013, su correcta aplicación no se ha venido dando de la manera más adecuada y esto debido a la complejidad de las mismas; por lo cual el tratamiento jurídico que se le tiene que dar a los delitos informáticos contra el patrimonio, tiene que darse de una manera distinta a la tradicional como cuando se califican delitos contra el patrimonio; como por ejemplo hurto, robo, etc.	Pese a que el legislador desde hace varios años trato de resguardar los diferentes bienes jurídicos que pueden ser vulnerados a través de la tecnología, en la realidad la aplicación de la investigación fiscal no es la más adecuada para esta clase de delitos, debido a que no se le da el interés adecuado por parte de los afectados.

GUÍA DE ANÁLISIS DE FUENTE DOCUMENTAL

Título: "El Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, Distrito Judicial de Lima Norte 2019."

Objetivo General: Determinar de qué manera se da el Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019.

AUTOR (A): Jean Carlos Gómez Vásquez

FECHA : 05-06-2020

FUENTE DOCUMENTAL	CONTENIDO DE LA FUENTE A ANALIZAR	ANÁLISIS DEL CONTENIDO	CONCLUSIÓN
Dlamini, S., y Mbambo, C. (2019). Understanding policing of cybercrime in South Africa: The phenomena, challenges and effective responses. *Cogent Social Sciences, 5(1),* 1-13. ISSN: 2331-1886. https://doi.org/10.1080/ 23311886.2019.1675404	La investigación que involucra computadoras a menudo falla debido a errores cometidos en la etapa inicial del proceso de investigación donde la evidencia digital esencial se ignora, destruye, compromete o es manejado de manera inapropiada. Esencialmente, durante una investigación de cibercrimen debe haber retrasos mínimos en la respuesta al delito. Los retrasos durante una investigación comprometen la efectividad de la investigación y hace que la respuesta sea irrelevante y sin valor cuando se trata de atrapando al cibercriminal.	Luego de realizado el acto ilícito, se deben recabar adecuadamente los indicios que se dejaron para cometerlos, pero son pocos los rastros que se pueden dejar en el ciber espacio, por lo cual es importante poder mantener y actuar de manera célere en la investigación en cuanto se tengan los mínimos elementos suficientes para poder realizar la individualización del acusado.	Debido a la particularidad de los delitos informáticos contra el patrimonio, es que se debe dar una adecuada calificación del delito por parte del fiscal, ya que como señala el autor son pocas las pistas que se dejan en esta clase de actos, más sin embargo si se tiene una dirección IP asociado el acto debería ser elemento suficiente para tratar de individualizar al sujeto que habría cometido el delito.

GUÍA DE ANÁLISIS DE FUENTE DOCUMENTAL

Título: "El Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, Distrito Judicial de Lima Norte 2019."

Objetivo Específico 1: Determinar cómo la criminalidad informática influye en el acceso no autorizado a servicios informáticos, en el Distrito Judicial de Lima Norte 2019.

AUTOR (A): Jean Carlos Gómez Vásquez

FECHA : 05-06-2020

FUENTE DOCUMENTAL	CONTENIDO DE LA FUENTE A ANALIZAR	ANÁLISIS DEL CONTENIDO	CONCLUSIÓN
Santivañez, D**.** (2015). Ciberterrorismo: amenaza fulminante. Resumen de la tesis "El delito de terrorismo informático como figura jurídica en el código penal vigente. Propuesta para su inclusión en la Ley sobre Delitos Informáticos en el Perú". *Ius et Praxis, Revista de la Facultad de Derecho, (46),* 225-240. ISSN: 1027-8168. http://revistas.ulima.edu.pe/index.php/Ius_et_Praxis/article/view/673/649	La principal herramienta para cometer esta clase de delitos es poder tener acceso a una computadora o cualquier otro elemento electrónico, que va permitir al usuario de estos equipos cometer una conducta punible como si se tratara de un delincuente común, por lo cual aportan nuevas conductas delictivas a cometer, pero usando a la tecnología como medio para cometer un acto ilícito.	La particularidad en esta clase de delitos es que se cometen los actos delictivos, pero con la necesidad de un equipo tecnológico, llámese computadora, smartphone, etc. Generando así la fácil accesibilidad por parte de los criminales informáticos a servicios de terceros generándoles un perjuicio que puede ser tanto monetario como administrativo.	Cuando nos referimos a criminales informáticos debemos entenderlo como aquella persona que tiene poco o abundante conocimiento sobre informática con la finalidad de acceder y obtener algún beneficio por lo que no solo se necesita de un equipo tecnológico sino también de alguien que lo manipule.

GUÍA DE ANÁLISIS DE FUENTE DOCUMENTAL

Título: "El Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, Distrito Judicial de Lima Norte 2019."

Objetivo Específico 1: Determinar cómo la criminalidad informática influye en el acceso no autorizado a servicios informáticos, en el Distrito Judicial de Lima Norte 2019.

AUTOR (A): Jean Carlos Gómez Vásquez

FECHA : 05-06-2020

FUENTE DOCUMENTAL	CONTENIDO DE LA FUENTE A ANALIZAR	ANÁLISIS DEL CONTENIDO	CONCLUSIÓN
Kello, L. (2013), The Meaning of the Cyber Revolution. *International Security, 38(2)*, 7-40. ISSN: 1531-4804. https://doi.org/10.1162/ISEC_a_00138	La facilidad de proliferación de las armas cibernéticas significa que, excepto en caso de las acciones ofensivas sean más sofisticadas, el número de posibles asaltantes es largo. Segundo, probar la identidad o ubicación de cualquiera de estos, los asaltantes pueden ser un gran desafío, porque el ciberespacio le permite a un atacante grado excesivo de anonimato. Tercero, donde la atribución es posible, puede no ser del tipo adecuado para organizar una respuesta punitiva. Conociendo la dirección IP de una máquina de ataque, la forma más básica de atribución técnica, no necesariamente revela la identidad de su controlador humano.	Actualmente se puede considerar al internet como un arma sofisticada, debido a su naturaleza de interconectar personas al mismo tiempo en diferentes lugares, por lo cual cuando hablamos de criminalidad informática en el ciberespacio, está referida al sin número de personas que pueden participar para aun mismo acto ilícito para hacer más compleja la investigación y mantenerse en el anonimato.	Generalmente cuando el acto delictivo es cometido por varios sujetos, en la calificación de la disposición fiscal se van a clasificar como imputados, que a lo largo de la investigación se dará con el grado de participación de cada uno, sin embargo, en los delitos informáticos, la pluralidad de sujetos tan solo dificultaría la labor de investigación ya que no necesariamente todos los sujetos están en el mismo lugar, sino que están en distintos lugares generando así diferentes direcciones electrónicas, que no necesariamente revelará la identidad de la persona que cometió los ilícitos.

GUÍA DE ANÁLISIS DE FUENTE DOCUMENTAL

Título: "El Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, Distrito Judicial de Lima Norte 2019."

Objetivo Específico 1: Determinar cómo la criminalidad informática influye en el acceso no autorizado a servicios informáticos, en el Distrito Judicial de Lima Norte 2019.

AUTOR (A): Jean Carlos Gómez Vásquez

FECHA : 05-06-2020

FUENTE DOCUMENTAL	CONTENIDO DE LA FUENTE A ANALIZAR	ANÁLISIS DEL CONTENIDO	CONCLUSIÓN
Ranganayaki, T. y Venkatachalam, M. (2015). Investigation on Cyber Crime, Cyber Law and Cyber Security. *International Journal of Computer Science and Information Security*, 68-71. http://sites.google.com /site/ijcsis/ ISSN 1947-5500	Se puede decir que el cibercrimen son esos crímenes, de que, el género es el crimen convencional, donde Computadora una herramienta o medio de conducir o cometer crimen. El cibercrimen es fácil de cometer, difícil de detectar y a menudo difícil de localizar en términos jurisdiccionales, dada la geografía indeterminada de la red. Los ciberdelincuentes pueden destruir los sitios web y portales pirateando y plantando virus, juegos en línea, fraudes por transferencia de fondos desde un rincón del mundo a otro y obtener acceso a altamente confidencial y sensible información.	La criminalidad informática y los crímenes convencionales contra el patrimonio son similares, la diferencia se da a partir de que en la criminalidad informática se usa la computadora como medio o fin de realizar el acto lesivo, por lo cual se convierte en una herramienta para acceder a diferentes sistemas informáticos, dándose así que sea más accesible para cometer ilícitos, pero dificultando la localización de los criminales informáticos, en términos jurisdiccionales.	El anonimato que se da en el ciberespacio es el principal aliado para estos ciberdelincuentes, ya sea que se use a la tecnología como medio o fin para acometerlos, siempre tendrán la ventaja debido a que no tiene contacto con un objeto tangible. Por otro lado, dependiendo de la acción que realicen es posible poder obtener pistas sobre los atacantes, por ejemplo, en el caso de fraude electrónico lo que se busca es el lucro, por lo cual siempre se va tener un registro de la persona beneficiada en el sistema, por lo cual la investigación puede partir desde ese punto, sin embargo, en el caso que la finalidad solo era atacar una página web los rastros que se pueden obtener son mínimos.

GUÍA DE ANÁLISIS DE FUENTE DOCUMENTAL

Título: "El Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, Distrito Judicial de Lima Norte 2019."

Objetivo Específico 2: Establecer que tan efectivo es el reconocimiento del bien jurídico protegido en el fraude informático en el Distrito Judicial de Lima Norte 2019.

AUTOR (A): Jean Carlos Gómez Vásquez

FECHA : 05-06-2020

FUENTE DOCUMENTAL	CONTENIDO DE LA FUENTE A ANALIZAR	ANÁLISIS DEL CONTENIDO	CONCLUSIÓN
Sabillon, R., Cano, J., Cavaller Reyes V. y Serra Ruiz, J. (2016). Cybercrime and Cybercriminals: A Comprehensive Study. *International Journal of Computer Networks and Communications Security, 4(6),* 165-176. ISSN: 2410-0595. http://hdl.handle.net/10609/78507	El fraude o la falsificación en línea se dan de muchas maneras posibles. Las víctimas son engañadas usando tecnologías digitales. Algunos ejemplos combinan en subastas en línea, fraude de acciones, fraude de tarjetas de crédito, fraude de telemercadeo, esquemas publicitarios falsos, reclamos por daños falsos, información privilegiada, campañas de difamación cibernética, fraude ad hoc, fraudes informáticos, fraude de clics, esquemas Ponzi / piramidales, lotería / sorteos y estafas de concursos, esquemas para hacerse rico rápidamente, estafa nigeriana, estafa de tono de llamada, estafa de llamadas perdidas, estafa de mensajes de texto, estafa de trivia SMS, estafa de salud, estafa de emergencia, estafa de citas, estafa de trabajo, estafa de pequeñas empresas y estafa de servicio.	Para los delitos informáticos contra el patrimonio van a existir diferentes formas para llegar a vulnerar el patrimonio de un tercero, gran parte de esos métodos, no son necesariamente vulnerando las medidas de seguridad existente en los sistemas informáticos, sino por el contrario, ya que son los propios afectados o posibles afectados quienes brindan información relevante para que los ciberdelincuentes puedan acceder con mayor facilidad.	Debido a la gran variedad de métodos para engañar a las personas y capturar sus datos, es que nos encontramos ante un creciente fenómeno delincuencial, que en la mayoría de sus acciones afectan al patrimonio, sin embargo, es en la variedad de métodos para cometer estos delitos que podemos apreciar que ya sea la tecnología como medio o fin siempre va a ir de la mano con la afectación al patrimonio.

GUÍA DE ANÁLISIS DE FUENTE DOCUMENTAL

Título: "El Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, Distrito Judicial de Lima Norte 2019."

Objetivo Específico 2: Establecer que tan efectivo es el reconocimiento del bien jurídico protegido en el fraude informático en el Distrito Judicial de Lima Norte 2019.

AUTOR (A): Jean Carlos Gómez Vásquez

FECHA : 05-06-2020

FUENTE DOCUMENTAL	CONTENIDO DE LA FUENTE A ANALIZAR	ANÁLISIS DEL CONTENIDO	CONCLUSIÓN
Mayer Lux, L. (2017). El bien jurídico protegido en los delitos informáticos. Revista Chilena de Derecho, 44(1), 261-285. ISSN: 0718-3437. http://dx.doi.org/10.4067/S0718-34372017000100011	La funcionalidad informática sirve al conjunto de las personas y es, a partir de esta figura que se presenta como un bien jurídico colectivo. Por ende, se presenta de forma que el uso y disfrute no es propio ni excluyente de persona alguna, ni puede distribuirse entre algunos individuos. Se presenta, asimismo, de un interés social relevante para el individuo, que está vinculado, de una u otra forma, con la labor habitual de todos quienes integran un determinado sistema. Esta transgresión al funcionamiento informático afecta al libre desarrollo de las personas que usan algún dispositivo electrónico con acceso a una interconexión, como lo es el internet.	Es así que tenemos que la funcionalidad informática está a disposición de otros bienes jurídicos, pero al verse afectados estos bienes jurídicos por una afectación al correcto funcionamiento del sistema informático, nace la necesidad de resguardar y conservar un adecuado funcionamiento de dichos sistemas.	Lo que se trata de resguardar en estos supuestos es proteger los bienes jurídicos tradicionales, como el patrimonio, a través de bienes jurídicos no tradicionales, como el correcto funcionamiento del sistema informático, por lo cual al momento de aperturar una investigación fiscal debería consignarse de esa manera para darle un adecuado tratamiento jurídico penal

GUÍA DE ANÁLISIS DE FUENTE DOCUMENTAL

Título: "El Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, Distrito Judicial de Lima Norte 2019."

Objetivo Específico 2: Establecer que tan efectivo es el reconocimiento del bien jurídico protegido en el fraude informático en el Distrito Judicial de Lima Norte 2019.

AUTOR (A): Jean Carlos Gómez Vásquez

FECHA : 05-06-2020

FUENTE DOCUMENTAL	CONTENIDO DE LA FUENTE A ANALIZAR	ANÁLISIS DEL CONTENIDO	CONCLUSIÓN
Chaisse, J. y Bauer, C. (2019). Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration. *Vanderbilt Journal of Entertainment & Technology Law, 21(3)*, 549-589. ISSN: 1536-3872 https://ssrn.com/ abstract=3382749	Los activos digitales pueden incluir componentes físicos como hardware y servidores de datos, que pueden requerirse ubicados dentro el estado del host para cumplir con los requisitos de localización de datos. Sin embargo, Los activos digitales también incluyen componentes no físicos, como lógicos software, datos de clientes y empleados, bases de datos, información, digital bienes y secretos comerciales de la empresa. Dado lo a veces etéreo y naturaleza intangible de los activos digitales, la expansión de la protección FPS es una consideración importante al analizar si los activos son adecuadamente protegidos contra los ciberataques.	Las herramientas usadas para acceder de forma legítima o ilegítima a cualquier sistema informático, son tangibles por lo que son los componentes más fáciles de ubicar en un servidor, sin embargo, la facilidad con la que se pueden varias estos datos generan que no se pueda dar una adecuada protección por cualquier vulneración, para lo cual es materia de investigación del delito si la finalidad del ataque fue lucrativa o quizás acceder a una base de datos etc.	De acuerdo con lo analizado en la presente cita, las consecuencias de los delitos informáticos contra el patrimonio, no siempre van a ser lucrativas ya que dependiendo de cuál era la finalidad del acto ilícito, el fiscal deberá proceder con la apertura de la investigación, debemos tener en claro que dentro de la ley de delitos informáticos existen otros delitos los cuales se pueden encuadrar en la protección de datos informáticos y no el de patrimonio.

ANEXO 8.- ENTREVISTAS REALIZADAS A FISCALES.

FICHA DE ENTREVISTA
(FISCALES)

El Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, Distrito Judicial de Lima Norte 2019.

Entrevistado/a: MARIAN ISABEL MENACHO ZAMORA

Cargo/profesión/grado académico: Fiscal Adjunta Provincial

Institución: Ministerio Público

Objetivo general

Determinar de qué manera se da el Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019.

1.- ¿Considera Ud. que se tienen las adecuadas herramientas y colaboración policial para un correcto Tratamiento Jurídico Penal por parte del Fiscal contra los Delitos Informáticos contra el Patrimonio?

Dentro del Ministerio Público no hay herramientas adecuadas para investigar delitos informáticos, pero la unidad especializada de la Policía si, ellos tienen los mecanismos idóneos para llevar a cabo una investigación ordenada por la fiscalía en relación a dichos delitos.

2.- ¿Qué opina sobre la adhesión de Perú al Convenio de Budapest, considera que se han visto cambios significativos en la lucha en contra de los delitos informáticos contra el patrimonio?

En relación a dicho tratado lo que se ha buscado es encontrar mejoras para evitar la ciberdelincuencia, y en ese sentido han hecho que mínimamente, la policía especializada en dicha materia, pueda tener mejores implementos para investigar y realiza coordinaciones con el extranjero para verificar las identidades de los ciberdelincuentes.

3.- ¿Considera Ud. que exista una limitación jurídica o algún otro factor que impida la formulación de cargos e imputaciones en la comisión de delitos informáticos contra el patrimonio?

No existe limitaciones jurídicas para proceder a formalizar la investigación preparatoria o formular cargos en una investigación relacionada a delitos

informáticos; sin embargo, existen factores extra jurídicos que no permiten llegar a determinar el sujeto activo de dicho delitos, por ejemplo, en la aplicación WhatsApp cada conversación se realiza a través de un código encriptado que resulta tedioso descifrar para recuperar la conversación, pero para ello se tiene que solicitar primero al juez que conceda el levantamiento del secreto de las comunicaciones y contactar con dicha resolución concesoria a la empresa que gestiona dicha base de datos para que remitan la conversación completa que posiblemente favorecería en una investigación.

Objetivo específico 1

Determinar cómo la criminalidad informática influye en el acceso no autorizado a servicios informáticos, en el Distrito Judicial de Lima Norte 2019.

4.- ¿Dentro de su consideración, cree Ud. que las nuevas modalidades de criminalidad informática influyen en el acceso no autorizado a servicios informáticos? ¿sí o no? ¿Por qué?

La mayoría de delitos informáticos se encuentran en el rango del acceder a información no autorizada por sus propietarios, motivo por el cual las nuevas modalidades delictivas en el tema informático han evolucionado con el fin de evitar los medios de seguridad de ciertas compañías o entidades bancarias para que cometan dichos delitos.

5- ¿Bajo su experiencia, considera Ud. que son las personas naturales son las más vulnerables ante la comisión de fraude informático, en comparación con las personas jurídicas en la sociedad? ¿Por qué?

La mayoría de agraviados relacionados a delitos informáticos son personas naturales, ya que se encuentran en juego información personal, cosa que una persona jurídica no realiza en su mayoría por que tienen quizás áreas encargadas para fines electrónicos patrimoniales.

6.- ¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos contra el patrimonio?

Hasta la fecha no todos los medios electrónicos relacionados al internet no cuentan con sistemas de prevención para evitar que se cometan delitos informáticos con el

patrimonio.

Objetivo específico 2

Establecer que tan efectivo es el reconocimiento del bien jurídico protegido en los delitos informáticos, ante el fraude informático en el Distrito Judicial de Lima Norte 2019.

7.- Bajo su percepción, ¿Qué tan efectivo es el reconocimiento del bien jurídico protegido en los delitos informáticos, especialmente en el delito de fraude informático?

El reconocimiento del bien jurídico es esencial para todas las investigaciones, dado que si no existe el bien jurídico afectado no podemos revelar el delito cometido, y sería una afectación el principio de legalidad si no se establece cual es el delito y el bien jurídico afectado.

8.- ¿Qué opina Ud. sobre establecer como bien jurídico protegido, no solo al patrimonio sino también a bienes jurídicos no tradicionales, como el correcto funcionamiento del sistema informático, en los delitos de fraude informático?

Para ello primero debería de haber una legislación de por medio, porque si consignamos como fiscales que el bien jurídico protegido debe de ser el correcto funcionamiento de los sistemas informáticos, quizás se debería tomar como agravante al delito contra el patrimonio.

9.- ¿Considera Ud. idóneo que solo se encuentre tipificado el delito de Fraude Informático para tratar de contemplar las diferentes acciones ilícitas que se llevan a cabo en los delitos informáticos contra el patrimonio?

La idea es que el delito informático como cualquier otro tengas sus agravantes para no considerarlo como un delito simple, dado que existen diversas herramientas que develan la alevosía de la actuación de los delincuentes informáticos.

MARIAN ISABEL MENACHO ZAMORA
Fiscal Adjunta Provincial (P)
07° Fiscalía Provincial Penal de Lima Norte

FICHA DE ENTREVISTA
(FISCALES)

El Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, Distrito Judicial de Lima Norte 2019

Entrevistado/a: Marlene Anyela Falcón Oré

Cargo/profesión/grado académico: Fiscal Provincial Adjunta

Institución: Ministerio Público

Objetivo general

Determinar de qué manera se da el Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019.

1.- ¿Considera Ud. que se tienen las adecuadas herramientas y colaboración policial para un correcto Tratamiento Jurídico Penal por parte del Fiscal contra los Delitos Informáticos contra el Patrimonio?

En el presente caso, aunque el titular de la acción penal es el fiscal, en las disposiciones de apertura estas pueden ser designadas a nivel policial, más aún en casos específicos como el de delitos informáticos ya que ellos cuentan con las herramientas específicas para recabar suficiente información con la que se pueda establecer una futura imputación.

2.- ¿Qué opina sobre la adhesión de Perú al Convenio de Budapest, considera que se han visto cambios significativos en la lucha en contra de los delitos informáticos contra el patrimonio?

Pese a la adhesión del Perú al Convenio de Budapest, en la práctica no se han visto cambios significativos, específicamente en los delitos informáticos contra el patrimonio; sin embargo, si se hace claro énfasis en el apoyo de jurisdicciones internacionales ante la identificación de estos ciberdelincuentes que gran parte cometen ilícitos desde diferentes países.

3.- ¿Considera Ud. que exista una limitación jurídica o algún otro factor que impida la formulación de cargos e imputaciones en la comisión de delitos informáticos contra el patrimonio?

Como lo mencione anteriormente, una de las más grandes complicaciones se da entorno a la identificación del imputado ya que la misma tecnología permite ocultar rastros en la red informática. Otro punto resaltante y conflictivo se da en los criterios

establecidos por el NCPP, como por ejemplo en la competencia territorial, ya que en esta clase de delitos no se puede determinar un lugar físico y exacto donde se comete la vulneración.

Objetivo específico 1

Determinar cómo la criminalidad informática influye en el acceso no autorizado a servicios informáticos, en el Distrito Judicial de Lima Norte 2019.

4.- ¿Dentro de su consideración, cree Ud. que las nuevas modalidades de criminalidad informática influyen en el acceso no autorizado a servicios informáticos? ¿sí o no? ¿Por qué?

Si considero que las distintas modalidades que usan los criminales informáticos les brinda una mayor accesibilidad a datos de sus posibles víctimas, más aún que con el avance de la tecnología se ha buscado simplificar el acceso de los usuarios de banca móvil a través de dispositivos como los smartphones; lo que conlleva a que estos dispositivos tengan datos bancarios guardados en un bien que puede ser sustraído fácilmente.

5- ¿Bajo su experiencia, considera Ud. que son las personas naturales son las más vulnerables ante la comisión de fraude informático, en comparación con las personas jurídicas en la sociedad? ¿Por qué?

Ambos son vulnerables, pero debemos tener en cuenta el grado de complejidad que favorece al criminal informático toda vez que las denuncias por fraude informático suelen ser por montos no tan excesivos, por lo cual estos criminales tienden a realizar ataques en mayor cantidad a personas naturales ya que normalmente las empresas tienen un sistema de seguridad informático que generaría mayores esfuerzos.

6.- ¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos contra el patrimonio?

Considero que las estrategias que se deben tomar en cuenta para la prevención de estos delitos no deben venir solo por parte del derecho, sino en trabajo conjunto con las entidades bancarias para que los usuarios no se encuentren expuestos a estos ataques sin poner trabas burocráticas al momento de la investigación y con respecto a las sanciones estas ya se encuentran establecidos dentro de la norma.

Objetivo específico 2

Establecer que tan efectivo es el reconocimiento del bien jurídico protegido en los delitos informáticos, ante el fraude informático en el Distrito Judicial de Lima Norte 2019.

7.- Bajo su percepción, ¿Qué tan efectivo es el reconocimiento del bien jurídico protegido en los delitos informáticos, especialmente en el delito de fraude informático?

Parte importante en la norma penal es la protección al bien jurídico, por lo cual es importante señalar la afectación del mismo, es así que en el delito de fraude informático se tiene al patrimonio de manera general como bien tutelado. Por otro lado, la Ley de delitos informáticos sigue siendo muy general tratando de abarcar diferentes comportamientos en un solo delito.

8.- ¿Qué opina Ud. sobre establecer como bien jurídico protegido, no solo al patrimonio sino también a bienes jurídicos no tradicionales, como el correcto funcionamiento del sistema informático, en los delitos de fraude informático?

Para determinar ello debemos partir por el concepto de patrimonio como el conjunto de relaciones jurídicas pertenecientes a una persona que abarca el pasivo y activo, por lo cual si la vulneración afecta al funcionamiento del sistema informático y este conlleva a un deterioro del patrimonio del afectado debería considerarse como afectación también al patrimonio, pero como se había mencionado anteriormente la norma no precisa detalles sobre ello; lo recomendable sería incluirlo también del correcto funcionamiento del sistema informático posiblemente como un agravante dela conducta principal.

9.- ¿Considera Ud. idóneo que solo se encuentre tipificado el delito de Fraude Informático para tratar de contemplar las diferentes acciones ilícitas que se llevan a cabo en los delitos informáticos contra el patrimonio?

No es lo más idóneo tener solo un artículo que refiera sobre afectaciones al patrimonio, toda vez que la criminalidad informática cada vez encuentra diferentes modalidades para lucrar a través de la tecnología, pero por el momento puede ser suficiente ya que gran parte de las denuncias realizadas son por fraudes o pagos realizados sin consentimiento.

FICHA DE ENTREVISTA
(FISCALES)

El Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, Distrito Judicial de Lima Norte 2019

Entrevistado/a: Ruth Evelyn Zubieta Quineche.

Cargo/profesión/grado académico: Fiscal Adjunta Provincial Provisional.

Institución: Ministerio Público.

Objetivo general

Determinar de qué manera se da el Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019.

1.- ¿Considera Ud. que se tienen las adecuadas herramientas y colaboración policial para un correcto Tratamiento Jurídico Penal por parte del Fiscal contra los Delitos Informáticos contra el Patrimonio?

En lo particular no se cuenta con las herramientas pues por lo general este tipo de delitos son derivados a la división de informática sito en la Av España, dado que cuando se trata de una investigación más profunda, lo cual hace que el personal policial a cargo de la investigación donde son derivadas las investigaciones estas las derivan y lo cual se hace más largo el plazo de la investigación.

2.- ¿Qué opina sobre la adhesión de Perú al Convenio de Budapest, considera que se han visto cambios significativos en la lucha en contra de los delitos informáticos contra el patrimonio?

Solo es un gran avance, pero no se hace nada o implementa a cada institución lo cual hace que no se vea ningún avance ante este tipo de acuerdos, un ejemplo claro es Chile quien tiene todas sus instituciones interconectadas, es decir en el pueblo más lejano si alguien desea contraer nupcias solo tiene que verificar su nombre y saldrá, situación que no se presenta en Perú

3.- ¿Considera Ud. que exista una limitación jurídica o algún otro factor que impida la formulación de cargos e imputaciones en la comisión de delitos informáticos contra el patrimonio?

La limitación más grande sería el hecho que cada ley que existe en nu stop país no se encuentra reglamentada, situación por lo cual existen vacíos.

Objetivo específico 1

Determinar cómo la criminalidad informática influye en el acceso no autorizado a servicios informáticos, en el Distrito Judicial de Lima Norte 2019.

4.- ¿Dentro de su consideración, cree Ud. que las nuevas modalidades de criminalidad informática influyen en el acceso no autorizado a servicios informáticos? ¿sí o no? ¿Por qué?

Si, pues en la actualidad y debido a la emergencia sanitaria que atravesamos solo existen ventas online donde uno tiene que consignar el número de la tarjeta y sino uno no paga por un seguro, este podría ser usado.

5- ¿Bajo su experiencia, considera Ud. que son las personas naturales son las más vulnerables ante la comisión de fraude informático, en comparación con las personas jurídicas en la sociedad? ¿Por qué?

No, creo que todos somos vulnerables a este tipo de fraude, pues si uno pone en Google su nombre aparece en que rubro o actividad se dedica siendo víctimas potenciales.

6.- ¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos contra el patrimonio?

En Perú no, dado que para rastrear el IP donde salió la información es solo accesible a personas que cuentan con los medios necesarios. En tal sentido, no existe forma de prevención a menos que no sea por cuenta propia y no por parte del estado y mucho menos sanción en caso de incurrir en ello.

Objetivo específico 2

Establecer que tan efectivo es el reconocimiento del bien jurídico protegido en los delitos informáticos, ante el fraude informático en el Distrito Judicial de Lima Norte 2019.

7.- Bajo su percepción, ¿Qué tan efectivo es el reconocimiento del bien jurídico protegido en los delitos informáticos, especialmente en el delito de fraude informático?

A que se configuran diferentes tipos de delitos por separados como el fraude, el cual debe estar vinculado a la informática, por ello vuelvo a reiterar que si bien se reconoce el bien jurídico en un delito informático este no se encuentra reglamentado, ósea bajo qué medidas, circunstancias, etc.

8.- ¿Qué opina Ud. sobre establecer como bien jurídico protegido, no solo al patrimonio sino también a bienes jurídicos no tradicionales, como el correcto funcionamiento del sistema informático, en los delitos de fraude informático?

Para ello debe hacerse una diferenciación y reiteró toda ley necesita su reglamento para que no ocurra este tipo de situación, que no sean genéricas sino específicas, para que no se tenga, a menos que no sea necesario de usar una ley general para cada tipo de caso.

9.- ¿Considera Ud. idóneo que solo se encuentre tipificado el delito de Fraude Informático para tratar de contemplar las diferentes acciones ilícitas que se llevan a cabo en los delitos informáticos contra el patrimonio?

Pues no estaría demás considerar a la estafa, pero bajo qué circunstancias, otra alternativa que debería evaluarse.

FICHA DE ENTREVISTA
(FISCALES)

El Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019

Entrevistado/a: Dimas Hugo Lázaro Rivera

Cargo/profesión/grado académico: Fiscal Provincial- Segundo Despacho- 1FPPC

Institución: Ministerio Publico

Objetivo general

Determinar de qué manera se da el Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019.

1.- ¿Considera Ud. que se tienen las adecuadas herramientas y colaboración policial para un correcto Tratamiento Jurídico Penal por parte del Fiscal contra los Delitos Informáticos contra el Patrimonio?

Siendo específicos dentro del labor de la fiscalía no hay una herramienta adecuada para tratar estos delitos debido a su particularidad de desarrollarse en un espacio intangible por lo que es primordial que sea tratado por la División de Investigación de Alta Tecnología (DIVINDAT).

2.- ¿Qué opina sobre la adhesión de Perú al Convenio de Budapest, considera que se han visto cambios significativos en la lucha en contra de los delitos informáticos contra el patrimonio?

A inicios del 2019 el Perú se adhirió al Convenio de Budapest, sin embargo, en la práctica no se ha logrado realizar grandes cambios a nivel de investigación y sanción, ya que nuestra ley de delitos informáticos (Ley N° 30096) del año 2013 ya seguía las reglas generales del Convenio de Budapest, por lo cual el gran avance que se ha dado va relacionado a la cooperación internacional para los países adscritos a este Convenio.

3.- ¿Considera Ud. que exista una limitación jurídica o algún otro factor que impida la formulación de cargos e imputaciones en la comisión de delitos informáticos contra el patrimonio?

La principal limitación que se da en esta clase de delitos no es necesariamente jurídica, sino que radica en la falta de interés del agraviado de proseguir con las

investigaciones ya que gran parte de las denuncias realizadas son solo exigencias que la entidad bancaria le solicita al agraviado para que pueda atender su reclamo, por lo cual una vez atendido ello, ya no continúan con la denuncia.

Objetivo específico 1

Determinar cómo la criminalidad informática influye en el acceso no autorizado a servicios informáticos, en el Distrito Judicial de Lima Norte 2019.

4.- ¿Dentro de su consideración, cree Ud. que las nuevas modalidades de criminalidad informática influyen en el acceso no autorizado a servicios informáticos? ¿sí o no? ¿Por qué?

Dese luego que sí, mucho más en la actualidad debido a la coyuntura en la que nos encontramos, lo que ha generado que las personas adquieran productos realizando pagos por internet, lo que ha sido aprovechado por los criminales para desenvolverse de manera mas eficiente dentro del anonimato del ciberespacio.

5- ¿Bajo su experiencia, considera Ud. que son las personas naturales son las más vulnerables ante la comisión de fraude informático, en comparación con las personas jurídicas en la sociedad? ¿Por qué?

Debido a la avanzada criminalidad informática considero que tanto las personas naturales como las personas jurídicas son propensas a ser víctimas de fraude informático, sin embargo para estos criminales resulta mas sencillo atacar a una persona natural que tiene como único medio de protección la clave de una tarjeta; que atacar a un sistema de una empresa para generar ganancias. La vulnerabilidad es en ambos sujetos de derecho, pero las denuncias realizadas casi en su totalidad son hechas por agravio netamente a personas naturales.

6.- ¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos contra el patrimonio?

Una estrategia para la prevención propiamente dicha para los delitos informáticos sería muy complicada, debido a la facilidad con la que se puede ocultar los rastros dentro de la navegación a través de internet, a lo mucho se podría seguir informando al publico en general no brindar datos personales vinculados a su registro bancario, pero de todas maneras para realizar compras a través de internet te siguen pidiendo datos como dígitos de la tarjeta, la fecha de vencimiento, el CVV,

etc. Con respecto a las sanciones estas ya se encuentran establecidas dentro de la norma penal (Ley N° 30096).

Objetivo específico 2

Establecer que tan efectivo es el reconocimiento del bien jurídico protegido en los delitos informáticos, ante el fraude informático en el Distrito Judicial de Lima Norte 2019.

7.- Bajo su percepción, ¿Qué tan efectivo es el reconocimiento del bien jurídico protegido en los delitos informáticos, especialmente en el delito de fraude informático?

Como lo había señalado anteriormente la Ley N° 30096, solo ha transcrito las reglas generales que se habían estipulado dentro del Convenio de Budapest, por lo cual solo se empeñaron en reconocer la afectación del patrimonio con la particularidad de ser cometido a través de medios tecnológicos, lo cual genera que no sea muy efectiva la norma al ser muy general.

8.- ¿Qué opina Ud. sobre establecer como bien jurídico protegido, no solo al patrimonio sino también a bienes jurídicos no tradicionales, como el correcto funcionamiento del sistema informático, en los delitos de fraude informático?

Es importante resaltar que en los delitos informáticos dentro de la Ley N°30096 se tiene al sistema informático en el capitulo II como una afectación a la base de datos según las alteraciones que se hagan en este, pero no se toma en cuenta que el sistema informático también es parte del patrimonio, toda vez que cualquier tipo de vulneración o daño de este, puede menguar en el patrimonio del titular del sistema informático.

9.- ¿Considera Ud. idóneo que solo se encuentre tipificado el delito de Fraude Informático para tratar de contemplar las diferentes acciones ilícitas que se llevan a cabo en los delitos informáticos contra el patrimonio?

Debemos tener en claro que la norma contempla diferentes acciones a cometer dentro del delito de fraude informático, más sin embargo aún existen diferentes comportamientos que no señala específicamente la norma, como se da en el caso de secuestro informático para tener un beneficio lucrativo.

DIMAS HUGO LAZARO RIVERA
FISCAL PROVINCIAL
Primera Fiscalía Provincial Penal
Corporativa de Los Olivos
Distrito Fiscal de Lima Norte

FICHA DE ENTREVISTA
(FISCALES)

El Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019

Entrevistado/a: Ruth Yojany Chinguel Guerrero

Cargo/profesión/grado académico: Fiscal Adjunto Provisional- segundo despacho-1FPPC

Institución: Ministerio Publico- Lima Norte

Objetivo general

Determinar de qué manera se da el Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019.

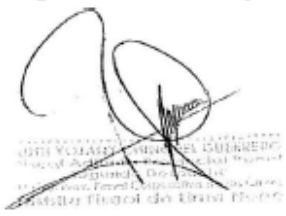
1.- ¿Considera Ud. que se tienen las adecuadas herramientas y colaboración policial para un correcto Tratamiento Jurídico Penal por parte del Fiscal contra los Delitos Informáticos contra el Patrimonio?

Debido a la peculiaridad de esta clase de delitos, a nivel fiscal no se cuentan con las herramientas necesarias para determinar pruebas tecnológicas, por lo cual las disposiciones fiscales son aperturadas a nivel policial, para que el área de investigación de delitos informáticos pueda recabar los elementos necesarios para una futura imputación si se diera el caso. Es necesario precisar que estas disposiciones derivadas en sede policial suelen tardar en retornar al despacho fiscal lo que genera que los plazos de investigación subidos al SGF se han mas largos de los establecidos.

2.- ¿Qué opina sobre la adhesión de Perú al Convenio de Budapest, considera que se han visto cambios significativos en la lucha en contra de los delitos informáticos contra el patrimonio?

El Convenio de Budapest se da con el objetivo de establecer una política penal común y armonizar la cooperación internacional, sin embargo, en el Perú no se han visto cambios significativos en la persecución de estos delitos contra el patrimonio debido a que no se presenta personal bien preparado y una cooperación errática con otras partes responsables de la seguridad electrónica.

3.- ¿Considera Ud. que exista una limitación jurídica o algún otro factor que impida la formulación de cargos e imputaciones en la



comisión de delitos informáticos contra el patrimonio?

Una limitación jurídica como tal no creo, pero si existen impedimentos netamente relacionados con la naturaleza de estos delitos, como lo es en el caso de las evidencias que debido a su intangibilidad estas pueden desaparecer o ser alteradas rápidamente.

Objetivo específico 1

Determinar cómo la criminalidad informática influye en el acceso no autorizado a servicios informáticos, en el Distrito Judicial de Lima Norte 2019.

4.- ¿Dentro de su consideración, cree Ud. que las nuevas modalidades de criminalidad informática influyen en el acceso no autorizado a servicios informáticos? ¿sí o no? ¿Por qué?

Con los avances en redes de telecomunicaciones e información digital se ha abierto una gran brecha para la criminalidad informática por lo que nuevos comportamientos influyen en el acceso no autorizado de servicios informáticos, mas aun hoy en día donde las personas han incrementado el consumo de productos vía online por la coyuntura que estamos viviendo.

5- ¿Bajo su experiencia, considera Ud. que son las personas naturales son las más vulnerables ante la comisión de fraude informático, en comparación con las personas jurídicas en la sociedad? ¿Por qué?

Ambos pueden ser posibles victimas de la criminalidad informática, pero de acuerdo al contexto actual son mas los casos que se dan a persona naturales debido a la simplicidad para cometer estos ataques; situación contraria que se han venido dando en países vecinos como es el caso de chile que en el año 2019 sufrió un ataque a 13 instituciones bancarias.

6.- ¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos contra el patrimonio?

No existen estrategias como tal para prevenir estas clases de delitos, si bien la norma prevé una sanción por este tipo de conductas, la complejidad al momento de recabar información para individualizar al sujeto activo sigue siendo una lucha constante a través de los medios informáticos; es ahí donde radica la importancia de una colaboración eficiente entre la fiscalía y las

entidades financieras que tengan conocimiento ante afectación de sus usuarios.

Objetivo específico 2

Establecer que tan efectivo es el reconocimiento del bien jurídico protegido en los delitos informáticos, ante el fraude informático en el Distrito Judicial de Lima Norte 2019.

7.- Bajo su percepción, ¿Qué tan efectivo es el reconocimiento del bien jurídico protegido en los delitos informáticos, especialmente en el delito de fraude informático?

Si bien es cierto que la Ley de delitos informáticos prevé la protección del patrimonio como bien jurídico tutelado, pero esto no es suficiente ya que no sería efectivo solo por estar en la norma, sino que se deben tratar de acuerdo a la particularidad en las que son afectados y es algo que en la norma no se puede apreciar ya que se da de una manera general.

8.- ¿Qué opina Ud. sobre establecer como bien jurídico protegido, no solo al patrimonio sino también a bienes jurídicos no tradicionales, como el correcto funcionamiento del sistema informático, en los delitos de fraude informático?

Podría ser viable como un agravante siempre y cuando se pueda sustentar que la alteración al correcto funcionamiento del sistema informático conlleve en un deterioro del patrimonio del sujeto pasivo, pero como lo había señalado anteriormente la norma es muy general.

9.- ¿Considera Ud. idóneo que solo se encuentre tipificado el delito de Fraude Informático para tratar de contemplar las diferentes acciones ilícitas que se llevan a cabo en los delitos informáticos contra el patrimonio?

No considero idóneo contemplar las diferentes modalidades de delitos informáticos contra el patrimonio (hurto, sabotaje, secuestro electrónico, etc.) dentro del delito de fraude informático, esto debido a que se siguieron las pautas generales del Convenio de Budapest dado en el 2001, y como sabemos el derecho es cambiante por lo cual con el paso de los años se han venido dando nuevas modalidades que no pueden ser tuteladas de manera general por un solo artículo en la ley penal.