VICERRECTORADO ACADÉMICO
ESCUELA DE POSGRADO

TESIS

DELITOS INFORMÁTICOS Y SU RELACIÓN CON EL PROCESO DE INVESTIGACIÓN PRELIMINAR EN EL DISTRITO FISCAL DE LIMA NORTE AÑO 2019

PRESENTADO POR:

Bach: HAYDEE AYMA HUALLPA

PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN DERECHO PENAL

LIMA – PERÚ

2020

VICERRECTORADO ACADÉMICO
ESCUELA DE POSGRADO

TÍTULO DE LA TESIS

DELITOS INFORMÁTICOS Y SU RELACIÓN CON EL PROCESO DE INVESTIGACIÓN PRELIMINAR EN EL DISTRITO FISCAL DE LIMA NORTE AÑO 2019

LÍNEA DE INVESTIGACIÓN

DERECHO PENAL

ASESOR

Dra. CYNTHIA MARIA CONTRERAS GALVEZ

HOJA DE INFORMACIÓN BÁSICA

GENERALIDADES:

TÍTULO DE LA TESIS

Delitos Informáticos y su Relación con el Proceso de Investigación Preliminar en el Distrito Fiscal de Lima Norte, Año 2019.

AUTOR

Bach: Haydee Ayma Huallpa

ASESOR

Dra. Cynthia María Contreras Gálvez

TIPO DE INVESTIGACIÓN

Básica

ENFOQUE DE LA INVESTIGACIÓN

Cuantitativo

LÍNEA DE LA INVESTIGACIÓN

Derecho penal

LOCALIDAD

Ciudad de Lima - Distrito Fiscal de Lima Norte

DURACIÓN DE LA INVESTIGACIÓN:

Desde Julio del 2019 a Febrero del 2020.

DEDICATORIA

A mis padres, que con sus amorosos consejos me formaron como persona de bien, perseverante para el logro de mis propósitos.

AGRADECIMIENTO

Agradecimiento especial a la Dra., Cynthia Contreras, por sus orientaciones especializadas para la consecución del informe final.

RECONOCIMIENTO

A la universidad Alas Peruanas, por darme la oportunidad de concretar uno de mis anhelos.

Índice

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Este trabajo de tesis tuvo como finalidad examinar los datos bibliográficos y los datos estadísticos, respecto a los delitos informáticos, en tal sentido, los resultados obtenidos al respecto dan cuenta, que en el ministerio público de cono norte, viene aplicando de manera incorrecta la norma jurídica respecto al delito informático, dañando de esta manera los derechos fundamentales de personas procesadas, en algunos casos del estado. La informática es imperiosa para desarrollar las organizaciones dentro de la sociedad, en tal sentido es importante ponderar su uso correcto, para no afectar los derechos individuales y colectivos. En sus conclusiones se evidencian que las autoridades deben capacitar a los operadores del ministerio público en la valoración correcta de las pruebas, con evaluaciones precisas para no cometer excesos ni omitir los datos desistemas informáticos, sobre todo de aquellas que han sido obtenidos de manera ilegal, cuya valoración será evaluada excepcionalmente por el organismo competente. Finalmente se concluye que las evidencias dan cuenta que los procedimientos jurídicos referido al tratamiento penal, respecto delitos informáticos para preservar los bienes patrimoniales del estado, son deficientes. El cual genera desorden, porque al no aplicar la norma correctamente sobre el delito informático, se comete omisión en desmedro del estado. Las fiscalías especializadas en esta materia, deben asumir su competencia con ponderación, promoviendo actualizaciones académicas permanentes en convenio con las instituciones académicas. Que la aparición de la informática, ha creado un desafío y nuevos paradigmas para la ciencia del derecho, que ha tenido que cambiar sus paradigmas para poder describir los usos y costumbres y las conductas sociales de pobladores. El derecho ha tenido que modernizar sus herramientas jurídicas acorde con los entornos digitales para poder valorar las evidencias.

Palabras clave: delitos informáticos y su relación con el proceso de investigación preliminar

ABSTRACT

The purpose of the research was to analyse the bibliographical data and statistical data on computer-related crime, in this regard, the results obtained in this regard show that, in the Public Prosecutor's Office of the Northern Cone, has been incorrectly applying the legal norm regarding computer crime, thus affecting the fundamental rights of the persons prosecuted, in some cases in the state. Informatics is important for the development of organizations and society, so it is important to weigh its correct use, so as not to affect individual and collective rights. Its conclusions show that the state must train public prosecutors in the correct assessment of evidence, with precise evidence to avoid committing excesses or omitting data from computer systems, in particular those which have been obtained illegally, the assessment of which shall exceptionally be assessed by the competent body Finally, it is concluded that the evidence indicates that the legal procedures regarding the criminal treatment of computer crimes to preserve the state's patrimonial assets are deficient. This generates disorder, because by not applying the rule correctly on computer crime, omission is committed to the detriment of the state. The prosecutor's offices specializing in this area must assume their competence with weight, promoting permanent academic updates in agreement with academic institutions. That the appearance of informatics has created a challenge and new paradigms for the science of law, which has had to change its paradigms in order to describe the uses and customs and social behaviors of the inhabitants. The law has had to modernize its legal tools in line with digital environments in order to assess evidence.

Key words: computer crimes and their relation to the preliminary investigation process

INTRODUCCIÓN

La Tesis titulada: “Delitos Informáticos relacionado con el proceso de Investigación Preliminar en distrito fiscal de Lima norte, Año 2019”, tuvo como campo de estudio a los expedientes documentarios presentados por denuncias en distrito fiscal de Lima norte en relación al problema causada en la integridad desistemas informáticos del rubro de empresas públicas, privadas y la ciudadanía en general. Viéndose necesaria la evaluación en el derecho penal, la probidad desistemas informáticos en razón a que determina la capacidad de garantizar qué información ha sido modificada desde su creación y sin autorización, en razón a que la información es el recurso intangible más valioso de las organizaciones y en la comunidad. Es de gran importancia que los usuarios enfoquen su atención al grado de vulnerabilidad y seguridad para hacer frente a posibles deterioros y ataques perniciosos a los programas de software y a los sistemas informáticos.

El objetivo general de la tesis fue determinar en qué medida los delitos informáticos guardan relación con el proceso de investigación preliminar en distrito fiscal de Lima norte, año 2019. La investigación fue de tipo aplicada porque se buscó contribuir con los principios normativos en el derecho penal en donde este marco de normas jurídico está representado por un conjunto de reglas que garantizan su cumplimiento a través de la fuerza pública. El derecho penal informático exige a la ciudadanía estar preparado para determinar que el mal uso y aplicación desistemas y programas informáticos crean infracciones, que son sancionados con penas de libertad, en un contexto regulativo a nivel local, nacional e internacional.

La tesis ponderó en vinculo existente entre las variables del estudio, el primer variable denominado independiente: delitos informático, frente a la segunda variable denominado dependiente e identificada como: proceso de investigación preliminar en distrito fiscal de Lima norte. El nivel de indagación fue descriptivo - correlacional debido a que fue realizado desde el planteamiento de sus problemas, objetivos e hipótesis, observándose que las dimensiones y la estructuras de la variable independiente: Los delitos informáticos se relacionan frente a las dimensiones estructurales de las variables dependientes: Proceso de investigación preliminar en distrito fiscal de Lima norte.

El diseño corresponde a no experimental y corte transversal dado que se realizó sin manipular de manera deliberada las variables siendo lo más preponderante la observación de las acciones para poder analizar sus incidencias, características, efectos, relaciones. Vale decir, los elementos se observaron en su hábitat natural. Y se apoya en resultados que ya fueron evidenciados sin la manipulación del investigador. El método científico permitió observar y expresar el problema e hipótesis, para generar resultados. El muestreo de datos fue probabilístico, estratificado y proporcional pero se considera como probabilístico, dado que la muestra fue conformada por categoría poblacional expresada en su totalidad, donde componentes de la muestra tienen la misma probabilidad de ser seleccionados.

El cuestionario se diseñó en base a las interrogantes seleccionadas de las dimensiones de las variables de la indagación; donde su uso estadístico fue desarrollado con Chi-cuadrado que permitió finiquitar los resultados a partir de examinar ambas variables. Se utilizó las pruebas no paramétrica "Chi-cuadrado" con nivel de confianza al 95% y un grado de significancia del 5% hacia arriba y hacia abajo. La investigación evidencio que se hace necesario medir el grado de relación que existen entre las variables, dimensiones e indicadores del estudio.

Para el desarrollo metodológico y temático de la tesis se ha necesitado enumerar y describir la secuencia lógica y estructura de capítulos relacionados con el desarrollo de la presente, siendo los siguientes:

En cap. I: se desarrolló la problemática planteada en la realidad social del tema en estudio, describiendo los posibles problemas a ser planteadas y los objetivos que deben ser alcanzados en la indagación, también se elaboró en contenido de las justificaciones, argumentado su importancia con sus posibles limitaciones.

En cap. II: se desarrolló marco teórico del estudio, con sus respectivos antecedentes nacionales e internacionales, complementados con sus bases teóricas con sus contenidos teóricos, complementados con definición de términos básicos que complementan el valor académico de la investigación.

En cap. III: se desarrolla las posibles hipótesis, tomando como referencia las variables, con posibles conjeturas a ser contratados con trabajos de campo, operacionalizando las variables con sus respectivos conceptos.

En cap. IV: se desarrolló los aspectos relacionados a la metodología de la indagación, considerando su enfoque dentro de la indagación, considerando su Tipo y nivel de estudio, respetando su método y diseño de indagación, su universo poblacional especificando las muestras de la investigación, referenciando a sus técnicas e instrumentos en los datos recolectados.

Capítulo V: se desarrolló los resultados, de manera descriptiva con el análisis inferencial, las discusiones, resultados, posteriormente se desarrolló conclusiones y recomendaciones, referenciando las bibliografías y sus anexos.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la Realidad Problemática.

En las naciones del primer mundo, la globalización y aparición tecnología nuevas en la informática, ofrecen a la comunidad y a las empresas del mercado, un servicio dinámico, oportuno, flexible e interactivo, que a su vez se relacionada con la transferencia, el procesamiento y almacenamientos digitalizados de sistemas informáticos. Permitiendo en tiempo real la viabilidad e interacción de la comunicación entre personas y organizaciones.

En los países de América Latina, la problemática se presentó frente al plano cultural, tecnológico, político, comercial, educativo, económico y social, que es asistido por las tecnologías de información, es, sin lugar a dudas: internet, los sistemas informáticos, las redes sociales, los servicios y plataformas virtuales en celulares y computadoras.

En el Perú, existe un promedio de mil trescientos sesenta Fiscalías distribuidas entre la ciudad de Lima y Regiones Descentralizadas, donde se observaron causas y efectos de problemas a cargo de operadores de justicia y los expedientes de las denuncias ante la presencia de bandas organizadas y el flagelo de la ciber-delincuencia a través del uso equivoco de sistemas informáticos, accesos a datos, base de datos, redes de información, celulares, tecnologías avanzada de multiplataforma, medios interactivos de internet y el ciberespacio de la información para cometer en la ciudadanía actos delictivos a nivel de temor, robos, asaltos, muerte, zozobra, espionaje, chantaje, pornografía a menores de edad, malestar e inseguridad.

La problemática en las fiscalías locales y regionales peruanas exigió la necesidad de combatir, contrarrestar y eliminar la brecha delictiva informática mediante normas y drásticas leyes penales decididas a que contribuyan con el proceso de la investigación preliminar. El avance de sistemas informáticos distribuido en forma local, regional, nacional e internacional supera el paradigma del binomio espacio-tiempo en la relación humana, dado que hoy en día la comunicación se ejecuta al instante y en unidades de tiempo denominadas nanos segundos, sin que la distancia se impedimento.

Por otro lado, la sobre aplicación de las tecnologías y los sistemas informáticos a partir de internet, entre ellos se identificaron las partes o componentes desistemas informáticos como son las estructuras físicas-tangibles y las estructuras lógicas o los programas del software que conforman en conjunto integral al sistema de información. La tabulación de datos genera en los sistemas informáticos los resultados en base a las entradas exigidas por los datos e información. El deterioro mal intencionado físico o lógico a las estructuras y los componentes del sistema informático determinan que las funciones de usabilidad, seguridad, portabilidad, accesibilidad de sistemas informáticos queden totalmente inoperativas.

La administración del Nuevo Código Procesal Penal (NCPP) ha ocasionado en el Perú, cambios organizacionales en el sistema de justicia, así como un cambio en la mentalidad en los Fiscales y Administradores de justicia respecto del modo de ejecutar sus funciones. El rol que aborda el personal fiscal en el manejo de justicia, que esta con integrado por el conjunto de actividades destinados para lograr los fines y objetivos que las normas y la Constitución mandan. Donde se señala que los principios jurídicos son lineamientos generales que condiciona el accionar de operadores de la justicia con el objetivo alcanzar justicia plena.

Los principios que regulan el sistema de justicia están alineados al amparo de la legalidad, que son principios de autonomía, de objetividad, de imparcialidad, de jerarquía y unidad. El desarrollo y crecimiento de la tecnología informática ha traído nuevas formas o nuevos esquemas de delinquir que tienen como objetivo utilizar el computador o el celular para generar distorsiones penales en la ciudadanía y escondidos en el terreno oculto y negativo en la Integridad de Sistemas Informáticos.

En tal razón, ante esta nueva forma delictiva en la seguridad del sistema informático se promulgo la Ley penal especial con el propósito de prevenir y condenar las acciones delictivas que dañan los documentos y cifras de la informática, así como los secretos de la comunicación, y demás recursos jurídicos que resultan perjudicados con estas acciones delictuosas como atentado a los patrimonios, la pornografía en menores de edad, la fe pública y libertad sexual. Para ello, se creó Ley N° 30096 "Ley de delitos informativos. Promulgado el 22 de octubre del 2013 en diario oficial "El Peruano". Posteriormente, fue modificado por Ley N° 30171 "Ley que modifico la Ley 30096, Ley de delitos informativos", promulgado el 10 de marzo del 2014. Es importante ante esta problemática analizar las siguientes interrogantes. ¿Cómo se convierten los sistemas de información en los negocios o empresas? ¿Por qué los sistemas de información son tan esenciales para operar y administrar una empresa? ¿Que comprende la seguridad de sistemas informáticos? ¿Cómo se relaciona internet con la integridad de documentos de información en las organizaciones públicas, privadas y ciudadanía?

Los expedientes documentarios presentados ante los administradores de justicia en el poder judicial de Lima norte identifican las incidencias y las secuelas del problema ante la falta de una Ley penal contra delitos a la seguridad desistemas informáticos, relacionados con el proceso de indagación preliminar en los expedientes judiciales.

Este marco judicial penal valoró el contexto de la problemática entre los operadores de la justicia como: Fiscales, Jueces y Policías al no disponer o poseer de capacitación técnica, entrenamiento, cultura y principios de las leyes y normas penales de delitos en la seguridad de documentos informáticos y la fundamentación en el proceso de indagación preliminar. El espacio de la problemática identificó que no se valora la importancia, los roles y las características relacionados con la vulnerabilidad de las informaciones en los sistemas informáticos. Como parte del problema se observó la falta de administración y control en las redes de datos que permitan definir sistemas de seguridad, que limitan la verificación a la seguridad de documentos informáticos.

El incremento acelerado de usuarios y su fácil acceso a los medios tecnológicos e informáticos. El uso secreto de cibernautas pone en dificultad la persecución de las acciones

ilícitas cometidos mediante el uso de este medio. La comodidad para acceder a la documentación para tergiversar la información, destruir los sistemas y bases de datos, presencia y constante vulnerabilidad a las estructuras y componentes de la integración a los sistemas informáticos.

En tanto, el Informe de 12º Congreso de Naciones Unidas respecto a la Previsión de Delitos y Justicia Penal, señala por qué con los avances tecnológicos viabilizan una modalidad nueva de cometer ilícitos penales como fraudes y la comercialización de pornografías infantiles, que amerita la tipificación delitos nuevos como el mal uso de redes informáticos, para enviar correos denominados basuras, la captura de datos "pishing", la piratería digital, la difusión malévola del virus y atentados contra las instalaciones de sistemas electrónicos de información. Pero, resulta importante observar la necesidad de que los delitos informáticos debieran comprenderse como comportamientos delictivos, donde la computadora o celular es la herramienta u objeto de hecho.

Se observó a los delitos informáticos como un delito de criminalidad organizada que se encuentran directa o indirectamente, relacionados al proceso electrónico de datos, lo cual es cometido con uso de equipos electrónicos para procesar datos.

La delincuencia informática debe ser evaluada como aquellos delitos que están dirigidas a burlarse de sistemas de seguridad, invadiendo las informaciones en las plataformas virtuales, correos o sistemas de datos manipulando claves de acceso, conductas atípicas que se cometen mediante la mala utilización de las tecnologías de la información y comunicación.

La evaluación de la problemática se observó entre los operadores de justicia que necesita comprender que derecho sustantivo representa una serie de normas que son conocidas y admitidas, por medio de diversos sistemas jurídicos que dan seguridad y certeza a las personas, a su vez, se refiere sobre el fondo del asunto, que reconoce los derechos y obligaciones. Este tipo de derechos son aquellas que se encuentran en normativas que dan vida a determinadas figuras jurídicas. En ese sentido cabe evaluar que el derecho adjetivo, representa normativas destinadas a garantizar el ejercicio del derecho y cumplimiento de obligaciones que se encuentran consagradas en el derecho sustantivo. En tanto el derecho adjetivo, está constituido por mecanismos procedimentales que permiten hacer valer los derechos, dando mayor efectividad a dichas relaciones.

El contexto de la investigación se presentó como necesidad el medir la relación entre la variable independiente que son los delitos informáticos y la variable dependiente que representa al proceso de la investigación preliminar en el ministerio público de Lima norte. Fortaleciendo, el dispositivo a evaluar corresponde a lo que señala el art. 4. Sobre el atentado a la seguridad del Sistema Informático de la Ley Penal Nº 30171. Que de manera discutida e ilegítima, inutilizan, total o parcialmente, los documentos informáticos, que impiden accesos limitando su funcionamiento y la prestación del servicio, que es sancionado con penas efectivas de libertad no menor de tres años, ni mayor de seis años, con multas a 80 a 120 días de multa

En tal sentido, la problemática quedó identificada frente a la baja relación existente que se genera entre la variable independiente denominada como norma de delitos informáticos y la variable dependiente denominada como proceso de investigación preliminar en distrito fiscal de Lima norte. Es una necesidad que operadores de justicia examinen la investigación preliminar porque ésta comprendió las huellas iniciales de toda indagación penal, esto hace referencia a primeras declaraciones del inicio, actividades investigativas que asegura los elementos de prueba, que serán sustanciales para la evaluación del fiscal para la acusación o cancelación de la causa. Luego, surge la interrogante principal: ¿En qué medida los delitos informáticos se relaciona con el proceso de investigación preliminar en distrito fiscal de Lima Norte, 2019?

Esta tesis está relacionado con el “derecho penal porque contribuye con un gran despertar entre los operadores de la justicia y la ciudadanía y el interés de una profunda especialización de la materia a fin de contribuir a combatir y eliminar la criminalidad delictiva en la integridad desistemas informáticos utilizando como apoyo el marco legal eficiente para que logre generar paz, tranquilidad y prosperidad en nuestra sociedad peruana.

1.2 Delimitación de la investigación

Luego de analizar problemas planteados en el estudio planteado para su indagación, con la finalidad de cumplir con la metodología propuesta, se delimita de la siguiente manera.

1.2.1 Delimitación espacial

La presente indagación se realizó en el ministerio público de Lima norte, donde se realizaron denuncias penales por la comisión especializada de atención a los delitos informáticos.

1.2.2 Delimitación social

Esta tesis en su desarrollo involucró a los operadores de la justicia penal como: fiscales, abogados litigantes y la policía nacional y la sociedad, en razón a que ambos trabajan con los registros y expedientes documentarios en la el Distrito Fiscal de Lima Norte.

1.2.3 Delimitación temporal

El trabajo de tesis fue desarrollado entre meses de julio de 2019 a febrero del 2020, dividido en dos etapas.

Primera etapa

Del mes de julio a setiembre del 2019, se cumplió con etapas planificadas del plan de tesis, vale decir; se elaboró el planteamiento de problemas, describiendo la realidad problemática basado en las delimitaciones, los problemas en forma de interrogantes, los objetivos a ser alcanzados, con su respectiva argumentación de la viabilidad, elaborando las bases teóricas.

Segunda etapa

En los meses de octubre del 2019 a febrero del 2020, se desarrolló las hipótesis referenciando las variables, respetando los protocolos metodológicos de la indagación, respecto a conclusiones y recomendaciones.

1.2.4 Delimitación conceptual

En el presente estudio se desarrolló los fundamentos teóricos, análisis de casos, referente a las investigaciones cuantitativas relacionado a delitos informáticos y el proceso de la investigación preliminar en distrito fiscal de lima norte, 2019.

- **Delitos Informáticos.**

  Son conductas típicas y antijurídicas, medio por el cual los sujetos de mal vivir que ingresando al sistema informático comete delitos, en contra de personas naturales o personas jurídicas. Al desarrollo acelerado de la tecnología, ha permitido en mal uso del sistema informático, para poner en peligro los bienes protegidos. Jiménez (2017)

- **Investigación Preliminar**

  Se denomina investigación preliminar, toda indagación inicial, cuando la denuncia es recibida por las autoridades competentes, o en su defecto en ministerio público inicia indagación de oficio ante las evidencias conocidas, según la gravedad del caso la fiscalía puede actuar con celeridad, para ello, contando con apoyo policial. (Pablo Sánchez, 2017).

1.3 Problema de la investigación

1.3.1 Problema principal

¿En qué medida los delitos informáticos se relacionan con el proceso de investigación preliminar en distrito fiscal de Lima Norte, año 2019?

1.3.2 Problemas específicos

a) ¿De qué manera los delitos informáticos se relacionan con las declaraciones realizadas en el proceso de investigación preliminar en el distrito fiscal de Lima Norte, año 2019?

b) ¿De qué manera los delitos informáticos se relacionan con los plazos establecidos en el proceso de investigación preliminar en distrito fiscal de Lima Norte, año 2019?

c) ¿De qué manera los delitos informáticos se relacionan con el aseguramiento de pruebas en el proceso de investigación preliminar en distrito fiscal de Lima Norte, año 2019?

1.4 Objetivos de la Investigación:

1.4.1 Objetivo General

Determinar la medida en que los delitos informáticos se relacionan con el proceso de investigación preliminar en distrito fiscal de Lima Norte, año 2019.

1.4.2 Objetivos Específicos

a) Determinar la manera en que los delitos informáticos se relacionan con las declaraciones realizadas en el proceso de investigación preliminar en distrito fiscal de Lima Norte, año 2019.

b) Determinar la manera en que los delitos informáticos se relacionan con los plazos establecidos en el proceso de investigación preliminar en el distrito fiscal de Lima Norte, año 2019.

c) Determinar la manera en que los delitos informáticos se relacionan con el aseguramiento de pruebas en el proceso de investigación preliminar en el distrito fiscal de Lima Norte, año 2019.

1.5 Justificación e importancia y limitaciones de la Investigación:

1.5.1 Justificación

El estudio encuentra su justificación, debido a que busca respuesta mediante el análisis de las variables de estudio, por lo que para dar respuesta las líneas de investigación se desarrolla los siguientes tópicos.

Justificación teórica

El estudio aportó argumentos teóricos prácticos que permitirán al ministerio público, conocer la aplicación real de la implementación de la norma respecto a los delitos informáticos y su incidencia con el proceso de la investigación preliminar. Utilizar el contexto del derecho sustantivo que tipifica el fondo de la cuestión para reconocer derechos y obligaciones. El uso del derecho adjetivo el cual tiene como característica primordial regular las acciones jurídicas «poniendo en agenda la actividad judicial», vale decir, una serie de normas que rigen las actividades en los tribunales, los reclamos planteados conformes los requisitos.

La problemática analizó y comprendió, la indagación de alta tecnología de la Policía Nacional del Perú, creada para combatir delitos informáticos, que tienen que ver los casos relacionados con instrumentos tecnológicos. Tienen capacidad técnica y metodológica para desarrollar las actividades involucradas. Por otro lado, se sabe que la fiscalía no tiene un área especializada, para prevenir los atentados contra la seguridad de documentos informáticos. Por lo que, existe un vacío institucional porque no se tienen a tiempo tecnología, personal, materiales y equipos, recursos financieros, y especialistas preparados para perseguir este contexto o campo relacionado a las agresiones a la integridad dedelitos informáticos.

Cabe precisar también, que existen delincuentes especializados que desaparecen todas las huellas de su participación en acciones delictivas. Ostentando información privilegiado que la convierten en un espacio idóneo

para cometer distintos ciber-delitos. Asimismo, lo idóneo está determinado por el caudal de información acumulada y el fácil acceso que se tiene a él, provocando lo que ya se conoce como delitos llamadas ciber-delincuencia.

Social

Respecto a la sensibilización social, la indagación sobre el crimen y la delincuencia informática o la ciber-delincuencia conforman una fuerte corriente delictiva de última generación y que afecta con voracidad a personas, organizaciones y sociedad a nivel global, nacional y local. Miró (2012). En su obra El ciber-crimen y criminología de delincuentes en ciberespacio, definen el crimen informático como actividad dirigida para evadir los sistemas de seguridad, es decir, invasión a computadores y correos o expedientes mediante las claves de accesos; conductas típicas que son acometidos mediante el uso de las tecnologías.

Metodológica

Respecto a la justificación metodológica, se hace uso de la guía oficial que propone la Universidad, por medio de su escuela de Posgrado, que considera en el desarrollo de la investigación formulación de problemas y objetivos, con el único propósito llegar a resolver los interrogantes planteados.

Legal

Respecto al delito informático es un delito que vulnera la privacidad y el patrimonio de las personas, cuenta con base jurídica en el art. 2 de la carta magna del Perú, donde se señalan defender el aspecto privado de personas jurídicas y personas naturales. La Ley Penal sobre delitos informáticos Nº 30171, modificados por Ley Nº 30096, Ley de delitos informáticos, describen delitos informáticos en el sistema jurídico del Perú.

Cabe reiterar la importancia de la indagación, dado que es obligación del Estado proteger la privacidad de información personal. El Estado, por intermedio de la carta magna en su artículo (Art.2, numeral 6 y 10) sostiene como derechos humanos de

personas, la no difusión de información que afecte, integridad personal y familiar además, sus comunicaciones y documentos privados.

Practico

Respecto a la justificación práctica, se organizó el trabajo maximizando metodológicamente la calidad y calidad de la comunicación, evitando en error sistemático, de tal forma que se puede monitorear a las personas que cometen delitos informáticos, aprovechando su autonomía.

1.5.2 Importancia

Esta tesis es importante porque a través de su análisis, referencia, evaluación permitió formular y plantear acciones concretas, tendientes a buscar opciones de solución ante los altos índices de la presencia del flagelo ciber-delincuencia.

Actualmente, la informática se ha diversificado a nivel universal. Tanto en sector privado y sector estatal, en sector académico, a nivel de indagación científica, el uso de la informática se ha convertido en imprescindibles, mediante el internet nace una gran tecnología que permite desarrollar la cultura y la ciencia para los seres humanos, asimismo, nace la ciber-delincuencia, lo que se conoce como “delitos informáticos”. La infracción que cometen los ciber-delincuentes son variadas, viendo las estadísticas se puede colegir, que el uso de las redes por las mafias internacionales es dominado por los criminales que maneja la prostitución infantil.

En el nivel del estudio de la integridad sobre los sistemas informáticos, que desarrollan las tecnologías informáticas ofrecen aspectos negativos, porque, se ha generado actitudes antisociales y delictivas. Los sistemas operativos que ofrecieron nuevas oportunidades, pero complicadas que infringen la ley creando posibilidades de acometer delitos de tipo tradicional de maneras no tradicionales. La importancia también radica desde el desarrollo de las nuevas tecnologías, que ha abierto puertas para los delincuentes. El avance desmedido de las tecnologías, las mafias han utilizado para manipular, utilizando de manera indebida las informaciones para lucrar con negocios ilícitos.

De este modo la informática se ha vuelto indispensable para la sociedad en general, ventana que aprovechan los delincuentes para cometer sus delitos, en tal sentido se requiere, legislaciones específicas para combatir este ciber-delito.

1.6 Factibilidad de la investigación

Para la ejecución y desarrollo de esta indagación fue necesario oportunamente disponer de recursos como el investigador, el docente y el personal académico de la organización educativa universitaria. Gran parte de investigación desarrollada por el investigador, basándose en libros y Códigos actualizados para el resultado eficiente del presente. Siendo los recursos financieros y económicos fueron únicamente asumidos por el investigador. Los materiales necesarios como libros, revistas, equipo de cómputo, material de oficina y ofimático fueron de gran soporte para preparar y elaborar el presente estudio.

1.7 Limitaciones del estudio

Como en toda investigación, existieron limitaciones, sin embargo, la parte presupuestal fue financiado por el investigador por lo que el informe final fue culminado en tiempo establecido.

Tiempo.

Respecto al tiempo estimado para desarrollar esta investigación, fue estrictamente cumplido conforme el cronograma establecido, por la escuela de posgrado, por lo que no fue terminado en el tiempo establecido.

Material.

Para desarrollar el trabajo, no hubo limitaciones respecto a los materiales, debido que toda la logística fue financiada por el investigador.

Personal.

El recurso humano que formó parte de esta investigación fue seleccionado por conveniencia, dado que es complicado convencer a las personas para ser parte de un proyecto, sin embargo se con el apoyo por lo que se pudo terminar con éxito el trabajo.

CAPÍTULO II: MARCO TEÓRICO CONCEPTUAL

2.1 Antecedentes del Problema

2.1.1 Antecedentes Internacionales

Gonzales (2013). Delincuencia Informática: Daños Informáticos del Artículo 264 Del Código Penal y Propuesta de Reforma. España. Este estudio fue desarrollado en campo jurídico penal, para precisar actos cometidos delictuosos cometidos utilizando sistemas informáticos. Considerando como parte fundamental, de derecho como elemento reguladores de las socializaciones, pero que no pueden ponderarse los diversos sistemas convivencia respecto a los delitos informáticos. Haciendo un poco de referencia historia, por la mitad del XX, evoluciona la informática, acelerando el desarrollo de la sociedad y alterando el modo de vida de pobladores, creando una culturad de dependencia tecnológica y cambio de conducta de las sociedades. En otro sentido, aparecen los delincuentes que aprovechan las bondades de la informática para cometer dolos, siendo de obligado participación de la ciencia del derecho en materia de delito informático.

Montaño (2008). La Problemática Jurídica en la Regulación de Delitos Informáticos. Tesis. México. En su tesis abordo el análisis de las normas jurídicas respecto al crimen organizado que hace uso de la tecnología para cometer delitos como lavado de dinero. En tal sentido, se analiza el art. 400 del Código Penal Federal. Lo cual los legisladores reformaron concerniente a los delitos, regulando de manera específica los términos de prescripción, de delitos graves, permitiendo de esta manera su correcta aplicación. Permitiendo de esta forma, el desarrollo de la sociedad respecto a la

tecnología informática, que ha simplificado las actividades de pobladores, con solo usar un computador. En estos momentos, todo el universo está invadido por la tecnología, el uso del internet, se ha hecho popular en cada rincón del mundo, que permite comunicarse en tiempo real. Empero, los delincuentes, también han hecho lo suyo, hacen mal uso de la tecnología para cometer delitos informáticos, estos delincuentes organizados, utilizan las tecnologías para fines ilícitos, utilizan el sistema operativo para cometer robos, fraudes, estafas financieras, falsificación de identidades, muchos otros delitos que se encuentran penados en la legislación mexicana.

Ureta (2009). Retos a superar en la Administración de Justicia ante los Delitos Informáticos - Ecuador. El autor tuvo como propósito analizar la visión universal respecto a delitos informáticos en Ecuador. En relación a su reglamentación, en cuanto al delito informático, en la formación de especialistas, son retos, que la doctrina jurídica pone énfasis para tratamiento. Este estudio aporta, conceptos doctrinarios sobre crimen informático, así como las leyes relacionadas en la legislación ecuatoriana en general. Asimismo, explica iniciativas que convergen en forma de proposiciones y recomendaciones fuera de contexto para hacerle frente a los delitos informáticos, de igual manera hace un análisis jurisprudencial respecto a los países latinoamericanos de que forman están afrontando el delito informático. Por último, observa retos a nivel de conformación, dificultades de tecnologías, dentro del marco legal que los ecuatorianos deben superarse para combatir delitos tecnológicos.

Chávez (2012). Policía Cibernética: Vigilancia preventiva, permanente y reactiva a los ilícitos Informáticos (Tesis de pregrado). Universidad Rafael Landívar, Guatemala. En su tesis la investigación versó sobre seguridad y expedientes informáticos y delitos relacionados al desarrollo de una investigación tecnológica y las autoridades encargados de la prevención, identificación y corrección. La investigación pondera la seguridad informática y su propósito de sustentar su integridad, su reserva, su privacidad, control y su originalidad respecto a las informaciones controladas por el computador, así como los delitos informáticos como elementos vitales para temas que se investigan. Es un reto constante para aquellos que optan por identificar y examinar la prueba digital para hallar la verdad, ya que la prueba electrónica es un instrumento de prevención muy especial para poder conservar las medidas preventivas necesarias para no infectar y que no sean motivo de descalificación durante un proceso litigio. La seguridad pública se encuentra

resguardo por el estado, encargado en el momento que toca prevenir los problemas de orden social y para alcanzar los objetivos planteados de manera eficaz de parte de la policía, y el procedimiento del poder judicial, de políticas públicas y de la realidad social. Para poder ofrecer y preservar el orden y la tranquilidad a la sociedad, el caos y los delitos cometidos por los criminales.

Rincón (2015). El delito en la ciber-sociedad y la justicia penal internacional. Madrid, España. El autor en su tesis, propuso elaborar bases teóricas desde la concepción dogmático penal de nivel internacional, permitiendo discernir la necesidad de incorporar dentro de la indagación en materia de juzgamiento sobre delitos informáticos y las telecomunicaciones, conforme sentencia el Estatuto de Roma. En esta indagación, el autor señala la importancia de la información en la aldea global llamado ciber-sociedad que ha obligado al derecho crear nuevos conceptos jurídicos para combatir los delitos informáticos. Posteriormente, el autor recorre en su estudio la legislación comparada en los países de habla española, especialmente la sudamericana, tomando como referencia muchas de ellas, europeas y latinoamericanas, con finalidad conceptualizar las conductas universales consideradas delitos dentro del comportamiento informático y así como de las penas y evoluciones legislativas. Finalmente se busca materializar la ejecución de la justicia penal internacional respecto a los ilícitos perpetrados en ciber-sociedad, donde precisamente, esta investigación cumple su propósito final, que propone juzgamiento de ciber-delitos, mediante un órgano de orden mundial donde conflictos jurisdiccionales no impidan la sanción de ilícitos cometidos alrededor del mundo.

2.1.2 Antecedentes Nacionales

Angulo (2016). Licitud en la obtención de voz, imagen u otros medios, en marco del Derecho a la intimidad personal a nivel del Código Penal Peruano - Perú. El autor preciso los fundamentos jurídicos-doctrinarios respecto a la licitud para obtener pruebas no autorizadas, cualquiera sea los medios; voz, imagen, que vulnere los derechos a la intimidad personal, por carecer del interés público, como un aporte para la comunidad. De tal modo, que el autor pondera la forma de obtener de manera no autorizada de pruebas de voz o imagen resulte razonable que sea de interés para la sociedad, su obtención será lícita de manera excepcional, soslayando el delito de violación a su

intimidad que esta normado y tipificado en art. 154 de Código Penal Peruano. En ese sentido el estudio se centra en el campo doctrinario y jurisprudencial para demostrar las hipótesis planteadas. De esta manera, el autor logra determinar los aspectos por los cuales se pueden argumentar la licitud respecto a la forma de obtener pruebas no autorizadas sean de voz o imagen por cualquier modalidad, valorando que se tipifique como delito del vulneración a la intimidad individual tipificado en Art. 154 de Código Penal. Aclarando claro está, por contribuir a la sociedad y que sea de interés público.

Sequeiros (2015). Vacíos Legales Que Imposibilitan La Sanción deDelitos Informáticos En El Nuevo Código Penal Peruano - Huánuco, Perú. El autor en su tesis se desarrolló la nueva modalidad de crimen llamado delitos informáticos. Respecto a esta modalidad delictiva, se ha publicado diversas normas, para poder fiscalizar y sancionar malas acciones de las personas que mellan el sistema informático, violando la reserva de la comunicación, y bien jurídicos protegido que resultaran perjudicados con este accionar delincuencial respecto a los patrimonios, de libertar sexual de las personas y preservación de la fe pública. Al respecto la Ley N° 30096, que tipifican los ilícitos informáticos, se promulgo el año 2013, parcialmente modificada por la Ley N° 30171, respecto a los delitos informativos que especifica las penas. Sin embargo, las conductas desarrolladas en el mundo informático, no implican negar ventajas brindadas a la justicia por el sistema informático. Cabe reconocer las ventajas que ha traído los avances tecnológicos para la comunidad. Empero, el desarrollo tecnológico creo diversos modalidades de acometer delitos informáticos como; fraudes y dolos que facilitan la comisión de nuevas modalidades de delitos.

Romero (2005). Marco conceptual de delitos informáticos - Lima, Perú. El autor señala en su tesis, la desarrollo de un nuevo marco teórico respecto a delitos informáticos y principales forman que involucran su utilización como punto de apoyo jurídico-científico para quienes legislan la justicia y otras organizaciones gubernamentales comprometidos en la lucha contra el ciber-delito. En tal sentido, el autor considera como casos de estudio, las concepciones teóricas recopilados por el INEI, por su parte, los autores, Julio Núñez, Julio Téllez y Blossiers Calderón, hicieron público sus estudios respecto al Internet. Ponderan como arte los Delitos Informáticos fundamentados varios especialistas en el tema. En tal sentido, el estudio presento una propuesta novedosa respecto al marco conceptual, los delitos

informáticos, las conclusiones y recomendaciones para perfeccionar el nuevo marco teórico.

Parra (2016). Proyecto legal para un esquema nacional de ciber seguridad. Lima, Perú. El autor en su tesis desarrolla sobre la Seguridad Nacional, como garante principal, que permite adoptar medidas pertinentes para la implementación y aplicación de la legislación, conforme al entorno internacional. El autor pondera el análisis sobre Ciber Delitos, en el escenario internacional. Al respecto la OEA clasifica como delitos, el impacto negativo en la economía por los ataques deciber delincuentes. Por lo que ha recomendado a las naciones modernizar sus legislaciones del Derecho cibernético, con el esquema de Ciber seguridad. En tal sentido, esta investigación, demostró que internet y las TICs han alterado las normas de convivencia, rebasado la falta de reglamentación en delitos penales de Cibernética. Que ha aumentado de manera exorbitante los Ciber crímenes y los delitos informáticos, donde la soberanía de países se ve amenzada. Finalmente, el trabajo recomienda aplicar nueva normativa que haga posible contrarrestar las secuelas en situaciones de tensión y ciber ataque.

Pardo (2018). Tratamiento jurídico penal de delitos informáticos contra el patrimonio. Lima, Perú. El autor en su indagación tuvo como propósito analizar la ponderación jurídico penal respecto a los delitos informáticos contra los patrimonios. En tal sentido, el autor utilizó la técnica de entrevista para recolectar datos, con guías elaboradas de entrevistas respecto a temas nacionales e internacionales, llegándose a conclusiones precisas. El tratamiento jurídico penal respecto al delito informático es deficiente, dado que dentro del fraude informático no se especifican las particularidades de delitos informáticos. Lo que genera desconcierto en la interpretación, de las normas que omiten una sanción efectiva de delitos informáticos. En tal sentido, cabe recomendar a los congresistas de la republica que pudiera formular, iniciativas legislativas para legislar en forma adecuada conforme a las modalidades, sean éstas, fraudes, estafas, sabotajes o hurtos informáticos.

2.2 Bases Teóricas o Científicas

Ley Penal de Delitos Informáticos Nº 30171 que modifica a la Ley Nº 30096 del Código Penal

Ley N° 30171. Ley que modifica la Ley 30096, Ley de Delitos Informáticos. La presente Ley tiene por objeto, modificar los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096, Ley de Delitos Informáticos en los siguientes términos:

"Artículo 2. Acceso ilícito. El que manera deliberada e ilegítima accede a todo o en parte a un sistema informático sin autorización, infraccionando las medidas de seguridad que son establecidos por la autoridad competente para prevenirlo, quienes cometen los ilícitos serán reprimidos con penas efectivas de libertad no menor de 1, ni mayor de 4 años

"Artículo 3. Quienes atenten contra la integridad de documentos informáticos. El que de manera deliberada e ilegítima mella, introduce, borra, deteriora, altera, suprime o hace inaccesible los documentos de informática, serán reprimidos con penas privativas de libertad no menor de 3, ni mayor de 6 años

"Artículo 4. Quienes atentan contra la seguridad de sistemas informáticos. El que de manera deliberada e ilegítima daña, total o parcialmente, los documentos informáticos, impidiendo los accesos o entorpeciéndose sus funcionamientos, limitando las prestaciones de servicios, serán reprimidos con pena privativa de libertad no menor de 3, ni mayor de 6 años.

"Artículo 5. Quienes hacen proposiciones indecentes a adolescentes con fines de explotación sexual por medios virtuales. Quienes contactan menores de edad mediante internet, para solicitar prostituirlo mediante materiales pornográficos, con consecuencia actividades sexuales. Por lo que fueron reprimidos con una pena efectiva de libertad no menor de 4, ni mayor de 8 años.

2.2.1 Delito Informático

Se típica como delito informático, toda actividad ilícita cometidas por el mal uso del sistema informático en contra de personas naturales o personas

jurídicas, violando las normas existentes, por lo que son pasibles de ser sancionados por el derecho penal.

En tal sentido, Jiménez (2017) nos define el delito informático como conducta típica y antijurídica, que aprovecha el delincuente para cometer los ilícitos. Que el delincuente ingresa al ciber-espacio mediante uso del sistema informático, comete delitos, lesionando y poniendo en peligro bienes jurídicos convencionales y no convencionales culpablemente, protegidos por la ley de la materia (p. 137)"

Los delitos informáticos inciden en actos criminales que al inicio las naciones han pretendido obviar sus acciones tradicionales, tales como; hurto, fraude, falsificación, estafa, sabotaje, entre otros., empero, debiera ponderarse que el mal uso de las computadoras han propiciado las necesidades de regular desde el derecho.

El desarrollo tecnológico que ha recibido la sociedad, les ha permitido a los delincuentes evolucionar en formas diversas de infringir la ley, que da lugar, a diversas infracciones tradicionales con el emerger de nuevos delitos. Esta realidad ha ameritado la necesidad de debatir la necesidad de especificar los ilícitos informáticos del resto de las infracciones para un tratamiento dentro de la normativa legal. Los delitos informáticos en su sentido amplio son "conductas criminales que en sus delitos hacen usos de las tecnologías informáticas ya sea como métodos en un sentido más prestiño, el delito informático, es "todo acto ilícito penal que en las plataformas virtuales, sus técnicas y funciones cumplen un papel, un método, medio o fin".

Otra conceptualización de delitos informáticos, en formas típicas y atípicas, entendido en las formas típicas son "conductas típicas, antijurídicas y culpables, que tienen las computadoras como instrumento"

Tal como se puede apreciar los nuevos conceptos que establecen los autores, empero, perduran conceptos de índole universal propia de delitos informáticos, empero se debe valorar que han sido logrados con esfuerzo de las autoridades que

se han ocupado de la situación y han precisado conceptos prácticos y modernos especificando problemas nacionales, tipificando el encasillamiento de parte de delitos informáticos.

Las infracciones informáticas, son más sofisticados cada vez más, debido a la vulnerabilidad que presentan los sistemas, en el campo deusuarios, dado que "los gobiernos en su conjunto son millones de usuarios que utilizan esta tecnología para desarrollarse en sus funciones diarias. la seguridad en internet se transforma en un trabajo crítico que ocasiona estragos en la vida diaria. Cada día se realizan miles de agresiones que se materializan por países, naciones, gobiernos, y ciber-delincuentes". (López, López & jerónimo, 2017).

Lamperti (2017) precisa que son hechos que constituyen delitos cuando son relevantes jurídicamente, que se relaciona con cualquiera de hechos para ser tipificado como delito debe estar regulado en el código penal; en consecuencia, podría decirse que los hechos encuadras en un tipo penal, que se identifica como principio de legalidad, donde el letrado tiene la prohibición de sancionar otras acciones que no están tipificadas en la normativa penal (p. 85).

Levin y Ilkina, (2013), el ciber-delito llamados delitos informáticos, son tipificados como crimines, donde las tecnologías de las informaciones y la comunicaciones son utilizados como herramientas para cometer delitos, en este caso, el propósito de la comisión del delito es apropiarse del sistema de almacenamiento de la información (p. 14).

Villavicencio (2014) señala que la crimen cibernético es una acción dirigida sobre un propósito que tiene como finalidad burlar los sistemas de seguridad, que significa invadir los archivos almacenados en las memorias de las computadoras, apropiándose de las claves que permiten acceder, con el uso de sofisticados software que rompen cualquier sistema de seguridad. (p. 286). En tal sentido, Laredo & Ramírez (2013) señalan que el "delito informático es el uso de todo sistema informático como instrumento de un delito" (p. 45).

Ramírez y Castro (2018) señalan que: el “los delitos informáticos son todos aquellos actos antijurídicos y de carácter culpable que se da por métodos informáticos que manipula o dañan las memorias de computadores, en redes de internet o medios electrónicos” (p. 57). Los delitos informáticos implican actividades ilícitas que las naciones han enfrentado sin valorar sus alcances. Dado que no son delito cualquiera que deja evidencias como delitos tradicionales que se puede valorar con las pruebas, sino, que son delitos cometidos en tiempo real de un país a otro sin salir de casa, con el uso de las herramientas tecnológica.

El delito cibernético involucra diversos actos ilícitos que las autoridades depaíses han tratado de priorizar, sin embargo su error radica en el aspecto penal, al no estar tipificados los delitos informáticos, toda ez que se pretende tipificar con delitos tradicionales como: robo, fraude, estafa, entre otros, en tal sentido, lo que las autoridades tienen que hacer es modernizar sus normativas de tal forma que pueden enfrentar a los criminales con el uso de las herramientas tecnológicas.

Delincuencia y criminalidad informática

Para Carlos Sarzana, “criminalista e tecnología”, los delitos cometidos por computadora corresponde a “cualquier comportamiento criminógeno, donde la computadora como objeto ha estado involucrada como material probatorio en la acción criminógena, o como un simple símbolo”, en consecuencia, en esta descripción las sujetos que cometen delitos o crímenes informáticos, están comprendidos dentro de lo que se tipifica como criminología, y la investigación de dichas infracciones, están sujetos a las ciencias criminalísticas.

Es preciso reconocer la diferencia entre la criminología y la criminalística; la criminología refiere de investigar el por qué y que fue lo que ocasiono al individuo a cometer esa infracción, mientras que la criminalística según Montiel sosa, se definen como “ciencia multidisciplinaria que posee conocimientos generales, de manera sistemática ordenados, verificables y experimentables, para poder estudiar explicar y predecir la manera, dónde, cuándo, quién o quienes cometen”, la

criminalística al ser multidisciplinaria es aplicado en temas de balística, medicina forense, física, química, incluido la informática.

Conocer el comportamiento de cómo los incidentes de seguridad, las vulnerabilidades y la criminalidad informática, es vital para el análisis de delitos informáticos, ya que han tenido un repunte a los largo de últimos años, por ello, se requiere analizar la tendencia de dichos componentes.

Crimen organizado con uso de la informática ha crecido de manera acelerada, de acuerdo con los informes relacionados con incidentes de seguridad, vulnerabilidades identificadas de altos costos que estos involucran para la empresa, los mismos, que utilizan en beneficio propio los intrusos, estos facinerosos conocen al detalle las bondades que ofrece la tecnología, saben aprovechar muy sus limitaciones para aprovecharlos malévolamente para delinquir, son astutos que desaparecen las pruebas en tiempo real.

Como fue señalado con anterioridad algunos enfoques doctrinales, señalan el delito informático, como una pluralidad de modalidades actividades vinculadas, de alguna manera con los computadores.

Las normas respecto a delito informático deben ser usadas de manera plural, para poder atender la multiplicidad de conductas ilícitas, no solamente los de carácter general, cuando se determina las referencias unas modalidades en particular.

Sujetos del Delito Informático

En derecho penal, la aplicación de la conducta punible refiere a la existencia de dos personas, es decir, un sujeto activo y otro pasivo. Quienes pueden ser personas naturales o jurídicas, de esta manera, el bien jurídico protegido es en definitiva el instrumento localizador de las y de su posición frente a los ilícitos. Así, el titular del bien jurídico perjudicado será la persona pasiva, quien puede diferir de la persona perjudicada, el cual circunstancialmente, ser un tercero.

Por otro lado, quien lesione el bien que se protege, mediante la realización del tipo penal, será el infractor o sujeto activo.

Sujeto Activo:

Mario Garrido Montt, señala al sujeto activo, como aquella persona que realiza toda o una parte de la infracción descrita por el tipo penal. las sujetos que cometen los "delitos informáticos" son personas que poseen algunas características que no algunos de ellos son el denominador común de delincuentes, estos llamados sujetos activos son hábiles para manejar los sistemas informáticos y por su condición laboral están ubicados en lugares estratégicos donde se manejan informaciones de carácter sensible, o bien son hábiles para el uso de sistemas informáticos, aun cuando, en muchos de casos, no realicen actividades laborales que ocasionan la comisión de este tipo de delitos. Con transcurrir del tiempo ha sido comprobado que los autores del delito informático son muy variados y se diferencian entre sí, conforme la naturaleza de delitos que los diferencia entre sí, respecto a la naturaleza de delitos cometidos. de esta manera, la persona que delinque con uso de sistema informático, desviando fondos de las cuentas de clientes a cuenta de terceros.

Sujeto Pasivo:

Se denomina como tal al sujeto titular del bien jurídico que el operador de la justica protege y sobre quien recaen las acciones típicas del sujeto activo. Se tiene que distinguir en primer término que sujeto pasivo o víctima de ilícitos es el ser sobre el cual recae la culpabilidad de las acciones u omisiones que realiza el sujeto activo, y en caso específico del delito informático, las víctimas pueden ser personas, instituciones de crédito, estados entre otros, que usan sistemas informáticos automatizados, generalmente conectados a otros. En tal sentido, el sujeto pasivo del ilícito, su aporte es muy importante dado que por de sus actividades se puede identificar los diferentes delitos que cometen los delincuentes informáticos, para poder prevenir estas acciones, se necesita acciones concretas de las autoridades para descubrir el modus operandi de sujetos activos. Ya que es complicado conocer la verdadera magnitud de este tipo de delitos informáticos que muchas veces no se puede descubrir, por lo mismo que no son denunciados ante las autoridades, a esto se puede agregar en algunos casos falta de normas específicas, que de protección los bienes individuales y colectivos, muchas

veces ante el temor de ser expuestos, por cuidar el prestigio de sus empresas, este tipo de delitos mantienen como cifra oculta en la auditoria de sus empresas.

Tipos de Delitos Informáticos

Se conocen diversos tipos de delitos informáticos, con comportamientos diferentes, es evidente que dentro de estas modalidades existentes, hay tres condiciones que son las más importantes dado que permite desarrollar toda una estrategia. Conforme señala Camacho Losa, el primero, es la imaginación del autor para idear el delito, segundo su capacidad técnica para identificar las acciones y tercero conocer las deficiencias de control existentes en las empresas, cuyas instalaciones son vulnerables, respecto sus redes informáticos. En tal sentido, los delitos informáticos, crecen cada día y las normas pertinentes para sancionarlos quedan desfasados en el tiempo, por lo que las autoridades tienen que estar a la altura de las circunstancias.

- **Los Fraudes**

  Este concepto se refiere a los datos paralelos llamados falsos o engañosos (data diddling), que el código penal tipifica como introducción de datos falsos, mediante manipulación de datos a los sistemas operativos en el computador de las empresas con la finalidad de introducir operaciones falsos sin el conocimiento de las empresas. Este tipo de fraudes en la empresa, se convierte en delito informático más común, debido a que es más fácil de cometer desde el exterior, sin necesidad de entrar al archivo de las empresas, pero que en el tiempo son descubiertos, siendo muy tarde la reacción. En tal sentido, el fraude es una modalidad muy desarrollado por los delincuentes, dado que existen sin fin de sistemas operativos que rompen la seguridad de las empresas.

- **Manipulación de Programas o Los "Caballos De Troya" (Troya Horses)**

  La manipulación de datos es difícil de descubrir, porque son desarrollados finamente por los delincuentes, quienes poseen conocimiento sofisticado respecto al sistema informático. Son delincuentes que conocen a la perfección los sistemas operativos de las empresas, quienes modifican datos y programas en el sistema operativo de las computadoras, programándolos desde cualquier lugar

sin necesidad de entrar a los espacios físicos. Estos usan el virus llamado caballo de Troya que consiste en insertar manuales operativos en las computadoras de forma encubierta para que pueda cumplir la función no autorizada al mismo tiempo que su función normal.

- **La Técnica Del Salami (Salami Technique/Rounching Down)**

  Esta técnica es una modalidad muy aprovechada por los delincuentes, es una técnica bien sofisticada que aprovechan los delincuentes que las autoridades lo llaman como la "técnica del salchichón" como si se partiera tal producto en "rodajas muy finas" que apenas son identificadas, en tal sentido, la técnica del salami significa, sacar de una cuenta a otra monedas en sentimos, para ello, utilizan programas introducidos a las computadoras de las cajas que transfieren automáticamente a otras cuentas no autorizadas.

- **Falsificaciones Informáticas**

  Las falsificaciones en la informática, lo que busca es alterar los documentos almacenados en el sistema operativo de las computadoras que pertenecen a las empresas. En tal sentido, las computadoras infectados con el troyano, pueden utilizarse para cometer falsificaciones de documentos de diverso índoles, judiciales o comerciales. Para esto se presta en mayor grado, las impresoras fotocopiadoras laser porque permiten falsificar todo tipo de documentos alterando datos oficiales. Estas fotocopiadoras reproducen con alta resolución que difícilmente puede ser detectado un usuario cualquiera, por lo que los especialistas son los responsables de detectar los expedientes falsificados.

- **Manipulación de Datos de Salida**

  Se refiere a la manipulación del sistema informático con datos específicos para propiciar salida deobjetos hacia el exterior. Este delito básicamente se observa en los cajeros automáticos, donde introducen datos falsificados para robar a los usuarios. este tipo de fraudes básicamente son cometidos en bancos con tarjetas robadas a los usuarios, que usan sofisticados sistemas operativos para computadoras

que permite codificar información electrónica en las bandas magnéticas de las tarjetas bancarias y las tarjetas de crédito robadas.

- **Pishing**

  Esta modalidad de fraude informático, tiene como objetivo robar identidad. Este tipo de delitos son para obtener información sobre la identidad detitulares de las tarjetas de crédito, nombres, números, contraseñas, nro. De cuenta, por medio de engaños en redes sociales y cuentas falsas que generalmente son perpetrados por medio de mensajes de textos, correos electrónicos, ventanas emergentes. Este tipo de delitos han aumentado en los últimos tiempos. la mayoría de estas víctimas sufren secuestros de cuentas de tarjetas de crédito, que en últimos cinco años, más de 10 millones de ciudadanos han sufrido robo de identidades con esta modalidad de delito, la policía especializada conjuntamente con la fiscalía en delitos informáticos vienen combatiéndolo lento pero acertadamente.

- **El sabotaje Informático**

  Se refiere al acto de desaparecer las pruebas mediante la eliminación o modificación de datos sin autorización del titular. Se refieres a introducir los troyanos a las computadoras para eliminar y obstaculizar uso de sistemas informáticos, para ello, existen diversas técnicas que permiten cometer los delitos podrían ser.

- **Bombas Lógicas (Logic Bombs)**

  Como su nombre lo indica, son bombas de tiempo que ocasionan daños colaterales, para combatirlos requiere especialistas en programación de datos informáticos, de tal manera que puedan modificar datos legales por datos ilegales, con el uso de troyanos, virus, gusanos, entre diversas bombas digitales para burlar las leyes sin ser detectadas. Por tanto detonación de esta bomba causa daños irreversibles a las empresas y personas, que muchas veces son utilizados como instrumento de extorsión, que para descifrar donde se halla esta bomba, piden sumas de dinero.

- **Gusanos**

Se llaman así, a la fábrica de virus de delincuentes, para introducirlos e infectar las datas de las empresas, una vez infiltrados a las computadoras destruyen datos, modifican datos. Vale decir, estos gusanos son tumores benignos que causan graves problemas. Estos gusanos tienen la particularidad de introducirse a las cuentas de bancos para desviar depósitos de manera permanente a otras cuentas sin ser detectados.

- **Virus Informáticos y Malware**

  Se llama así, troyanos informáticos, que son microorganismos biológicos, que se producen y se expanden dentro de las datas de las computadoras de las empresas, que son contagiados en forma deliberada, en diferentes grados de gravedad en las instituciones, que causan daños a unos más que a otros, que algunos combaten el troyano con otros troyanos que tienen licencia para operar llamados antivirus, que en muchos casos son difíciles de destruir.

  Este virus puede ingresar a la data de la computadora de una empresa, con accesorios legítimos porque podría haber sido infectado de manera casual o deliberada, con el famoso caballo de Troya, un micro virus virtual que es capaz de auto reproducirse una vez infectado al computador.

  Este malware, se identifica por su ataque al sistema informático, que lee la lectura del virus informático instalado en las computadoras para atacarlos a su sistema operativo inutilizando a sus códigos de operación.

- **Ciberterrorismo**

  El ciber-terrorismo informático, se llama el acto de realizar algo para atentar contra los intereses un país, para desestabilizar al gobierno, para ello, utiliza métodos clasificados para evadir los delitos informáticos, especialmente, lo que refiere al tipo de sabotaje, para lanzar ataques en modalidad de terrorismo informático, que requiere muchos recursos humanos y financieros para financiar los delitos.

- **Ataques de Denegación de Servicio**

Estos ataques se refieren al uso de recursos en mayor para atentar contra los sistemas informáticos. Con la utilización de datas con memorias troyanas en las máquinas de las victimas hasta que se produzca error general en el sistema por falta de memoria, dejándolo fuera de servicio a la máquina, que abre miles de ventanas con virus, de tan manera que la maquina queda inutilizada sin que respondan sus partes. Que trae consecuencias graves para las víctimas.

2.2.2 El Espionaje Informático y el Robo de Software

Este delito (data leakage), se conoce también como la publicación no autorizada de documentos reservados, es una modalidad del espionaje industrial que roba información confidencial de las empresas. Como señala Luis Camacho, se refiere a las facilidades generadas para copiar facilidad para un fichero mecanizado con una rapidez y simplicidad son formas de delitos que caracteriza al espionaje que dicho sea de paso está al alcance de hackers, a pesar que las informaciones están encriptados.

Reproducción no autorizada de programas

Reproducción no autorizada de programas informáticos de protección legal. Este tipo de actividades genera en el mercado informalidad, ocasionado pérdidas económicas a las empresas formales. Este tipo de actividades, son tipificados como delitos informáticos, quienes infringen son sometidos a sanciones penales, en últimos años, este delito ha alcanzado su pico más alto a nivel internacional, con la producción de productos informáticos no autorizadas por medio de las redes de informáticos modernas.

El robo de servicios:

El robo de servicios, se tipifica como delito desde el tiempo empleado para hacker a la computadora utilizando internet, donde la empresa que provee servicios permite acceder al uso de la computadora donde se encuentra la información, pero ocurre que el usuario de ese servicio otorga esa clave a otra

persona que sin esta autorizado para utilizarlo, causando un perjuicio patrimonial a las empresas proveedoras de servicios.

Apropiación de Informaciones

Se conoce como apropiación de información residual (scavenging), para el aprovechamiento de la información descuidada sin ningún cuidado como residuo de un trabajo autorizado previamente, esta apropiación puede surgir efectuándose físicamente cogiendo las papeleras de desecho que electrónicamente es posible su recuperación.

Parasitismo Informático

Se conoce como suplantación de identidad, que se configuran como delito por robo de identidad de personas o nombres mediante el espionaje informático. Para tales efectos los delincuentes utilizan la suplantación de personas, con la finalidad de cometer actos ilícitos mediante el uso de redes informáticos. Para ello, utiliza una serie argucias para engañar a su víctima hasta lograr acceder a su código privado. Accediendo a datos reservados de cuentas de ahorros y tarjetas de créditos.

El acceso no autorizado a servicios informáticos:

Se conoce las llamadas puertas falsas (trap doors), que se refieres a la práctica de introducir interrupciones a la data de programas con la finalidad de chequear mediante procesos complejos. En esta modalidad sobre el acceso no autorizado se conoce por el almacenamiento de datos que producen, resultados intermedios en algunas áreas para comprobarlos más adelante.

La Llave Maestra

Se llama así, programas informáticos que tienen la particularidad de abrir cualquier archivo en las datas del computador, no hay una computadora que se resista a este virus llamado llave maestra, que puede alterar, borrar, copiar, insertar o utilizar, los datos en cualquiera de las formas no permitidas, de documentos almacenados en el computador. Este es un programa de acceso internacional, que permite penetrar en sistema operativo del computador por muy protegido que esta se encuentre, es como su nombre indica, llave maestra que abre cualquier archivo sin dejar huella, es como una especie de llave que abre cualquier rincón del computador.

Pinchado de Líneas

Se refiere a interferir las líneas telefónicas que trasmite datos para rescatar la información que circula por sus circuitos, por medio de una radio, llamada módem. En tal sentido el método más eficiente para resguardar la información que se envía por líneas de teléfonos es la criptografía, consistente en la aplicación de claves que codifican la información, transformando en una serie de caracteres ininteligibles entre letras y números sin sentido aparente, por defecto la clave, se recompone hasta lograr fidelizar la información tal igual que se envió en el dato original.

Piratas Informáticos

También son conocidos como hackers. Estas personas son los que cometen robos de informaciones desde el exterior con uso de diversas herramientas informáticos. El pirata informático aprovecha la falta de seguridad en las empresas, para obtener acceso a las informaciones, generalmente estos delincuentes, se hacen pasar con clientes formales para confundirse con los usuarios, ganarse la confianza para robar información.

Integridad de delitos Informáticos.

Es la calidad de la información que considerada exacta, completa, homogénea, sólida y coherente calificado por los creadores dedatos. Esta calidad se obtiene impidiendo eficazmente la inserción, modificación o destrucción no autorizada, accidental o intencional del contenido de las bases de datos, conforme avanza la tecnología son complejos en su detección. En tan sentido, cabe precisar que el estado debe mantenerse alerta respecto a mantener a buen recaudo sus sistemas informáticos para no ser víctima del delito informático, para toda organización del siglo xxi, la seguridad informática tiene que ser primordial, por la constante amenaza en que se encuentran su sistema de seguridad, las empresas deben evaluar su vulnerabilidad con herramientas informáticos modernos para hacerle frente a los hackers antes que ocasionen grandes pérdidas.

2.2.3 El Derecho Informático

El derecho informático es la norma jurídica para hacerle frente a los delincuentes informáticos, encuentra sus fundamentos en una serie de articulaciones dentro de las normativas jurídicas que reglamentan la utilización debienes y servicios informáticos en la comunidad, que incluye como objeto de estudio:

1º Los ordenamientos jurídicos del software;
2º Los derechos de transferencia de redes de datos;
3º Las documentaciones electrónicas;
4º Las contrataciones electrónicas;
5º Los ordenamientos jurídicos respecto a las bases de datos;
6º Los derechos a la privacidad;
7º Los diversos delitos informáticos; y
8º Otras conductas ilícitas surgidas del mal uso deordenadores y de las redes de transferencias de datos.

Al margen de la creación especifica del derecho informático, puede abordarse la regulación jurídica respecto al ámbito de digitalización en el mundo empresarial, administrativo, desde la concepción de las ramas del derecho donde el ordenamiento jurídico existente, que podría dar como base para el análisis las nuevas realidades.

Posibles Bienes Jurídicos en el Delito Informático

Existen discrepancias doctrinales respecto a la existencia de conceptos sobre delito informático, cada vez son diversas las voces doctrinales que se refieren a la delincuencia informática que señalan la necesidad de crear una nueva categoría jurídico penal, que aborde situaciones vinculadas con hechos informáticos, hechos que lesionan los bienes jurídicos tradicionales, de interés social, que el derecho penal debe ponderar. Al respecto existen diferentes opiniones de cómo definir el bien jurídico penal a que se refiere, empero,

predominara de la convergencia de ideas para ponderar el derecho penal respecto al delito informático.

La Seguridad Informática

Se refiere a la seguridad informática entendido como bien jurídico colectivo a tutelar, cuyo objeto de ataque se refiere a las conductas vinculadas al sistema informático. En tal caso lo que se persigue es la protección de las lesiones a los bienes jurídicos de carácter individual, que son víctimas de conductas atentatorias contra la seguridad de las redes y sistemas informáticos de personas jurídicas y personales. Se pretende velar por el correcto funcionamiento de la seguridad jurídica, tanto público como privado, cuya seguridad de su sistema jurídico sea la protección de bienes patrimoniales de carácter supraindividual. Con dependencia informática de las tics, que son herramientas para evitar la alteración de la seguridad jurídica.

En consecuencia, se trata de analizar la protección de un bien jurídico de naturaleza colectiva, indispensable para resguardar de manera concreta la protección mediante la salvaguarda del bien jurídico protegido de naturaleza individual, al margen de otras consideraciones, que pondera los bienes de protección en situaciones de peligro

Intimidad informática

Se refiere a la protección de un bien jurídico, vale decir; la protección al bien jurídico referido a la intimidad informática, al habeas data o la autodeterminación informática, donde se contempla de modo especial la doctrina italiana como jurisprudencia para tener en cuenta este ordenamiento que contempla como delito el acceso abusivo a un sistema informático. Desde el año 1993, se conoce la manera de protegerse de las conductas delictivas vinculados al hecho informático respecto al bien jurídico individual “intimidad e inviolabilidad informáticas. la intimidad informática, también se conoce como libertad informática plateada como bien jurídico autónomo de naturaleza estrictamente informática, protegido por el derecho penal, su contenido central se basa en el derecho del individuo, es decir en la información personal y la familia. Por lo que se entiende como necesario los nuevos conceptos sobre intimidad informática, que muchos de ellos abarcan derechos individuales

garantizando los medios de protección y tutela de la propiedad o la optimización de las cosas materiales en su poder, por medio de protección prestada a la intimidad personal y domiciliaria.

Propuestas

Se refiere al nuevo bien jurídico de carácter supraindividual respecto a delitos informáticos para el funcionamiento de sistemas informatizados. Vale decir; son propuestas referentes a la idea de la seguridad informática, para el tratamiento de delitos vinculados con la informática, que dañan los bienes jurídicos individuales y concretos, que evidencian los peligros existentes para la sociedad. la gravedad de esta propuesta analiza el quebrantamiento de confianza en la dependencia de la sociedad actual, que depende del uso de las TIC´s para el desarrollo colectivo de individuos. Por lo que urge la iniciativa de una legislación jurídica respecto a la reglamentación del delito informático que tenga como finalidad proteger los bienes jurídicos colectivos. Para poder garantizar las normas de conducta vinculadas con la informática, para que pueda garantizar el acceso y conocimiento de la información, que permita regular todas las conductas denominadas como delitos informáticos.

2.2.4 Antecedentes en el Perú:

En el Perú, el delito informático en sus inicios se fue tipificado en el artículo 186, inciso 3, segundo de código penal de 1991. Esta reglamentación no era propia de una infracción autónoma, sino como agravante del delito de robo. Se reguló posteriormente, como delito informático en capítulo x de código penal, cuyos articulados 207-a (delito informático, uso e ingreso indebido de datos, sistema o red), 207-b (alteración, daño o destrucción de base de datos), 207-c (circunstancias valorativas agravantes), 207-d (tráfico ilegal de datos). con aprobación de leyes especiales, los articulados antes mencionados fueron derogados en octubre del 2013, dichas normativas fueron la ley 30096 (ley de delitos informáticos). referido a ley de delitos informáticos conformada por siete capítulos estructuradas de la siguiente manera: finalidad y objeto de la ley (capítulo i), delitos contra los datos y sistemas informáticos (capítulo ii),

delitos informáticos contra la indemnidad y libertad sexual (capítulo iii), delitos informáticos contra la intimidad y secreto de las comunicaciones (capítulo iv), delitos informáticos contra el patrimonio (capítulo v), delitos informáticos contra la fe pública (capítulo vi) sobre las disposiciones comunes (capítulo vii). Luego fue promulgada la ley 30171 (ley que modifica, a la ley 30096, ley de delitos informáticos). el propósito de esta ley, fue adecuar la ley 30096 a los estándares legales del convenio sobre la ciber-criminalidad (convenio de budapest), al incorporar en su redacción típica de artículos 2, 3, 4, 7, 8 y 10 de la referida ley, sobre la posibilidad de cometer el delito de manera deliberada e ilegítimamente. (Villavicencio, 2014, p. 287). En tal sentido, las principales normas en el Perú respecto a la ciber-delincuencia llamado también delitos informáticos en permanente avance.

2.2.5 Investigación Preliminar

Según Edmond Locard, catalogado como el Sherlock Holmes francés, del delito informático, es el autor de la frase universal «el tiempo que pasa es la verdad que huye». Esta frase permite hacer reflexiones respecto a la importancia de la indagación inmediata ante un crimen, dado que es innegable que el paso del tiempo es perjudicial para recopilar los elementos de prueba.

La Naturaleza de la Investigación preliminar

La Investigación Reactiva:

Se refiere a la presentación de una denuncia, es decir, denunciar para conocimiento de las autoridades competentes en hechos considerados delictuosos , para que las autoridades pongan en marcha estrategias legales de persecución penal, esta actitud del ministerio público se denomina indagación reactiva, que hace frente a hechos, evidentes de muerte violenta donde se aprecia violencia con signos de resistencia que amerita la diligencia de expertos en este tipo de delitos, para hallar huellas de quien o quienes son los sospechosos.

Empero, no pasa lo mismo respecto a otro tipo de noticias o denuncias, donde no se puede determinar si estamos frente a un hecho delictuoso o no. por lo que la indagación tendrá que determinar la conducta delictuosa de quiénes serían los autores, por lo que los investigadores lo denominan investigación reactiva.

La Investigación Proactiva:

Se refiere a una modalidad de investigación, llamado «proactiva», que no origina una sospecha inicial; sino que construya una sospecha. la indagación proactiva o investigación estratégica de un delito, se tiene que ponerse en un escenario del derecho penal, que a su vez tiene que contar con respaldo de políticas públicas. en tal sentido, la investigación proactiva parte de un enfoque tradicional que le sirve de base para tipificar el delito, buscando patrones comunes y analizando las causas directas e inmediatas, siendo su prioridad encontrar información relevante que permita al investigador esclarecer los presuntos delitos, imputados, para poder prevenir las ocurrencias de hechos delictivos en el futuro. en este tipo de investigación se requiere analizar el escenario del robo, tipos de productos robados, el valor de objetos robados, posibles lugares donde comercia lo robado, con la finalidad de valorar de manera estratégica para poder afrontar la criminalidad y proponer una nueva política de prevención, que incluya participación directa de operadores judiciales.

Duración de La Investigación Preliminar

Respecto a las sospechas en la duración de una indagación preliminar se refiere al inicio de la indagatoria sobre diversos casos que vulnerarían derechos personales y colectivos, sin antes atribuirse los cargos, amparando su presunción de inocencia, a pesar de una sospecha existe. Empero, la investigación conforme avance puede demostrar la culpabilidad del imputado en base a las interrogantes planteadas.

Durante el tiempo que transcurre la indagación preliminar se recaban valiosos medios de prueba, que dan un panorama concreto, que en su proceso indagatorio cuentan con testimonios, declaraciones de testigos, que evidencian la confirmación de esas presunciones preliminares.

Según la jurisprudencia internacional, en especial referido al Tribunal Europeo de Derechos Humanos, han sido decepcionados por los tribunales nacionales, que deben valorar los conceptos de «plazo razonable» conforme a las circunstancias de la causa, considerando las circunstancias que componen los tres elementos: a) la complejidad de casos; b) los comportamientos de peticionarios; y c) las conductas de las autoridades competentes.

Empero, en la actualidad el respeto al derecho a obtener una acción en un plazo razonable significa la intervención y control en el durante del proceso con la finalidad de que no se vulneren los derechos.

Respecto al tema, el CPP de 2004, estableció un sistema de control de plazos, que constituye fase de diligencias preliminares. En tal sentido, duración de la indagación preliminar debiera ser razonable, orientando la búsqueda de verdad que debieran perseguirse los operadores judiciales.

2.3 Definición de términos Básicos

Ataque: se refiere a una agresión del sujeto externo que altera un sistema o los datos de las empresas atacándolas con fines nada santos. Estos ataques pueden ser a personas naturales o a personas jurídicas, con la finalidad de sustraer información para vender o utilizar como medio de extorción.

Ataque de Red a un Ordenador: se refiere a la agresión de un hacker externo mediante la red, a las computadores de las empresas para extraer información, inutilizar los datos en el sistema operativo de computadores.

Base de Datos: se refiere a los documentos informáticos que pertenecen a las personas naturales o personas jurídicas, son datos digitales almacenados en sistemas operativos de las maquinas privadas.

Computadora: se refiere una maquina compuesto por un sistema operativo que componen el hardware y software, que son programados conforme la necesidad del usuario con una velocidad precisada.

Cookie: se refiere a los archivo con datos almacenados en el computador, programado a un servidor para registrar información sobre las actividades diarias, de informaciones personalizadas. Empero, hay diversidad de anti-cookie software que automáticamente que hacen frente a los troyanos para mantener el sistema operativo.

Ciber: se refiere a una palabra que nace de un prefijo compuesta, por lo general representa a la palabra cibernética, cuyo contenido es el almacenamiento de información electrónica de (datos), según los especialistas el termino significa (modificador + cabeza) que en el tiempo podría alcanzar un significado real.

Datos: se refiere a diversos documentos que contienen información de interés de las personas que sirven para su gestión institucional o desarrollo académico.

Delitos informáticos: se refiere a las conductas dolosas que cometen las personas para robar información vía virtual. Lo que se tipifica como delincuencia informática, que causa daños a las personas naturales y jurídicas. En este tipo de delito, el objetivo de delincuentes son los sistemas operativos que se encuentran e las computadoras, para cometer fraudes.

Firma digital: se refiere a una firma autorizada en forma digital de una autoridad competente, para gestiones específicas de la institución, que obra en el archivo de las empresas.

Hardware: se refiere a una serie expedientes agrupados en un solo elemento almacenado en un sistema informático, que alimenta funcionamiento de una empresa.

Información: se refiere a la noticia referida al cúmulo de informaciones, que es el producto del proceso de datos que son útiles para las empresas.

Proveedor de Servicio de Internet: se refiere a las personas que venden servicios del sistema operativo y acceso al internet, que alimenta a toda la comunidad universal económicamente activa.

Infraestructuras Criticas Cibernéticas: se refieren a las infraestructuras cibernéticas que son esenciales para brindar servicios informáticos a las empresas públicas, de las infraestructuras digitales depende la estabilidad económica empresarial, la seguridad pública, la seguridad nacional, la estabilidad internacional, vale decir, el ciberespacio controlado es vital para seguridad jurídica de las personas.

Mensaje de Datos: se refiere toda información visualizada, los datos recibidos, almacenados, electrónicos, es decir, todo tipo de documentos digitalizados se llama datos.

Modem: se refieren a los aparatos que cambian datos de las computadoras a formatos, que puedan transmitirse fácilmente por líneas telefónicas, por otros medios digitales más sofisticados.

Página Web: se refieren a una serie de cuadernos digitales que almacena y transmite información en sus diversos formatos. Dicho de otro modo, son un conjunto de páginas web integradas en internet, interconectadas con el mundo.

Password: se refiere una clave de acceso a un sistema operativo de una empresa o persona que contiene una serie de caracteres reservados combinados con números y letras, que solamente tienen conocimiento las personas responsables.

Programa: se refiere a una serie dispositivos entre hardware y software instalados en las computadoras que permite realizar un trabajo con el sistema operativo.

Red de computadoras: se refiere una serie de máquinas interconectadas con un sistema operativo programados con los mismos datos en una plataforma virtual. Que en algunos casos son inalámbricos y cableados.

Red de Defensa de Ordenadores: se refieren a las previsiones adoptadas para proteger las actividades externas en contra de las redes internas instaladas en los ordenadores. Por lo que son monitoreados, para detectar las filtraciones.

Sistema Informático: se refieren al conjunto de programas organizados con datos informáticos, que permite preparar, almacenar, la información de forma automatizada con datos o información cualquiera que esta sea.

Servicios críticos cibernéticos: se refieren a todo servicio digital que se denomina cibernético, que son necesarios para preservar la seguridad pública, que permita la estabilidad económica de la nacional.

Sociedad de la Información: se refiere al desarrollo digital en el sistema informático, donde las (TIC) han creado plataformas en algunos casos de libre acceso, en otras de acceso privado, siendo uno de ellos, el uso del internet que se ha convertido en un recurso de uso obligado a nivel mundial.

Software: se refiere a data lógica que compone el sistema operativo de las computadoras para poder realizar los trabajos, que contiene una serie de procesos desarrollados, llamados como soporte técnico, que desde el punto de vista legal se llama propiedad intelectual.

CAPÍTULO III: HIPÓTESIS Y VARIABLES

3.1 Hipótesis general

Los delitos informáticos, se relacionan significativamente con el proceso de investigación preliminar, en distrito fiscal de Lima Norte, año 2019.

3.2 Hipótesis Específicos

a) Los delitos informáticos se relacionan significativamente con las declaraciones realizadas en el proceso de investigación preliminar en distrito fiscal de Lima Norte, año 2019.

b) Los delitos informáticos se relacionan significativamente con los plazos establecidos en el proceso de investigación preliminar en distrito fiscal de Lima Norte, año 2019.

c) Los delitos informáticos se relacionan significativamente con el aseguramiento de pruebas en el proceso de investigación preliminar en distrito fiscal de Lima Norte, año 2019

3.3 Definición conceptual y operacional de las variables

3.3.1 Variable Independiente

- **Delitos Informáticos.**

  Son conductas típicas y antijurídicas, medio por el cual los sujetos de mal vivir que ingresando al sistema informático comete delitos, en contra de personas naturales o personas jurídicas. Al desarrollo acelerado de la tecnología, ha permitido en mal uso del sistema informático, para poner en peligro los bienes protegidos. Jiménez (2017)

  Definición Operacional

  Delito informático implica cualquier actividad ilegal que encuadra en figuras tradicionales ya conocidas como robo, hurto, fraude, falsificación, perjuicio, estafa y sabotaje, pero siempre que involucre la informática de por medio para cometer la ilegalidad.

3.3.2 Variable dependiente

- **Proceso de Investigación Preliminar**

  Investigación Preliminar es la investigación inicial ante la denuncia, que se presenta a la Autoridad; o cuando por propia iniciativa deciden dar inicio a los primeros actos de investigación, (Pablo Sánchez, 2017).

  Definición Operacional

  Es el primer acto de proceder con investigación con más profundidad. Pretende identificar al primer momento o a los actos iniciales de la Investigación, en que se confirmará o descartará la existencia del ilícito para continuar- lleva el mensaje de que no se ha querido crear una etapa ni sub etapa previa a la investigación preparatoria, sino que se identifica apenas una situación o lapso temporal en el cual se Acumularán elementos de juicio para determinar la existencia del ilícito penal”

3.4 Operacionalización de las variables

Variable	Dimensiones	Indicadores	Escala
Variable Independiente (X) Delitos Informáticos	**1.** Sustantiva **2.** Objetiva	• Normas • Obligaciones • Derechos • Contenidos • Regulación • Garantía • Cumplimiento	Ordinal
Variable Dependiente (Y) Proceso de Investigación Preliminar.	**1.** Declaraciones **2.** Actuaciones de la investigación **3.** Plazos **4.** Aseguramiento de pruebas	• Oficio • Denuncia • Noticias • Documentación • Procedimientos • Tiempo ordinario • Plazo común • Pericias • Monitoreo • Verificación • Pruebas	Ordinal

Fuente: Elaborado por el autor

Figura 1

CAPÍTULO IV: METODOLOGÍA DE LA INVESTIGACIÓN

4.1 Enfoque, tipo y nivel de Investigación

4.1.1 Enfoque de investigación

Según Galeano (2004) el enfoque define si la investigación es cualitativa o cuantitativa, que busca explicar una realidad estudiada desde el escenario del investigador.

El enfoque lo que busca es la certeza metodológica de la investigación para medir sus resultados en el universo poblacional, las muestras y los datos.

4.1.2 Tipo de Investigación

Según su propósito la tesis, partió de la problemática planteada, con la formulación de objetivos, con tipo de investigación aplicada, dado que se caracterizan por buscar la aplicación o utilización de datos encontrados para desarrollar los datos.

4.1.3 Nivel de Investigación

El nivel de indagación de la tesis, es descriptivo – correlacional; ya que por medio este tipo de indagación, se utiliza el método de análisis, para lograr caracterizar los objetos de estudio, en un escenario concreta.

4.2 Diseño y Método de la Investigación

4.2.1 Método de Investigación

a) Método general

El método de la indagación fue hipotético deductivo, consistente en dar a conocer conjeturas sobre las hipótesis con probables soluciones a los interrogantes planteados, con los datos encontrados.

Hipotético - Deductivo. Estos métodos permitieron aseverar la efectividad de conjeturas planteadas en las hipótesis, para su posterior comprobación. Este proceso corresponde a la guía metodológica que busca lograr una nueva ciencia. Con los hechos y conceptos planteados para mejorar los existentes. Oviedo (2018).

b) Métodos Específicos

Método específico: se refiere a un modelo estadístico que sirve para tabular los datos encontrados en formato de figuras y figuras para poder interpretarlos utilizando las dimensiones e indicadores, variables, con la aplicación correcta de la estadística descriptiva.

Hernández (2006), quien define que el método especifico, tiene una función importante, toda vez que contribuye para determinar las muestras en estudio, permite tabular datos encontrados para analizar cada una de ellas, en ese sentido se establece sujetos de estudio para explicar los

resultados deseados. En este sentido los métodos estadísticos son instrumentos necesarios, porque permiten inferenciar o describir los resultados.

4.2.2 Diseño de Investigación:

El diseño de esta indagación, por su naturaleza pertenece a no experimental de corte transversal, porque no necesita manipular las muestras, ni los datos.

Según Niño (2011) el diseño de una indagación es equivalente al desarrollo de un plan para analizar el tema planteado, en el proyecto, que comprende una serie de actividades que comprender dar respuesta a los interrogantes planteados.

4.3 Población y muestra de la investigación

4.3.1 Población

Según Mendoza, Hernández y Méndez (2015) Corresponde al universo poblacional materia del estudio, en este caso específico comprendió a 100 personas que laboran en los juzgados de Lima norte, Jueces, Fiscales, Abogados

4.3.2 Muestra

Según Tamayo (2013), el universo muestral es aquel método que facilita definir la cantidad de muestras que definen los resultados de las interrogantes planteadas, para poder generar nuevos datos. Se refiere también como muestra al conjunto

de personas, que intervienen en una investigación. Que son parte del grupo estadístico que conforma la indagación.

En este sentido, calculamos que la muestra para aplicar en la indagación, son de 80 personas que trabajan en los juzgados de cono norte de Lima.

$$n = \frac{N \times Z_a^{\,2} \times p \times q}{d^2 \times (N-1) + Z_a^{\,2} \times p \times q}$$

Donde:

Z: Valor de la curva normal para probabilidad al 95% de confianza.

P: Observación variable (x)

q: Observación variable (y)

e : Margen de error 5%

N: Población

n: Tamaño muestral

Donde:

N = 100

e = 0.05

Z = 1.96

P = 0.5

q = 1- 0.5 = 0.5

$$n = \frac{100*(1.96)^2*0.5*0.5}{(0.05)2*(100-1)*(1.96)2*0.5*0.5}$$

$$n = \frac{96.04}{1.2079}$$

n= 79.5098

n = 80

4.4 Técnicas e instrumentos de recolección de datos

4.4.1 Técnicas

Se refieren a la aplicación de la guía metodológica consistente que permite analizar los contenidos recolectados que permitirán dar respuesta a las variables aplicando la técnica de análisis documental.

Según Oré (2015), las técnicas son procedimientos empleados por el investigador, que le permite buscar informaciones para alcanzar los objetivos planteados en su trabajo de indagación, para este caso específico, la técnica empleada fue la encuesta. Que fue aplicado de la población seleccionada.

4.4.2 Instrumentos

- **Cuestionario:** Es un conjunto de interrogantes elaboradas por especialidad con rigor académico para lograr los propósitos planteados. Que en muchos casos respondidos por escrito sin la intervención de investigador. (García, 2004)

- **Formulario de encuesta:** Es una serie de documentos físicos bien estructurados que permite dar respuesta con facilidad a todas las interrogantes planteadas en la investigación. Generalmente son estructuradas con escala de Likert u otras (Borda et al, 2009, p.65)

4.5 Validez y confiabilidad

4.5.1 Validez del Instrumento por Juicio de Expertos

Conforme señala Gotuzzo (2016) la validez deinstrumentos reflejan la calificación del instrumento con rigor académico y rigor científico, de tal manera que se pueda evaluar los resultados deinterrogantes planteados.

En tal sentido, los instrumentos fueron validados por cada uno deprofesionales expertos, quienes son los especialistas en el área del derecho penal y delitos informáticos, por lo que analizaron la aplicabilidad deinstrumentos en bases a las variables en estudio.

N°	Grados Acad.	Apellidos y nombres	Coeficientes	Porcentajes
1	Doctor	Mauro estrada Gamboa	95	95%
2	Doctor	Silvia Chacon Jiménez	91	91%
3	Doctor	Eva Romero Loayza	93	93%
4	Doctor	Norvil Cieza Montenegro	92	92%
5	Doctor	Pedro Solís Céspedes	92	92%
Total				**92%**

Table 1

Los instrumentos validados cuentan con una opinión favorable al 92% que es bueno, conforme coeficiente de Cronbach.

4.5.2 Confiabilidad

Para expresar la confiablidad interna del instrumento de investigación se realizó una encuesta que se sometió al examen de Fiabilidad: Alfa de Cronbach, con el uso del programa estadístico SPSS 22, que permitió obtener el siguiente resultado:

Delitos Informáticos	
0,804	10
Proceso de Investigación Preliminar	
0,804	10

Table 2

4.6 Ética de la Investigación

Respecto a la ética en la indagación científica, existen diversas definiciones que reglamentan toda actividad humana, para no vulnerar los derechos, de tan forma que se puede orientar generación de conocimientos nuevos, aplicando soluciones prácticas para obtener los resultados esperados. (Lipman, 1988). En tal sentido, toda indagación por su naturaleza está sujeta a normativas éticas que son punto de partida para promover respeto mutuo entre todos los seres humanos, animales y cosas. De este modo se puede promover respeto a la propiedad y los derechos humanos de las personas, proteger su salud, los derechos de poblaciones vulnerables.

El universo poblacional, que conforma la estructura de esta investigación, han sido revisados por los expertos en sus diversos aspectos, de tal manera que reconoce y respeta, las necesidades primordiales de que están en desventaja económica, por lo que se tuvo un cuidado especial para no herir la susceptibilidad de la población estudiada. (Manzini, 2000). Por lo tanto, la ética en la investigación científica, es aplicada con valores en todas sus etapas, ponderando y motivando aquellas dificultades encontradas en el camino. En tal sentido, en toda investigación, la planificación debe contar con perfil ético, para poder evaluar en escenario donde se va a llevar la investigación, diseñar dentro del estudio los probables costos y beneficios de tal manera que se puede evitar el daño a la gente, el medio ambiente, propiedad privada, sin faltar los derechos.

CAPÍTULO V: RESULTADOS

5.1 Análisis Descriptivo

Respecto al análisis descriptivo los antecedentes, los datos bibliográficos y la recopilación de datos estadísticos, fueron mediante la aplicación del instrumento de manera ordenada para determinar los Delitos Informáticos y su incidencia en el Proceso de Indagación Preliminar en Distrito Fiscal de Lima Norte. Fue complementado con estudio de expedientes documentarios presentados por denuncias en Distrito Fiscal de Lima Norte en relación a la problemática encausada respecto a los sistemas informáticos. Siendo necesaria su evaluación, para su determinación, en razón a que la información es el recurso intangible más valioso en las organizaciones y en la comunidad.

En tal sentido, es de vital importancia que los usuarios enfoquen su atención al grado de vulnerabilidad y seguridad para hacer frente a posibles deterioros y ataques perniciosos a los programas de software y a los sistemas informáticos.

5.2 Análisis Inferencial

¿ALGUNA VEZ TUVO CONOCIMIENTO QUE EXISTE LA LEY PENAL DE DELITOS INFORMÁTICOS Nº 30171?	N° ENCUESTADO	%
Nunca	10	12%
Casi nunca	16	20%
A veces	22	28%
Casi siempre	12	15%
Siempre	20	25%
TOTAL	**80**	**100%**

Table 3

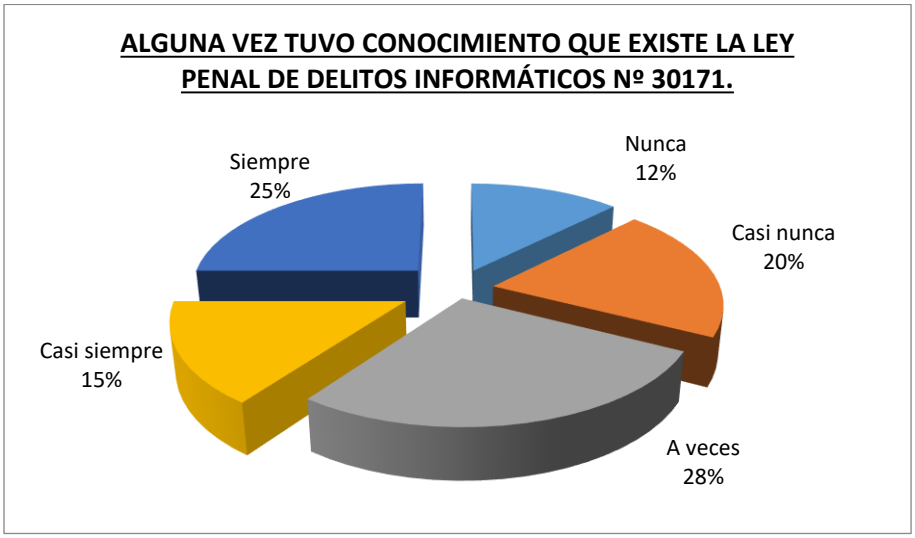

Figure 1

INTERPRETACIÓN:

En la figura, respecto a la interrogante: ¿Alguna vez tuvo conocimiento que existe la ley penal de delitos informáticos Nº 30171? El 12% (10) de encuestados manifiestan que nunca, el 20% (16) de encuestados manifiestan que casi nunca, el 28% (22) de encuestados manifiesta que a veces, el 15% (12) de encuestados manifiestan que casi siempre y el 25% (20) de encuestados manifiesta que siempre.

¿EN LA LEY PENAL DE DELITOS INFORMÁTICOS Nº 30171 SE EXPRESA CON DUREZA LAS SANCIONES A LA CIBERDELINCUENCIA?	N° ENCUESTADO	%
Nunca	12	15%
Casi nunca	8	10%
A veces	24	30%
Casi siempre	20	25%
Siempre	16	20%
TOTAL	**80**	**100%**

Table 4

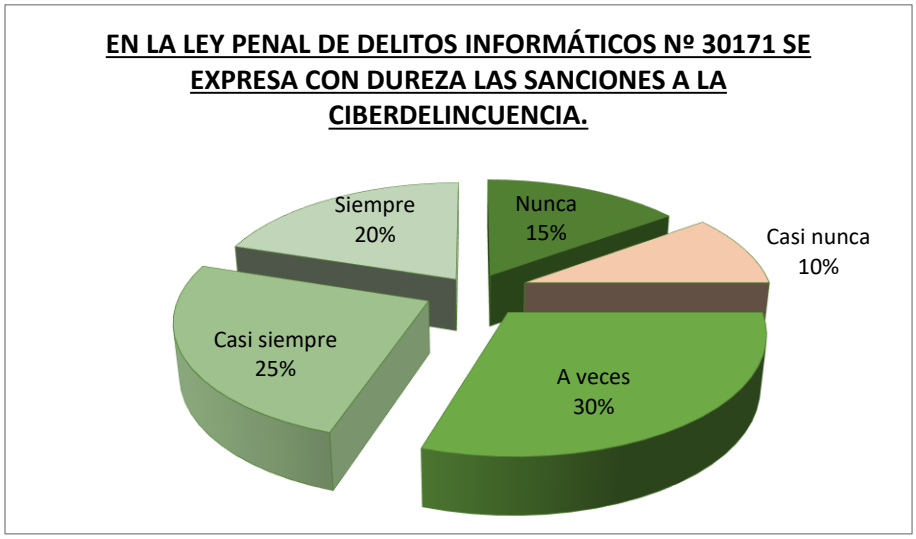

Figure 2

INTERPRETACIÓN:

En la figura, respecto a la interrogante: ¿En la ley penal de delitos informáticos Nº 30171 se expresa con dureza las sanciones a la ciberdelincuencia? El 15% (12) de encuestados manifiestan que nunca, el 10% (8) de encuestados manifiestan que casi nunca, el 30% (24) de encuestados manifiesta que a veces, el 25% (20) de encuestados manifiestan que casi siempre y el 20% (16) de encuestados manifiestan que siempre.

¿EXISTE EN LA LEY DE DELITOS INFORMÁTICOS UN ORDENAMIENTO ORGANIZADO DE LAS PENAS Y SANCIONES QUE AYUDA A LA PROTECCIÓN DESISTEMAS INFORMÁTICOS?	N° ENCUESTADO	%
Nunca	24	30%
Casi nunca	16	20%
A veces	20	25%
Casi siempre	12	15%
Siempre	8	10%
TOTAL	**80**	**100%**

Table 5

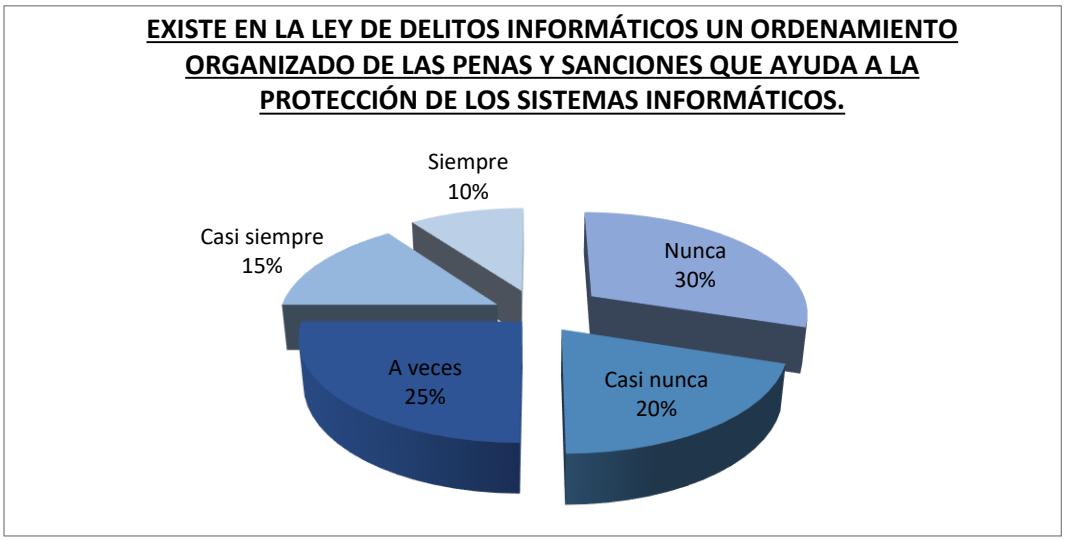

Figure 3

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿Existe en la ley de delitos informáticos un ordenamiento organizado de las penas y sanciones que ayuda a la protección de sistemas informáticos? El 30% (24) de encuestados manifiestan que nunca, el 20% (16) de encuestados manifiestan que casi nunca, el 25% (20) de encuestados manifiesta que a veces, el 15% (12) de encuestados manifiestan que casi siempre y el 10% (8) de encuestados manifiestan que siempre.

¿LA NORMATIVIDAD DE LA LEY PENAL DE DELITOS INFORMÁTICOS TIENE UNA EVIDENTE PROPAGACIÓN EN LOS MEDIOS DE COMUNICACIÓN?	N° ENCUESTADO	%
Nunca	24	30%
Casi nunca	26	33%
A veces	8	10%
Casi siempre	10	12%
Siempre	12	15%
TOTAL	**80**	**100%**

Table 6

FIGURA N° 1

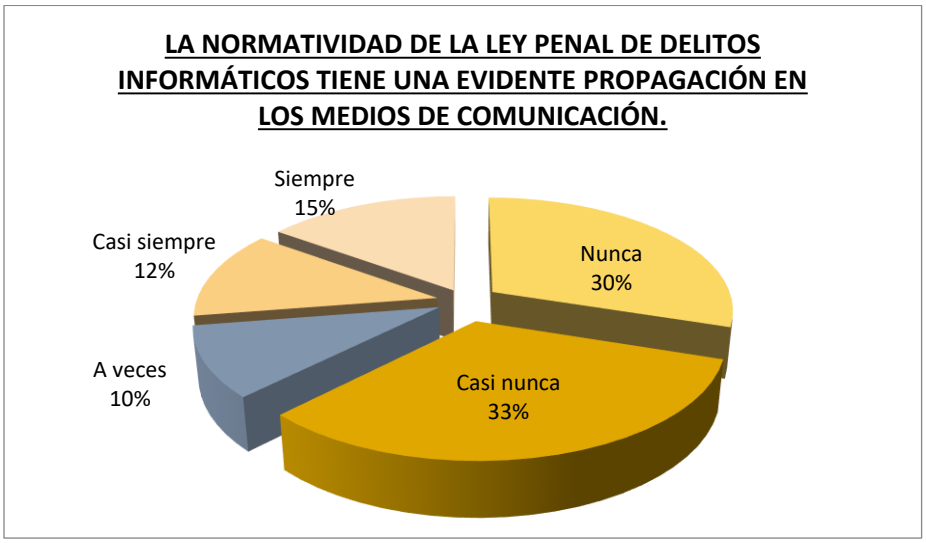

Figure 4

INTERPRETACIÓN:

En la figura, respecto a la interrogante: ¿La normatividad de la ley penal de delitos informáticos tiene una evidente propagación en los medios de comunicación? El 30% (24) de encuestados manifiestan que nunca, el 33% (26) de encuestados manifiestan que casi nunca, el 10% (8) de encuestados manifiestan que a veces, el 12% (10) de encuestados manifiestan que casi siempre y el 15% (12) de encuestados manifiesta que siempre.

¿CREE USTED QUE LA PROTECCIÓN JURÍDICA EN RELACIÓN A LOS DELITOS INFORMÁTICOS OBEDECE A UN PRINCIPIO DE LEGALIDAD?	N° ENCUESTADO	%
Nunca	22	28%
Casi nunca	16	20%
A veces	24	30%
Casi siempre	12	15%
Siempre	6	7%
TOTAL	**80**	**100%**

Table 7

FIGURA N° 2

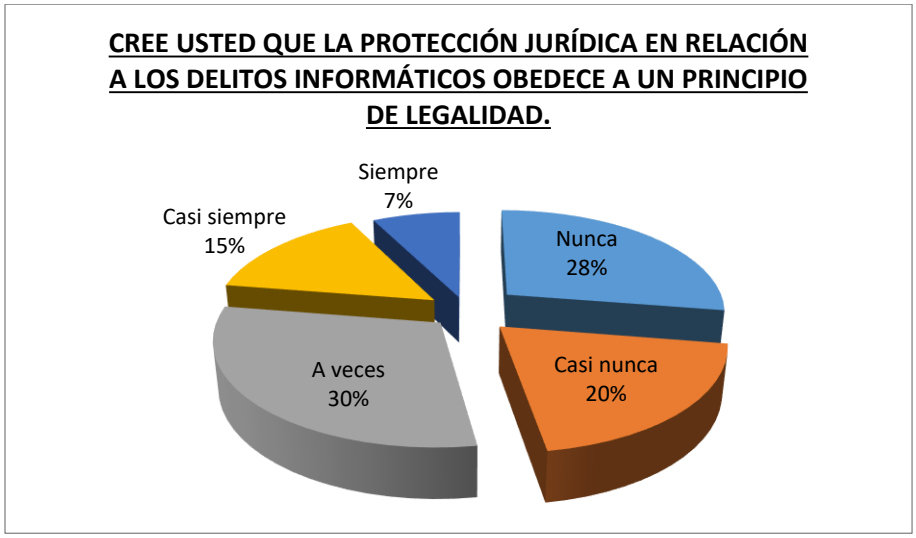

Figure 5

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿Cree usted que la protección jurídica en relación a los delitos informáticos obedece a un principio de legalidad? El 28% (22) de encuestados manifiesta que nunca, el 20% (16) de encuestados manifiestan que casi nunca, el 30% (24) de encuestados manifiesta que a veces, el 15% (12) de encuestados manifiestan que casi siempre y el 7% (6) de encuestados manifiesta que siempre.

¿PARA GARANTIZAR LA SEGURIDAD INFORMÁTICA LOS OPERADORES DE JUSTICIA ADMINISTRAN CON DUREZA LAS HERRAMIENTAS LEGALES?	N° ENCUESTADO	%
Nunca	22	28%
Casi nunca	20	25%
A veces	16	20%
Casi siempre	12	15%
Siempre	10	12%
TOTAL	**80**	**100%**

Table 8

FIGURA N° 3

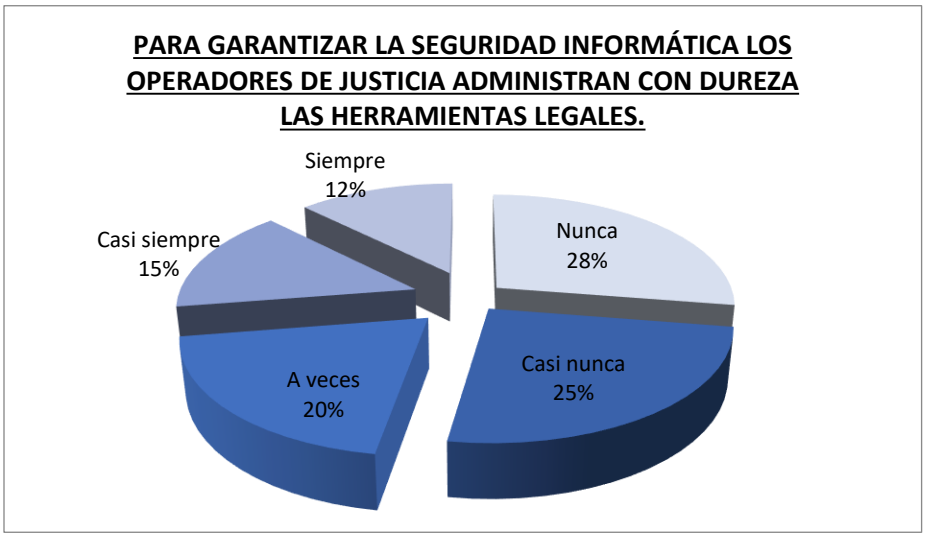

Figure 6

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿Para garantizar la seguridad informática los operadores de justicia administran con dureza las herramientas legales? El 28% (22) de encuestados manifiesta que nunca, el 25% (20) de encuestados manifiestan que casi nunca, el 20% (16) de encuestados manifiestan que a veces, el 15% (12) de encuestados manifiestan que casi siempre y el 12% (10) de encuestados manifiestan que siempre.

¿LOS OPERADORES DE LA JUSTICIA ESTÁN PREPARADOS EN LOS CONTENIDOS FUNDAMENTALES DE LA LEY PENAL DE DELITOS INFORMÁTICOS?	N° ENCUESTADO	%
Nunca	20	25%
Casi nunca	22	28%
A veces	10	12%
Casi siempre	12	15%
Siempre	16	20%
TOTAL	**80**	**100%**

Table 9

FIGURA N° 4

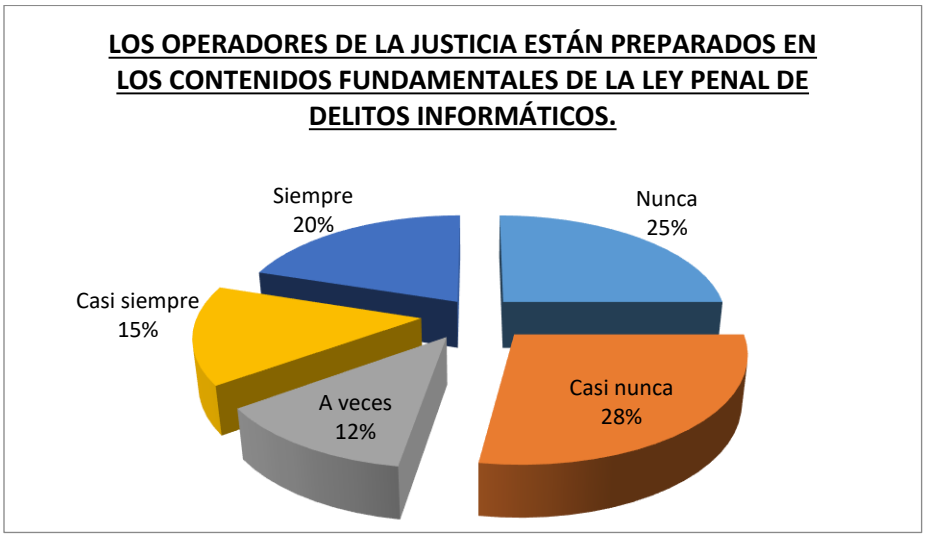

Figure 7

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿Los operadores de la justicia están preparados en los contenidos fundamentales de la ley penal de delitos informáticos? El 25% (20) de encuestados manifiesta que nunca, el 28% (22) de encuestados manifiesta que casi nunca, el 12% (10) de encuestados manifiesta que a veces, el 15% (12) de encuestados manifiesta que casi siempre y el 20% (16) de encuestados manifiestan que siempre.

¿USTED CONOCE CON PRECISIÓN LOS DERECHOS QUE SE MUESTRAN EN LA LEY PENAL DE DELITOS INFORMÁTICOS?	N° ENCUESTADO	%
Nunca	24	30%
Casi nunca	26	33%
A veces	12	15%
Casi siempre	10	12%
Siempre	8	10%
TOTAL	**80**	**100%**

Table 10

FIGURA N° 5

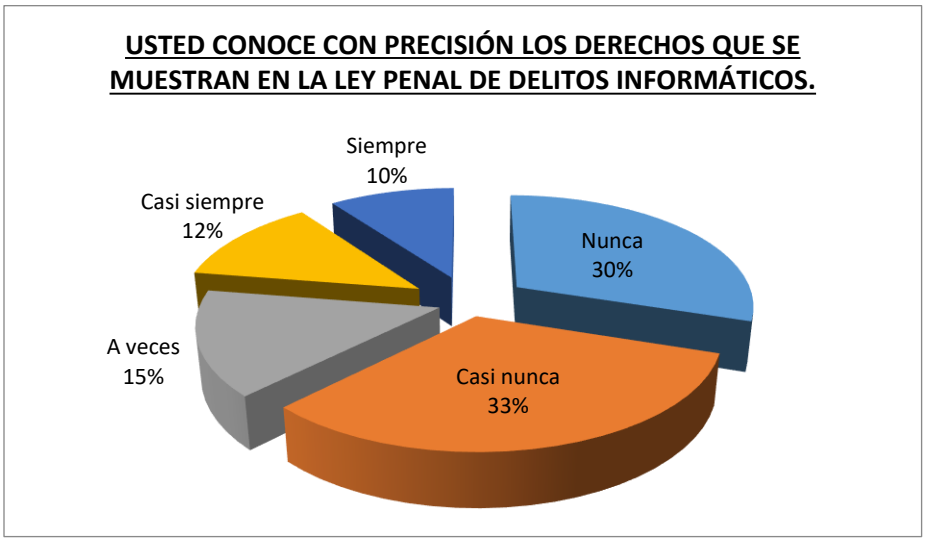

Figure 8

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿Usted conoce con precisión los derechos que se muestran en la ley penal de delitos informáticos? El 30% (24) de encuestados manifiesta que nunca, el 33% (26) de encuestados manifiesta que casi nunca, el 15% (12) de encuestados manifiestan que a veces, el 12% (10) de encuestados manifiestan que casi siempre y el 10% (8) de encuestados manifiestan que siempre.

¿EN LA LEY PENAL DE DELITOS INFORMÁTICOS Nº 30171 LOS DEMANDANTES REVELAN LA PRESENCIA DE VACÍOS EN LAS HERRAMIENTAS LEGALES?	N° ENCUESTADO	%
Nunca	16	20%
Casi nunca	22	28%
A veces	20	25%
Casi siempre	18	22%
Siempre	4	5%
TOTAL	**80**	**100%**

Table 11

FIGURA N° 6

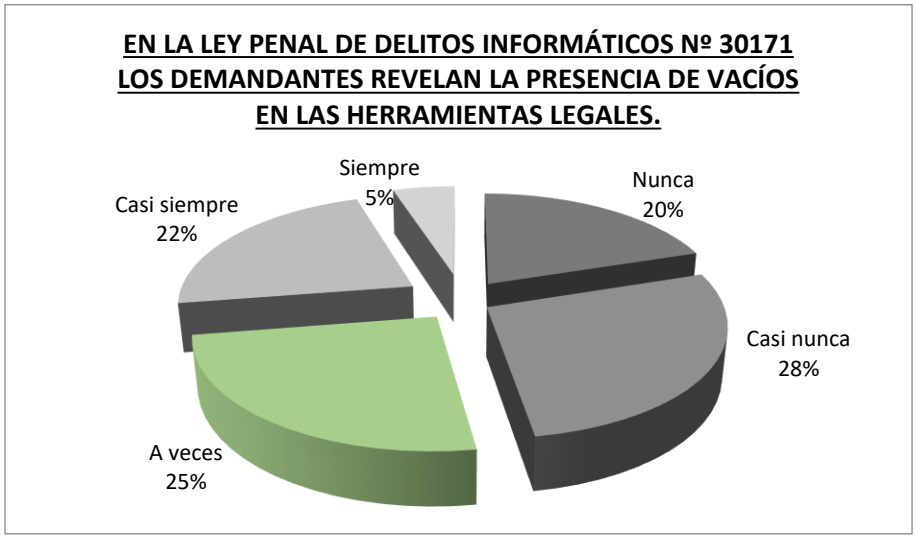

Figure 9

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿En la ley penal de delitos informáticos Nº 30171 los demandantes revelan la presencia de vacíos en las herramientas legales? El 20% (16) de encuestados manifiestan que nunca, el 28% (22) de encuestados manifiestan que casi nunca, el 25% (20) de encuestados manifiesta que a veces, el 22% (18) de encuestados manifiestan que casi siempre y el 5% (4) de encuestados manifiestan que siempre.

¿EXISTE UNA LEY COMPLEMENTARIA EN EL NUEVO CÓDIGO PROCESAL PENAL QUE DIFUNDE EL ENDURECIMIENTO A LAS SANCIONES POR DELITOS INFORMÁTICOS?	N° ENCUESTADO	%
Nunca	22	28%
Casi nunca	16	20%
A veces	20	25%
Casi siempre	12	15%
Siempre	10	12%
TOTAL	**80**	**100%**

Table 12

FIGURA N° 7

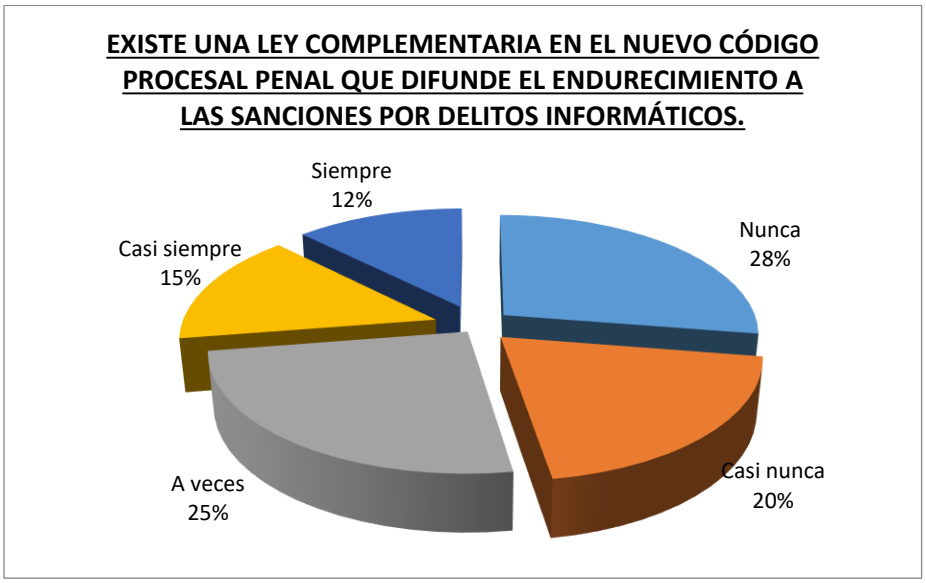

Figure 10

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿Existe una ley complementaria en el nuevo código procesal penal que difunde el endurecimiento a las sanciones por delitos informáticos? El 28% (22) de encuestados manifiesta que nunca, el 20% (16) de encuestados manifiestan que casi nunca, el 25% (20) de encuestados manifiesta que a veces, el 15% (12) de encuestados manifiesta que casi siempre y el 12% (10) de encuestados manifiestan que siempre.

¿CREE USTED QUE LA APLICACIÓN DE LA LEY PENAL Nº 30171 ES LA CORRECTA PARA FRENAR ESTE PROTOTIPO DE DENUNCIA ILÍCITA?	N° ENCUESTADO	%
Nunca	20	25%
Casi nunca	16	20%
A veces	22	28%
Casi siempre	10	12%
Siempre	12	15%
TOTAL	**80**	**100%**

Table 13

FIGURA N° 8

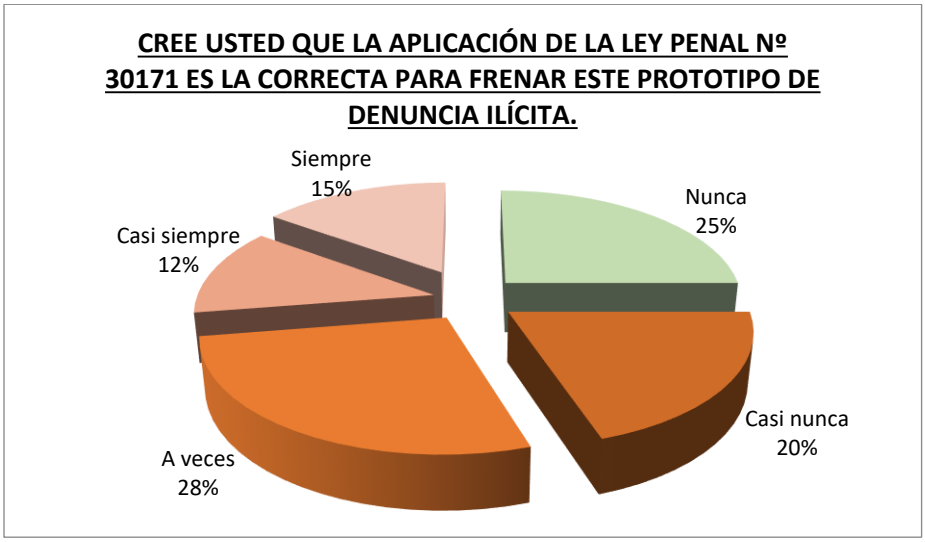

Figure 11

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿Cree usted que la aplicación de la ley penal Nº 30171 es la correcta para frenar este prototipo de denuncia ilícita? El 25% (20) de encuestados manifiesta que nunca, el 20% (16) de encuestados manifiestan que casi nunca, el 28% (22) de encuestados manifiestan que a veces, el 12% (10) de encuestados manifiestan que casi siempre y el 15% (12) de encuestados manifiestan que siempre.

FIGURA N° 1

¿LAS DENUNCIAS POR DELITOS INFORMÁTICOS EN LA INVESTIGACIÓN PRELIMINAR DEBEN SER PRESENTADAS DE MANERA FORMAL Y DE OFICIO?	N° ENCUESTADO	%
Nunca	8	10%
Casi nunca	20	25%
A veces	10	12%
Casi siempre	26	33%
Siempre	16	20%
TOTAL	**80**	**100%**

Table 14

FIGURA N° 9

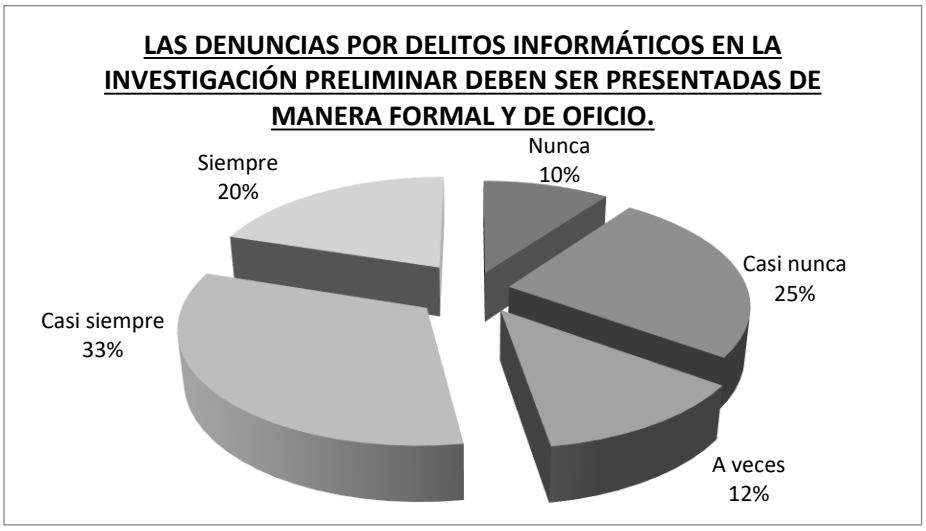

Figure 12

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿Las denuncias por delitos informáticos en la investigación preliminar deben ser presentadas de manera formal y de oficio? El 10% (8) de encuestados manifiesta que nunca, el 25% (20) de encuestados manifiestan que casi nunca, el 12% (10) de encuestados manifiestan que a veces, el 33% (26) de encuestados manifiestan que casi siempre y el 20% (16) de encuestados manifiestan que siempre.

¿CONSIDERA UN FACTOR EVIDENTE LA APLICACIÓN DE LA ESTRATEGIA EN EL PROCESO DE LA INVESTIGACIÓN PRELIMINAR ANTE LAS DENUNCIAS POR LA CIBERDELINCUENCIA?	N° ENCUESTADO	%
Nunca	10	12%
Casi nunca	16	20%
A veces	22	28%
Casi siempre	24	30%
Siempre	8	10%
TOTAL	**80**	**100%**

Table 15

FIGURA N° 10

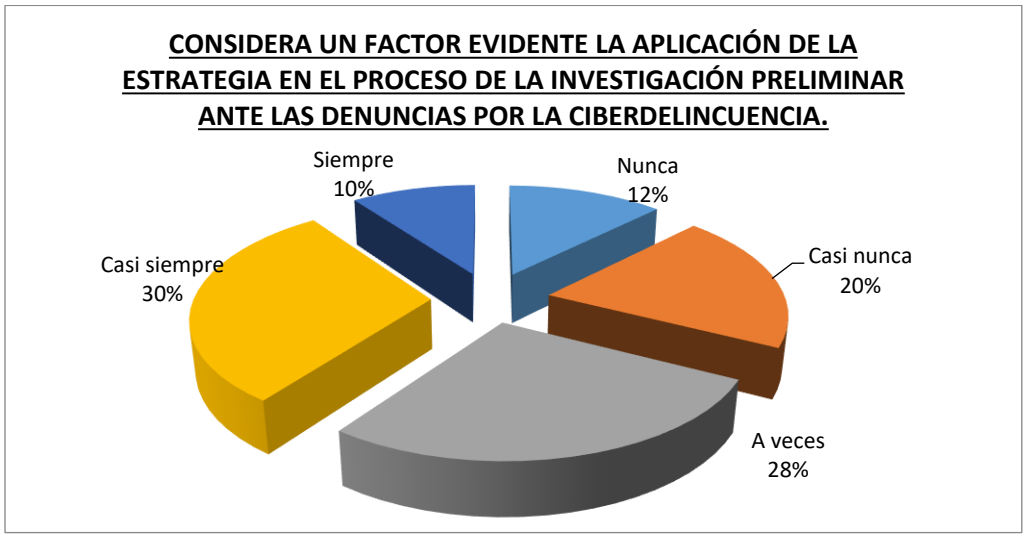

Figure 13

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿Considera un factor evidente la aplicación de la estrategia en el proceso de la investigación preliminar ante las denuncias por la ciberdelincuencia? El 12% (10) de encuestados manifiesta que nunca, el 20% (16) de encuestados manifiesta que casi nunca, el 28% (22) de encuestados manifiestan que a veces, el 30% (24) de encuestados manifiestan que casi siempre y el 10% (8) de encuestados manifiestan que siempre.

¿LA OPERATIVIDAD EN EL PROCESO DE LA INVESTIGACIÓN PRELIMINAR RESULTA UN FACTOR INNEGABLE PARA EL ASEGURAMIENTO DE LAS PRUEBAS Y LAS EVIDENCIAS?	N° ENCUESTADO	%
Nunca	16	20%
Casi nunca	20	25%
A veces	22	28%
Casi siempre	12	15%
Siempre	10	12%
TOTAL	**80**	**100%**

Table 16

FIGURA N° 11

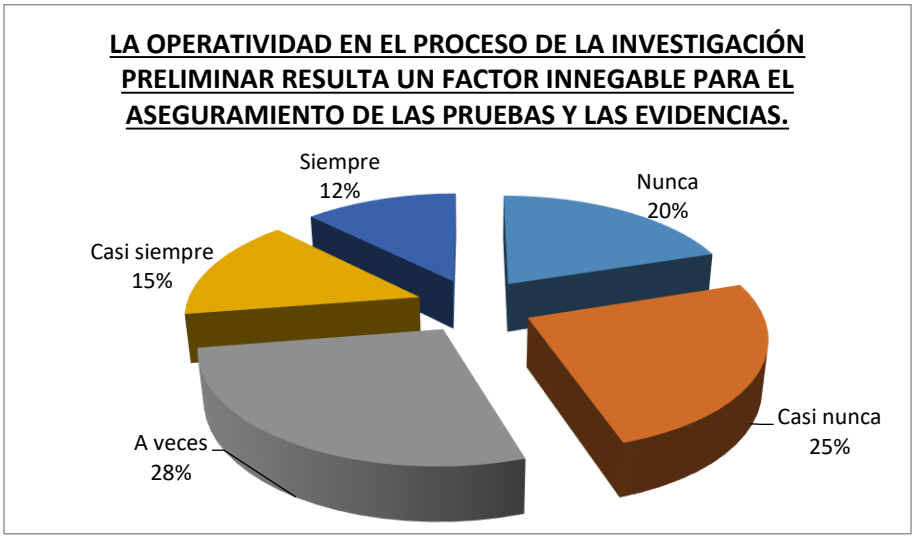

Figure 14

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿La operatividad en el proceso de la investigación preliminar resulta un factor innegable para el aseguramiento de las pruebas y las evidencias? El 20% (16) de encuestados manifiestan que nunca, el 25% (20) de encuestados manifiestan que casi nunca, el 28% (22) de encuestados manifiestan que a veces, el 15% (12) de encuestados manifiestan que casi siempre y el 12% (10) de encuestados manifiesta que siempre.

¿EN EL PROCESO DE LA INVESTIGACIÓN PRELIMINAR RESULTA INELUDIBLE TENER EN CUENTA LA COMPLEJIDAD Y EL ALCANCE DEL TIPO DE DENUNCIA?	N° ENCUESTADO	%
Nunca	10	12%
Casi nunca	16	20%
A veces	24	30%
Casi siempre	18	23%
Siempre	12	15%
TOTAL	**80**	**100%**

Table 17

FIGURA N° 12

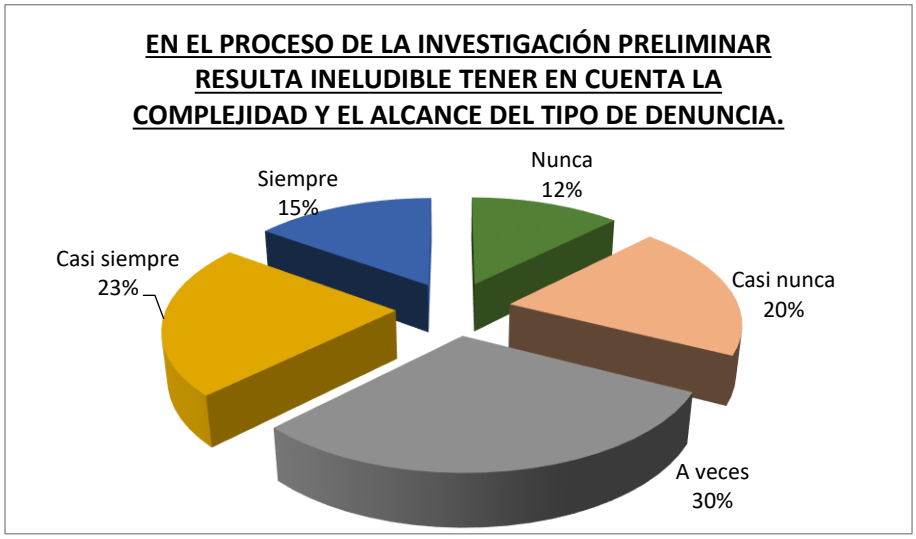

Figure 15

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿En el proceso de la investigación preliminar resulta ineludible tener en cuenta la complejidad y el alcance del tipo de denuncia? El 12% (10) de encuestados manifiesta que nunca, el 20% (16) de encuestados manifiestan que casi nunca, el 30% (24) de encuestados manifiestan que a veces, el 23% (18) de encuestados manifiestan que casi siempre y el 15% (12) de encuestados manifiestan que siempre

¿LA DURACIÓN DE LA INVESTIGACIÓN PRELIMINAR ESTÁ EN FUNCIÓN A LA NATURALEZA Y A LA RAZONABILIDAD DEL DELITO COMETIDO?	N° ENCUESTADO	%
Nunca	20	25%
Casi nunca	16	20%
A veces	22	28%
Casi siempre	12	15%
Siempre	10	12%
TOTAL	**80**	**100%**

Table 18

FIGURA N° 13

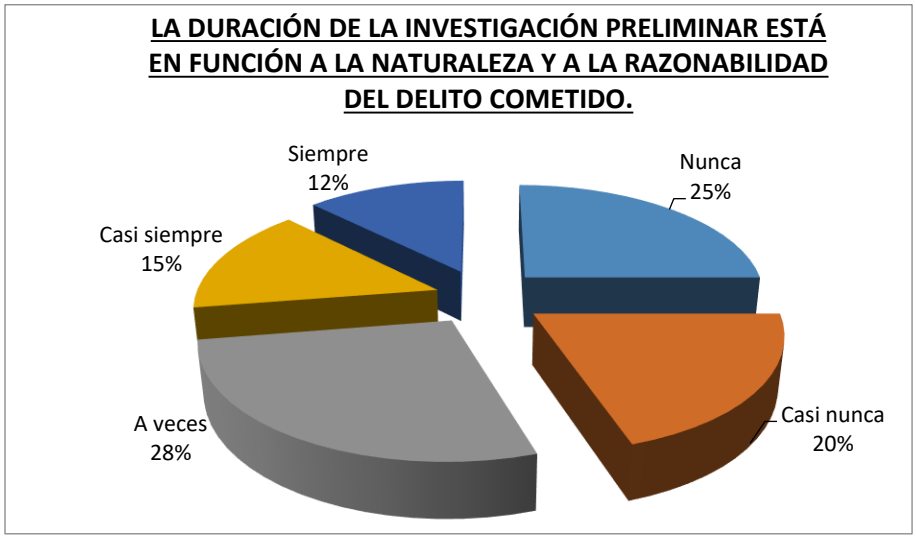

Figure 16

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿La duración de la investigación preliminar está en función a la naturaleza y a la razonabilidad del delito cometido? El 25% (20) de encuestados manifiesta que nunca, el 20% (16) de encuestados manifiestan que casi nunca, el 28% (22) de encuestados manifiestan que a veces, el 15% (12) de encuestados manifiestan que casi siempre y el 12% (10) de encuestados manifiestan que siempre.

¿EL FACTOR TIEMPO ES IMPORTANTE Y ESTRATÉGICO DURANTE LA EJECUCIÓN DEL PROCESO DE LA INVESTIGACIÓN PRELIMINAR?	N° ENCUESTADO	%
Nunca	10	12%
Casi nunca	12	15%
A veces	20	25%
Casi siempre	22	28%
Siempre	16	20%
TOTAL	**80**	**100%**

Table 19

FIGURA N° 14

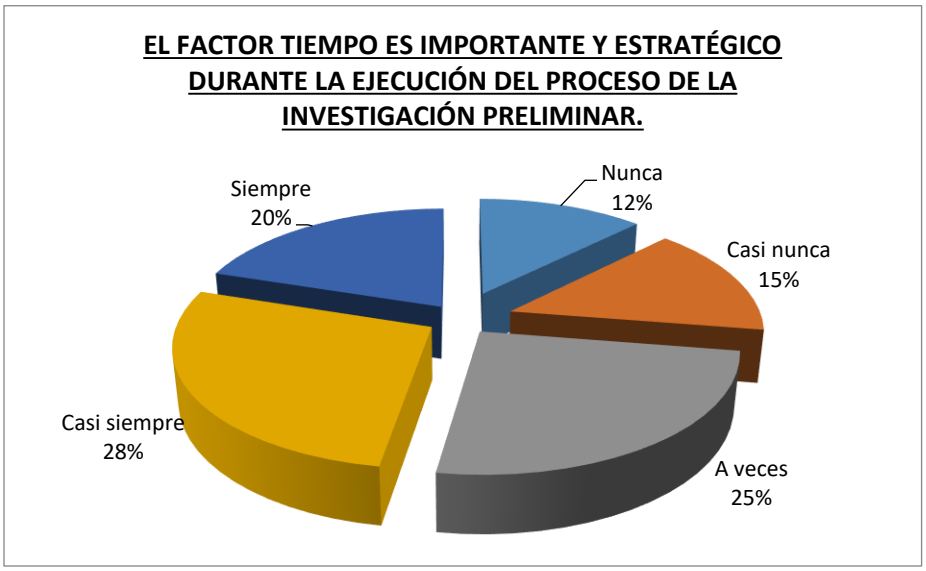

Figure 17

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿El factor tiempo es importante y estratégico durante la ejecución del proceso de la investigación preliminar? El 12% (10) de encuestados manifiestan que nunca, el 15% (12) de encuestados manifiestan que casi nunca, el 25% (20) de encuestados manifiestan que a veces, el 28% (22) de encuestados manifiestan que casi siempre y el 20% (16) de encuestados manifiestan que siempre.

¿EN LAS DENUNCIAS DELICTIVAS ES UN FACTOR SUSTANCIAL EL ASEGURAMIENTO DE LAS EVIDENCIAS Y PERICIAS PRESENTADAS POR LOS DEMANDANTES?	N° ENCUESTADO	%
Nunca	10	12%
Casi nunca	12	15%
A veces	22	28%
Casi siempre	20	25%
Siempre	16	20%
TOTAL	**80**	**100%**

Table 20

FIGURA N° 15

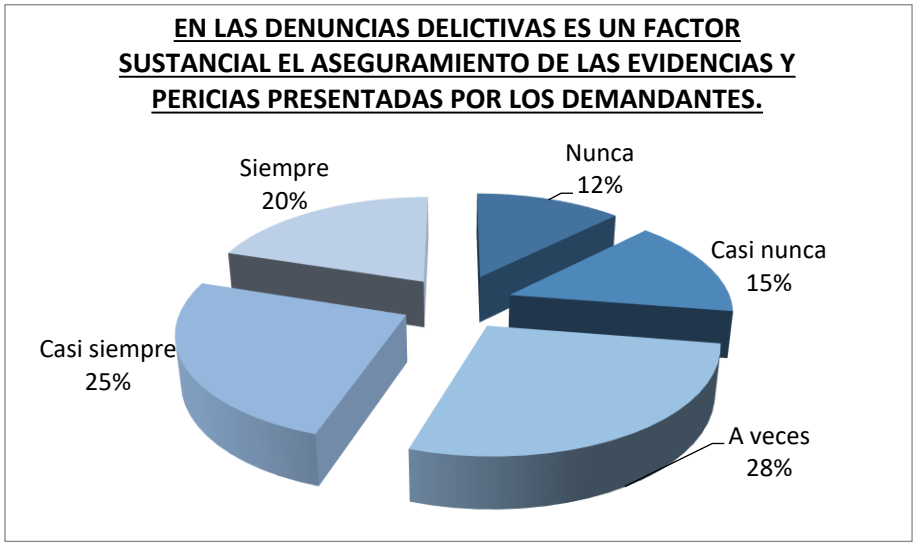

Figure 18

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿En las denuncias delictivas es un factor sustancial el aseguramiento de las evidencias y pericias presentadas por los demandantes? El 12% (10) de encuestados manifiestan que nunca, el 15% (12) de encuestados manifiestan que casi nunca, el 28% (22) de encuestados manifiestan que a veces, el 25% (20) de encuestados manifiesta que casi siempre y el 20% (16) de encuestados manifiestan que siempre.

¿LOS TIEMPOS ORDINARIOS SON FACTORES DEFINITIVOS EN EL PROCESO DE LA INVESTIGACIÓN PRELIMINAR?	N° ENCUESTADO	%
Nunca	20	25%
Casi nunca	10	12%
A veces	8	10%
Casi siempre	16	20%
Siempre	26	33%
TOTAL	**80**	**100%**

Table 21

FIGURA N° 16

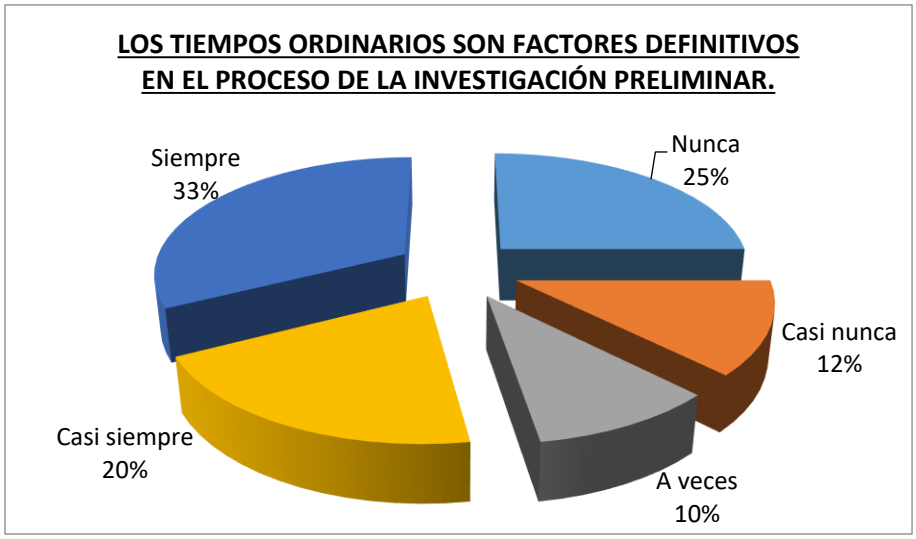

Figure 19

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿Los tiempos ordinarios son factores definitivos en proceso de la investigación preliminar? El 25% (20) de encuestados manifiesta que nunca, el 12% (10) de encuestados manifiesta que casi nunca, el 10% (8) de encuestados manifiestan que a veces, el 20% (16) de encuestados manifiestan que casi siempre y el 33% (26) de encuestados manifiestan que siempre.

¿LOS PROCEDIMIENTOS PARA LAS DENUNCIAS PUNIBLES DEDELITOS INFORMÁTICOS MANTIENEN UN FLUJO ORGANIZADO DE LAS DIFERENTES LABORES Y ACTIVIDADES?	N° ENCUESTADO	%
Nunca	12	15%
Casi nunca	10	12%
A veces	16	20%
Casi siempre	22	28%
Siempre	20	25%
TOTAL	**80**	**100%**

Table 22

FIGURA N° 17

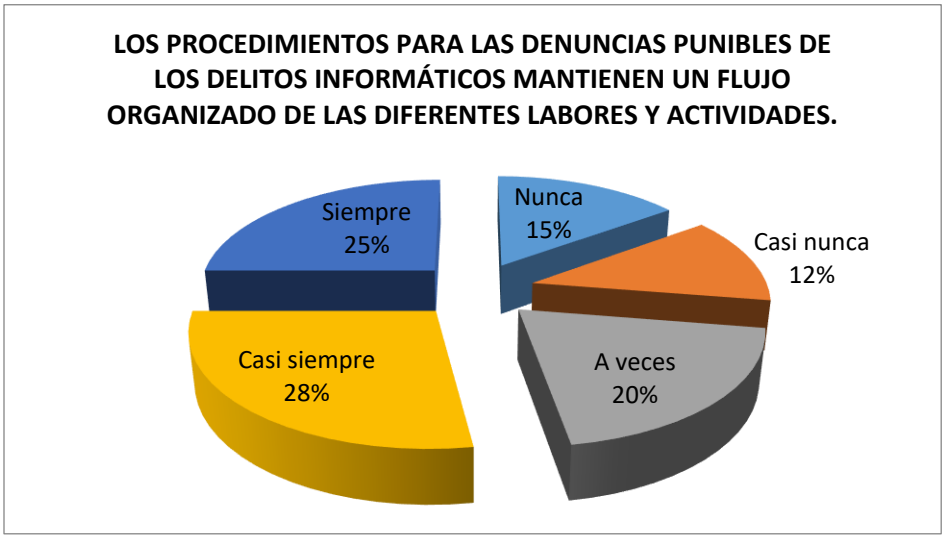

Figure 20

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿Los procedimientos para las denuncias punibles de delitos informáticos mantienen un flujo organizado de las diferentes labores y actividades? El 15% (12) de encuestados manifiesta que nunca, el 12% (10) de encuestados manifiestan que casi nunca, el 20% (16) de encuestados manifiestan que a veces, el 28% (22) de encuestados manifiestan que casi siempre y el 25% (20) de encuestados manifiestan que siempre.

¿EXISTE CLARIDAD EN EL OBJETIVO QUE REVELA LA INVESTIGACIÓN PRELIMINAR POR LOS ACTOS DELICTIVOS QUE GENERA EL FACTOR DE LA CIBERDELINCUENCIA?	N° ENCUESTADO	%
Nunca	8	10%
Casi nunca	24	30%
A veces	16	20%
Casi siempre	12	15%
Siempre	20	25%
TOTAL	**80**	**100%**

Table 23

FIGURA N° 18

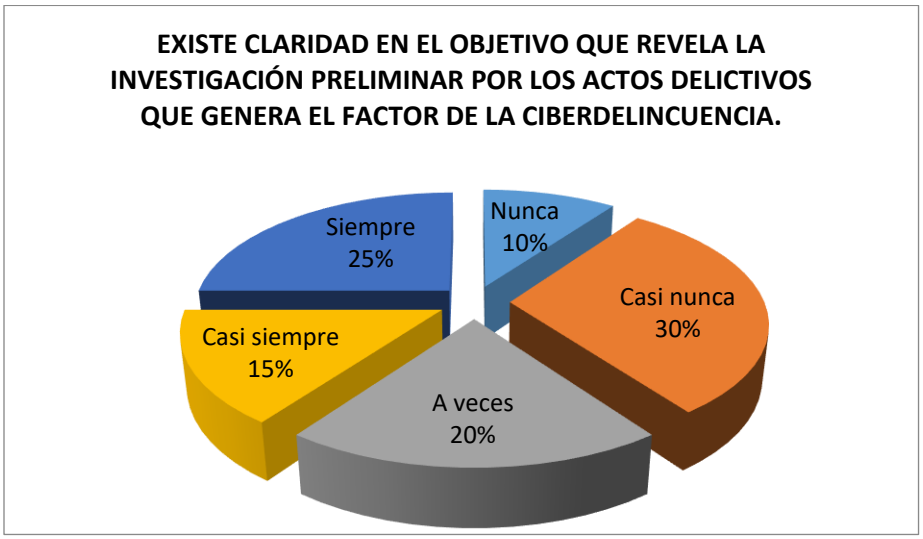

Figure 21

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿Existe claridad en objetivo que revela la investigación preliminar por los actos delictivos que genera el factor de la ciberdelincuencia? El 10% (8) de encuestados manifiesta que nunca, el 30% (24) de encuestados manifiestan que casi nunca, el 20% (16) de encuestados manifiestan que a veces, el 15% (12) de encuestados manifiestan que casi siempre y el 25% (20) de encuestados manifiesta que siempre.

¿LOS PLAZOS Y EL CONTROL DETIEMPOS EN LOS PROCESOS INTERNOS SON FACTORES IMPERATIVOS EN LA INVESTIGACIÓN PRELIMINAR?	N° ENCUESTADO	%
Nunca	10	12%
Casi nunca	8	10%
A veces	22	28%
Casi siempre	16	20%
Siempre	24	30%
TOTAL	**80**	**100%**

Table 24

FIGURA N° 19

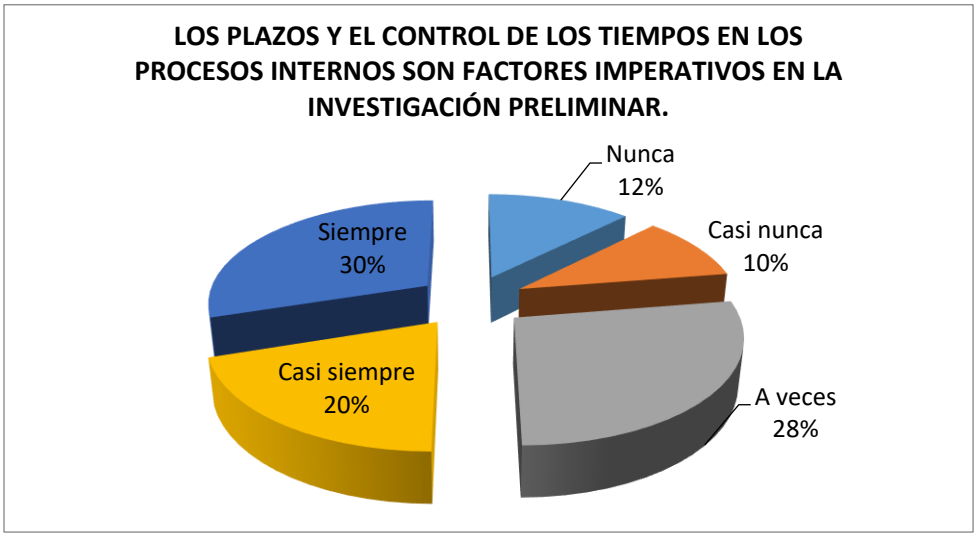

Figure 22

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿Los plazos y control del tiempo en los procesos internos son factores imperativos en la investigación preliminar? El 12% (10) de encuestados manifiestan que nunca, el 10% (8) de encuestados manifiestan que casi nunca, el 28% (22) de encuestados manifiestan que a veces, el 20% (16) de encuestados manifiestan que casi siempre y el 30% (24) de encuestados manifiestan que siempre.

¿LAS ACTAS POLICIALES PRESENTAN CON REGULARIDAD Y PRECISIÓN LOS ELEMENTOS RELACIONADOS A LA INCAUTACIÓN, HALLAZGO, REGISTRO DOMICILIARIO Y CONSTATACIÓN?	N° ENCUESTADO	%
Nunca	12	15%
Casi nunca	10	12%
A veces	22	28%
Casi siempre	16	20%
Siempre	20	25%
TOTAL	**80**	**100%**

Table 25

FIGURA N° 20

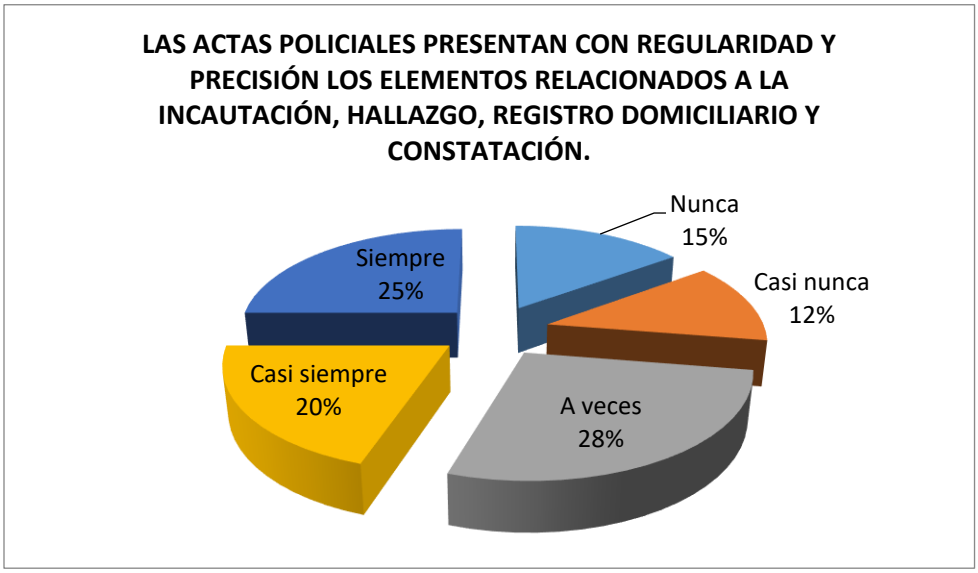

Figure 23

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿Las actas policiales presentan con regularidad y precisión los elementos relacionados a la incautación, hallazgo, registro domiciliario y constatación? El 15% (12) de encuestados manifiestan que nunca, el 12% (10) de encuestados manifiestan que casi nunca, el 28% (22) de encuestados manifiestan que a veces, el 20% (16) de encuestados manifiestan que casi siempre y el 25% (20) de encuestados manifiestan que siempre.

¿LA RESERVA DE LA INFORMACIÓN EN LA INVESTIGACIÓN PRELIMINAR POR PARTE DE LAS AUTORIDADES SON LOS ELEMENTOS SUSTANCIALES EN LA PERSECUCIÓN PENAL?	N° ENCUESTADO	%
Nunca	10	12%
Casi nunca	12	15%
A veces	26	33%
Casi siempre	8	10%
Siempre	24	30%
TOTAL	**80**	**100%**

Table 26

FIGURA N° 21

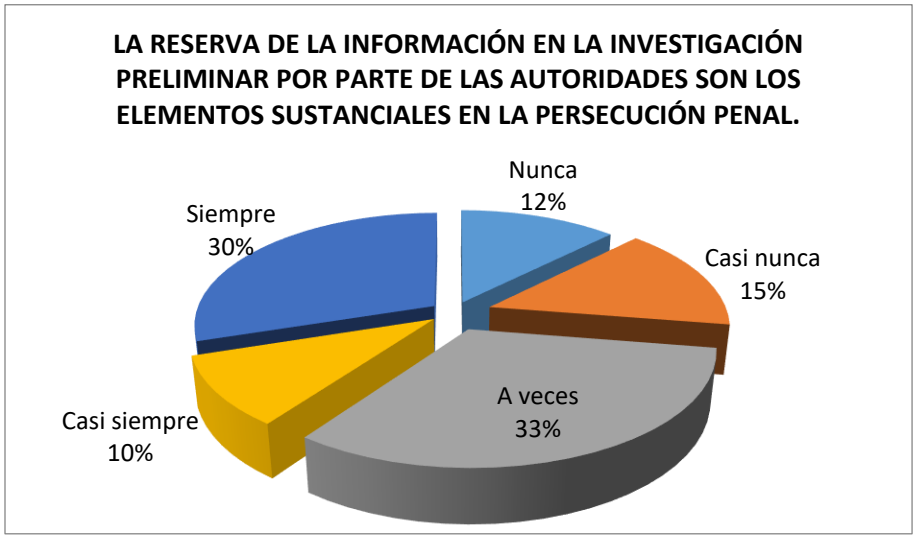

Figure 24

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿La reserva de la información en la investigación preliminar por parte de las autoridades son los elementos sustanciales en la persecución penal? El 12% (10) de encuestados manifiesta que nunca, el 15% (12) de encuestados manifiestan que casi nunca, el 33% (26) de encuestados manifiestan que a veces, el 10% (8) de encuestados manifiestan que casi siempre y el 30% (24) de encuestados manifiestan que siempre.

¿CREE USTED QUE EL FISCAL Y LA POLICÍA GARANTIZAN LOS DERECHOS QUE ASISTEN A LA VÍCTIMA EN ESTE PROCESO DELICTIVO?	N° ENCUESTADO	%
Nunca	16	20%
Casi nunca	10	12%
A veces	20	25%
Casi siempre	12	15%
Siempre	22	28%
TOTAL	**80**	**100%**

Table 27

FIGURA N° 22

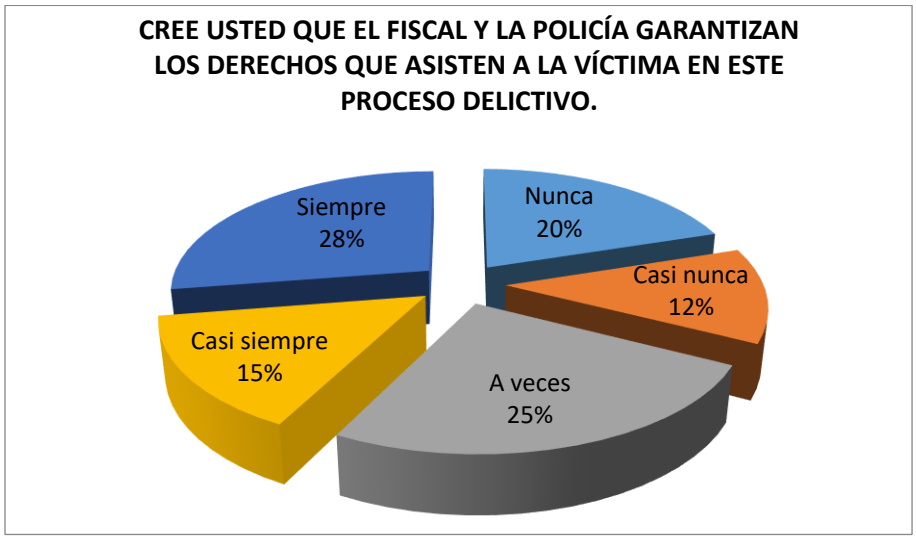

Figure 25

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿Cree usted que el fiscal y la policía garantizan los derechos que asisten a la víctima en este proceso delictivo? El 20% (16) de encuestados manifiestan que nunca, el 12% (10) de encuestados manifiestan que casi nunca, el 25% (20) de encuestados manifiestan que a veces, el 15% (12) de encuestados manifiestan que casi siempre y el 28% (22) de encuestados manifiesta que siempre.

¿CREE USTED QUE EL PROTOCOLO DE LAS PERICIAS CONTIENE LOS ELEMENTOS NECESARIOS Y LOS PROCEDIMIENTOS NORMALIZADOS DURANTE LA INVESTIGACIÓN PRELIMINAR?	N° ENCUESTADO	%
Nunca	12	15%
Casi nunca	16	20%
A veces	24	30%
Casi siempre	20	25%
Siempre	8	10%
TOTAL	**80**	**100%**

Table 28

FIGURA N° 23

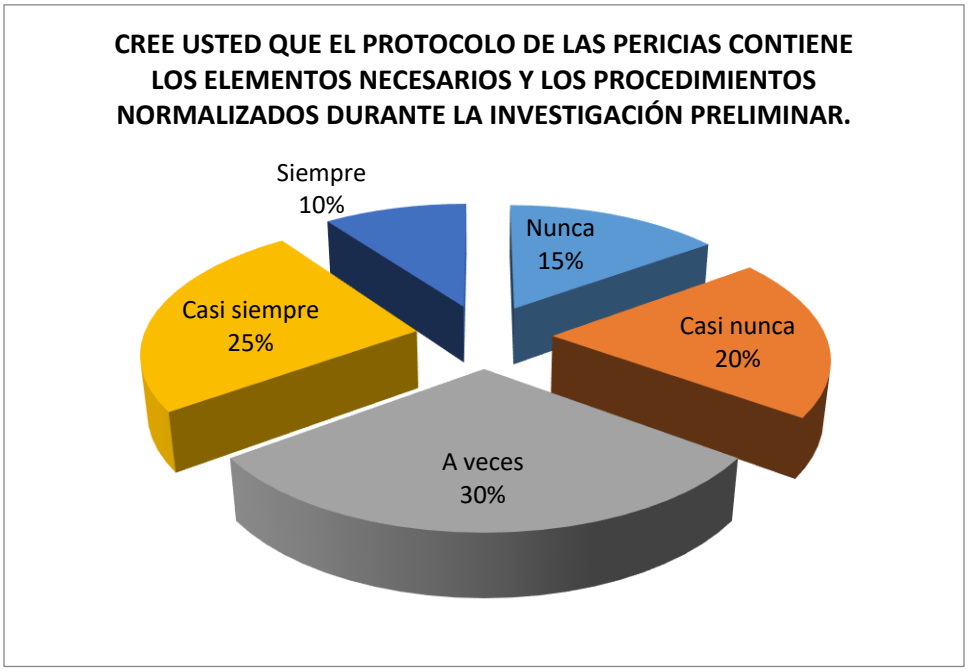

Figure 26

INTERPRETACIÓN:

En la figura, respecto a la interrogante: ¿Cree usted que el protocolo de las pericias contiene los elementos necesarios y los procedimientos normalizados durante la investigación preliminar? El 15% (12) de encuestados manifiestan que nunca, el 20% (16) de encuestados manifiestan que casi nunca, el 30% (24) de encuestados manifiesta que a veces, el 25% (20) de encuestados manifiestan que casi siempre y el 10% (8) de encuestados manifiestan que siempre.

¿LA INVESTIGACIÓN PRELIMINAR CONTIENE DE MANERA ORDENADA LOS PASOS NECESARIOS DE TODA INVESTIGACIÓN PENAL?	N° ENCUESTADO	%
Nunca	12	15%
Casi nunca	18	22%
A veces	26	33%
Casi siempre	8	10%
Siempre	16	20%
TOTAL	**80**	**100%**

Table 29

FIGURA N° 24

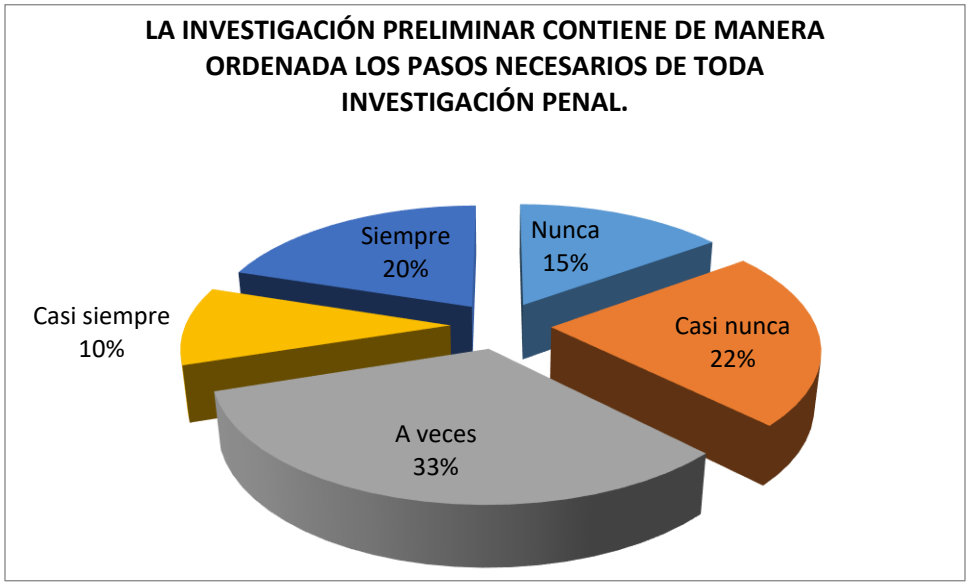

Figure 27

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿La investigación preliminar contiene de manera ordenada los pasos necesarios de toda investigación penal? El 15% (12) de encuestados manifiesta que nunca, el 22% (18) de encuestados manifiestan que casi nunca, el 33% (26) de encuestados manifiesta que a veces, el 10% (8) de encuestados manifiestan que casi siempre y el 20% (16) de encuestados manifiestan que siempre.

¿CREE USTED QUE EL MINISTERIO PÚBLICO DEFIENDE LA LEGALIDAD, LOS DERECHOS HUMANOS DECIUDADANOS ANTE LOS ACTOS DE LA CIBERDELINCUENCIA?	N° ENCUESTADO	%
Nunca	26	33%
Casi nunca	20	25%
A veces	16	20%
Casi siempre	10	12%
Siempre	8	10%
TOTAL	**80**	**100%**

Table 30

FIGURA N° 25

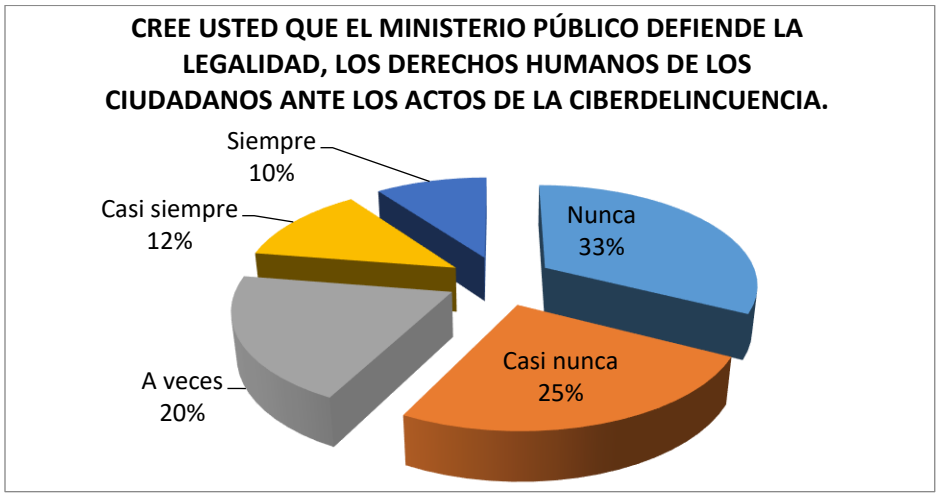

Figure 28

INTERPRETACIÓN:

En la figura, respecto a la interrogante: en su opinión, ¿Cree usted que el ministerio público defiende la legalidad, los derechos humanos de ciudadanos ante los actos de la ciberdelincuencia? El 33% (26) de encuestados manifiesta que nunca, el 25% (20) de encuestados manifiestan que casi nunca, el 20% (16) de encuestados manifiestan que a veces, el 12% (10) de encuestados manifiestan que casi siempre y el 10% (8) de encuestados manifiestan que siempre.

¿SE DESARROLLAN PROGRAMAS DE CAPACITACIÓN PARA LA CIUDADANÍA ACERCA DEPROCESOS DE LA INVESTIGACIÓN PRELIMINAR FRENTE A LOS DELITOS INFORMÁTICOS?	N° ENCUESTADO	%
Nunca	20	25%
Casi nunca	12	15%
A veces	24	30%
Casi siempre	8	10%
Siempre	16	20%
TOTAL	**80**	**100%**

Table 31

FIGURA N° 26

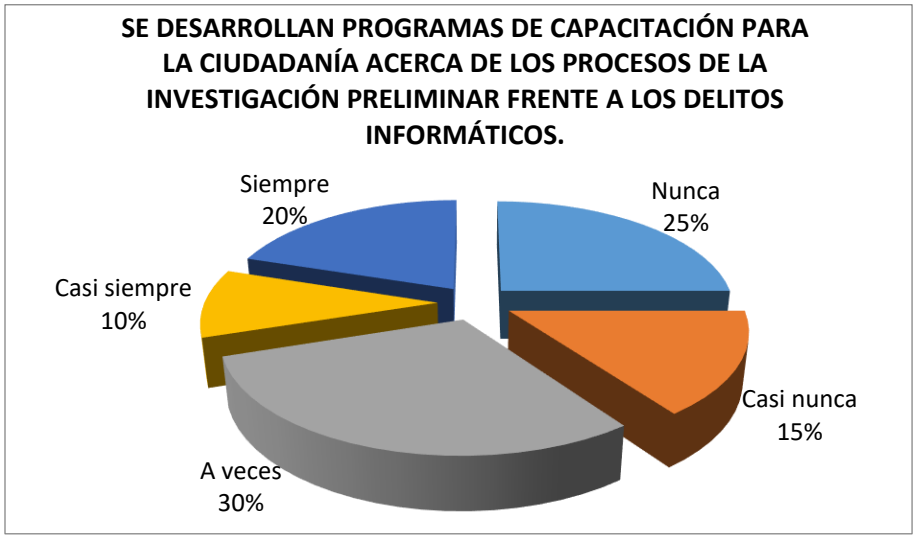

Figure 29

INTERPRETACIÓN:

En la figura, respecto a la interrogante ¿Se desarrollan programas de capacitación para la ciudadanía acerca de procesos de la investigación preliminar frente a los delitos informáticos? El 25% (20) de encuestados manifiestan que nunca, el 15% (12) de encuestados manifiestan que casi nunca, el 30% (24) de encuestados manifiestan que a veces, el 10% (8) de encuestados manifiestan que casi siempre y el 20% (16) de encuestados manifiestan que siempre.

5.3 Discusión de los resultados

Respecto a los delitos informáticos y su relación con el proceso de investigación preliminar en el distrito fiscal de lima norte año 2019.

Según Gonzales, J. (2013). En su tesis analiza la delincuencia Informática: Daños Informáticos del Art. 264 de Código Penal como Propuesta de Reforma, España. Este estudio desarrollo en campo jurídico penal, para precisar actos cometidos contra los sistemas informáticos. Considerando como parte fundamental, del derecho como elemento regulador de la socialización, pero que no pueden ponderarse los diversos sistemas de convivencia respecto a los delitos informáticos.

Al respecto se hizo la siguiente interrogante: ¿Alguna vez tuvo conocimiento que existe la ley penal de delitos informáticos Nº 30171? El 12% (10) de encuestados manifiestan que nunca, el 20% (16) de encuestados manifiestan que casi nunca, el 28% (22) de encuestados manifiesta que a veces, el 15% (12) de encuestados manifiesta que casi siempre y el 25% (20) de encuestados manifiesta que siempre. Lo que evidencia la ley penal respecto al delito informático es poco difundido. A pesar de que la tecnología ha, acelerado su desarrollo en la sociedad, alterando el modo de vida de pobladores, creando una culturad de dependencia tecnológica y cambio de conducta de las sociedades.

Según Montaño (2008). Sobre la Problemática Jurídica en la Regulación de Delitos Informáticos México. El autor en su tesis abordo el análisis de las normas jurídicas respecto al crimen organizado que hace uso de la tecnología para cometer delitos como lavado de dinero.

Al respecto se hizo la siguiente interrogante: ¿En la ley penal de delitos informáticos Nº 30171 se expresa con dureza las sanciones a la ciberdelincuencia? El 15% (12) de encuestados manifiesta que nunca, el 10% (8) de encuestados manifiestan que casi nunca, el 30% (24) de encuestados manifiesta que a veces, el 25% (20) de encuestados manifiestan que casi siempre y el 20% (16) de encuestados manifiestan que siempre. Lo que evidencia poco conocimiento de la ley penal, por lo que se requiere regular de manera específica los términos de

prescripción, de delitos graves, permitiendo de esta manera su correcta aplicación. Permitiendo de esta forma, el desarrollo de la sociedad respecto a la tecnología informática, que ha simplificado las actividades de pobladores, con solo usar un computador. En estos momentos, todo el universo está invadido por la tecnología, el uso del internet, se ha hecho popular en cada rincón del mundo, que permite comunicarse en tiempo real.

Por su parte Ureta (2009). En su estudio retos a superar en la Administración de Justicia ante los Delitos Informáticos en Ecuador. Sostiene como propósito analizar una visión universal de delitos informáticos. Respecto a su reglamentación, en cuanto al delito informático, en la formación de especialistas, son retos, que la doctrina jurídica pone énfasis para tratamiento.

Al respecto se hizo la siguiente interrogante: ¿Existe en la ley de delitos informáticos un ordenamiento organizado de las penas y sanciones que ayuda a protección de sistemas informáticos? El 30% (24) de encuestados manifiestan que nunca, el 20% (16) de encuestados manifiestan que casi nunca, el 25% (20) de encuestados manifiestan que a veces, el 15% (12) de encuestados manifiestan que casi siempre y el 10% (8) de encuestados manifiestan que siempre. Lo que evidencia relativo conocimiento. En tal sentido se puede colegir que los conceptos doctrinarios sobre crimen informático, así como las leyes relacionadas en la legislación en general, explican iniciativas que convergen en forma de propuestas y recomendaciones externas para hacerle frente a los delitos informáticos, de igualmente hace un análisis jurisprudencial respecto a los países latinoamericanos de que forman están afrontando el delito informático.

Por su parte Chávez, A. (2012). En su estudio sobre Policía Cibernética: Vigilancia preventiva, permanente y reactiva a los ilícitos Informáticos. En Guatemala. Señala que su investigación versó sobre la seguridad informática, aspectos informáticos y delitos que se le relacionan con el desarrollo de la investigación tecnológica y los cuerpos encargados de su prevención, detección y corrección. Dentro del mismo se abarca la seguridad informática y su propósito de mantener su integridad, su disponibilidad, su privacidad,

control y su autenticidad respecto a las informaciones controladas por el computador, así como el delito informático como elemento vital para el tema que se investiga.
Al respecto se hizo la siguiente interrogante: ¿La normatividad de la ley penal de delitos informáticos tiene una evidente propagación en los medios de comunicación? El 30% (24) de encuestados manifiesta que nunca, el 33% (26) de encuestados manifiestan que casi nunca, el 10% (8) de encuestados manifiesta que a veces, el 12% (10) de encuestados manifiestan que casi siempre y el 15% (12) de encuestados manifiestan que siempre. Lo que evidencia escaso conocimiento sobre la ley penal de delitos informáticos, lo que equivale un constante desafío para aquellos que desean identificar y analizar la prueba digital en busca de la verdad, ya que la prueba digital es un instrumento de especial cuidado con el objeto de preservar todas las medidas necesarias para no infectar y que no sean objetos de descalificación ante procesos en litigios.

Por su parte Rincón, J. (2015). En su estudio sobre el delito en la ciber- sociedad y la justicia penal internacional - España. El autor propuso elaborar bases teóricas desde la concepción dogmático penal de nivel internacional, permitiendo discernir la necesidad de incorporar dentro de la indagación en materia de juzgamiento sobre delitos informáticos y las telecomunicaciones, conforme sentencia el Estatuto de Roma.

Al respecto se hizo la siguiente interrogante: ¿Cree usted que la protección jurídica en relación a los delitos informáticos obedece a un principio de legalidad? El 28% (22) de encuestados manifiestan que nunca, el 20% (16) de encuestados manifiestan que casi nunca, el 30% (24) de encuestados manifiestan que a veces, el 15% (12) de encuestados manifiestan que casi siempre y el 7% (6) de encuestados manifiestan que siempre. Lo que evidencia que existe conocimiento sobre protección jurídica de delitos informáticos, esta situación ha obligado a la ciencia del derecho, crear nuevos conceptos jurídicos para combatir los delitos informáticos. Por lo que se busca materializar la forma de aplicar de la justicia penal Internacional respecto a delitos perpetrados en ciber- sociedad, donde precisamente, esta investigación cumple su propósito final.

Por su parte Angulo, G. (2016). Sobre la Licitud en la obtención de voz, imagen u otros medios, en el marco del Derecho a la intimidad personal a nivel del Código Penal - Perú.

En su tesis el autor preciso los fundamentos jurídicos-doctrinarios respecto a la licitud para obtener pruebas no autorizadas, cualquiera sea los medios; voz, imagen, que vulnere los derechos a la intimidad personal, por carecer del interés público, como un aporte para la comunidad.

Al respecto se hizo la siguiente interrogante: ¿Para garantizar la seguridad informática los operadores de justicia administran con dureza las herramientas legales? El 28% (22) de encuestados manifiestan que nunca, el 25% (20) de encuestados manifiestan que casi nunca, el 20% (16) de encuestados manifiestan que a veces, el 15% (12) de encuestados manifiestan que casi siempre y el 12% (10) de encuestados manifiestan que siempre. Lo que evidencia el conocimiento sobre la aplicación de herramientas legales, en tal sentido lo que se pondera la forma de obtener de manera no autorizada de pruebas de voz o imagen resulte razonable que sea de interés para la sociedad, su obtención será lícita de manera excepcional, obviando los delitos de violación de su intimidad que esta normado y tipificado en art. 154 de Código Penal Peruano.

Por su parte Sequeiros, I. (2015). En su estudio sobre Vacíos Legales Que Imposibilitan La Sanción de Delitos Informáticos En El Nuevo Código Penal Peruano. El autor en su tesis se desarrolló la nueva modalidad de crimen llamado delitos informáticos. Respecto a esta modalidad delictiva, se ha publicado diversas normas, con finalidad de fiscalizar y sancionar las malas conductas de las personas que mellan los sistemas informáticos, violando la reserva de la comunicación, y el bien jurídico que resultaran afectados con este accionar delincuencial respecto a los patrimonios, fe pública y libertad sexual.

Al respecto se hizo la siguiente interrogante: ¿Los operadores de la justicia están preparados en los contenidos fundamentales de la ley penal de delitos informáticos? El 25% (20) de encuestados manifiestan que nunca, el 28% (22) de encuestados manifiesta que casi nunca, el 12% (10) de encuestados manifiesta que a veces, el 15% (12) de encuestados manifiestan que casi siempre y el 20% (16) de encuestados manifiestan que siempre. Lo que evidencia que los operadores de justicia tienen conocimiento sobre delito informático. Al respecto la Ley N° 30096, que tipifica el delito informático, se promulgo 21 y se publicó 22 de octubre del 2013, parcialmente modificado por la Ley N° 30171,

respecto a los delitos informativos que especifica las penas. Las conductas desarrolladas en el mundo informático, no implican negar ventajas brindadas a la justicia por el sistema informático.

Por su parte Romero, L. (2005). Marco conceptual de delitos informáticos - Lima, Perú. El autor señala en su tesis, la desarrollo de un Nuevo Marco Teórico respecto a los Delitos Informáticos y principales forman que involucran su utilización como punto de apoyo jurídico-científico para quienes legislan la justicia y otras organizaciones gubernamentales comprometidos en la lucha contra el ciber-delito.

Al respecto se hizo la siguiente interrogante: ¿Usted conoce con precisión los derechos que se muestran en la ley penal de delitos informáticos? El 30% (24) de encuestados manifiestan que nunca, el 33% (26) de encuestados manifiestan que casi nunca, el 15% (12) de encuestados manifiestan que a veces, el 12% (10) de encuestados manifiestan que casi siempre y el 10% (8) de encuestados manifiestan que siempre. Se evidencia que conocen la ley penal, sobre derecho informático. Para tal efecto el estudio considera las concepciones teóricas recopilados por el INEI. En tal sentido, el estudio presento una propuesta novedosa respecto al marco conceptual, los delitos informáticos, las conclusiones y recomendaciones para perfeccionar el nuevo marco teórico.

Por su parte Parra, R. (2016). Proyecto legal para un esquema nacional de ciber seguridad. Lima, Perú. El autor desarrolla su estudio sobre la Seguridad Nacional, como garante principal, que permite adoptar medidas pertinentes que permita implementar y aplicar una legislación conforme a la realidad transnacional. El autor pondera el análisis sobre Ciber Delitos, en el escenario internacional.

Al respecto se hizo la siguiente interrogante: ¿En la ley penal de delitos informáticos Nº 30171 los demandantes revelan la presencia de vacíos en las herramientas legales? El 20% (16) de encuestados manifiestan que nunca, el 28% (22) de encuestados manifiestan que casi nunca, el 25% (20) de encuestados manifiestan que a veces, el 22% (18) de encuestados manifiestan que casi siempre y el 5% (4) de encuestados manifiestan que

siempre. Lo que evidencia el conocimiento respecto a los vacíos en la norma. Al respecto la OEA clasifica como delitos, el impacto negativo en la economía por los ataques de ciber delincuentes. Por lo que ha recomendado a las naciones modernizar sus legislaciones del Derecho cibernético, con el esquema de Ciber seguridad. En tal sentido, esta investigación, demostró que internet y las TICs, han alterado la realidad y rebasado las normas jurídicas existentes, por ende falta regular en materia de delitos Cibernéticos.

Por su parte Pardo, A. (2018). Tratamiento jurídico penal de delitos informáticos contra el patrimonio, Distrito Judicial de Lima. El autor en su indagación tuvo como propósito analizar la ponderación jurídico penal respecto a los delitos informáticos contra los patrimonios. En tal sentido, el autor utilizó la técnica de entrevista para recolectar datos, con guías elaboradas de entrevistas respecto a temas nacionales e internacionales, llegándose a conclusiones precisas.

Al respecto se hizo la siguiente interrogante: ¿Existe una ley complementaria en nuevo código procesal penal que difunde el endurecimiento a las sanciones por delitos informáticos? El 28% (22) de encuestados manifiestan que nunca, el 20% (16) de encuestados manifiestan que casi nunca, el 25% (20) de encuestados manifiestan que a veces, el 15% (12) de encuestados manifiestan que casi siempre y el 12% (10) de encuestados manifiestan que siempre. Lo que evidencia del conocimiento respecto al nuevo código procesal penal. Sin embargo, el tratamiento jurídico penal respecto al delito informático es deficiente, dado que dentro del fraude informático no se especifican las modalidades de delitos informáticos.

CONCLUSIONES

PRIMERA CONCLUSIÓN: Luego de examinar los datos bibliográficos y los datos censales del campo, se concluyó que los delitos informáticos, se relacionan con el proceso de investigación preliminar, en distrito fiscal de Lima Norte. Los datos obtenidos al respecto dan cuenta, que en el ministerio público de cono norte, viene aplicando de manera incorrecta la norma jurídica respecto al delito informático, que afecta de esta manera, derechos fundamentales de sujetos procesados, en algunos casos del estado. La informática es de suma importancia para desarrollar a las organizaciones y la sociedad, por lo que es importante ponderar su uso correcto, para no afectar los derechos individuales y colectivos.

SEGUNDA CONCLUSIÓN: Asimismo se concluye que los delitos informáticos se relacionan con las declaraciones realizadas en el proceso de investigación preliminar en distrito fiscal de Lima. Los resultados obtenidos demuestran que el estado debiera actualizar a los operadores del ministerio público en la valoración correcta de las pruebas, con pruebas precisas para no cometer excesos ni omitir los datos de sistemas informáticos, sobre todo de aquellas que han sido obtenidos de manera ilegal, cuya valoración será evaluada excepcionalmente por el organismo competente

TERCERA CONCLUSIÓN: Del mismo modo se concluye que los delitos informáticos se relacionan significativamente con los plazos establecidos en proceso de investigación preliminar en distrito fiscal de Lima. Las evidencias dan cuenta que los procedimientos jurídicos relacionados al tratamiento penal de delitos informáticos para preservar los bienes patrimoniales del estado, son deficientes. El cual genera desorden, porque al no aplicar la norma correctamente sobre el delito informático, se comete omisión en desmedro en contra del estado y en cuanto a su efectividad. Las fiscalías especializadas en esta materia, deben asumir su competencia con ponderación, promoviendo actualizaciones académicas permanentes en convenio con las instituciones académicas.

CUARTA CONCLUSIÓN: En el mismo sentido se concluye que los delitos informáticos se relacionan con el aseguramiento de pruebas en el proceso de investigación preliminar en distrito fiscal de Lima Norte. Las estadísticas finales evidencian, que la aparición de la informática, ha creado un desafío y nuevas para la ciencia del derecho, que ha tenido que cambiar sus paradigmas para poder

describir los usos y costumbres y las conductas sociales de pobladores. El derecho ha tenido que modernizar sus herramientas jurídicas acorde con los entornos digitales para poder valorar las evidencias.

RECOMENDACIONES

PRIMERA RECOMENDACIÓN: Analizados las conclusiones se recomienda que el ministerio público debe promover la aplicación correcta de normas, respecto a las infracciones al sistema informático, relacionados con el proceso de investigación preliminar. Los datos obtenidos al respecto deben valorarse con responsabilidad para no afectar los derechos fundamentales de los seres humanos procesados, en algunos casos del estado.

SEGUNDA RECOMENDACIÓN: Asimismo se recomienda que los operadores de la fiscalía deban capacitar a los fiscales especializados en los delitos informáticos, a fin de que puedan valorar de manera correcta las evidencias para no cometer excesos ni omitir los datos de los sistemas informáticos, sobre todo de aquellas que han sido obtenidos de manera ilegal.

TERCERA RECOMENDACIÓN: Del mismo modo se recomienda establecer plazos para los procesos preliminares de investigación establecidos dentro de los procedimientos jurídicos relacionados al tratamiento penal de las infracciones a las normas informáticos para preservar los bienes patrimoniales del estado, son deficientes. Se recomienda aplicar la norma correctamente sobre el delito informático, sin cometer omisión.

CUARTA RECOMENDACIÓN: Finalmente se recomienda, que el ministerio público debe modernizar su sistema informático respecto a los delitos informáticos relacionados con el aseguramiento de pruebas en el proceso de investigación preliminar en el distrito fiscal de Lima Norte.

REFERENCIAS BIBLIOGRÁFICAS

Almeida, J. (2007). El Derecho frente a la Ciencia y Tecnología. Lima: Grández Gráficos SAC.

Angulo, G. (2016). Licitud en la obtención de voz, imagen u otros medios, en el marco del Derecho a la intimidad personal a nivel del Código Penal Peruano. Trujillo: Ediciones UPAO.

Arias, F. (2012). Introducción a la Metodología Científica. Venezuela: Ediciones El Pasillo.

Ávila, L. (2006). Introducción a la Metodología de Investigación. México: Eumed.net.

Bernal, C. (2010). Metodología de la Investigación Científica. Colombia: Pearson Educación.

Caballero, A. (2006). Guías metodológicas para los planes y tesis de maestría y doctorado. Lima: Instituto Metodológico Alen Caro.

Camacho, L. (2013). El Delito Informático. Madrid: Astrea.

Carrasco, S. (2006). Metodología de la Investigación Científica. Jesús María - Lima: San Marcos.

Córdova, M. (2003). Estadística: Descriptiva e Inferencial. Lima - Perú: Moshera S.R.L.

De la Luz, M. (2013). Delitos Informáticos. México: Porrúa.

Fernández, H. (2014). Manual de Derecho Informático. Buenos Aires: Abeledo Perrot.

Garrido, M. (2013). Nociones Fundamentales de la Teoría del Delito. Editorial Jurídica de Chile, 2012 - Los Delitos Informáticos y la Protección Penal a la Intimidad. Chile: Jurídica de Chile.

Gonzales, J. (2013). Delincuencia Informática: Daños Informáticos del Artículo 264 Del Código Penal y Propuesta de Reforma. Madrid: UCdM.

Guibourg, R., Alende, J., & Campanella, E. (2014). Manual de Informática Jurídica. Buenos Aires: Astrea.

Guzmán, P., & Canales, J. (2010). Informática Jurídica. Lima: Fondo Editorial UIGV.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). Fundamentos de metodología de la investigación. México, D.F.: Sexta Edición.

Hernández, S., Fernández, C., & Baptista, P. (2010). Metodología de la Investigación.

Hernández, S., Fernández, C., & Baptista, P. (2014). Metodología de la Investigación. México D.F.: McGraw-Hill.Interamericana.

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

Llambias, M. (2016). Informática Jurídica. Lima: Ediciones Jurídicas.

Montaño, A. (2008). La Problemática Jurídica en la Regulación de los Delitos Informáticos. México: UNAM.

Pardo, A. (2018). Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018. Lima: Ediciones Vallejo.

Parra, R. (2016). Proyecto legal para un esquema nacional de ciber seguridad. Lima: Castellanos Editores.

Ramos, J. (2008). Epistemología Jurídica. Lima: Editorial San Marcos EIRL.

Rincón, J. (2015). El delito en la cibersociedad y la justicia penal internacional. Madrid: Ucm.

Romero, L. (2005). Marco conceptual de los delitos informáticos. Lima: Ediciones Biblioteca UNMSM.

Sabino, C. (1987). Cómo Hacer una Tesis, Guía para Elaborar y Redactar. Caracas: Panapo.

Sarzana, C. (2012). Criminalitá e Tecnología en Computer Crime Rasaggna Penitenziaria e Criminalitá. Roma: Coe.

Tamayo, M. (1996). Metodología Formal de la Investigación Científica. México D.F.: Limusa.

Tamayo, M. (2012). Metodología de Investigación, pautas para la elaboración de Tesis. México: Limusa.

Ureta, L. (2009). Retos a superar en la Administración de Justicia ante los Delitos Informáticos en el Ecuador. Guayaquil: Espol.

Valdés, J. (2014). Derecho Informático. México: Mc Graw Hill

ANEXOS

Anexo 1: Matriz de consistencia

ANEXO 1: MATRIZ DE CONSISTENCIA

Problemas	Objetivos	Hipótesis	Dimensiones	Metodología
Problema General ¿En qué medida los delitos informáticos se relacionan con el proceso de investigación preliminar en el distrito fiscal de Lima Norte, año 2019? **Problemas Específicos** a) ¿De qué manera los delitos informáticos se relacionan con las declaraciones realizadas en el proceso de investigación preliminar en el distrito fiscal de Lima Norte, año 2019? b) ¿De qué manera los delitos informáticos se relacionan con los plazos establecidos en el proceso de investigación preliminar en el distrito fiscal de Lima Norte, año 2019? c) ¿De qué manera los delitos informáticos se relacionan con el aseguramiento de pruebas en el proceso de investigación preliminar en el distrito fiscal de Lima Norte, año 2019?	**Objetivo General** Determinar en qué medida los delitos informáticos se relacionan con el proceso de investigación preliminar en el distrito fiscal de Lima Norte, año 2019. **Objetivos Secundarios** a) Determinar la manera en qué los delitos informáticos se relacionan con las declaraciones realizadas en el proceso de investigación preliminar en el distrito fiscal de Lima Norte, año 2019. b) Determinar la manera en qué los delitos informáticos se relacionan con los plazos establecidos en el proceso de investigación preliminar en el distrito fiscal de Lima Norte, año 2019. c) Determinar la manera en qué los delitos informáticos se relacionan con el aseguramiento de pruebas en el proceso de investigación preliminar en el distrito fiscal de Lima Norte, año 2019	**Hipótesis General** Los delitos informáticos, se relacionan significativamente con el proceso de investigación preliminar, en distrito fiscal de Lima Norte, año 2019. **Hipótesis Específicos** a) Los delitos informáticos se relacionan significativamente con las declaraciones realizadas en el proceso de investigación preliminar en el distrito fiscal de Lima Norte, año 2019. b) Los delitos informáticos se relacionan significativamente con los plazos establecidos en el proceso de investigación preliminar en el distrito fiscal de Lima Norte, año 2019. c) Los delitos informáticos se relacionan significativamente con el aseguramiento de pruebas en el proceso de investigación preliminar en el distrito fiscal de Lima Norte, año 2019	**Variable independiente** Delitos Informáticos. **Indicadores** ➢ Normas ➢ Obligaciones ➢ Derechos **Variable dependiente** Proceso de Investigación Preliminar. **Indicadores** ➢ Oficio ➢ Denuncia ➢ Noticias	**Enfoque** Cuantitativo **Tipo de Investigación** Aplicada **Nivel de Investigación** El nivel es descriptivo correlacional. **Método** Hipotético – Deductivo **Diseño de la Investigación** Tipo No experimental **Población** Operadores de Justicia **Muestra** Un total 80 personas **Técnicas** Análisis de contenidos **Instrumentos** Cuestionario

ANEXO 2: INSTRUMENTOS DE RECOLECCIÓN DE DATOS

La presente investigación permite recolectar información importante sobre los delitos informáticos y su relación con el proceso de investigación preliminar en el distrito fiscal de lima norte, año 2019.

Por lo que agradeceré se sirva responder con total sinceridad a las siguientes preguntas:

Leyenda:

1	NUNCA	2	CASI NUNCA	3	A VECES	4	CASI SIEMPRE	5	SIEMPRE

1	NUNCA	2	CASI NUNCA	3	A VECES	4	CASI SIEMPRE	5	SIEMPRE

DELITOS INFORMÁTICOS

Preguntas	1	2	3	4	5
Alguna vez tuvo conocimiento que existe la Ley Penal de delitos informáticos Nº 30171.					
En la Ley Penal de delitos informáticos Nº 30171 se expresa con dureza las sanciones a la ciberdelincuencia.					
Existe en la Ley de delitos informáticos un ordenamiento organizado de las penas y sanciones que ayuda a la protección de los sistemas informáticos.					
La normatividad de la Ley Penal de delitos informáticos tiene una evidente propagación en los medios de comunicación.					
Cree usted que la protección jurídica en relación a los delitos informáticos obedece a un principio de legalidad.					
Para garantizar la seguridad informática los operadores de justicia administran con dureza las herramientas legales.					
Los operadores de la justicia están preparados en los contenidos fundamentales de la Ley Penal de delitos informáticos.					
Usted conoce con precisión los derechos que se muestran en la Ley Penal de delitos informáticos.					
En la Ley Penal de delitos informáticos Nº 30171 los demandantes revelan la presencia de vacíos en las herramientas legales.					
Existe una ley complementaria en el Nuevo Código Procesal Penal que difunde el endurecimiento a las sanciones por delitos informáticos.					
Cree usted que la aplicación de la ley penal Nº 30171 es la correcta para frenar este prototipo de denuncia ilícita.					

PROCESO DE INVESTIGACIÓN PRELIMINAR

Preguntas	1	2	3	4	5
Las denuncias por delitos informáticos en la investigación preliminar deben ser presentadas de manera formal y de oficio.					
Considera un factor evidente la aplicación de la estrategia en el proceso de la investigación preliminar ante las denuncias por la ciberdelincuencia.					
La operatividad en el proceso de la investigación preliminar resulta un factor innegable para el aseguramiento de las pruebas y las evidencias.					
En el proceso de la investigación preliminar resulta ineludible tener en cuenta la complejidad y el alcance del tipo de denuncia.					
La duración de la investigación preliminar está en función a la naturaleza y a la razonabilidad del delito cometido.					
El factor tiempo es importante y estratégico durante la ejecución del proceso de la investigación preliminar.					
En las denuncias delictivas es un factor sustancial el aseguramiento de las evidencias y pericias presentadas por los demandantes.					
Los tiempos ordinarios son factores definitivos en el proceso de la investigación preliminar.					
Los procedimientos para las denuncias punibles de los delitos informáticos mantienen un flujo organizado de las diferentes labores y actividades.					
Existe claridad en el objetivo que revela la investigación preliminar por los actos delictivos que genera el factor de la ciberdelincuencia.					
Los plazos y el control de los tiempos en los procesos internos son factores imperativos en la investigación preliminar.					
Las actas policiales presentan con regularidad y precisión los elementos relacionados a la incautación, hallazgo, registro domiciliario y constatación.					
La reserva de la información en la investigación preliminar por parte de las autoridades son los elementos sustanciales en la persecución penal.					
Cree usted que el fiscal y la policía garantizan los derechos que asisten a la víctima en este proceso delictivo.					
Cree usted que el protocolo de las pericias contiene los elementos necesarios y los procedimientos normalizados durante la investigación preliminar.					
La investigación preliminar contiene de manera ordenada los pasos necesarios de toda investigación penal.					
Cree usted que el Ministerio Público defiende la legalidad, los derechos humanos de los ciudadanos ante los actos de la ciberdelincuencia.					
Se desarrollan programas de capacitación para la ciudadanía acerca de los procesos de la investigación preliminar frente a los delitos informáticos.					

Anexo 3: Declaratoria de autenticidad de tesis

ANEXO 3: DECLARATORIA DE AUTENTICIDAD DE TESIS.

Yo, Haydee Ayma Huallpa (Tesista) Identificada con D.N.I. 42790459 de la Escuela Profesional de Maestría en Derecho, autor (a es) de la Tesis titulada:

"Delitos Informáticos y su Relación con el Proceso de Investigación Preliminar en el Distrito Fiscal de Lima Norte, Año 2019"

DECLARO QUE:

El tema de la tesis es auténtico, siendo resultado de mi trabajo personal, que no se ha copiado, que no se ha utilizado ideas, formulaciones, citas integrales e ilustraciones diversas, sacadas de cualquier tesis, obra, artículo, memoria, etc., (en versión digital o impresa), sin mencionar de forma clara y exacta su origen o autor, tanto en el cuerpo del texto, u otros que tengan derechos de autor.

En este sentido, soy consciente de que el hecho de no respetar los derechos de autor y hacer plagio, son objeto de sanciones universitarias y o legales.

Lima, Febrero del 2020.

Firma

D.N.I.: 42790459

UAP UNIVERSIDAD ALAS PERUANAS

FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTOS

I. DATOS GENERALES

- **1.1 . APELLIDOS Y NOMBRES** : SOLIS CÉSPEDES, PEDRO ANÍBAL
- **1.2 GRADO ACADÉMICO** : DOCTOR
- **1.3 INSTITUCIÓN QUE LABORA** : UNIVERSIDAD ALAS PERUANAS
- **1.4 TITULO DE LA INVESTIGACIÓN:** DELITOS INFORMÁTICOS Y SU RELACIÓN CON EL PROCESO DE INVESTIGACIÓN PRELIMINAR EN EL DISTRITO FISCAL DE LIMA NORTE, AÑO 2019.
- **1.5 AUTOR DEL INSTRUMENTO** : HAYDEE AYMA HUALLPA
- **1.6 DOCTORADO / MAESTRÍA** : MAESTRÍA
- **1.7 MENCIÓN** : MAESTRO EN DERECHO
- **1.8 NOMBRE DEL INSTRUMENTO:** CUESTIONARIO
- **1.9 CRITERIOS DE APLICABILIDAD**

a) De 01 a 09: (No válido, reformular)
b) De 10 a 12:(No válido, modificar)
b) De 12 a 15: (Válido, mejorar)
d) De 15 a 18: (Válido, precisar)
c) De 18 a 20: (Válido, aplicar)

II. ASPECTOS A EVALUAR:

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-12)	Bueno (12-15)	Muy Bueno (15-18)	Excelente (18-20)
		01	02	03	04	05
1. CLARIDAD	Esta formulado con lenguaje apropiado					X
2. OBJETIVIDAD	Esta expresado con conductas observables					X
3. ACTUALIDAD	Adecuado al avance de la ciencia y tecnología					X
4. ORGANIZACIÓN	Existe una organización y lógica					X
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad					X
6. INTENCIONALIDAD	Adecuado para valorar los aspectos de estudio					X
7. CONSISTENCIA	Basado en el aspecto teórico científico y del tema de estudio.					X
8. COHERENCIA	Entre las variables, dimensiones y variables					X
9. METODOLOGÍA	La estrategia responde al propósito de estudio					X
10. CONVENIENCIA	Genera nuevas pautas para la investigación y construcción de teorías					X
Sub Total						
Total						**93 %**

VALORACIÓN CUANTITATIVA (total x 0.4) 17
VALORACIÓN CUALITATIVA ES PERTINENTE
OPINIÓN DE APLICABILIDAD ES APLICABLE

Lima, 07 de Enero del 2020

FIRMA Y POS FIRMA DEL EXPERTO
DNI: 26607922

UAP UNIVERSIDAD ALAS PERUANAS

FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTOS

I. DATOS GENERALES

- **1.1 . APELLIDOS Y NOMBRES** : CIEZA MONTENEGRO, NORVIL EMILIANO
- **1.2 GRADO ACADÉMICO** : DOCTOR
- **1.3 INSTITUCIÓN QUE LABORA** : UNIVERSIDAD ALAS PERUANAS
- **1.4 TITULO DE LA INVESTIGACIÓN:** DELITOS INFORMÁTICOS Y SU RELACIÓN CON EL PROCESO DE INVESTIGACIÓN PRELIMINAR EN EL DISTRITO FISCAL DE LIMA NORTE, AÑO 2019.
- **1.5 AUTOR DEL INSTRUMENTO** : HAYDEE AYMA HUALLPA
- **1.6 DOCTORADO / MAESTRÍA** : MAESTRÍA :
- **1.7 MENCIÓN** : MAESTRO EN DERECHO :
- **1.8 NOMBRE DEL INSTRUMENTO:** CUESTIONARIO
- **1.9 CRITERIOS DE APLICABILIDAD**

a) De 01 a 09: (No válido, reformular)
b) De 10 a 12:(No válido, modificar)
b) De 12 a 15: (Válido, mejorar)
d) De 15 a 18: (Válido, precisar)
c) De 18 a 20: (Válido, aplicar)

II. ASPECTOS A EVALUAR:

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-12)	Bueno (12-15)	Muy Bueno (15-18)	Excelente (18-20)
		01	02	03	04	05
1. CLARIDAD	Esta formulado con lenguaje apropiado					X
2. OBJETIVIDAD	Esta expresado con conductas observables					X
3. ACTUALIDAD	Adecuado al avance de la ciencia y tecnología					X
4. ORGANIZACIÓN	Existe una organización y lógica					X
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad					X
6. INTENCIONALIDAD	Adecuado para valorar los aspectos de estudio					X
7. CONSISTENCIA	Basado en el aspecto teórico científico y del tema de estudio.					X
8. COHERENCIA	Entre las variables, dimensiones y variables					X
9. METODOLOGÍA	La estrategia responde al propósito de estudio					X
10. CONVENIENCIA	Genera nuevas pautas para la investigación y construcción de teorías					X
Sub Total						
Total						**90 %**

VALORACIÓN CUANTITATIVA (total x 0.4) 16
VALORACIÓN CUALITATIVA ES PERTINENTE
OPINIÓN DE APLICABILIDAD ES APLICABLE

Lima, 07 de Enero del 2020

FIRMA Y POSTFIRMA DEL EXPERTO
DNI: 08192761

UAP UNIVERSIDAD ALAS PERUANAS

FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTOS

I. DATOS GENERALES

- **1.1 . APELLIDOS Y NOMBRES** : ROMERO LOAYZA, EVA EDY
- **1.2 GRADO ACADÉMICO** : DOCTOR
- **1.3 INSTITUCIÓN QUE LABORA** : UNIVERSIDAD ALAS PERUANAS
- **1.4 TITULO DE LA INVESTIGACIÓN:** DELITOS INFORMÁTICOS Y SU RELACIÓN CON EL PROCESO DE INVESTIGACIÓN PRELIMINAR EN EL DISTRITO FISCAL DE LIMA NORTE, AÑO 2019.
- **1.5 AUTOR DEL INSTRUMENTO** : HAYDEE AYMA HUALLPA
- **1.6 DOCTORADO / MAESTRÍA** : MAESTRÍA
- **1.7 MENCIÓN** : MAESTRO EN DERECHO
- **1.8 NOMBRE DEL INSTRUMENTO:** CUESTIONARIO
- **1.9 CRITERIOS DE APLICABILIDAD**

a) De 01 a 09: (No válido, reformular)
b) De 12 a 15: (Válido, mejorar)
c) De 18 a 20: (Válido, aplicar)
b) De 10 a 12:(No válido, modificar)
d) De 15 a 18: (Válido, precisar)

II. ASPECTOS A EVALUAR:

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-12)	Bueno (12-15)	Muy Bueno (15-18)	Excelente (18-20)
		01	02	03	04	05
1. CLARIDAD	Esta formulado con lenguaje apropiado					X
2. OBJETIVIDAD	Esta expresado con conductas observables					X
3. ACTUALIDAD	Adecuado al avance de la ciencia y tecnología					X
4. ORGANIZACIÓN	Existe una organización y lógica					X
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad					X
6. INTENCIONALIDAD	Adecuado para valorar los aspectos de estudio					X
7. CONSISTENCIA	Basado en el aspecto teórico científico y del tema de estudio.					X
8. COHERENCIA	Entre las variables, dimensiones y variables					X
9. METODOLOGÍA	La estrategia responde al propósito de estudio					X
10. CONVENIENCIA	Genera nuevas pautas para la investigación y construcción de teorías					X
Sub Total						
Total						**95 %**

VALORACIÓN CUANTITATIVA (total x 0.4) 18
VALORACIÓN CUALITATIVA ES PERTINENTE
OPINIÓN DE APLICABILIDAD ES APLICABLE

Lima, 07 de Enero del 2020

Firma y Pos firma del experto
DNI 06624980

UAP UNIVERSIDAD ALAS PERUANAS

FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTOS

I. DATOS GENERALES

- **1.1 . APELLIDOS Y NOMBRES** : CHACÓN JIMÉNEZ, SILVIA
- **1.2 GRADO ACADÉMICO** : DOCTOR
- **1.3 INSTITUCIÓN QUE LABORA** : UNIVERSIDAD ALAS PERUANAS
- **1.4 TITULO DE LA INVESTIGACIÓN:** DELITOS INFORMÁTICOS Y SU RELACIÓN CON EL PROCESO DE INVESTIGACIÓN PRELIMINAR EN EL DISTRITO FISCAL DE LIMA NORTE, AÑO 2019.
- **1.5 AUTOR DEL INSTRUMENTO** : HAYDEE AYMA HUALLPA
- **1.6 DOCTORADO / MAESTRÍA** : MAESTRÍA
- **1.7 MENCIÓN** : MAESTRO EN DERECHO
- **1.8 NOMBRE DEL INSTRUMENTO:** CUESTIONARIO
- **1.9 CRITERIOS DE APLICABILIDAD**

a) De 01 a 09: (No válido, reformular)
b) De 10 a 12:(No válido, modificar)
b) De 12 a 15: (Válido, mejorar)
d) De 15 a 18: (Válido, precisar)
c) De 18 a 20: (Válido, aplicar)

II. ASPECTOS A EVALUAR:

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-12)	Bueno (12-15)	Muy Bueno (15-18)	Excelente (18-20)
		01	02	03	04	05
1. CLARIDAD	Esta formulado con lenguaje apropiado					X
2. OBJETIVIDAD	Esta expresado con conductas observables					X
3. ACTUALIDAD	Adecuado al avance de la ciencia y tecnología					X
4. ORGANIZACIÓN	Existe una organización y lógica					X
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad					X
6. INTENCIONALIDAD	Adecuado para valorar los aspectos de estudio					X
7. CONSISTENCIA	Basado en el aspecto teórico científico y del tema de estudio.					X
8. COHERENCIA	Entre las variables, dimensiones y variables					X
9. METODOLOGÍA	La estrategia responde al propósito de estudio					X
10. CONVENIENCIA	Genera nuevas pautas para la investigación y construcción de teorías					X
Sub Total						
Total						**97 %**

VALORACIÓN CUANTITATIVA (total x 0.4) 18
VALORACIÓN CUALITATIVA ES PERTINENTE
OPINIÓN DE APLICABILIDAD ES APLICABLE

Lima, 07 de Enero del 2020

FIRMA Y POSTFIRMA DEL EXPERTO
DNI: 40965259

UAP UNIVERSIDAD ALAS PERUANAS

FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTOS

I. DATOS GENERALES

- **1.1 . APELLIDOS Y NOMBRES** : ESTRADA GAMBOA, MAURO
- **1.2 GRADO ACADÉMICO** : DOCTOR
- **1.3 INSTITUCIÓN QUE LABORA** : UNIVERSIDAD ALAS PERUANAS
- **1.4 TITULO DE LA INVESTIGACIÓN:** DELITOS INFORMÁTICOS Y SU RELACIÓN CON EL PROCESO DE INVESTIGACIÓN PRELIMINAR EN EL DISTRITO FISCAL DE LIMA NORTE, AÑO 2019.
- **1.5 AUTOR DEL INSTRUMENTO** : HAYDEE AYMA HUALLPA
- **1.6 DOCTORADO / MAESTRÍA** : MAESTRÍA
- **1.7 MENCIÓN** : MAESTRO EN DERECHO
- **1.8 NOMBRE DEL INSTRUMENTO:** CUESTIONARIO
- **1.9 CRITERIOS DE APLICABILIDAD**

a) De 01 a 09: (No válido, reformular)
b) De 10 a 12:(No válido, modificar)
b) De 12 a 15: (Válido, mejorar)
d) De 15 a 18: (Válido, precisar)
c) De 18 a 20: (Válido, aplicar)

II. ASPECTOS A EVALUAR:

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-12)	Bueno (12-15)	Muy Bueno (15-18)	Excelente (18-20)
		01	02	03	04	05
1. CLARIDAD	Esta formulado con lenguaje apropiado					X
2. OBJETIVIDAD	Esta expresado con conductas observables					X
3. ACTUALIDAD	Adecuado al avance de la ciencia y tecnología					X
4. ORGANIZACIÓN	Existe una organización y lógica					X
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad					X
6. INTENCIONALIDAD	Adecuado para valorar los aspectos de estudio					X
7. CONSISTENCIA	Basado en el aspecto teórico científico y del tema de estudio.					X
8. COHERENCIA	Entre las variables, dimensiones y variables					X
9. METODOLOGÍA	La estrategia responde al propósito de estudio					X
10. CONVENIENCIA	Genera nuevas pautas para la investigación y construcción de teorías					X
Sub Total						
Total						90 %

VALORACIÓN CUANTITATIVA (total x 0.4) 16
VALORACIÓN CUALITATIVA ES PERTINENTE
OPINIÓN DE APLICABILIDAD ES APLICABLE

Lima, 07 de Enero del 2020

.....
Firma y Pos firma del experto
DNI. 09994766

Anexo 5: Informe del asesor de la tesis con enfoque cuantitativo

UAP UNIVERSIDAD ALAS PERUANAS

INFORME DEL ASESOR DE LA TESIS CON ENFOQUE CUANTITATIVO

INFORME DE ASESOR [X] REVISOR [ ]

Programa Académico	:	Maestría en Derecho
Título del Plan de Tesis	:	Delitos Informáticos y su Relación con el Proceso de Investigación Preliminar en el Distrito Fiscal de Lima Norte, Año 2019.
Apellidos y Nombres del Tesista	:	Haydee Ayma Huallpa

TÍTULO DE LA TESIS

		CUMPLE	NO CUMPLE
1.	Sugiere una idea clara del problema investigado.	X	
2.	Incluye las variables de investigación.	X	

Observaciones a implementar:

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

		CUMPLE	NO CUMPLE
1.1	Realiza la descripción de la realidad problemática de lo general a lo particular.	X	
1.2	Se define y delimita el problema adecuadamente.	X	
1.3	El problema es coherente con las líneas de investigación del programa cursado.	X	
1.4	El problema general es relevante, está claramente formulado y guarda relación con el problema planteado.	X	
1.5	Los problemas específicos (si hubiese) son derivados del problema general y contribuyen a resolverlo.	X	
1.6	Los objetivos de la investigación son claros y contienen las variables y sus dimensiones.	X	
1.7	Los objetivos específicos (si hubiese) contribuyeron a alcanzar el objetivo general.	X	
1.8	La justificación expresa la relevancia e importancia de la investigación.	X	
1.9	Describe la factibilidad y las limitaciones que afectaron trabajo de investigación.	X	

Observaciones a implementar:

CAPÍTULO II. MARCO TEÓRICO CONCEPTUAL

		CUMPLE	NO CUMPLE
2.1	Incluyó como antecedentes investigaciones nacionales e internacionales relacionadas con el problema de investigación en el número señalado en la guía correspondiente.	X	
2.2	Las bases teóricas están organizadas en forma lógica y dan fundamento a la investigación y sustentan la conceptualización de las variables y sus dimensiones.	X	
2.3	Se precisa con claridad el significado de los términos básicos y se citan a sus autores.	X	
2.4	La cobertura bibliográfica del tema es pertinente y se ajusta a lo solicitado.	X	

Observaciones a implementar:

CAPÍTULO III. HIPÓTESIS Y VARIABLES

		CUMPLE	NO CUMPLE
3.1	Son claras y coherentes con los problemas y objetivos.	X	
3.2	Son coherentes con el marco teórico.	X	
3.3	Son susceptibles de verificación empírica.	X	
3.4	Son planteadas afirmativamente.	X	
3.5	Contienen y precisan la relación entre las variables y dimensiones.	X	
3.6	Ha realizado la definición conceptual y operacional de las variables correctamente.	X	
3.7	Se estableció la operacionalización de las variables de una manera correcta.	X	

Observaciones a implementar:

CAPÍTULO IV: METODOLOGÍA DE LA INVESTIGACIÓN

		CUMPLE	NO CUMPLE
4.1	Se señala y explica adecuadamente el tipo y nivel de la investigación.	X	
4.2	Se indica el método y diseño de la investigación.	X	
4.3	Se establecen las variables en función al tipo y diseño de la investigación.	X	
4.4	Se describe la población y muestra de la investigación.	X	
4.5	Se describen las técnicas e instrumentos que se utilizó en el estudio.	X	
4.6	Se describe el procesamiento de datos y el estadístico utilizado.	X	
4.7	Los instrumentos fueron apropiados para la investigación.	X	
4.8	Se ha realizado la valides y confiabilidad de los instrumentos de una manera adecuada.	X	
4.9	Se ha incluido la validación del número de expertos solicitados en la guía correspondiente.	X	
4.10	Se describe el procedimiento para la obtención de los resultados, según el tipo y naturaleza de la investigación.	X	

Observaciones a implementar:

CAPÍTULO V: RESULTADOS

		CUMPLE	NO CUMPLE
5.1	En el análisis descriptivo se explican los procedimientos utilizados en el trabajo de campo.	X	
5.2	Los resultados se han descrito por variables y dimensiones.	X	
5.3	En el análisis inferencial se ha realizado la prueba de normalidad	X	
5.4	El análisis de cada resultado aporta a la identificación o solución de algún problema propuesto.	X	

Observaciones a implementar:

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

		CUMPLE	NO CUMPLE
6.1	Las conclusiones son lógicas y pertinentes.	X	
6.2	Las conclusiones son coherentes con los resultados encontrados.	X	
6.3	Las recomendaciones se derivan de las conclusiones.	X	
6.4	Las recomendaciones son factibles de realización y responden a los objetivos de la investigación.	X	

Observaciones a implementar:

CAPÍTULO VII: REDACCIÓN DEL IN FORME DE TESIS

		CUMPLE	NO CUMPLE
7.1	En la redacción se ha usado el lenguaje científico, con propiedad semántica, sintáctica y ortográfica.	X	
7.2	Está redactado en tercera persona y en tiempo pasado.	X	
7.3	Las citas de los textos y referencia bibliográfica se ajustan a un modelo determinado según la guía correspondiente.	X	

Observaciones a implementar:

CAPÍTULO VIII: REFERENCIAS BIBLIOGRÁFICAS

		CUMPLE	NO CUMPLE
8.1	Se encuentran todos los autores citados en el cuerpo del trabajo y siguen las normas internacionales aplicables.	X	

Observaciones a implementar:

CAPÍTULO IX: ANEXOS

		CUMPLE	NO CUMPLE
9.1	Se incluye la matriz de consistencia.	X	
9.2	Se incluye los instrumentos de recolección de datos organizado en variables, dimensiones e indicadores.	X	
9.3	Se incluye la ficha de validación de los instrumentos.	X	
9.4	Se incluye la matriz de validación de los instrumentos.	X	
9.5	Se incluye la validación de los instrumentos realizados por el número de expertos solicitados en la guía correspondiente.	X	
9.6	Se incluye el consentimiento informado.	X	
9.7	Se incluye la declaratoria de autenticidad del informe de tesis	X	

Observaciones a implementar:

X. COMENTARIOS FINALES:

Aprobado para continuar con el trámite

Fecha del Informe : 04 02 2020

DRA. CYNTHIA CONTRERAS GALVEZ
ASESOR
DNI: 41678197