FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogada

AUTORA:

Custodio Cumpa, Yulisa (ORCID: 0000-0003-1052-1830)

ASESORES:

Dr. Fernández de la Torre, Héctor Luis. (ORCID: 0000-0002-1370-1776)

Mg. Yaipén Torres, Jorge José (ORCID: 0000-0003-3414-0928)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal

CHICLAYO – PERÚ

2021

DEDICATORIA.

El presente trabajo está dedicado a Dios sobre todas las cosas, ya que él, es el motivo de nuestra existencia.

Del mismo modo este trabajo lo dedico a mis padres y familiares por el apoyo incondicional en mi faceta de estudiante

AGRADECIMIENTO

A mis docentes del curso de metodología de la investigación y a mi asesor temático, a quien les expreso mi más profundo agradecimiento por hacer posible la realización de este trabajo y por darme las orientaciones oportunas en cada momento que fue necesario.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación tiene como objetivo principal determinar las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático, que se deben de regular expresamente en la ley especial, incorporándola en el artículo 8 de la ley N°30096; siendo necesario que se desarrolle como principales teorías: cibercrímenes, delito informático, fraude informático y las modalidades delictivas.

Así mismo para que se desarrolle esta investigación se ha tenido en cuenta el diseño de investigación cuantitativo, y tipo de investigación descriptivo; de la misma manera se tuvo una población conformada por jueces penales, fiscales penales y los abogados inscritos en el Ilustre Colegio de Abogados de Lambayeque; obteniéndose una muestra de 5 jueces penales, 5 fiscales penales y 60 abogados penalistas, a quienes se les aplicó la técnica de la encuesta y de instrumento el cuestionario.

Luego de aplicarse el cuestionario se obtuvieron diversos resultados, siendo el principal que, se debe regular de manera expresa las circunstancias de hecho del delito de fraude informático en la Ley de Delitos Informáticos – Ley N° 30096. Concluyéndose que, se debe regular de manera expresa dichas circunstancias de hecho en el artículo 8 de la Ley de Delitos Informáticos.

Palabras clave: Cibercrímen, delito informático, fraude informático, circunstancias de hecho.

ABSTRACT

The main objective of this investigation is to determine the current criminal modalities of cybercrimes in the crime of computer fraud, which must be expressly regulated in the special law, incorporating it in article 8 of Law No. 30096; being necessary that it be developed as main theories: cybercrimes, computer crime, computer fraud and criminal modalities.

Likewise, for this research to be carried out, the quantitative research design and the descriptive type of research have been taken into account; in the same way, there was a population made up of criminal judges, criminal prosecutors and lawyers registered in the Lambayeque Bar Association; obtaining a sample of 5 criminal judges, 5 criminal prosecutors and 60 criminal lawyers, to whom the survey technique and the questionnaire were applied.

After applying the questionnaire, various results were obtained, the main one being that the factual circumstances of the crime of computer fraud must be expressly regulated in the Computer Crimes Law - Law No. 30096. Concluding that, it must be regulated in a manner expresses said factual circumstances in article 8 of the Law on Computer Crimes.

Keywords: Cybercrime, computer crime, computer fraud, factual circumstances.

INTRODUCCIÓN

Debido a la crisis sanitaria, las personas están utilizando sus tarjetas de crédito a través de páginas webs, con el objetivo de realizar operaciones bancarias por este medio. Pese a dicha situación los delincuentes han sacado provecho de ello, puesto que han cometido fraudes vía online perjudicando gravemente la economía de las personas.

Dichos actos delictivos cometidos a través del internet son denominados cibercrímenes, los cuales en su mayoría son desconocidos por las personas así como en nuestra normativa penal, por lo que ante dicho desconocimiento los delincuentes sacan provecho de ello para perjudicar patrimonialmente a sus víctimas y así obtener grandes beneficios económicos; pese a que en la actualidad surgen dichas situaciones éstas no se encuentran reguladas en la normativa especial como es la Ley N°30096 - Ley de delitos informáticos, la cual se encuentra en vigencia desde el año 2013, pasando así ocho años en los cuales han surgido nuevas circunstancias de hecho de los cibercrímenes.

En los últimos meses en las noticias se ha evidenciado esta situación, puesto que los usuarios del sector financiero han denunciado que sus cuentas bancarias han sido vaciadas, luego de haber registrado sus códigos de datos o de información de sus bancos, ingresando así a paginas falsas en las cuales colocaron datos como nombres, número de DNI, número de cuenta y la clave, elementos que son utilizados por los delincuentes para obtener beneficios económicos, puesto que es información importante y personal; diversos expertos señalan que los cibercrímenes más comunes que se están cometiendo actualmente es el smishing, pharming, vishing y phishing .

Pese a afrontarse a dicha situación, en nuestra normativa penal sea especial o sustantiva no se encuentran reguladas dichas circunstancias de hecho, solo se encuentra especificadas de manera general dentro del delito de fraude informático en el que se señalan términos como diseñar, introducir, borrar,

alterar, clonar, suspender; las cuales son acciones que se realizan en un sistema informático para obtener un provecho ilícito, pero dichos verbos no amparan situaciones como la creación de “URLS falsas” de las entidades financieras, transferencias no consentidas de dinero, uso de software malicioso entre otros; por lo que resulta importante la regulación de dichas circunstancias de hecho de manera específica.

Se expuso la formulación del problema con el objetivo de analizar la presente investigación formulándose la siguiente interrogación: ¿Cuáles son las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático: otra pandemia en tiempos de coronavirus?

La justificación del estudio se realizó con el propósito de que se especifiquen nuevas circunstancias de hecho de los cibercrímenes teniendo en cuenta el avance de la tecnología ha contribuido a la comisión de delitos de esta naturaleza; por ello es importante que en la norma especial se regulen expresamente dichas circunstancias.

Por otro lado, este trabajo se realizó para que se establezcan circunstancias de hecho de los cibercrímenes en la ley especial de delitos informáticos; siendo que es necesario que exista nuevas regulaciones acorde a lo que sucede en la realidad, puesto que la sociedad cambia y el derecho igual, tras ocho años de regulación de dicha norma especial, es necesario que se actualice nuevas situaciones, con el principal objetivo de no dejar impune un hecho delictivo.

Además los principales beneficiaros es la sociedad porque tendrá una seguridad jurídica de que los hechos delictivos cometidos en su agravio serán sancionados; por otro lado, a los jueces quienes podrán sancionar dichas conductas delictivas sin que exista duda de que dicho actuar se encuentra tipificado expresamente en la norma especial; así como a los fiscales y abogados quienes podrán basarse a lo señalado por la norma para formular acusación así como ejercer la defensa sea del agraviado o del sujeto activo.

Es menester señalar que en la presente investigación se estipuló como objetivo general:
Determinar las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático, que se deben de regular expresamente en la ley especial, incorporándola en el artículo 8 de la ley N°30096.

Se consignaron los siguientes objetivos específicos:
a) Analizar los cibercrímenes cometidos en el delito de fraude informático regulados en la normativa penal y extranjera.
b) Explicar la regulación normativa del delito de fraude informático regulado en nuestro país y en el derecho comparado.
c) Proponer mediante un proyecto de ley la incorporación de circunstancias de hecho de los cibercrímenes en el delito de fraude informático señalado en el artículo 8 de la Ley de Delitos Informáticos.

Ante el problema de la presente investigación se arribó a la siguiente hipótesis:

Es posible proponer la incorporación de las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático en el artículo 8 de la Ley de delitos informáticos.

II. MARCO TEÓRICO

Seguidamente se enunciarán los trabajos previos que están relacionados a esta investigación, los cuales serán señalados como a continuación se presentan

En el ámbito internacional, en Colombia Montañéz (2017) en su tesis titulada "Análisis de los delitos informáticos en el actual sistema penal colombiano" para obtener el grado académico de abogado en la Universidad Libre de Colombia, en su séptima conclusión refiere:

> "El tratamiento a la información que se le da actualmente, así como el avance de la tecnología, cada día va cambiando, siendo que los sistemas informáticos evolucionan de manera gigantesca, es por ello que el derecho debe estar a la par de dichos cambios, así mismo la Ley 1273 del año 2009, debe cambiar y evolucionar para que enfrente los nuevos fenómenos y retos sociales" (p.83)

Es necesario que el derecho y la tecnología estén a la par, debido a que la última va evolucionando; ante ello, el marco normativo debe de asegurar dichas situaciones que se estén presentado para que puedan ser sancionadas; a fin de que, se eviten vacíos legales.

Por otro lado, en España, Quevedo (2017) en su tesis titulada "Investigación y prueba del ciberdelito", para optar el grado académico de doctor en la Universidad de Barcelona, en su segunda conclusión refiere que:

> "En la actividad delictiva el internet tiene gran influencia, siendo que genera nuevas formas del cibercrímen, sirviendo como mecanismo de comisión de otros delitos comunes, siendo que, al investigarse dicho ciberdelito es necesario que se conozca cualidades que posee el internet al sr una red global que presenta conexión instantánea, estructuradas red descentralizadas basadas en la representación digital de la información, permitiendo conexiones entre personas

quienes no es necesario que se tenga la misma ubicación ” (p.121)

El cibercrímen, es lo que comúnmente se están cometiendo actualmente, en sus diversas modalidades y ello se ha evidenciado en los noticieros, en los que muchas personas denunciaron que fueron víctimas de fraude informático, al haber ingresado a link falsos de sus entidades financieras, ingresando datos importantes los cuales permiten a los deficientes vaciar las cuentas bancarias.

En Colombia Abushihab (2016) en su tesis titulada “Cibercrímen: Una aproximación a la delincuencia informática” para optar el título profesional de abogado en la Universidad Santo Tomás – Bogotá en su primera conclusión refiere que:

> “La sociedad moderna, está conformada por una estructura moderna, la cual se encuentra inmerso el avance que ha tenido la tecnología a lo largo de estos años, y lo que ha ocasionado que la población tenga acceso a mecanismos de cambio; es así que el derecho penal debe estar a la par de la tecnología para poder contrarrestar eventuales conductas delictivas” (p.51)

Lo referido por dicho autor tiene gran importancia de aporte para la presente investigación, puesto que se guarda plena concordancia con lo referido por el tesista, al mencionar que las conductas delictivas actuales en su mayoría son realizadas por formas tecnologías que van cambiando constantemente, ocasionando que existan más supuestos y por ende nuevas modalidades delictivas informáticas.

Así mismo en dicho país, Granados y Parra (2016), en su tesis titulada “El delito de hurto por medios informáticos que tipifica el artículo 269 - i de la Ley 1273 de 2009 y su aplicabilidad en el Distrito Judicial de Cúcuta en el período 2012 – 2014” para obtener el grado académico de abogado en la Universidad Libre de Colombia, en su primera conclusión señala:

> “La evolución informática es evidenciada desde mediados del siglo XX hasta la actualidad, trayendo con sigo varios beneficios sociales, especialmente aquellos que están relacionados al intercambio de información a nivel global; conforme a su evolución ha traído consigo importantes ventajas, pero también ha traído desventajas, puesto que conforme al avance tecnológico también ha surgido la delincuencia informática, delitos que se cometen a través de los medios informáticos cometiéndose delitos como la estafa, hurto, fraude, entre otros, delitos tipificados en la Ley 1273, en el cual se sanciona dichos delitos informáticos” (p.68).

De acuerdo al avance de la tecnología, la delincuencia ha ido mejorando su accionar de acuerdo a la evolución de esta, es por ello, que han surgido los diversos delitos informáticos los cuales en la legislación colombiana se encuentran tipificados de manera más amplia y explicita, en comparación en nuestro país que solo se encuentran regulados dichos delitos, pero de manera general.

En España, Rincón (2015) en su tesis titulada “El delito en la cibersociedad y la justicia penal internacional” para obtener el grado académico de doctor en la Universidad Complutense de Madrid, en su tercera conclusión refiere que:”

> “Al analizar la regulación normativa de los delitos informáticos como en la legislación colombiana y española, se ha demostrado el desarrollo histórico que ha pasado, así como la forma que se creó legalmente, el análisis doctrinario, enseñándonos la finalidad que tiene su protección desde el nivel constitucional, amparándose desde el ámbito penal creándose mecanismos de persuasión para que se investigue hasta el juzgamiento” (p.487).

Al analizar la descripción sobre la regulación que tienen los delitos informáticos en otro país, a comparación a la nuestra, la cual es deficiente debido a que se señala circunstancias que están defesadas en el tiempo, siendo que actualmente dichas circunstancias han cambiado, por el avance de la tecnología; es por ello que el

derecho cambia de acuerdo a los avances que haya en la sociedad, teniéndose en cuenta que dentro de cinco años pueden surge grandes cambios.

En México, Larios y Sánchez (2014) en su tesis titulada “Ciberdelito” para obtener el grado académico de ingeniero en la Universidad Nacional Autónoma de México, en su décima conclusión refiere que:

> “La solución de esta controversia está amparada de acuerdo lo que refiere el internet, por ello deben de existir normas penales que castiguen verazmente a los culpables verdaderos de las conductas delictivas sin que se vulneren derechos humanos, así como la libertad que tiene toda persona de usar las ventajas que proporciona el internet” (p.146).

Lo señalado por dicho tesista es importante para la presente investigación debido a que el internet tiene muchas ventajas de comunicación para las personas, pero también ocasionan un medio para cometerse delitos que en su mayoría es difícil identificar a sus autores, teniendo en cuenta, que se debe hacer uso de la misma tecnología para identificarlos.

En el ámbito nacional, en Lima Cotrina (2018) en su tesis titulada “Los factores principales que impiden la aplicación de la Ley N° 30171 – Lima Norte en el año 2016”, para obtener el título profesional de abogado en la Universidad Cesar Vallejo, en su primera conclusión refiere que:

> “No se ha tenido una adecuada utilización de los delitos informáticos, siendo que no hay elementos necesarios como son las capacitaciones, indumentaria, entes encargados; siendo que no hay una cooperación entre los órganos estatales, quienes tienen contacto directo con dicha prueba; pese a lo señalado por la Ley Especial de Delitos Informáticos en su cuarta disposición complementaria final hace mención que al cumplirse se castigaría por la comisión de estos delitos, por ello al aplicarse los delitos informáticos no pueden

> utilizarse de manera adecuada porque hay ausencia de cooperación y de capacitaciones, siendo necesaria la incorporación del Convenio de Budapest" (p.89).

Cada autoridad encargada debe de amparar a los ciudadanos en cada diligencia que realicen, a fin de que no se vulneren derechos fundamentales o procesales; es por ello que las coordinaciones o cooperaciones que se realicen entre autoridades competentes deben ser suficientemente eficaces puesto que, la contribución de los conocimientos que tengan ambas autoridades se podrá resolver los casos de acuerdo al derecho.

Así mismo en dicho departamento, Pardo (2018), en su tesis titulada "Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018" para obtener el grado académico de bachiller en la Universidad Cesar Vallejo, en su primera conclusión señala:

> "En nuestra normativa existe una deficiencia en la aplicación jurídica del delito informático que atentan contra el patrimonio, siendo que de manera ilógica entiende dentro del delito de fraude informático las modalidades de los delitos informáticos contra el patrimonio, generándose así indecisión jurídica en cuanto a su exégesis ocasionando que no se sancione efectivamente los delitos informáticos" (p.153)

Lo señalado por dicho autor se tiene plena concordancia debido a que, en nuestra normativa existe una deficiencia al no regularse los actuales delitos informáticos que se cometen en nuestra sociedad, ocasionando que se queden impugnes dichos ilícitos.

Por otro lado en la misma región, Chávez (2018), en su tesis titulada: "El delito contra datos y sistemas informáticos en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Lima Norte, 2017", para obtener el

grado académico de doctor, en la Universidad Nacional Federico Villareal, en su primera conclusión refiere:

> “De acuerdo a lo señalado por los operadores del derecho de la muestra escogida para la aplicación del instrumento, aquellos ilícitos que se cometen en contra de los sistemas informáticos y datos informáticos menoscaban de manera significativa el derecho a la intimidad personal, así como el patrimonio del agente” (p.67).

Cuando se realicen actos ilícitos a través de los medios informáticos o tecnológicos, se puede vulneran diversos derechos, entre el derecho al patrimonio, a la intimidad entre otros; teniéndose en cuenta que la tecnología mientras más avanza abarca más aspectos personales de toda persona.

En Ancash, Zorrilla (2018), en su tesis titulada “Inconsistencias y ambigüedades en la ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171, que imposibilitan su eficaz cumplimiento”, para obtener el grado académico de abogado en la Universidad Nacional de Ancash “Santiago Antúnez de Mayolo”, en su primera conclusión refiere:

> “Al analizar críticamente la Ley Especial de Delitos Informáticos, así como su modificatoria a través de la Ley N° 30171, se videncia en dichos artículos que lo conforman, varias imprecisiones en su redacción, ocasionando confusión en los operadores del derecho, puesto que muchos delitos graves no son denunciados, o temen denunciar dichos ilícitos, siendo que ante la falta de imprecisiones es imposible encontrar a los verdaderos culpables ocasionando desanimo en las victimas” (p.105).

Al analizar la ley normativa de los delitos informáticos se puede diferir que existen diversas imprecisiones en diversos artículos, lo que ocasiona que las personas que no tienen conocimiento de la regulación de dichos delitos no denuncien los hechos

delictivos en los cuales son víctimas, así como los operadores del derecho quienes no sabrán aplicar la norma de acuerdo al derecho.

En la ciudad de Huánuco, la tesista Sequeiros (2016), en su tesis denominada: "Vacíos legales que imposibilitan la sanción de los delitos informáticos en el nuevo Código Penal Peruano-2015", para optar por el título profesional de abogado en la Universidad de Huánuco, en la primera conclusión afirma que:

> "Por la naturaleza especial de los delitos informáticos, la cual es virtual en comparación de los otros delitos, que se realizan de manera presencial; se vuelve confusa su tipificación al tener escasos conocimientos tecnológicos, así como las herramientas necesarias de cómo combatir dicha cibercriminalidad y poder manejar dichas situaciones de manera virtual". (p.44)

Se tiene plena concordancia con lo referido por el mencionado autor, siendo que en nuestra normativa existen vacíos legales en la normativa penal, así como las leyes especiales como son la N° 30171 y N° 30096, ocasionándose deficiencias normativas.

Finalmente, en nuestra región Lambayeque, León (2018), en su tesis titulada "Bloqueo del IP dinámico dentro del comercio electrónico como medida de prevención de los delitos informáticos de la Ley 30096", para optar el título profesional de abogado en la Universidad Señor de Sipán, en su segunda conclusión señala:

> "De acuerdo a la investigación realizada se logró identificar en base a los resultados obtenidos que, a través del bloqueo del IP dentro de un soporte informático, se podría prevenir los delitos informáticos al ser una medida de seguridad, es por ello que la muestra estudiada menciona que la propuesta señalada es viable" (p.85).

Se ha buscado diversas formas de evitar la comisión de los delitos informáticos, a fin de que el índice de criminalidad disminuya de manera notable, por ello el bloqueo del IP en cada soporte informático ocasionaría que se tenga seguridad informática a fin de prevenir delitos.

Carrillo y Montenegro (2018), en su tesis titulada “La criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos”, para optar el título profesional de abogado en la Universidad Señor de Sipán, en su segunda conclusión refiere:

> “De acuerdo al avance y uso de la tecnológico ha ocasionado que surjan nuevas y diferentes modalidades delictivas, las que no se encuentran específicamente reguladas en nuestro ordenamiento jurídico penal, ante dicha situación se promulgó en el año 2013 la Ley Especial de Delitos Informáticos, pero no regula de manera específica el delito de atentado contra la integridad de sistemas informáticos, es por ello que es necesario que se modifique el artículo 4 de dicha ley, por lo cual se incorporaría los medios tecnológicos de comunicación e información, así como los medios comisivos de este delito, fin de que se proteja los intereses de cada persona y de sus sistemas informáticos” (p. 108)

Por el avance de la tecnología, han surgido nuevas modalidades de ciberdelitos los cuales en nuestro país se encuentran regulados desde el año 2013, año a partir del cual los cibercrímenes han evolucionado y se han adaptado a las situaciones actuales en que se está afrontando como sociedad.

Delgado (2016) en su tesis titulada “La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú-2015”, para optar el título profesional de abogado en la Universidad Señor de Sipán, en su segunda conclusión señala:

> “En un mundo globalizado en el que surge nuevas tecnologías se presentan constantes y nuevos beneficios para la persona humana,

> pero también trae consigo desventajas puesto que han surgido nuevas modalidades delictivas, por ello es necesario que en la legislación se prevea de dichos aspectos para que ante los nuevos problemas que surjan se puedan combatir de manera factible" (p.117).

Conforme al avance de la tecnología produce que las autoridades adopten las medidas preventivas a dicho avance, a veces están complicado de conocer de donde provienen dichas páginas web en los que se producen los actos delictivos, por ello es necesario que existan nuevas tipificaciones en relación a los avances tecnológicos.

Amoros (2015) en su tesis titulada: "Incidencias sobre el delito de Grooming en adolecentes: Caso región Lambayeque", para optar el título profesional de abogado en la Universidad Señor de Sipán, en su tercera conclusión señala que:

> "Ante el incumplimiento a la ley especial de los delios informáticos que atentan contra la intimidad y la libertad sexual han sido menoscabados a los adolescentes de nuestro departamento de Lambayeque, así se tiene que los operadores del derecho no tienen conocimiento de los conceptos básicos de la norma, es por ello que es necesario que se tenga en cuenta lo especificado en las legislaciones comparadas, en las cuales se estipulan dichos ilícitos acorde a nuestra realidad, sancionándose así a los autores del delito". (p.129)

La falta de la regulación expresa de ciertas modalidades del cibercrímen ocasiona que los operadores del derecho no puedan conocer de manera adecuada la aplicación e interpretación de los delitos informáticos estipulados en la ley especial, ocasionando que dichas conductas delictivas queden impugnes.

Luego de haber expuesto los trabajos previos, seguidamente se señalará cada teoría relaciona al tema, en el primer punto se señaló lo referente a los cibercrímenes, exponiéndose su evolución histórica la cual se ha evidenciado a los fines del año setenta en el siglo XX, fecha en que surgieron los cibercrímenes y delitos informáticos, los cuales se evidenciaron con transferencias no consentidas, daños informáticos; lo cual ha contribuido a que las nociones y categorías dogmáticas tradicionales se deban de cambiar por los factores políticos – criminales; lo cual permitirá enfrentar a lo que es considerado como paradigma delictivo; puesto que son actos delictivos que colocan en riesgo la confiabilidad, disponibilidad de datos, entre otros (Posada, 2015).

Dichos delitos tienen como lugar de comisión los sitios web o ciberespacios, al existir una realidad simulada dentro de las redes digitales y computadoras; si bien es cierto existe un favorecimiento a la gestión mundial sobre ámbitos políticos, económicos y sociales, fortaleciendo riesgos delictivos que se producen en un ámbito digital.

Por otro lado, sobre su definición, se podría mencionar que el cibercrímen es, aquel comportamiento idóneo de destrozar computadoras, medios electrónicos, redes de internet, así mismo es señalado como un comportamiento doloso que es ejecutada a través de vías informáticas (Salazar 2015). En ese mismo sentido Acosta (2016) señala que el cibercrímen presenta un concepto aceptado como la capacidad de acceder a datos primordiales como son los datos personales que son importantes para las empresas y gobiernos; para que sea utilizado en agravio del agente pasivo.

Así mismo, la mayoría de la sociedad relaciona al cibercrímen con los delitos tecnológicos, esto es que, con el uso de la tecnología se cometen crímenes; lo cual es erróneo pues actualmente es amplio dicho concepto, debido a que hay varios tipos de delitos que se cometen con el uso de la tecnología sin que se dística un crimen en específico.

Así mismo Posada (2015) refiere que los doctrinarios con conocimiento en la materia refieren que los delitos informáticos de manera estricta castiga aquellos

comportamientos que ponen en riesgo ilícitamente la seguridad de las funciones informáticas, no obstante también puede colocar en riesgo otros bienes jurídicos protegidos, puesto que no son delitos comunes, puesto que son especiales al ser cometidos por medios informáticos, cuyo contexto virtual, lo deslocalizan en el ciberespacio y la afectación de objetos inmateriales rompen los paradigmas probatorios propios de los delitos comunes.

Tllez (2016), argumenta que son conductas ilícitas, cometidos a través de los equipos informáticos como instrumentos a fines para cometer sus conductas ilícitas, es decir, los computadores son utilizadas como mecanismos auxiliares de apoyo a las diversas conductas humanas, con el objetivo de conseguir información importante, que contribuye a la comisión de dichos ilícitos.

Seguidamente como tercer punto, se expondrá sobre las modalidades del cibercrímen, el cual puede ser de acuerdo a lo señala Morales (2014) de la siguiente manera:

> a) Intrusismo Informático: Comprende aquellos actos ilícitos que atienden al modo operativo que se realiza y puede consistir en el apoderamiento indebido, sea apropiándose de la información, usar dicha información para fines ilícitos, conocimiento indebido de la información, interceptando o accediendo a tratamientos de datos.
>
> b) Sabotaje informático: es la acción de borrar, modificar, o suprimir sin permiso aquellos datos o funciones del sistema informático con el dolo de obstaculizarse el funcionamiento del sistema, teniéndose en cuenta que dichas conductas delictivas se han focalizado al objeto que se atenta con las acciones delictivas, el funcionamiento del sistema informáticos, obteniendo datos del sistema de tratamiento de información, dichos actos son realizados por medo de la inutilización, destrucción o modificación.
>
> c) Phishing: Este delito se da por la suplantación de identidad, se trata de adquirir datos confidenciales de manera fraudulenta, los cuales están

relacionados a contraseñas de cuentas bancarias, tarjetas de crédito, es una trampa que es compartida por correos electrónicos, mensajes de texto o a través de redes sociales; todo ello se realiza a fin de obtener información.

d) Skimming: Es el robo de información de tarjetas de crédito, es realizado a través de cajeros automáticos, bares, y restaurantes; siendo que se copia la banda magnética de las tarjetas de crédito, para poder clonarlas y vaciar las cuentas bancarias.

e) Carta Nigeriana: Es realizada por correo electrónico, a través de la cual generan una carta en la que ofrece fortuna que no existe a cambio de que la víctima pague un dinero adelantado.

f) Estafa cibernética: Se realiza a través de un enlace de una página en la cual pide datos personales a fin de hacker el dispositivo, para obtener algún beneficio.

g) Malware: Este es realizado a través de un link, en el cual se le reporta a la víctima alguna cobranza o investigación para que pueda acceder a dicho link, lo que hace que descargue automáticamente un virus, el cual daña los ordenadores informáticos, así como robar información.

h) Smishing: Es realizado a través de mensajes de texto al celular o también a través de llamadas, las cuales intentan suplantar a alguna persona, a fin de que acceda a un link en el cual supuestamente reclamaría un premio, pero a cambio el sujeto activo le solicita dinero.

i) Ramsomware: Es un software malicioso que afecta las computadoras, mostrando mensajes de restablecimiento del funcionamiento del sistema, pero antes se debe de realizar un pago de dinero; este virus tiene la capacidad de bloquear la pantalla de las computadoras.

Actualmente las relaciones del cibercrímen que más se utiliza es aquella que posee el Convenio sobre la Ciberdelincuencia del Consejo de Europa firmado por Budapest en Hungría en el año 2001; el cual define a dichas conductas en cuatro tipos de delitos: a) delitos contra la confidencialidad, disponibilidad e integridad de los datos y sistemas informáticos; b) delitos informáticos propiamente dichos; c) delitos con contenidos ilícitos; y d) infracciones al derecho de autor.

En la legislación extranjera en el país de Argentina, en junio del 2008 se reguló la ley de delitos informáticos – Ley 26388, a través del cual se incorporó modificaciones en su Código Penal, es decir dichos delitos se encuentra establecidos en el mismo cuerpo normativo, no estando separado en una ley especial como sucede en nuestro país.

En Chile a través de la Ley N° 19 223 (regulada en el año 1993), la cual es una ley "Relativa a Delitos Informáticos" de acuerdo a su propio título, en el que se estipula cuatro artículos, en los cuáles se tipifican varios delitos informáticos.

En Colombia, el país con mayor énfasis en los delitos informáticos a través de la Ley 1.273 (regulada en el año 2009), realiza modificaciones en el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos". Siendo que se está en la búsqueda de preservar en dicha norma aquellos sistemas que usen tecnologías de comunicación e información. A partir de dicha norma se protegió un bien titular estableciéndose conductas delictivas que están concomitantes a la tecnología de acuerdo a los medios informáticos, siendo este país el primero a nivel global legalizar estos tipos de delitos. En dicho país se castigan dichos ilícitos con penas de 48 y 12 meses, así como el pago de días multa.

Es menester precisar en el presente capitulo lo referido al Convenio de Budapest o el denominado "Convenio de Ciberdelincuencia", el cual es un tratado internacional generado por naciones que conforman el Consejo Europeo, con el objetivo de combatir el fenómeno del cibercrímen, presentando herramientas de homologación de normas del derecho penal; nuestro país, en el 2014 solicitó su inscripción, es así

que en el año siguiente aprobó dicho pedido. Seguidamente el Poder Legislativo en el 2019 aproó el Convenio de Budapest, a través de la Resolución Legislativa N° 30913, ratificado por el Poder Ejecutivo con fecha 09 de marzo del 2019, estableciéndose en diciembre del mismo año se reguló su entrada en vigencia.

Como segundo capítulo definiremos lo que es el delito informático, el cual es señalado como aquel hecho delictivo que es relevante jurídicamente al cometerse a través de la tecnología, es decir es una herramienta de comisión de delitos; esto quiere decir que la criminalidad informática es aquella conducta dirigida a burlarse de los sistemas de dispositivos informáticos; ante ello es necesario que el sujeto activo debe emplear o usar dispositivo informático (Villavicencio, 2014).

Así mismo Temperini (2014) refiere que este tipo de delito es un acto antijurídico ocasionado a través de los medios informáticos, pretendiendo manipular computadoras, medios electrónicos; por ello implica actividades criminales que la mayoría de países han querido regular dichas figuras típicas, pero es un reto debido a que el uso de las técnicas informáticas provoca que se realicen nuevas modalidades de uso indebido de las computadoras. En esa misma línea, Besares (2015) argumenta que este tipo de delito es una conducta licita y culpable que menoscaba la certeza informática, así como el derecho a tener una intimidad, es por ello que los delincuentes de manera dolosa tratan esa información, es así que se distingue de los demás delitos electrónicos o computacionales.

También es menester precisar sus principales características, el cual según Delgado (2016) pueden ser las siguientes:

a) Es de carácter internacional, siendo que para su comisión no es necesario que haya cercanía entre los sujetos, activo y pasivo para que se realice dicha conducta delictiva.
b) El alcance de la justicia en estos actos delictivos es reducida, siendo que las denuncias son escasas, al igual que su regulación normativa, puesto que la mayoría de países no han regulado dichas conductas.

c) Su comisión es dolosa e intencional, pero puede cometerse de manera culposa.

d) Se concretiza en un diminuto tiempo y espacio, puesto dichas conductas se concretizan en cuestión de segundos, al no requerirse grandes aparatos informáticos, siendo que se puede realizar desde un celular.

e) Se trata de conductas ocupacionales, siendo que el sujeto pasivo labora con el uso de medios informáticos, ante dicha situación los delincuentes sacan provecho de ello para cometer sus ilícitos.

f) La investigación que se realiza a dichos ilícitos son complejos, puesto que es necesario que grandes especialistas puedan corroborar e investigar dichas conductas, teniéndose en cuenta que se realizan a través de medios electrónicos.

g) Son delitos especiales, puesto que son cometidos a través de ilícitos ya estipulados como estafa, hurto, fraude entre otros, pero se realizan a través de medios informáticos, por lo cual es necesaria su regulación especializada.

Luego de haber señalado sus características, a continuación mencionaremos su regulación en nuestro país, el delito informático de manera general se encontraba tipificado en el artículo 186 inciso 3 en el párrafo segundo del Código Penal de 1991; el cual no era regulado como delito autónomo, sino como agravante del delito de hurto; seguidamente en dicho Código Penal en el capítulo X se reguló los delitos informáticos, estipulándose los artículos 207- A (delito informático, ingreso y uso de datos, red o sistema); 207 - B (daño, alteración o destrucción de base de datos),articulo 207 -C (circunstancias agravantes), 207 – D (tráfico ilegal de datos).

Ante la aprobación de dicha ley especial, los artículos antes mencionados, se derogaron en el año 2013, fecha en que entra en regulación la Ley Especial de Delitos Informático – Ley N° 30096, la cual está conformado por siete capítulos, el primero establece la finalidad y objeto de la ley, el segundo capítulo hace mención

de los delitos contra datos y sistemas informáticos, en el tercer capítulo sobre delitos contra la indemnidad y libertad sexual, seguidamente se regla los delitos informáticos contra la intimidad y el secreto de las comunicaciones, así mismo sobre los delitos informáticos contra el patrimonio, en el capítulo penúltimo hace mención sobre los delitos informáticos contra la fe pública y finalmente sobre las disposiciones comunes.

Posteriormente, se ha promulgado la Ley N° 30171, la cual modifica la Ley Especial de Delitos Informáticos, la cual fue regulada para adecuarla a los estándares legales del convenio sobre la cibercriminalidad (Convenio de Budapest).

A continuación, se expondrá sobre la tipicidad objetiva, señalando en primer lugar la conducta típica de los delitos contra el patrimonio, esta es dada por la vulneración de la seguridad de los sistemas informáticos para que se realice un provecho indebido, el cual es realizada por la sustracción de valores, datos, bienes; así mismo sea hace uso de las tecnologías informáticas para que se pueda inducir en error a las personas.

En cuanto al sujeto activo, varios doctrinarios la denominan delitos de cuello blanco, por ser de característica especial que el sujeto activo posee, al tener un conocimiento avanzado de las tecnologías informáticas, puesto que cualquier persona no puede cometer dichos ilícitos siendo que debe tener conocimiento suficiente de cómo funcionan los sistemas informáticos. Por otro lado, sobre el sujeto pasivo, puede ser cualquier individuo, órgano estatal, instituciones crediticias, que utilicen sistemas automatizados de información, que están conectados a sistemas computarizados.

Sobre la tipicidad subjetiva, por su propia naturaleza y el nivel de conocimiento que debe tener el sujeto activo, son netamente dolosos, pero no es óbice para que no se concrete por descuido o culpa quien sin tener intención para cometer dicho ilícito vulnera el bien jurídico protegido.

En relación a su bien jurídico, Villavicencio (2014) señala que en este tipo de delito es concebido en dos planos, el primero está relacionado a la información la cual es transmitida mediante los sistemas de tratamiento automatizado de datos; en relación al segundo plano los bienes afectados por la comisión de este delito es la indemnidad, intimidad, sexual entre otros; dichos bienes tienen un importante valor económico por la información que se obtiene. Pero dicho bien jurídico no es el único, pues hay un conjunto de bienes que se afectan, teniendo en cuenta la conducta típica de acuerdo a la modalidad delictiva.

Puede suceder el hecho de que a una persona se le extraiga información importante contenida en su nube, a través de la cual le sustraen su patrimonio, por lo que se podría decir que son varios delitos que se menoscaban.

A continuación, se expondrá sobre el fraude informático, el cual es señalado como aquel acceso indebido a datos, bienes inmateriales y materiales con valor económico, ocasionando burla a las medidas de seguridad, redes o medios informáticos, con el objetivo de aprovecharse indebidamente del acto fraudulento. De lo que se puede diferir, que el fraude informático es aquella mentira que se produce a las medidas de seguridad de los datos informáticos para que se obtenga un provecho ilícito, es por ello, que este delito afecta la seguridad de los medios informáticos, mientras que el delito de estafa afecta a la propia persona en si (Chávez, 2018).

Así mismo Montañez (2017) menciona que el fraude informático es aquel menoscabo patrimonial, ocasionado por el perjuicio a los medios informáticos a través de la manipulación de los datos que se obtienen de ellos mismo, es así que se interfiere el correcto funcionamiento del sistema informático, con el objetivo ilegal de obtener un beneficio patrimonial ya sea para el propio sujeto activo o para una tercera persona.

De acuerdo al artículo 8 del Convenio de Budapest sanciona las conductas delictivas ilegitimas y deliberadas que causan menoscabo patrimonial a una persona, sea por medio de la introducción, alteración, supresión o borrado de datos

informáticos; además se puede interferir en el adecuado funcionamiento del sistema informático, en el que el sujeto activo de manera dolosa interviene para obtener de manera ilegítima un provecho económico.

En cuanto a los tipos de fraude informático que se encuentran establecidos en nuestra normativa se encuentran especificados de acuerdo al avance de la tecnología de información y las comunicaciones (TIC) así como el crecimiento de las operaciones comerciales que se realizan en internet han ocasionado que surjan nuevas conductas fraudulentas que están relacionados al uso de instrumento de pago electrónico, así se tiene que por emplearse las tarjetas de crédito ocasiona que se realicen conductas ilícitas siendo en el interior o fura del internet, empleándose la informática para que se clone o se falsifique; teniéndose en cuenta que los mecanismos de pago en su mayoría son las tarjetas sean a través de las transferencias electrónicas.

Otro tipo de delito que se ocasiona a través de la tarjeta de crédito es la clonación, la cual es mencionada como skimming, siendo una tipificación de fraude, a través del cual se duplica la tarjeta de crédito a fin de que se realice transacciones como retiros sin la autorización previa del titular; así mismo se pueden cometer en cajeros automáticos y en tiendas comerciales, este se realiza a través del dispositivo denominado skimmer el que permite leer la banda magnética con solo deslizar la ranura.

Este delito puede ser de dos tipos, el fraude al sistema, el cual hace referencia que el sujeto activo miente a las medidas de seguridad, puesto que comete esta conducta dolosa utilizando su conocimiento en la tecnología para que las medidas de seguridad no sean suficientes para que se impida la ciberdelincuencia. La manera de actuar del delincuente es romper aquellas barreras del sistema a fin de aprovecharse ilegítimamente de manera económica, es por ello, que el delincuente puede cometer un concurso de delitos, donde se mofa de las medidas de seguridad del sistema informático, para acceder de manera ilegítima al patrimonio digital.

Como segundo tipo, se tiene al fraude en los datos, el cual el delincuente informático altera los datos de los sistemas informáticos con el objetivo de obtener un beneficio patrimonial, esto es que accede a una plataforma virtual, en la que el sujeto activo puede burlar las medidas de seguridad para varias su contenido y así beneficiarse.

Seguidamente se expondrá sobre la tipicidad objetiva, en relación la acción al tipo penal este sanciona diversas conductas; la primera es señalada como diseña siendo un proyecto o plan; introducir (ingresar a un lugar), borrar (quitar, desvanecer), suprimir (hacer desaparecer), alterar (lo cual es dañar, estropear, descomponer), clonar datos informáticos o manipular (operar con las manos o con cualquier instrumento), por ello al funcionar un sistema informático se procura una ventaja para sí o para un tercero perjudicando así al sujeto activo; es un delito de resultado siendo que no solo es suficiente que se cumpla con la acción penal, siendo necesario que se consiga un resultado esperado sino quedaría en tentativa.

En relación al bien jurídico protegido, de acuerdo a lo establecido en la propia norma es el delito contra el patrimonio económico, si bien la doctrina hace mención al delito de carácter pluriofensivo siendo que atentan el orden económico, la libertad e intimidad persona, el sistema informático entre otros. Este bien jurídico es concebido como el derecho a que se persevere el patrimonio económico que es sustento del sujeto pasivo, el cual comprende el conjunto de bienes sean materiales e inmateriales, que tienen una valoración económica.

En cuanto al sujeto activo, este es genérico pues no es necesario que tenga una cualidad específica, de la misma manera el sujeto pasivo es también genérico, siendo que puede ser cualquier persona; sobre su materialidad el agente debe hacer uso de la tecnología de la información para que procure un beneficio ilícito en menoscabo de un tercero mediante la acción de cada verbo rector.

Sobre la tipicidad subjetiva, es de tipo doloso se excluye la culpa, además la propia norma presupone como condición de punibilidad el comportamiento egoísta de procurar para su o para otro un provecho ilícito, exigiéndose el animus lucrandi.

Como cuarto punto se tiene, lo relacionado a las modalidades delictivas, Rodríguez (2016) menciona que es una circunstancia, es un hecho concreto, que el legislador toma en cuenta para que se gradué la responsabilidad penal, el cual está conformado por un vínculo preexistente de la conducta delictiva, generando cualquier antecedente que trate de traducir los fines de la responsabilidad penal; de lo que se puede diferir que, cada circunstancia modificatoria es una situación de carácter personal, así como un hecho material, además este elemento conformado por una circunstancia modificatoria, poseyendo un amplio sentido, siendo que debe estar expreso por mandato constitucional el cual está circunscrito al comportamiento humano.

De la misma manera Temperini (2014) argumenta que una circunstancia modificatoria, el aquel hecho, situación o dato, que es ajeno a la organización del tipo, en que la norma legal reviste a la pena en un caso en concreto; así mismo refiere que una circunstancia está definida por tres rasgos fundamentales: ser extraordinaria, accesoria o secundaria y ser accidental.

En relación de los efectos de estos hechos, algunos señalan que tiene el efecto propio de atenuar la punibilidad del hecho, otros refieren que consiste en disminuir o aumentar la gravedad de la infracción. Villavicencio (2014) argumenta que una circunstancia lo que realmente altera es la responsabilidad del autor, pero dicha modificación opera de manera indirecta, puesto que una persona puede estar sujeta a más de una responsabilidad, puesto que sobre ellas se colocan los efectos de cada circunstancia modificatoria.

Por otro lado, sobre su clasificación, esta puede ser clasificada por sus efectos: circunstancias agravantes, atenuantes y mixtas, de acuerdo a como aumenten o disminuyan la reacción sancionatoria; en cuanto a su clasificación puede distinguirse en: circunstancias modificatorias generales, las cuales se aplican a todos los delitos, a excepción que exista causal de incompatibilidad; y las circunstancias especiales, las cuales son contempladas por el legislador a ciertos delitos.

Finalmente, de expondrá sobre los términos comúnmente utilizados en la presente investigación:

Cibercrímen: es aquel ilícito que es cometido a través de medios informáticos, redes de internet, las cuales son realizadas de manera dolosa a través de los medios informáticos.

Delito informático: es un hecho delictivo que es relevante jurídicamente al cometerse a través de la tecnología.

Delito: son actos culposas o dolosas penados por la ley.

Fraude informático: es aquel perjuicio patrimonial que ocasiona el sujeto pasivo a través de los medios de la manipulación de datos informáticos.

Modalidad delictiva: se señala como un hecho concreto en el cual, el legislador la señala en la normativa penal a fin de gradúe la pena.

Proceso Penal: es el conjunto de etapas que se desarrolla desde las diligencias preliminares hasta la etapa de juzgamiento, en que se dictamina la culpabilidad o inocencia del investigado.

III. MÉTODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo de investigación

En esta investigación se ha utilizado el enfoque cuantitativo siendo que se busca utilizar la estadística en la población y muestra estudiada, con el objetivo de corroborar la hipótesis planteada, así como los resultados obtenidos; terminada la presente investigación se concluirá que se regularice las nuevas modalidades delictivas del delito de fraude informático.

Diseño de investigación

Así mismo como tipo de investigación utilizado ha sido descriptiva experimental, puesto que se buscó explicar la realidad problemática que aqueja nuestro ámbito jurídico, tal como es la falta de regulación de las nuevas modalidades delictivas del delito de fraude informático en la ley especial.

3.2. OPERACIONALIZACIÓN DE LAS VARIABLES

Variable independiente: Cibercrímenes

Definición conceptual: Miró (2013) argumenta que: "La cibercriminalidad puede ser entendida en sentido amplio, comprendiendo cualquier conducta ilícita que se comete en un medio informático o por las computadoras" (p.12).

Definición Operacional: Son acciones delictivas que cometen a través de la tecnología, utilizando el sistema informático para perjudicar a las personas.

Dimensiones: Doctrina, Normas legales, operadores del derecho.

Indicadores: Extranjera, Nacional, Código Penal.

Escala de Medición: Nominal.

Variable independiente: Circunstancias de hecho

Definición conceptual: Una circunstancia es una relación o datos en concreto, que el propio magistrado toma en cuenta al momento de graduar la responsabilidad penal de la conducta (Cerezo, 2019)

Definición Operacional: Son hechos que deben estar estipulados expresamente en la ley a fin de que la pena pueda ser graduada.

Dimensiones: Doctrina, Normas legales, operadores del derecho.

Indicadores: Nacional, Extranjera, Código Penal.

Escala de Medición: Nominal

Variable dependiente: Fraude informático

Definición conceptual: El fraude informático es el acto antijurídico de carácter culpable, que se realiza por medios informáticos a fin de manipular las computadoras o dañarlas, a fin de perjudicar económicamente a sus víctimas" (p. 57)

Definición Operacional: Este tipo de delitos es cometido con el objetivo de menoscabar el patrimonio de su víctima, obteniendo un provecho ilícito.

Dimensiones: Doctrina, Normas legales, operadores del derecho

Indicadores: Nacional, Extranjera, Código Penal.

Escala de Medición: Nominal

3.3. Población, muestra y muestreo

Población

Esta investigación se encontró conformado por: 10 Jueces Penales Unipersonales, 9 Jueces Penales, 45 fiscales de la primera, segunda, tercera y cuarta fiscalía penal provincial del departamento de Lambayeque, 8794 abogados penalistas del Ilustre Colegio de Abogados de Lambayeque.

Criterios de inclusión: Magistrados, abogados que tengan conocimiento en Derecho Penal, así mismo que realicen actividades relacionadas a dicha rama.

Criterios de exclusión: Personas que no tengan conocimiento en la cibercriminalidad y delitos informáticos.

Muestra

Se ha tenido en cuenta la siguiente muestra:

a) 05 jueces penales de la Corte Superior de Justicia de Lambayeque sede Lambayeque.

b) 05 fiscales Penal del Ministerio Público sede Chiclayo.

c) 60 abogados penalistas del Ilustre Colegio de Abogados de Lambayeque.

Muestreo

En la presente investigación se utilizó el muestreo no probabilístico selectivo por conveniencia, siendo que no se han utilizado fórmulas para emplearse criterios de exclusión e inclusión para que se determine la muestra que se estudiará.

Unidad de análisis

Abogados especialistas en Derecho Penal, y Jueces especializados en delitos informáticos.

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

Por otro lado, en esta investigación se utilizó como técnica la encuesta y como instrumento el cuestionario; en cuanto a la validez del instrumento este ha sido verificado en su totalidad por el asesor temático, quien es especialista en el tema de estudio. Y, por último, de acuerdo a la confiabilidad se obtuvo un porcentaje de 0.767 del grado de confiabilidad.

3.5. Procedimiento de datos

Para recopilar los datos obtenidos fue necesario realizarlo de manera virtual y directa por parte de los investigadores debido al actual coyuntura que se está afrontando, pero ello no será óbice para que no se aplique cada una de las encuestas a los conocedores del derecho penal, siendo estos fiscales, abogados y jueces, quienes a partir de sus conocimientos podrán contribuir al desarrollo de la presente investigación.

3.6 Métodos de análisis de datos

En la presente investigación se realizó el método deductivo debido a que se observa el problema de investigación el cual se encuentra evidenciado con la realidad, esto es que no se encuentra regulado de manera expresa la prueba digital como prueba autónoma en nuestro Código Procesal Penal.

3.7. Aspectos éticos

En relación a la presente investigación se declara bajo honestidad que el presente es original, siendo que es de propia autoría, además se ha tenido en cuenta las normas internacionales de referencias y citas; así mimo en la presente investigación no se afecta los derechos de los terceros, no se ha publicado ninguna tesis similar para obtener el grado académico o título procesional por ello se ha utilizado el programa de turnitin para que exista una adecuada confiabilidad en relación a su valides.

IV. RESULTADOS

4.1 Tabla 1

Condición de los encuestados

Profesional	Jueces	Fiscales	Abogados	Total
Cantidad	5	5	60	70
Porcentaje (%)	7	7	86	100.00

Fuente: Investigación propia

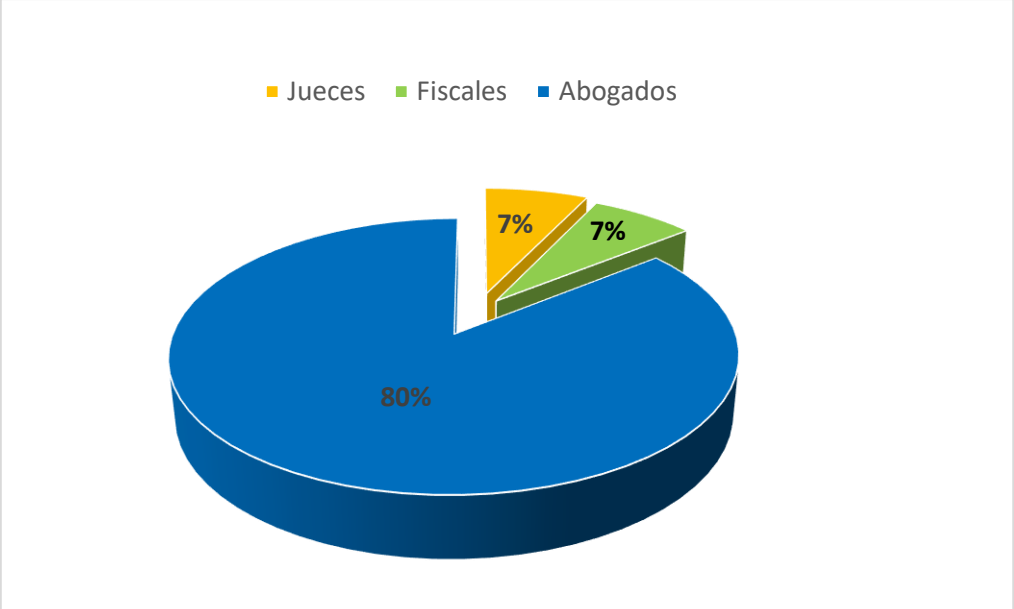


Figura 1: Investigación propia

En la tabla 1 y figura 1, se aprecia la condición de los encuestados donde se muestra que el 7% son jueces, 7% son fiscales y el 86% abogados.

4.2 Tabla 2.

¿Cree usted que, para facilitar la imputación de los delios informáticos, es necesaria la regulación de las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático?

Respuesta	Jueces		Abogados		Fiscales		Total Condición	
	n	%	n	%	n	%		%
Si	5	100	60	100	5	100	70	100
No	0	0	0	0	0	0	0	0
Total	5	100	60	100	5	100	70	100

Fuente: Elaboración propia

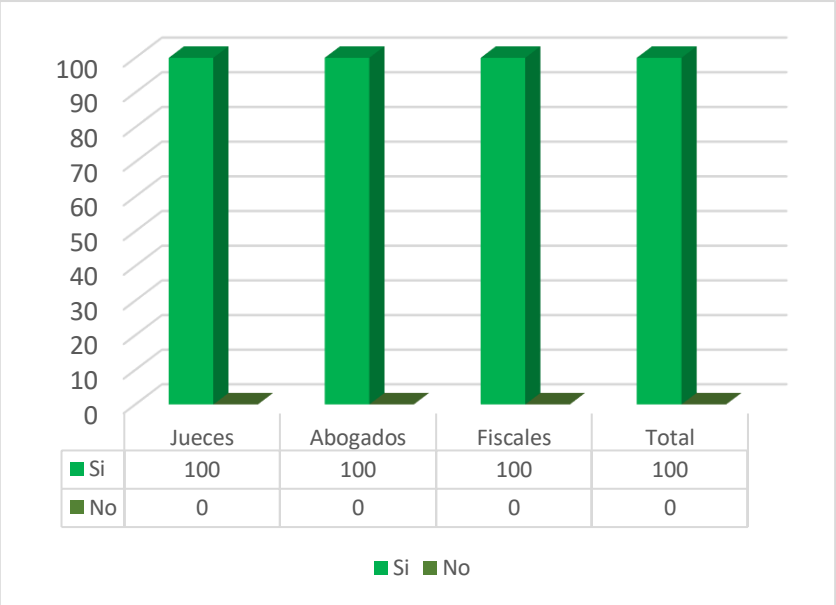


Figura 2: Elaboración propia

De acuerdo a la tabla y figura 2, se observa que 100% de jueces, abogados y fiscales refirieron que, para facilitar la imputación de los delios informáticos, es necesaria la regulación de las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático.

4.3 Tabla 3.

¿Considera usted que la incorporación de las actuales modalidades delictivas en el delito de fraude informático se ampararía aquellas situaciones que no están establecidas en la ley especial?

Respuesta	Jueces		Abogados		Fiscales		Total Condición	
	n	%	n	%	n	%	%	
Si	5	100	60	100	5	100	70	100
No	0	0	0	0	0	0	0	0
Total	5	100	60	100	5	100	70	100

Fuente: Elaboración propia

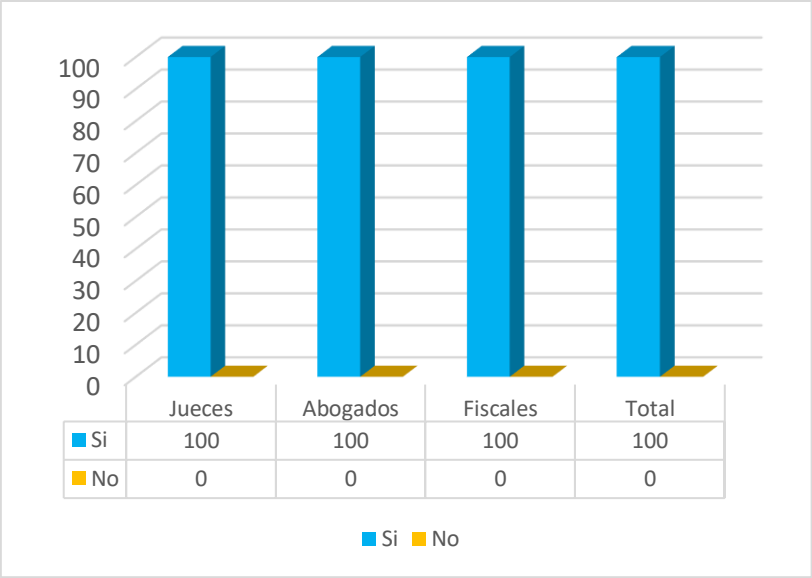


Figura 3: Elaboración propia

En la tabla y figura 3, se muestra que 100% de jueces, abogados y fiscales consideran por unanimidad que la incorporación de las actuales modalidades delictivas en el delito de fraude informático se ampararía aquellas situaciones que no están establecidas en la ley especial.

4.4 Tabla 4.

¿Conoce usted cuales son los cibercrímenes cometidos comúnmente en nuestro país?

Respuesta	Jueces		Abogados		Fiscales		Total Condición	
	n	%	n	%	n	%	%	
Si	2	40	16	32	1	20	19	32
No	3	60	34	68	4	40	41	68
Total	5	100	50	100	5	60	60	100

Fuente: Elaboración propia.

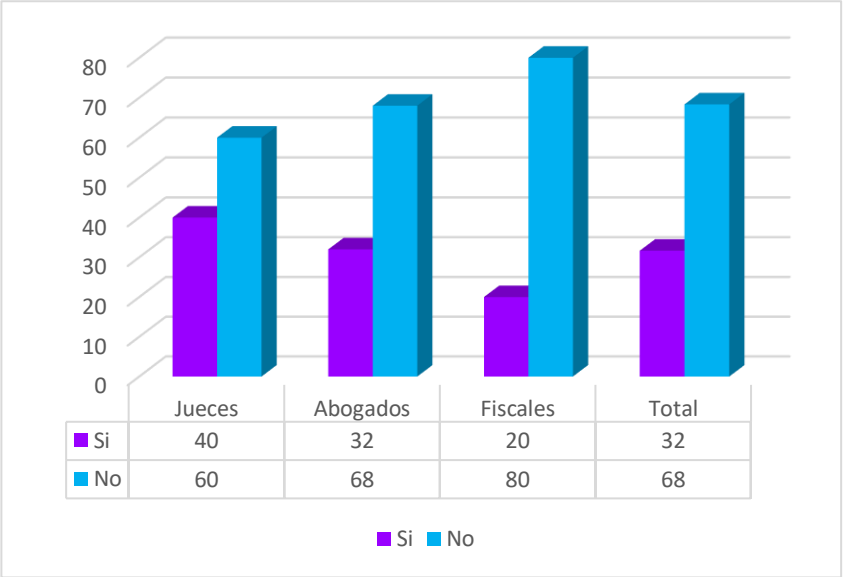


Figura 4: Elaboración propia

De acuerdo a la tabla y figura 4, se observa que 60% de jueces, 68% de abogados y 80% de fiscales refirieron no conocer cuáles son los cibercrímenes cometidos comúnmente en nuestro país. En definitiva, 68%, argumentaron desconocer los cibercrímenes cometidos comúnmente en nuestro país, mientras que 32% expusieron lo contrario.

4.5 Tabla 5.

¿Conoce usted si en nuestra normativa penal se encuentran sancionados dichos cibercrímenes?

Respuesta	Jueces		Abogados		Fiscales		Total Condición	
	n	%	n	%	n	%		%
Si	1	20	15	25	2	40	18	26
No	4	80	45	75	3	30	52	74
Total	5	100	60	100	5	70	70	100

Fuente: Elaboración propia.

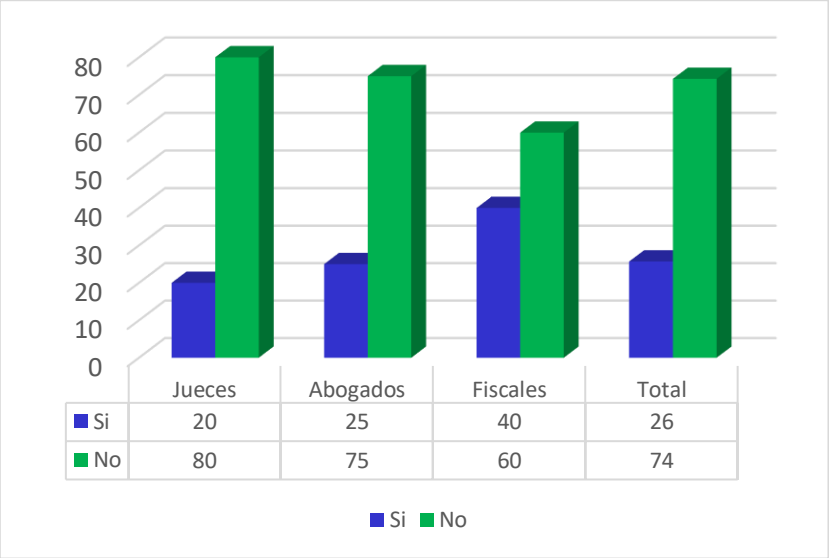


Figura 5: Elaboración propia.

En la tabla y figura 5, se aprecia que 80% de jueces, 75% de abogados y 60% de fiscales refirieron no conocer si en nuestra normativa penal se encuentran sancionados dichos cibercrímenes. Ante lo cual se concluye que, de los encuestados un 74% refirieron no conocer la regulación de los cibercrímenes en nuestra normativa penal, pero 26% argumentaron conocerlo.

4.6 Tabla 6.

¿Conoce usted la regulación de los cibercrímenes en la legislación extranjera?

Respuesta	Jueces		Abogados		Fiscales		Total Condición	
	n	%	n	%	n	%		%
Si	4	80	47	78	4	80	55	79
No	1	20	13	22	1	10	15	21
Total	5	100	60	100	5	90	70	100

Fuente: Elaboración propia.

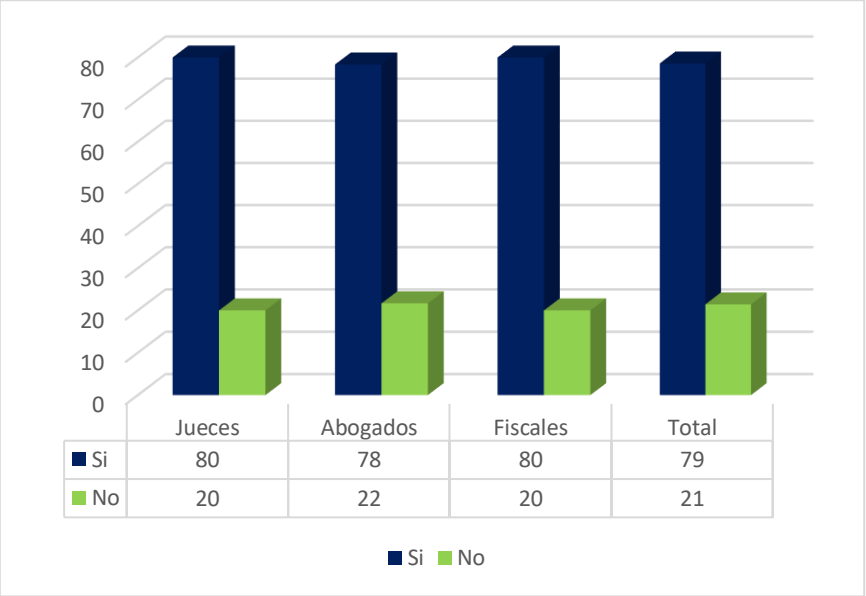


Figura 6: Elaboración propia**.**

En la tabla y figura 6, se aprecia que 80% de jueces y fiscales así como el 78% de abogados refirieron conocer la regulación de los cibercrímenes en la legislación extranjera. Ante lo cual se concluye que, de los encuestados un 79% tienen conocimiento de la regulación de los cibercrímenes en la legislación extranjera, pero 21% señalaron su desconocimiento.

4.7 Tabla 7.

¿Conoce usted en que consiste el delito de fraude informático regulado en la ley especial?

Respuesta	Jueces		Abogados		Fiscales		Total Condición	
	n	%	n	%	n	%	%	
Si	4	80	50	83	4	80	58	83
No	1	20	10	17	1	10	12	17
Total	5	100	60	100	5	90	70	100

Fuente: Elaboración propia.

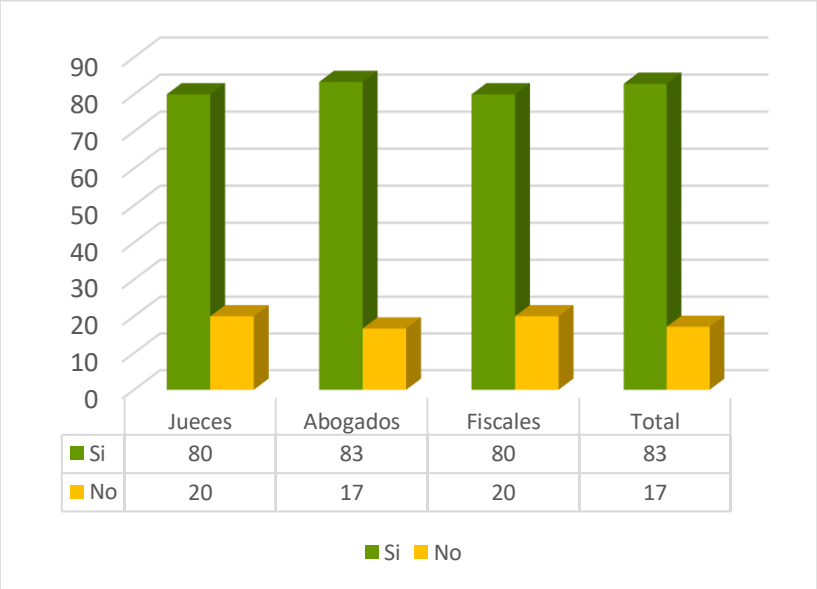


Figura 7: Elaboración propia**.**

En la tabla y figura 7, se aprecia que 80% de jueces y fiscales, así como el 83% de abogados señalaron conocer en que consiste el delito de fraude informático regulado en la ley especial. En definitiva, 83% argumentaron conocer el delito de fraude informático, mientras que 17% expusieron todo lo contrario.

4.8 Tabla 8.

¿Conoce usted si en la legislación comparada se encuentra regulado el delito de fraude informático?

Respuesta	Jueces		Abogados		Fiscales		Total Condición	
	n	%	n	%	n	%		%
Si	4	80	43	72	3	60	50	71
No	1	20	17	28	2	20	20	29
Total	5	100	60	100	5	80	70	100

Fuente: Elaboración propia.

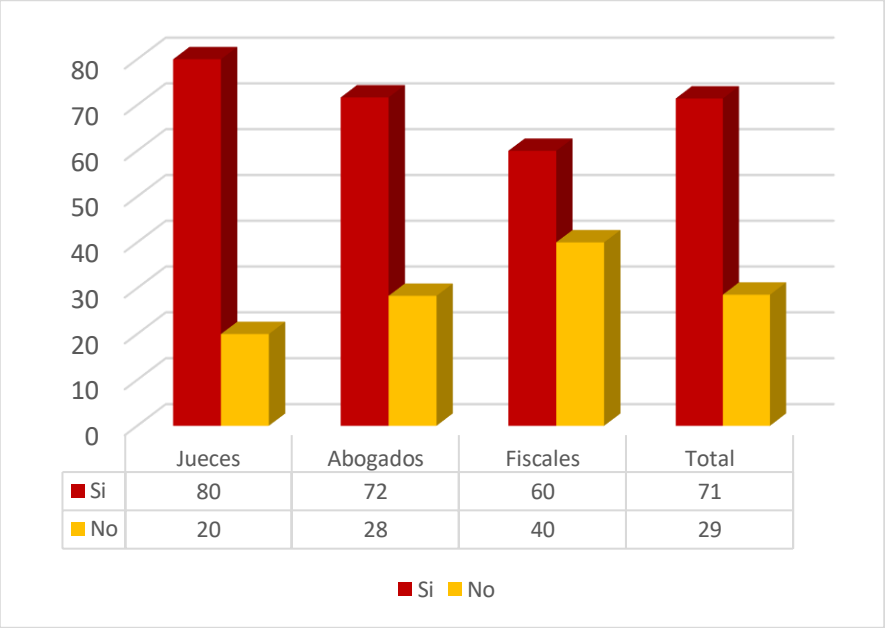


Figura 8: Elaboración propia**.**

De acuerdo a la tabla y figura 8, se observa que 80% de jueces, 72% de abogados y 60% de fiscales señalaron en conocer si en la legislación comparada se encuentra regulado el delito de fraude informático. Por lo que se puede diferir que, los encuestados en un 71% señalaron conocer la regulación del delito de fraude informático en la legislación comparada, pero 29% mencionaron no conocerla.

4.9 Tabla 9:

¿Cree usted, que es necesario incorporar el artículo 8 – A en la Ley Especial de Delitos Informáticos, las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático?

Respuesta	Jueces		Abogados		Fiscales		Total Condición	
	n	%	n	%	n	%	%	
Si	4	100	52	87	5	100	61	88
No	0	0	8	13	0	0	8	12
Total	4	100	60	100	5	100	69	100

Fuente: Elaboración propia.

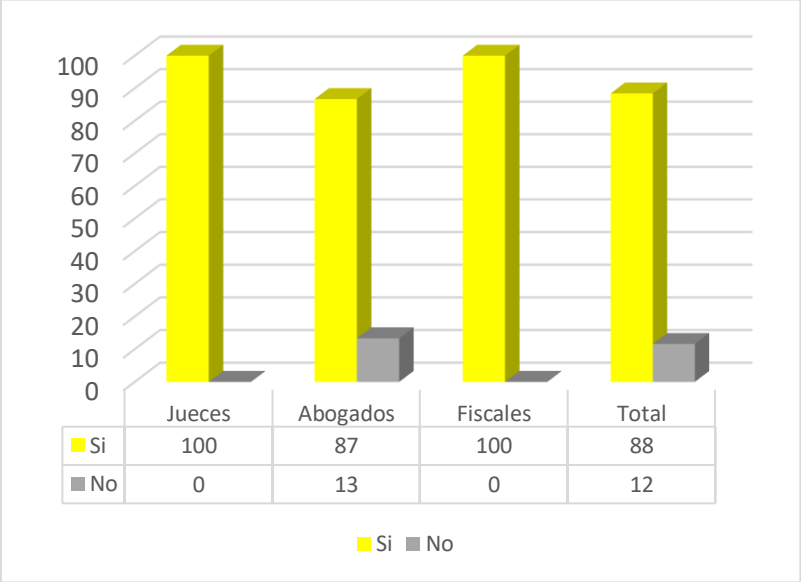


Figura 9: Elaboración propia**.**

En la tabla y figura 9, se muestra que 100% de jueces y fiscales, así como el 87% de fiscales señalaron que es necesario incorporar el artículo 8 – A en la Ley Especial de Delitos Informáticos, en relación a las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático. Por lo tanto 88% de los encuestados argumentaron que se debe de realizar dicha incorporación, en tanto 12% manifestaron lo contrario.

4.10 Tabla 10:

¿Considera usted que incorporar el artículo 8 – A en la Ley Especial de Delitos Informáticos sobre las actuales modalidades delictivas en los cibercrímenes, contribuiría a la resolución de procesos penales por delitos de fraude informático?

Respuesta	Jueces		Abogados		Fiscales		Total Condición	
	n	%	n	%	n	%	%	
Si	4	80	52	87	5	100	61	87
No	1	20	8	13	0	0	9	13
Total	5	100	60	100	5	100	70	100

Fuente: Elaboración propia.

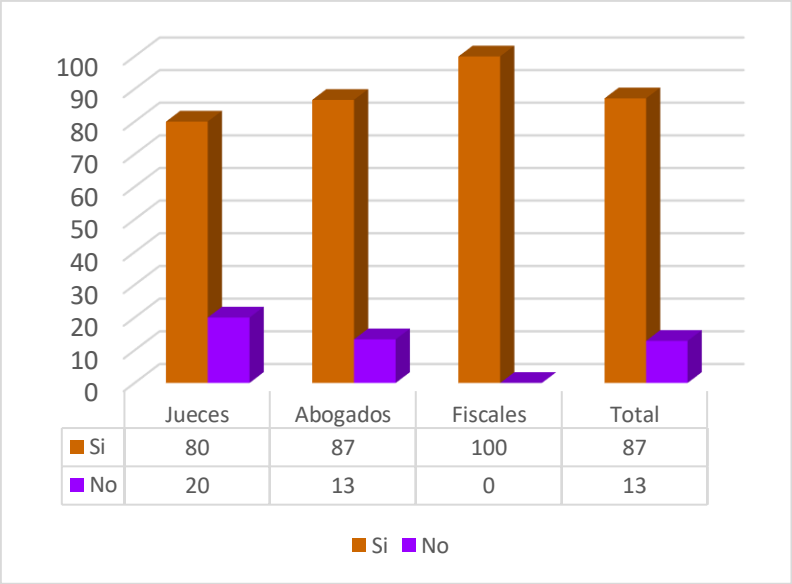


Figura 10: Elaboración propia**.**

En la tabla y figura 10, se muestra que 80% de jueces, 87% de abogados y 100% de fiscales consideraron que es importante incorporar el artículo 8 – A en la Ley Especial de Delitos Informáticos sobre las actuales modalidades delictivas en los cibercrímenes, porque contribuiría a la resolución de procesos penales por delitos de fraude informático. Por lo tanto 87% de los encuestados expresaron que, es necesaria dicha incorporación porque contribuirá a la resolución de procesos penales, en tanto 13% manifestaron en estar en desacuerdo.

V. DISCUSIÓN

Los cibercrímenes en los últimos años se han ido adaptando a las nuevas tecnologías y circunstancias, ocasionando que ingresen a los ordenadores de las víctimas a fin de obtener datos importantes para la comisión de dichos ilícitos, estos delitos son especiales debido a que usan la tecnología para su comisión, así se tiene el delito de fraude informático; el cual se ha incrementado por la situación actual que se están afrontando a nivel mundial, en el que las personas se han vinculado de manera más intrínseca en los medios tecnológicos a razón de ello han surgido nuevas modalidades delictivas de este tipo de delito como es la intercepción de datos informáticos, suplantación de sitios web a fin de capturar datos o se transfiere de manera no consentida.

En cuanto a dicho conocimiento los operadores del derecho han referido por unanimidad que ante dicha realdad problemática que se está afrontando es necesario que se regule las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático tal como se evidencia en la tabla y figura N° 1; relacionado a ello Rincón (2015) citado en trabajos previos a nivel internacional ha referido que al analizar la regulación normativa de los delitos informáticos como en la legislación Colombiana y Española, se ha demostrado el desarrollo histórico que ha pasado así como su creación legal y el análisis desde la dogmática penal; refiriéndose así que el desarrollo de las nuevas modalidades delictivas ayudan a proteger diversas circunstancias no amparadas.

En ese mismo sentido los encuestados han referido por unanimidad que la incorporación de las actuales modalidades delictivas en el delito de fraude informático se ampararía aquellas situaciones que no están establecidas en la Ley especial conforme se evidencia en la tabla y figura N° 3. Teniéndose en cuenta que este tipo de delito se ha incrementado de manera abismal en los últimos años, puesto que los ciberdelincuentes se han adaptado a los nuevos avances tecnológicos a través de las computadoras, redes de internet o vías informáticas conforme lo menciona Acosta (2016) citado en trabajos previos.

Además se debe tener en cuenta que este tipo penal es especial, al cometerse aquel acceso indebido a datos, bienes inmateriales y materiales con valor económico, ocasionando burla a las medidas de seguridad, redes o medios informáticos, con el objetivo de aprovecharse indebidamente del acto fraudulento; de lo que se puede diferir, que el fraude informático es aquella mentira que se produce a las medidas de seguridad de los datos informáticos para que se obtenga un provecho ilícito, es por ello, que este delito afecta la seguridad de los medios informáticos, mientras que el delito de estafa afecta a la propia persona en si (Chávez, 2018) citado en teorías relacionadas al tema.

Los cibercrímenes que se encuentran regulados en nuestra normativa penal y vigente y normativa extranjera, no son conocidos por los operadores del derecho conforme se aprecia en la tabla y figura N°4, en el que se evidencia que el 68% de encuestados mencionaron no conocer dichos cibercrímenes; esto se debe a que existe un desconocimiento sobre estos tipos de delitos que se encuentran estipulados en la ley, teniéndose en cuenta que nuestro país existen vacíos e imprecisiones legales sobre la regulación de delitos informáticos, teniéndose en cuenta que en la norma solo se encuentran regulados nueve delitos que amparan ciertas circunstancias dejando de lado las modalidades actuales.

En contraste a lo señalado precedentemente los operadores del derecho han referido en un 74% que no conocen si en nuestra normativa penal se encuentran sancionados dichos cibercrímenes, conforme se evidencia en la tabla y figura N° 5; siendo que señalaban que en nuestro país no existen muchas normas que amparen situaciones que se perjudique tecnológicamente a las víctimas, toda vez que existe un retraso normativo sobre dichas situaciones; así mismo los encuestados han mencionado en un 79% conocer la regulación de los cibercrímenes en la legislación extranjera como lo estipulado en la normativa Colombiana la cual es pionera sobre este tipo de delitos, los países vecinos como Chiles y Ecuador conforme se evidencia en la tabla y figura N° 6.

Sobre dicho enunciado Chávez (2018), citado en trabajos previos a nivel nacional ha referido que los cibercrímenes son cometidos contra de los sistemas

informáticos y datos informáticos que menoscaban de manera significativa el derecho a la intimidad personal de las víctimas, siendo que a través de dicha información se perjudica patrimonialmente al sujeto activo; relacionado a ello Tellez (2016), mencionado en teorías relacionadas al tema, argumenta que son conductas ilícitas que se cometen a través de los equipos informáticos como instrumentos a fines para cometer sus conductas ilícitas, es decir, las computadores son utilizadas como mecanismos auxiliares de apoyo a las diversas conductas humanas, con el objetivo de conseguir información vital.

La regulación normativa del delito de fraude informático regulado en nuestro país se encuentra regulado en el artículo 8 de la Ley N° 30096, sobre dicho conocimiento los encuestados ha referido en un 83% conocer en que consiste el delito de fraude informático que se encuentre regulado en la ley especial, conforme se evidencia en la tabla y figura N°7; en contraste a ello Pardo (2018) citado en trabajos previos en el ámbito nacional ha referido que en nuestra normativa existe una deficiencia en el tratamiento jurídico de los delitos informáticos contra el patrimonio, siendo que de manera ilógica se entiende dentro del delito de fraude informático las modalidades de los delitos informáticos contra el patrimonio, generándose así incertidumbre jurídica.

Así mismo, en relación a la regulación normativa extranjera, los encuestados han mencionado en un 71% que si conocen la regulación del delito de fraude informático en la legislación comparada tal como se demuestra en la tabla y figura N°8 ; relacionado a ello Chávez (2018) ha referido que Colombia es el país con mayor énfasis en los delitos informáticos a través de la Ley 1.273 (regulada en el año 2009), realiza modificaciones en el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos"; siendo que se está en la búsqueda de preservar en dicha norma aquellos sistemas que usen tecnologías de comunicación e información.

Por lo que se puede diferir que a partir de dicha norma se protegió un bien titular estableciéndose conductas delictivas que están concomitantes a la tecnología de acuerdo a los medios informáticos, siendo este país el primero a nivel global

legalizar estos tipos de delitos; en dicho país se castigan ilícitos con penas de 48 y 12 meses así como el pago de días multa, regulación distinta a la normada en nuestro país, demostrándose así las deficiencias normativas que existen así como los vacíos legales.

En relación al tercer objetivo específico, el cual es proponer mediante un proyecto de ley la incorporación de circunstancias de hecho de los cibercrímenes en el delito de fraude informático señalado en el artículo 8 de la Ley de Delitos Informáticos; los operadores del derecho han mencionado en un 88% que es necesario que se incorpore el artículo 8 – A en la Ley Especial de Delitos Informáticos, en relación a las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático tal como se evidencia en la tabla y figura N° 9, así mismo el 87% de encuestados han mencionado que es importante que se incorpore dicho artículo debido a que se contribuiría a la resolución de procesos penales por delitos de fraude informático.

En contraste a ello Zorrilla (2018) citado en trabajos previos en el ámbito nacional ha precisado que al analizar críticamente la Ley Especial de Delitos Informáticos así como su modificatoria a través de la Ley N° 30171, se videncia en dichos artículos que lo conforman, varias imprecisiones en su redacción, ocasionando confusión en los operadores del derecho, puesto que muchos delitos graves no son denunciados, o temen denunciar dichos ilícitos, siendo que ante la falta de imprecisiones es imposible encontrar a los verdaderos culpables ocasionando desanimo en las victimas; lo cual se tiene plena concordancia es por ello que en esta investigación se propone que exista una regulación más estricta sobre el delito de fraude informático.

Luego de haberse discutido cada uno de los objetivos que se han plantado en esta investigación, se ha logrado corroborar la hipótesis que fue planteada, siendo esta que, es posible proponer la incorporación de las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático en el artículo 8 de la Ley de delitos informáticos, es así que los encuestados han mencionado en un 88% que es necesario dicha regulación conforme se evidencia en la tabla y figura N° 9, así

mismo han referido en un 87% que dicha incorporación es importante porque se porque se contribuiría a la resolución de procesos penales por delitos de fraude informático de acuerdo a la tabla y figura N° 10.

Lo acotado anteriormente se contrasta a lo mencionado por Sequeiros (2016) el cual fue citado en trabajos previos en el ámbito nacional, han mencionado que por la naturaleza especial de los delitos informáticos, la cual es virtual en comparación de los otros delitos, se vuelve confusa su tipificación al tener escasos conocimientos tecnológicos de cómo combatir dicha cibercriminalidad y poder manejar dichas situaciones de manera virtual, ante dicha circunstancia se ocasiona una deficiente tipificación de modalidades delictivas actuales, las cuales se han adaptado a los avances tecnológicos.

Por otro lado es necesario mencionar que durante el desarrollo de esta investigación se han presentado diversas dificultades, una de ellas es que por la actual pandemia global que se afrontada no fue posible realizar las encuestas de manera presencial sino de manera virtual a través de correos, whtasapp y formularios de google; finalmente sobre la información de esta investigación ha sido escasa sobre la regulación de los delitos informáticos en nuestro país, encontrándose más en el ámbito internacional, pese a ello, se tomó dichas doctrinas para dar un sustento teórico a la presente investigación.

Si bien es cierto se presentaron diversas dificultades, ello no fue óbice para que se tenga fortalezas en esta investigación, una de ellas es que los encuestados respondieron de manera acertada a las interrogantes que se formularon en el cuestionario, lo cual ha contribuido para el desarrollo y comprobación de la hipótesis planteada, evidenciándose así que esta investigación es veraz y coherente.

VI. CONCLUSIONES

1. En la actual coyuntura mundial que estamos afrontando como humanidad la tecnología ha sido de suma importancia para la comunicación entre las personas así como realizar actividades laborales, académicas; ante dicha situación los ciberdelincuentes adaptaron nuevas modalidades delictivas para captar a sus víctimas a fin de perjudicarlas económicamente, destacándose el delito de fraude informático como el ilícito informático más cometido en estos tiempos, es así que se han actualizado nuevas modalidades delictivas como obstaculizar ilegítimamente un sistema informático, uso malicioso del software, violación de datos personales, suplantación de sitios web para capturar datos, así como la transferencia no consentida de dinero.

2. Se ha corroborado la hipótesis que se ha planteado, siendo que es necesario proponer la incorporación de las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático en el artículo 8 de la Ley de delitos informáticos, a fin de que se contribuya a la resolución de procesos penales de dicho delito para que aquellas circunstancias ilícitas no queden impugnes por el vacío legal que existe en la ley especial.

3. En nuestra normativa, existe una Ley Especial de Delitos Informáticos el cual está conformado por la tipificación de nueve artículos los cuales amparan ciertas circunstancias delictivas, que en su totalidad no amparan todas aquellas situaciones que actualmente se están evidenciando; teniéndose en cuenta que dicha ley está vigente desde el año 2013 habiendo transcurrido ocho años de desactualización, pese a que con el avance de la tecnológica los ciberdelincuentes han creado nuevas modalidades de menoscabo económico a sus víctimas, evidenciándose que nuestro país tiene una deficiente normativa penal sobre los delitos informáticos en comparación a países como Colombia el cual es pionero en la tipificación de ilícitos informáticos.

4. En el artículo 8 de la Ley Especial de Delitos Informáticos – Ley N° 30096, se regula como único delito informático contra el patrimonio el ilícito de fraude informático, en el cual se sanciona aquel que de manera ilegítima procura para sí

o para otro algún provecho ilícito ocasionando perjuicio a un tercero ante dicho accionar se le sanciona una pena entre tres a ocho años agravándose la pena de cinco a diez años cuando se afecta al patrimonio del Estado; en cambio en la legislación extranjera como el Código Penal Argentino se norma los delitos informáticos dentro de los delitos comunes como modalidades delictivas, generando que existe una mayor protección, así se tiene el delito de fraude informático tipificado en el artículo 173 literal 16.

5. Finalmente, ante dichos vacíos normativos existentes en los delitos informáticos tipificados en la ley especial más aun en el ilícito que se comete comúnmente en la actualidad como es el delito de fraude informático; por ello es necesario que se incorpore circunstancias de hecho en el artículo 8 – A de la Ley N° 30096 a fin de que no queden impugnes acciones ilícitas cometidas por dichos ciberdelincuentes.

VII. RECOMENDACIONES

1. Se le recomienda al Poder Legislativo promulgar una Ley, en la cual se incorpore el artículo 8 de la Ley de Delitos Informáticos, sobre las circunstancias de hecho de los cibercrímenes en el delito de fraude informático, a fin de que se regule actuales circunstancias actuales.

2. Se recomienda que la fiscalía al momento de formular acusación sobre el investigado quien ha perjudicado patrimonialmente al sujeto pasivo; tome en cuenta las nuevas circunstancias de hecho especificadas en el artículo en mención, a fin de que no quede impune dicho delito.

3. Finalmente, se recomienda a los magistrados que tengan en cuenta la regulación de dichas circunstancias de hecho sobre el delito de fraude informático, a fin de que condenen de manera motivada a los condenados.

VIII. PROPUESTA

PROYECTO DE LEY QUE MODIFICA EL ARTÍCULO N°8-A DE LA LEY DE DELITOS INFORMÁTICOS

La Bachiller en Derecho que suscribe Yulisa Custodio Cumpa., ejerciendo el derecho a iniciativa legislativa que le confiere el artículo 107° de la Constitución Política del Perú, presenta el siguiente Proyecto de Ley:

PROYECTO DE LEY QUE MODIFICA EL ARTÍCULO N° 8-A DE LA LEY DE DELITOS INFORMÁTICOS

I. FÓRMULA LEGAL

Artículo 1º.- Objeto de la ley

La presente ley tiene por objeto modificar el artículo N° 8-A de la Ley Especial de Delitos Informáticos, respecto a regular:

Artículo 2º. - Modificar el artículo 8 de la Ley de Delitos Informáticos

Modificase el artículo N° 8 de la ley de delitos informáticos, de la siguiente forma:

Artículo 8- A: Circunstancias de hecho

1. Obstaculizar ilegítimamente un sistema informático, aquel que bloquea en forma ilegal un sistema o impide que se ingrese, así mismo acceden a cuenta de correo electrónico u otras páginas personales de otras personas sin su consentimiento.
2. Uso malicioso del software, aquel que produce, adquiere, envía, distribuye, introduce o extrae del país software o programas de computador que producen daños en los recursos de las Tecnologías de la Información y las Comunicaciones (TIC)

3. Violación de datos personales, aquel que sin estar facultado vende, sustrae, envía, compra, divulga o emplea datos personales almacenados en medios magnéticos.
4. Suplantación de sitios web para capturar datos, aquel que crea una página similar de una entidad y envía correos, mensajes o llamadas engañosas, para obtener información personal del agente (tales como claves bancarias) a fin de transferirlas para su beneficio o de un tercero.
5. Transferencia no consentida de activo, aquel que por la acción cometida en el literal anterior, con ánimo de lucro y valiéndose de manipulaciones informáticas o artículo semejante, realice la transferencia no consentida de cualquier activo en perjuicio de un tercero.

II. EXPOSICIÓN DE MOTIVOS

II. 1 Aspectos Generales

En la actual coyuntura mundial que estamos afrontando como humanidad la tecnología ha sido de suma importancia para la comunicación entre las personas así como realizar actividades laborales, académicas entre otras; ante dicha situación los ciberdelincuentes adaptaron nuevas modalidades delictivas para captar a sus víctimas a fin de perjudicarlas económicamente, destacándose el delito de fraude informático, como el ilícito informático más cometido en estos tiempos, es así que se han actualizado nuevas modalidades delictivas.

Estos actos delictivos cometidos a través del internet son denominados cibercrímenes, los cuales en su mayoría son desconocidos por las personas así como en nuestra normativa penal, por lo que ante dicho desconocimiento los delincuentes sacan provecho para perjudicar patrimonialmente a sus víctimas y así obtener grandes beneficios económicos; pese a que en la actualidad surgen dichas situaciones éstas no se encuentran reguladas en la normativa especial como es la Ley N°30096 - Ley de delitos informáticos, la cual se encuentra en

vigencia desde el año 2013, pasando así ocho años en los cuales han surgido nuevas circunstancias de hecho de los cibercrímenes.

Pese a la existencia de nuevas circunstancias éstas no han sido reguladas por nuevas leyes que traten de amparar dichas situaciones, además se debe tener en cuenta que nuestro país tiene una deficiente cultura informática así como la obtención de implementos necesarios de investigación de este tipo de delitos, teniéndose en cuenta que no contamos con la principal herramienta de sanción que es la ley para sancionar penalmente a dichos agentes ciberdelincuentes, quienes tienen un conocimiento informático sobresaliente, razón por la cual implementan nuevas modalidades de delinquir cada día.

Las personas perjudicadas principalmente son aquellas vinculadas al sector financiero, debido a que, los usuarios de este sector han denunciado que sus cuentas bancarias han sido vaciadas, luego de haber registrado sus códigos de datos o de información de sus bancos, ingresando así a paginas falsas (que aparentemente pertenecían a su banco de confianza) en las cuales colocaron datos como nombres, número de DNI, número de cuenta y la clave, elementos que son utilizados por los delincuentes para obtener beneficios económicos, puesto que es información importante y personal; diversos expertos señalan que los cibercrímenes más comunes que se están cometiendo actualmente es el smishing, pharming, vishing y phishing .

Si bien es cierto existen dichos cibercrímenes que en su mayoría son alterados de acuerdo a la situación coyuntural que se esté presentado en la sociedad, pues los ciberdelincuentes al momento de adoptar una conducta delictiva toman en cuenta el entorno social en que se presentan, a fin de analizar cuál sería el delito que se adecuaría a dicho entorno para que éste permanezca y así se pueda obtener grandes beneficios económicos, pues al tratarse de delitos que se comenten en línea estos son realizados de manera simultánea en todo el país.

Pese a afrontarse a dicha situación, en nuestra normativa penal sea especial o sustantiva no se encuentran reguladas dichas circunstancias de hecho, solo se encuentra especificadas de manera general dentro del delito de fraude

informático en el que se señala en términos como diseñar, introducir, borrar, alterar, clonar, suspender; las cuales son acciones que se realizan en un sistema informático para obtener un provecho ilícito, pero dichos verbos no amparan situaciones como la creación de “URLS FALSAS” de las entidades financieras, transferencias no consentidas de dinero, uso de software malicioso entre otros; por lo que resulta importante la regulación de dichas circunstancias de hecho de manera específica.

Por dicha situación coyuntural que estamos afrontando a lo largo de estos años, se aplicó un instrumento a diversos operadores jurídicos, conocedores del derecho quienes nos han referido por unanimidad que ante dicha realdad problemática que se está afrontando es necesario que se regule las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático tal como se evidencia en la tabla y figura N° 1. Así mismo Acosta (2016) refiere que este tipo de delito se ha incrementado de manera abismal en los últimos años, puesto que los ciberdelincuentes se han adaptado a los nuevos avances tecnológicos a través de las computadoras, redes de internet o vías informáticas.

Además se debe tener en cuenta que este tipo penal es especial, al cometerse aquel acceso indebido a datos, bienes inmateriales y materiales con valor económico, ocasionando burla a las medidas de seguridad, redes o medios informáticos, con el objetivo de aprovecharse indebidamente del acto fraudulento; de lo que se puede diferir, que el fraude informático es aquella mentira que se produce a las medidas de seguridad de los datos informáticos para que se obtenga un provecho ilícito, es por ello, que este delito afecta la seguridad de los medios informáticos, mientras que el delito de estafa afecta a la propia persona en si (Chávez, 2018).

Por otro lado, un 88% han referido que es necesario que se incorpore el artículo 8 – A en la Ley Especial de Delitos Informáticos, en relación a las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático tal como se evidencia en la tabla y figura N° 9; así mismo el 87% de encuestados han mencionado que es importante que se incorpore dicho artículo debido a que

se contribuiría a la resolución de procesos penales por delitos de fraude informático.

En contraste a ello, Zorrilla (2018) ha precisado que al analizar críticamente la Ley Especial de Delitos Informáticos así como su modificatoria a través de la Ley N° 30171, se videncia en dichos artículos que lo conforman, presentan varias imprecisiones en su redacción, ocasionando confusión en los operadores del derecho, puesto que muchos delitos graves no son denunciados, o temen denunciar dichos ilícitos, siendo que ante la falta de imprecisiones es imposible encontrar a los verdaderos culpables ocasionando desanimo en las victimas; lo cual se tiene plena concordancia es por ello que en esta investigación se propone que exista una regulación más estricta sobre el delito de fraude informático.

De la misma manera, Pardo (2018) ha referido que en nuestra normativa existe una deficiencia en el tratamiento jurídico de los delitos informáticos contra el patrimonio, siendo que de manera ilógica se entiende dentro del delito de fraude informático las modalidades de los delitos informáticos contra el patrimonio, generándose así incertidumbre jurídica.

Por otro lado, lo concerniente a la legislación extranjera como Colombia país pionero en la tipificación de delitos informáticos, Chávez (2018) ha referido que Colombia es el país con mayor énfasis en los delitos informáticos a través de la Ley 1.273 (regulada en el año 2009), ha realizado modificaciones en el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos"; siendo que se está en la búsqueda de preservar en dicha norma aquellos sistemas que usen tecnologías de comunicación e información.

Relacionado a ello, Rincón (2015) ha referido que al analizar la regulación normativa de los delitos informáticos como en la legislación Colombiana y Española, se ha demostrado el desarrollo histórico que ha pasado así como su creación legal y el análisis desde la dogmática penal; refiriéndose así que el desarrollo de las nuevas modalidades delictivas.

Ante dicha situación problemática se ha logrado determinar que es posible proponer la incorporación de las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático en el artículo 8 de la Ley de delitos informáticos, es así que los encuestados han mencionado en un 88% que es necesario dicha regulación conforme se evidencia en la tabla y figura N° 9, así mismo han referido en un 87% que dicha incorporación es importante porque se porque se contribuiría a la resolución de procesos penales por delitos de fraude informático de acuerdo a la tabla y figura N° 10.

Lo acotado anteriormente se contrasta a lo mencionado por Sequeiros (2016) quien ha mencionado que por la naturaleza especial de los delitos informáticos, la cual es virtual en comparación de los otros delitos, se vuelve confusa su tipificación al tener escasos conocimientos tecnológicos de cómo combatir dicha cibercriminalidad y poder manejar dichas situaciones de manera virtual, ante dicha circunstancia se ocasiona una deficiente tipificación de modalidades delictivas actuales, las cuales se han adaptado a los avances tecnológicos.

Sobre dicho enunciado Chávez (2018) ha referido que, los cibercrímenes son cometidos contra de los sistemas informáticos y datos informáticos que menoscaban de manera significativa el derecho a la intimidad personal de las víctimas, siendo que a través de dicha información se perjudica patrimonialmente al sujeto activo; relacionado a ello Tellez (2016) argumenta que, son conductas ilícitas que se cometen a través de los equipos informáticos como instrumentos a fines para cometer sus conductas ilícitas, es decir, las computadores son utilizadas como mecanismos auxiliares de apoyo a las diversas conductas humanas, con el objetivo de conseguir información vital.

Ante el perjuicio patrimonial informático que se realiza al sujeto pasivo, dichas conductas delictivas deben ser sancionadas a fin de que no se queden impunes, por otro lado, ante la regulación de nuevas circunstancias de hecho permitirá prevenir la comisión de futuros delitos, siendo que los ciberdelincuentes tendrán en cuenta la sanción que se impone y así evitaran cometerlos.

II. 2 Marco Legal

1) Constitución Política del Perú

Articulo 107.-

(…) Así mismo lo tienen los ciudadanos que ejercen el derecho de iniciativa conforme a ley.

2) Ley Especial de Delitos Informáticos

Artículo 8- A: Circunstancias de hecho

1. Obstaculizar ilegítimamente un sistema informático, aquel que bloquea en forma ilegal un sistema o impide que se ingrese, así mismo acceden a cuenta de correo electrónico u otras páginas personales de otras personas sin su consentimiento.
2. Uso malicioso del software, aquel que produce, adquiere, envía, distribuye, introduce o extrae del país software o programas de computador que producen daños en los recursos de las Tecnologías de la Información y las Comunicaciones (TIC)
3. Violación de datos personales, aquel que sin estar facultado vende, sustrae, envía, compra, divulga o emplea datos personales almacenados en medios magnéticos.
4. Suplantación de sitios web para capturar datos, aquel que crea una página similar de una entidad y envía correos, mensajes o llamadas engañosas, para obtener información personal del agente (tales como claves bancarias) a fin de transferirlas para su beneficio o de un tercero.
5. Transferencia no consentida de activo, aquel que por la acción cometida en el literal anterior, con ánimo de lucro y valiéndose de manipulaciones informáticas o artículo semejante, realice la transferencia no consentida de cualquier activo en perjuicio de un tercero.

II. 3 Contenido de la norma

La presente norma busca agregar un literal en el artículo 8 de la ley Especial de Delitos Informáticos en el capítulo V relacionado a los delitos informáticos contra el patrimonio, en el cual solo se encuentra tipificado únicamente el delito de fraude informático, se señalan términos como diseñar, introducir, borrar, alterar, clonar, suspender; las cuales son acciones que se realizan en un sistema informático para obtener un provecho ilícito, pero dichos verbos no amparan situaciones como la creación de “URLS FALSAS” de las entidades financieras, transferencias no consentidas de dinero, uso de software malicioso entre otros; por lo que resulta importante la regulación de dichas circunstancias de hecho de manera específica.

III. EFECTOS DE LA VIGENCIA DE LA NORMA EN LA LEGISLACIÓN NACIONAL.

Ante la aprobación del presente proyecto de ley y su consecuente promulgación incorporándose la modificación propuesta, surtirá efecto únicamente sobre aquellos casos que se hayan presentado a partir de la publicación en el diario Oficial “El Peruano”, por lo mismo que no tendrá un efecto retroactivo.

IV. ANÁLISIS COSTO - BENEFICIO

El proyecto de ley no generará ningún costo al Estado Peruano, debido que a que no se generará un presupuesto adicional a ninguna entidad.

Custodio Cumpa Yulisa

REFERENCIAS

TESIS

Abushihab, A. (2016). “Cibercrímen: Una aproximación a la delincuencia informática”. (Tesis de Pregrado). Universidad Santo Tomás, Bogotá, Colombia.

Chávez, E. (2018). “El delito contra datos y sistemas informáticos en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Lima Norte, 2017”. (Tesis de postgrado). Universidad Nacional Federico Villareal, Lima, Perú.

Cotrina, S. (2018). “Los factores principales que impiden la aplicación de la ley N° 3071 – Lima Norte en el año 2016”. (Tesis de pregrado). Universidad Cesar Vallejo, Lima, Perú.

Delgado, A. (2016). “La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú-2015” (tesis de pregrado). Universidad Señor de Sipán, Lambayeque, Perú.

Granados, A. y Parra, J. (2016). “El delito de hurto por medios informáticos que tipifica el artículo 269 - i de la Ley 1273 de 2009 y su aplicabilidad en el Distrito Judicial de Cúcuta en el período 2012 – 2014”. (Tesis Pregrado). Universidad Libre de Colombia, Bogotá, Colombia.

Larios, J. y Sánchez, R. (2014). “Ciberdelito”. (Tesis de Pregrado). Universidad Nacional Autónoma de México, México D.F.

Montañéz, L (2017). “Análisis de los delitos informáticos en el actual sistema penal colombiano”. (Tesis Pregrado). Universidad Libre de Colombia, Bogotá, Colombia.

Sequeiros, I. (2016). Vacíos legales que imposibilitan la sanción de delitos

informáticos en el nuevo Código Penal peruano-2015. (Tesis de Pregrado). Universidad de Huánuco, Lima, Perú.

Torres, J. (2018). Análisis en torno a la tipificación del delito del sexting a propósito de la incorporación del artículo 154° B al Código Penal peruano. (Tesis de Pregrado). Universidad César Vallejo, Lima, Perú.

Zorrilla, K. (2018). "Inconsistencias y ambigüedades en la ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171, que imposibilitan su eficaz cumplimiento" (tesis pregrado). Universidad Nacional de Ancash "Santiago Antunez de Mayolo", Ancash, Perú.

REVISTAS INDEXADAS

Aguilar, M. (2015). Cybercrime and cybervictimization in Europe: Institutions involved in cybercrime prevention in the United Kingdom. Revista Criminalidad. N° 57, pp. 121-135.

Álvarez, D., Barreiro, A., Núñez, J. y Dobarro, A. (2016). Validity and reliability of the Cyber-Aggression Questionnaire for Adolescents (CYBA). Madrid, España. (SCIELO)

Arévalo, A., García, F., Navarro, J. y Pardo, A. (2012). An Approach to the Legal Problems of Virtual Social Networks. Revista Virtual Universidad Católica del Norte, núm. 37. pp. 62-92 Fundación Universitaria Católica del Norte Medellín, Colombia.

Borges, J. y Dell'Aglio, D. (2019). Stalking Following the Breakup of Dating Relationships in Adolescence. Trends in Psychology, N° 27(2), 413-426. (SCIELO)

Damarit, J. (2016). "Cybercrime and cyber-victimization". IDP. Revista de Internet, Derecho y Política. N° 22, pp. 30-31. (DIALNET)

Deluca, S. y Carril, E. (2017). Cooperação internacional en materia penal no MERCOSUL: o cibercrimen. Revista de la Secretaría del Tribunal Permanente de Revisión, 5(10), 13-28. (LATINDEX)

Dominguez, I. (2016). Towards Selective Memory On the Internet. Honor, Intimacy and Personal Image in The Digital Age On the Basis of Spanish CaseLaw. Revista iberoamericana de ciencia tecnología y sociedad, N° 11(32), pp. 4969. (SCIELO)

Matassoli, R. y Ferreira, S. (2017). “Cyber dating abuse in affective and sexual relationships: a literature review”. Cuadernos de Saúde Pública. N° 33(7). (SCIELO)

Miró, L. (2016). ¿Podemos ser víctimas de un ciberdelito? Descubre. Universidad Miguel Hernández. (DIALNET)

Miró, J. (2012). El Cibercrímen: Fenomenología y la Criminología de la delincuencia en el Ciberespacio, España: Marcial Pons.. (SCOPUS)

Miró, F. (2013). Delincuencia y TICs: Cibercrimen, Cibercriminales y Cibervictimas. Universitat Oberta de Catalunya.

Miró, L. (2016). Taxonomy of violent communication and the discourse of hate on the internet”. Cybercrime and cyber-victimization. IDP. Revista de Internet, Derecho y Política. N° 22, pp. 93-118. (DIALNET)

Parada, R. y Errecaborde, J. (2018). Cibercrímen y delitos informáticos: los nuevos tipos penales en la era de internet. Ciudad Autónoma de Buenos Aires: Erreius. Recuperado de: http://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO, Revista Latinoamericana de Estudios de Seguridad. España. (REDALYC)

Posada, R. (2017). The cybercrime and its effects in the theory of typicity: from a physical reality to a virtual reality. Nuevo Foro Penal. pp. 72-112. (DIALNET)

Quevedo, J. (2017). *Investigación y prueba del ciberdelito.* (Tesis de Postgrado). Universitad de Barcelona, España. Recuperado desde: https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?s equence =1&isAllowed=y (DIALNET)

Rodríguez, N. (18 de marzo de 2019). *Protegiendo a nuestros hijos del cibercrimen*. RPP. Recuperado de: https://rpp.pe/columnistas/nadiarodriguez/protegiendo-anuestros-hijos-del-cibercrimen-noticia-1185457 (ALICIA)

Silfredo, J. (2014). Typing Cybercrime Patrimonial In The New Law On Cybercrime N°30096, Ius Et Veritas, 24(49). (REDALYC).

Tamarit, J. (2016). *"Cybercrime and cyber-victimization".* IDP. Revista de Internet, Derecho y Política. N° 22, pp. 30-31. Recuperado de: http://doi.org/10.7238/idp.v0i22.2991 (DIALNET)

Vargas, R., Recalde, L. y Reyes, R. (2017). *Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance*. URVIO, Revista Latinoamericana de Estudios de Seguridad, núm. 20, España. Recuperado de:https://www.redalyc.org/jatsRepo/5526/552656641013/html/index.html (REDALYC)

Villa-Moral, M., & Fernández, S. (2019). *Problematic Internet Use in Spanish Adolescents and Their Relationship with Self-Esteem and Impulsivity*. Avances en Psicología Latinoamericana, N° 37(1), pp. 103-119. Recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794472420190001001 03&lang=es (SCIELO)

Villavicencio, F. (2014). Delitos informáticos. Ius Et Veritas, 24(49). (SCIELO).

Wall, D. (2007). Cybercrime: The transformation of crime in the information age. Cambridge: Polity Press. Recuperado de: http://www.lpbr.net/2008/06/cybercrime-transformation-of-crime.in.html.

LIBROS EN FÍSICO

Alas, D. (2015). *Comportamiento de la víctima del delito*. *La autopuesta en peligro.* Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=5456410 (DIALNET)

Bocij, P. (2015). *Victims of Cyberstalking:* An explory study of harrasment perpetrated via the internet. Recuperado de: https://www.ojphi.org/ojs/index.php/fm/article/view/1086/1006#b5. (ONLINE JOURNAL OF PUBLIC HEALTH INFORMATICS)

Michael C. (2016), Social Media Security: *Leveraging Social Networking While Mitigating Risk*, USA. Washington DC. Recuperado de: https://cdn.ttgtmedia.com/rms/security-Dialnet/Social-Media-Security-Ch10.pdf

Miró, F. (2012). *El Cibercrimen*: *Fenomenología y la Criminología de la delincuencia en el Ciberespacio*, España: Marcial Pons. Recuperado de: http://biblio.upmx.mx/indices/140032.pdf. (SCOPUS)

Palomino, W. (2014). El intrusismo y los otros delitos informáticos regulados en la Ley N° 30096. Tomo 56. N° 12, pp. 1-16. Lima, Perú: Gaceta Penal S.A. (LATINDEX)

Pérez, J. (2019). Delitos regulados en leyes penales especiales. pp. 130-145. Lima, Perú: Gaceta Jurídica S.A. (LATINDEX)

Pérez, L. (2019). El child grooming como delito informático en la Ley N° 30096 y sus modificaciones. Pp. 111-124. Actualidad Penal. Lima, Perú: Instituto Pacifico

ANEXOS

Variables	Definición Conceptual	Definición operacional	Dimensiones	Indicadores	Instrumento	Escala
V. Independiente Cibercrímenes Modalidades delictivas	Miró (2013) refiere que: "La cibercriminalidad puede ser entendida en sentido amplio, comprendiendo cualquier ilícito cometido por medio de un sistema informático o una red de computadores" (p.12). Son hechos adicionales que se tendrán en cuenta en el tipo penal y que según la descripción hecha atenúan o agravan la conducta (Jiménez, 2019)	Son acciones delictivas que cometen a través de la tecnología, utilizando el sistema informático para perjudicar a las personas. Son hechos que deben estar estipulados expresamente en la ley a fin de que la pena pueda ser graduada.	Doctrina	– Generalidades – Características – Tipos – Naturaleza jurídica	Encuesta	Nominal
			Normas	– Código Penal – Código Procesal Penal – Leyes Especiales		
			Jurisprudencia	- Resoluciones emitidas por el Tribunal Constitucional y Corte Suprema		

Variables	Definición Conceptual	Definición operacional	Dimensiones	Indicadores	Instrumento	Escala
V. Dependiente Fraude informático	"Es todo aquel acto antijurídico y de carácter culpable que se da por medios informáticos o que pretende manipular o dañar computadores, redes de internet o medios electrónicos a fin de perjudicar económicamente a sus víctimas" (p. 57)	Este tipo de delitos es cometido con el objetivo de menoscabar el patrimonio de su víctima, obteniendo un provecho ilícito.	Doctrina	– Teorías – Naturaleza jurídica – Tipos	Encuesta	Nominal
			Normas	– Ley Especial – Tratados		
			Jurisprudencia	– Sentencias vinculantes		

Anexo 2: Instrumento de recolección de datos

UNIVERSIDAD CÉSAR VALLEJO

"Las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático"

Instrucción: La encuesta es anónima y sus respuestas son confidenciales, así que le agradecemos ser lo más sincero posible. Llene los espacios en blanco y marque con un aspa la alternativa que considere más conveniente.

Condición

Fiscal Penal ☐ Jueces Penal ☐ Abogado Penal ☐

1. ¿Cree usted que, para facilitar la imputación de los delios informáticos, es necesaria la regulación de las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático?

SI ☐ NO ☐

2. ¿Considera usted que la incorporación de las actuales modalidades delictivas en el delito de fraude informático se ampararía aquellas situaciones que no están establecidas en la ley especial?

SI ☐ NO ☐

3. ¿Conoce usted cuales son los cibercrímenes cometidos comúnmente en nuestro país?

SI ☐ NO ☐

Si su respuesta es afirmativa, indique cuales:

_____

_____

4. ¿Conoce usted si en nuestra normativa penal se encuentran sancionados dichos cibercrímenes?

SI ☐ NO ☐

5. ¿Conoce usted la regulación de los cibercrímenes en la legislación extranjera?

SI ☐ NO ☐

6. ¿Conoce usted en que consiste el delito de fraude informático regulado en la ley especial?

SI ☐ NO ☐

7. ¿Conoce usted si en la legislación comparada se encuentra regulado el delito de fraude informático?

SI ☐ NO ☐

8. ¿Cree usted, que es necesario incorporar el artículo 8 – A en la Ley Especial de Delitos Informáticos, las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático?

SI ☐ NO ☐

9. ¿Considera usted que incorporar el artículo 8 – A en la Ley Especial de Delitos Informáticos sobre las actuales modalidades delictivas en los cibercrímenes, contribuiría a la resolución de procesos penales por delitos de fraude informático?

SI ☐ NO ☐

Anexo 3: Constancia de grado de confiabilidad

CONSTANCIA DE CONFIABILIDAD DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS

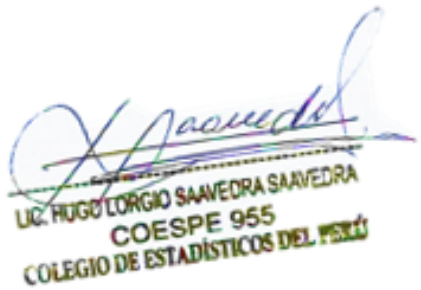
A través de este documento se constata la fiabilidad del instrumento de recolección de datos para medir la percepción del tema, el cual está contenido dentro de la tesis titulada "Las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático: otra pandemia en tiempos de coronavirus".

Ante ello, se ha utilizado el **Método de Kuder-Richardson (KR-20),** el cual queda evidenciado con la documentación anexada en el presente. Es así que para la interpretación del coeficiente de KR-20, se está tomando las siguientes escalas:

0.81 a1.00	Muy bueno
0.01 a 0.20	Baja
0.21 a 0.40	Moderada
0.41 a 0.60	Alta
0.61 a 0.80	Muy Alta

Dando fe que se utilizaron encuestas originales y que los resultados son fieles a la realidad a favor de la investigación, ya que el coeficiente de confiabilidad obtenido es igual a **0.767**, el mismo que refleja un coeficiente **"Alto"** dentro de la escala de fiabilidad, en conclusión el instrumento de recolección de datos es **confiable**.

Estampo mi sello, rubrica y número de registro para la conformidad del especialista y metodólogo de la investigación.



ANEXOS:

$$\textbf{KR-20}=\left(\frac{n}{n-1}\right)\left(1-\frac{\sigma 2-\sum p*q}{\sigma 2}\right)$$

En donde:

K= *Numero de ítems del instrumento*

K-1= *Numero de ítems del instrumento -1*

1= Unidad

$\sum p * q$ = *Sumatoria de los productos de p * q*

$\sigma 2$= *Varianza de las puntuaciones totales*

Aplicando la fórmula:

$$\textbf{KR-20}=\left(\frac{9}{9-1}\right)*\left(1-\frac{1.25}{3.23}\right)=0767$$

Finalmente:

Tabla 1:

Resultado obtenido al aplicar el coeficiente de KR-20 al cuestionario de 9 preguntas aplicado a: 5 jueces, 5 fiscales y 60 abogados.

KUDER-RICHARDSON	Encuestados
0.767	70

Fuente: Investigación propia