UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA ACADÉMICA PROFESIONAL DE DERECHO

LA FORMACIÓN PROFESIONAL EN DERECHO INFORMÁTICO Y LA PERSECUCIÓN PENAL DE DELITOS INFORMÁTICOS EN EL DISTRITO FISCAL DE HUÁNUCO - 2017

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE ABOGADO

TESISTA:

Br. LEONARDO EDGARD VILCA MORALES

ASESOR:

Dr. CESAR ALFONSO NAJAR FARRO

HUÁNUCO, PERÚ

2018

DEDICATORIA

La presente investigación la dedico a mi madre Marilú por formarme en ser una persona recta, profesional y de valores, como también a mi padre Edgar por sus enseñanzas que me motivaron a ingresar al mundo del saber, del conocimiento y de la ciencia.

AGRADECIMIENTO

Agradezco de manera especial al Dr. Cesar Alfonso Najar Farro por su valioso asesoramiento, como también a mis familiares, maestros, amigos y a todos aquellos que me ayudaron y motivaron a que esta investigación se concretice.

RESUMEN

La investigación que se presenta a continuación se titula “La formación profesional en derecho informático y la persecución penal de delitos informáticos en el distrito fiscal de Huánuco – 2017” el cual es un estudio del tipo descriptivo que tuvo como objetivo general determinar si existe una relación directa entre la formación profesional en derecho informático y la persecución penal de delitos informáticos, lo cual a través de la revisión teórica así como de la aplicación de los instrumentos de investigación se logró corroborar a través de comprobación de la hipótesis que planteaba la existencia de dicha relación.

El presente trabajo inicia a través del capítulo titulado “El problema de investigación” en el cual se detallan todos los aspectos fundamentales para que este estudio se realizará, como la formulación del problema de investigación, sus objetivos, hipótesis y así como la justificación e importancia de este estudio.

En el capítulo siguiente que se titula “Marco teórico”, recoge en primer lugar todos los antecedentes de estudio locales, nacionales e internacionales que el investigador ha revisado sobre el problema de investigación, siendo que se ha hecho el esfuerzo de incluir estudios redactados en un idioma diferente al español; seguidamente se ha continuado el marco teórico a través de tres marcos independientes, el primero denominado marco histórico, el cual recoge los antecedentes históricos de las variables de estudio, el segundo denominado el marco conceptual, en donde a través de conceptos y definiciones se han desarrollado teóricamente los temas concernientes a esta investigación, y el tercero que viene a ser el marco jurídico, uno de los más importantes pues esta investigación al ser un estudio en el campo del derecho tiene como médula el ordenamiento jurídico que rodea a la investigación; finalmente se ha

desarrollado más adelante como complemento la definición de los términos básicos, pues al ser esta una investigación que estudia parte de la informática y el derecho, implica el uso de términos especiales de ambos campos del conocimiento que necesitan aclararse conceptualmente.

Continuando con la investigación se tiene el capítulo titulado “Marco metodológico”, el cual contiene toda las precisiones metodológicas de este estudio, es decir el nivel, tipo y diseño de investigación, las técnicas e instrumentos utilizados, así como la población y muestra de estudio, la cual estuvo conformada por los fiscales de las fiscalías provinciales penales corporativas así como las carpetas fiscales archivadas en delitos informáticos, siendo que ambas poblaciones de estudio fueron delimitadas espacialmente en el distrito fiscal de Huánuco, y temporalmente en el año 2017.

Los siguientes capítulos titulados “Resultados” y “Discusión de resultados” son los capítulos en los cuales se presentan los datos obtenidos de la aplicación de los instrumentos de investigación, que incluyeron una encuesta, una guía de entrevista y una matriz de análisis de datos, datos que fueron cuantificados haciendo uso de la estadística, para luego ser interpretados y analizados, lo cual sirvió de base junto al marco teórico para realizar la contratación de las hipótesis general así como de las hipótesis específicas de este estudio, cumpliéndose con los objetivos planteados inicialmente como se explica en las conclusiones y recomendaciones de esta investigación.

PALABRAS CLAVE: Formación profesional, derecho informático, persecución penal, delitos informáticos.

ABSTRACT

The research presented below is entitled "Professional training in computer law and criminal prosecution of computer crimes in the tax district of Huánuco - 2017" which is a descriptive study whose general objective was to determine if there is a relationship direct between professional training in computer law and the criminal prosecution of computer crimes, which through the theoretical review as well as the application of research tools was corroborated through verification of the hypothesis that raised the existence of such relationship.

The present work begins through the chapter entitled "The research problem" in which all the fundamental aspects are detailed so that this study will be carried out, such as the formulation of the research problem, its objectives, hypothesis and justification and importance of this study.

In the following chapter entitled "Theoretical Framework", it gathers first all the local, national and international study background that the researcher has reviewed on the research problem, being that the effort has been made to include studies written in a language other than Spanish; then the theoretical framework has been continued through three independent frameworks, the first called historical framework, which includes the historical background of the study variables, the second called the conceptual framework, where through concepts and definitions have been developed theoretically the issues concerning this research, and the third that comes to be the legal framework, one of the most important because this research being a study in the field of law has as its core the legal system surrounding the investigation; finally the definition of the basic terms has been developed later as a complement, since being this a research

that studies part of the computer science and the law, it implies the use of special terms of both fields of knowledge that need to be clarified conceptually.

Continuing with the research we have the chapter entitled "Methodological Framework", which contains all the methodological details of this study, that is, the level, type and design of the research, the techniques and instruments used, as well as the population and study sample. , which was formed by the prosecutors of the provincial criminal prosecution offices as well as the fiscal files filed in computer crimes, being that both study populations were spatially delimited in the fiscal district of Huánuco, and temporarily in the year 2017.

The following chapters entitled "Results" and "Discussion of results" are the chapters in which the data obtained from the application of the research instruments are presented, which included a survey, an interview guide and a data analysis matrix, data that were quantified using the statistics, to be interpreted and analyzed later, which served as the basis for the theoretical framework to perform the hiring of the general hypotheses as well as the specific hypotheses of this study, fulfilling the objectives initially stated as explained in the conclusions and recommendations of this investigation.

KEY WORDS: Professional training, computer law, criminal prosecution, computer crimes.

INTRODUCCIÓN

En esta era de la información, en donde vivimos rodeados de entornos informatizados, los beneficios logrados han sido múltiples, desde comunicarse con otra persona al otro lado del mundo, hasta mejorar la productividad de su trabajo, o tener fuentes de información y entretenimiento en cualquier lugar; en suma se ha cambiado de forma radical el modo de vida del ser humano, sin embargo este entorno virtual representa también un riesgo para personas, empresas e inclusos gobiernos que operan en el campo de la informática, pues la criminalidad se ha trasladado también a este campo, en donde aprovechando fallas y errores de personas y máquinas logran causar graves perjuicios, ya sea atentando contra el patrimonio, la privacidad, o inclusive integridad y derechos de las personas, pues la informática es vista como una puerta abierta que habré una gran variedad de posibilidades para hacer un buen o mal uso de ella.

Por esta razón es que los gobiernos y organismos internacionales han salido en respuesta al problema de la criminalidad informática a través de normas que regulen dicha actividad , lo cual ha incluido en muchos países la penalización de diversos actividades que abusan de la informática para generar perjuicios de todo tipo, dando nacimiento al denominado derecho informático, el cual reúne todo ese marco jurídico de regulación que aún sigue desarrollándose pues se encuentra en constante cambio; sin embargo el problema de la criminalidad informática resulta aún complejo y no se soluciona generando solo normas jurídicas, necesita también enfrentarse desde otros frentes como la formación de especialistas y la implementación de equipos modernos que permitan por ejemplo investigar delitos informáticos y castigar a sus responsables con mayor celeridad; sin embargo estas medidas también seguirán siendo insuficientes si

no se ocupa el problema de la formación profesional de los operadores jurídicos en informática, y más específicamente en derecho informático, y es que recordemos que quienes se ocupan de operar todo ese marco jurídico que rodea a los delitos informáticos y al derecho informático son los abogados, por ello es que al enfocarnos en el problema de los delitos informáticos, se advierte que son los abogados que laboran en el Ministerio Publico quienes deberán hacer frente a la amenaza de los delitos informáticos, siendo que si no están preparados adecuadamente crearán involuntariamente cierto clima de impunidad (que es como viene ocurriendo actualmente) para los cibercriminales. Entonces es importante determinar esta relación que consiste entre el estar formado profesionalmente en esta nueva rama jurídica como es el derecho informático y la persecución a través del derecho penal de este tipo de delitos, pues como se demostró en esta investigación ambas variables de estudio se encuentran relacionadas, afirmación que se sostiene tanto de la revisión teórica que realizó el investigador, como también del análisis de las poblaciones de estudio, que vinieron a ser las carpetas fiscales archivadas sobre delitos informáticos y los fiscales de las Fiscalías Provinciales Penales Corporativas del Distrito Fiscal de Huánuco.

ÍNDICE

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

La presente investigación ocupa la problemática que rodea a los delitos informáticos o también llamados en el mundo como cybercrimes o computer crimes, siendo que para el contexto peruano el investigador identificó en general tres grandes causas a este problema: la primera entendida como la ineficaz legislación en delitos informáticos que tiene el Perú (Estrada, 2008); el segundo relacionado a la escasez de equipos y personal especializado en informática (Rayón & Gomez, 2014); y el tercero relacionado también en la escasa preparación que tienen los operadores jurídicos en informática (Acurio, s.f.), en especial en el denominado derecho informático.

Sobre la primera causa de esta problemática que se relaciona a la legislación peruana en delitos informáticos, se tiene como evidencias en el Perú las duras críticas que recibió la promulgación de la Ley N° 30096 Ley de Delitos informáticos en el año 2013, a la cual diferentes especialistas culparon de crear vacíos legales (AméricaTV, 2013) y confusión respecto a los tipos penales (RPP, 2013), creando en su momento tal problema que fue necesario se promulgue

una modificatoria a través de la Ley N° 30171 en el año 2014 para que se corrigiera las confusiones que la Ley N° 30096 había generado; desde entonces la legislación en materia de delitos informáticos no ha tenido mayores variaciones o cambios importantes hasta a la fecha, sin embargo es importante anotar que aunque se promulgó esta ley especial para combatir los delitos informáticos, lo cierto es que su efecto ha sido débil en la criminalidad informática, pues desde su entrada en vigencia, a nivel nacional los índices de delitos informáticos han seguido en aumento (Publimetro, 2017), y los casos en donde se han aplicado estos nuevos tipos penales son aun mínimos en comparación a otros delitos.

Respecto a la segunda causa de esta problemática descrita como la escases de equipos y personal especializado en informática, esta se evidencia con el hecho que en el Perú solo se cuente con la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional para combatir delitos informáticos, una realidad crítica que es agravada con el hecho de que dicha división policial solo cuenta con oficinas en Lima, un centralismo dañino pues los delitos informáticos se producen en todo el territorio de la nación, en donde la mayoría de departamentos lastimosamente no cuentan con personal ni equipos especializados para siquiera investigar apropiadamente delitos de esta naturaleza (como es el caso del departamento de Huánuco), teniéndose en todo caso que recurrir forzosamente a esta división policial con sede en Lima para obtener la información requerida, la cual incluso llega a demorar pues dicha división se encuentra con una alta carga de trabajo pues tienen casos de diversas partes del Perú, en donde al contar con el personal suficiente no pueden realizar adecuadamente su labor.

Sobre la tercera causa de esta problemática descrita como la escasa preparación que tienen los operadores jurídicos en informática y específicamente en derecho informático, se pone en evidencia cuando advertimos que tanto universidades como centros de especialización no brindan cursos completos y amplios de derecho informático, sino solo en informática básica o en algunos casos excepcionales en informática jurídica, un problema para quienes luego se desempeñan como abogados, incluso ejerciendo cargos importantes como jueces y fiscales, sólo con nociones básicas de informática, sin haber profundizado lo suficiente en el área; esta deficiencia en la preparación se ve luego reflejada en la práctica, así por ejemplo si tomamos el caso de los fiscales de las fiscalías penales, estos no desempeñan eficientemente su labor de investigación por desconocimiento de temas de derecho informático o inclusive de informática general.

1.1. DESCRIPCIÓN DEL PROBLEMA

De las indagaciones teóricas que hizo el investigador sobre los causas antes mencionadas, se encontró que la relacionada a la preparación de los operadores jurídicos era la que menos atención se le había dado, pues no se encontraron muchos estudios o publicaciones académicas al respecto, lo cual resulta preocupante pues era una de las causas más importantes al problema de perseguir adecuadamente los delitos informáticos; por tanto si queremos entender la problemática que viene ocurriendo actualmente, se puede explicar de la siguiente manera: los operadores jurídicos que no tienen una adecuada preparación en derecho informático, la cual les brinde los conocimientos básicos de esta rama nueva rama jurídica, se enfrentan día a día a un mundo informatizado que no todos pueden enfrentar debido a los conocimientos limitados o genéricos que tienen, lo cual sumado al propio desinterés puede

llevar a que se realice una labor poco eficiente cuando se enfrentan a problemas jurídicos dentro del campo de la informática.

Ahora bien, especificando este problema y llevándolo al campo del derecho penal, específicamente al de la persecución penal de delitos informáticos, se debe mencionar que en el proceso penal peruano, quien se ocupa de la persecución del delito es el Ministerio Público, por lo tanto la labor de investigación recae en las fiscalías penales, y por ende en los fiscales que laboran dentro de ellas, de este modo, la persecución penal de los delitos informáticos ha estado recayendo por mandato constitucional en un Ministerio Público aparentemente preparado en estos temas, el cual sin embargo no cuenta con fiscalías especializadas en delitos informáticos, ni personal que tenga sólidos conocimientos sobre dichos delitos, ni tampoco con programas de capacitación permanente o especialización en esta rama del derecho, que bien podría permitir a sus trabajadores informarse adecuadamente de este tema, por tanto la descripción del problema anteriormente se consolidaría en lo siguiente: los fiscales de las Fiscalías Provinciales Penales Corporativas no han tenido una adecuada formación en derecho informático, por tanto cuando se han ocupado de investigar casos de delitos informáticos estos no han tenido las suficientes competencias para lidiar con estos, lo cual deriva a que no se haya llevado en algunos casos eficientemente su labor, desembocando todo esto en investigaciones con muchas limitaciones; por tanto si la fiscalía, que es la encargada de perseguir el delito, no puede investigar y por ende perseguir los delitos informáticos adecuadamente, entonces en el Perú y en muchos departamentos como Huánuco se tiene un clima de impunidad para los cibercriminales, los cuales confían no solo en sus habilidades, sino también de

que quienes se ocupan de investigar sus actos delictivos no están bien preparados en el tema.

1.2. FORMULACIÓN DEL PROBLEMA

Lo que se ha ocupado investigar en la presente investigación es la problemática que rodea a los delitos informáticos, delimitándose como una primera variable a la formación profesional en derecho informático de los operadores jurídicos, específicamente de los fiscales, quienes como se mencionó son los titulares de la acción penal y se ocupan de la investigación del delito, siendo para el investigador una interrogante si dicha formación podría estar relacionada con la persecución de los delitos informáticos, entendida como un conjunto de normas, políticas, y acciones destinadas a identificar y castigar a todos aquellos responsables de cometer dichos delitos, una función que cumple el Ministerio Público. Ahora bien, el investigador ha delimitado como su población de estudio a las Fiscalías Provinciales Penales Corporativas, pues estas son las que se ocupan de la investigación de casos penales, y se ha delimitado espacialmente al distrito fiscal de Huánuco, en razón de que este ocupa dentro de su jurisdicción a la ciudad de Huánuco, la misma que por su naturaleza de capital de departamento, tiene la mayor cantidad de denuncias y casos por delitos informáticos. Por tanto, el investigador formuló a continuación la siguiente pregunta de investigación:

1.2.1. Problema general

¿Cuál es la relación que existe entre la formación profesional en derecho informático y la persecución penal de delitos informáticos en las Fiscalías Provinciales Penales Corporativas del distrito fiscal de Huánuco en el año 2017?

1.2.2. Problemas específicos

PE1. ¿La aplicación de las fuentes jurídicas del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos?

PE2. ¿La aplicación conceptos jurídicos de derecho informático se relaciona significativamente con la persecución penal de delitos informáticos?

PE3. ¿La aplicación del ordenamiento jurídico del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos?

PE4. ¿La resolución de problemas en el ámbito derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos?

PE5. ¿La aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional se relaciona significativamente con la persecución penal de delitos Informáticos?

1.3. OBJETIVOS DE LA INVESTIGACIÓN

1.3.1. Objetivo general

Determinar la relación que existe entre la formación profesional en derecho informático y la persecución penal de delitos informáticos en las Fiscalías Provinciales Penales Corporativas del distrito fiscal de Huánuco.

1.3.2. Objetivos específicos

OE1. Determinar si la aplicación de las fuentes jurídicas del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos.

OE2. Determinar si la aplicación de conceptos jurídicos de derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos.

OE3. Determinar si la aplicación del ordenamiento jurídico del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos.

OE4. Determinar si la resolución de problemas en el ámbito derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos.

OE5. Determinar si la aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional se relaciona significativamente con la persecución penal de delitos Informáticos.

1.4. HIPÓTESIS DE INVESTIGACIÓN

1.4.1. Hipótesis general

Existe una relación directa entre la formación profesional en derecho informático y la persecución penal de delitos informáticos.

1.4.2. Hipótesis específicas

HE1. La aplicación de las fuentes jurídicas del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos.

HE2. La aplicación de conceptos jurídicos de derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos.

HE3. La aplicación del ordenamiento jurídico del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos.

HE4. La resolución de problemas en el ámbito derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos.

HE5. La aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional se relaciona significativamente con la persecución penal de delitos Informáticos.

1.5. VARIABLES

La investigación por ser de tipo correlacional tuvo dos variables estudiadas, las mismas que se mencionan a continuación:

1.5.1. Variable 1

La formación profesional en derecho informático.

1.5.2. Variable 2

Persecución penal de delitos Informáticos.

1.5.3. Operacionalización de las variables

VARIABLE 1	DIMENSIONES	INDICADORES
La formación profesional en derecho informático	Aplicación de las fuentes jurídicas del derecho informático	-Identifica las fuentes de derecho informático. - Analiza las fuentes de derecho informático. - Argumenta utilizando las fuentes de derecho.
	Aplicación conceptos jurídicos de derecho informático	- Identifica los conceptos jurídicos de derecho informático. - Analiza los conceptos jurídicos de derecho informático. - Argumenta utilizando conceptos jurídicos de derecho informático.
	Aplicación del ordenamiento jurídico del derecho informático	- Identifica el ordenamiento jurídico del derecho informático. - Analiza el ordenamiento jurídico en derecho informático - Argumenta en base al ordenamiento jurídico en derecho informático.
	Resolución de problemas en el ámbito derecho informático	- Identifica problemas del ámbito del derecho informático - Analiza problemas del ámbito del derecho informático - Plantea soluciones con fundamentos a problemas del ámbito del derecho informático
	Aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional	- Identifica el uso de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional. - Analiza el uso de la informática jurídica y las Tecnologías de la Información y las Comunicaciones. - Utiliza la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional.

VARIABLE 2	DIMENSIONES	INDICADORES
Persecución penal de delitos Informáticos	Función del Ministerio Público de perseguir penalmente delitos informáticos.	- Investigan la presunta comisión de delitos informáticos. - Acusan a los que cometen delitos informáticos. -Prueban en el proceso penal la responsabilidad penal de los acusados de delitos informáticos. - Se desarrollan políticas de prevención y líneas de acción directa para la persecución de los delitos informáticos.
	Persecución penal de Delitos que afectan a sistemas informáticos.	- Cometidos mediante el acceso ilícito a sistemas informáticos. - Cometidos mediante el atentado a la integridad de los sistemas informáticos.
	Persecución penal de Delitos que afectan datos informáticos.	- Cometidos mediante el acceso ilícito a datos informáticos. - Cometidos mediante el atentando a la integridad de datos informáticos.
	Persecución penal de Delitos que afectan otros bienes jurídicos protegidos.	-Atentan contra la libertad sexual a través de medios informáticos. -Atentan contra la intimidad a través de medios informáticos. -Atentan contra la seguridad pública a través de medios informáticos. -Atentan contra el secreto de las comunicaciones a través de medios informáticos. -Atentan contra el patrimonio a través de medios informáticos.
	Persecución penal de Delitos que utilizan las TIC's.	-Utilizan las Tecnologías de la Información y las comunicaciones para cometer delitos.

1.6. JUSTIFICACIÓN E IMPORTANCIA

1.6.1. Justificación

Tomando como base los criterios que nos proporciona Hernandez Sampieri (2014, p.40) para justificar la realización de este estudio, la presente investigación se justificó en base a las siguientes razones:

- La investigación ha resultado ser conveniente académicamente porque a través de este estudio de carácter científico se ha logrado determinar satisfactoriamente que efectivamente existe una relación directa entre la formación profesional en derecho informático y la persecución de delitos informáticos.
- La investigación tuvo relevancia social porque se ha abarcado a través de este estudio el problema de los delitos informáticos, el cual cobra cada vez mayor relevancia en esta sociedad globalizada e informatizada, esto debido a que los delitos informáticos han estado evolucionando de forma constante y vertiginosa, por lo que los valores de los estudios sobre este tema son de vital importancia pues proporcionan valiosos conocimientos para combatirlos.
- La investigación también tuvo implicaciones prácticas pues en base a este estudio se investigó uno de los principales problemas que causan dificultades en la persecución de delitos informáticos, y nos referimos a la escasa preparación que tienen los operadores del derecho en temas de informática o de derecho informático, por lo que en base al aporte que provee este estudio se podrían diseñar e implementar medidas a futuro que ayuden a solucionar el problema.
- También se debe destacar el valor teórico de la investigación, y es que a través de este estudio se ha abarcado una nueva rama del derecho como es el Derecho Informático, un área aún poco explorado y estudiado en comparación a otras ramas del derecho, pero que cada año cobra mayor importancia en esta sociedad informatizada, por lo cual puede servir esta investigación como base para futuros estudios sobre esta área del derecho.

- La presente investigación tiene un valor metodológico pues se tuvieron que adaptar los instrumentos de investigación al estudio de esta nueva rama del derecho como es el derecho informático, como también para el estudio de los delitos informáticos, de modo que se pueda establecer la relación entre estas dos variables que se estudiaron en esta investigación.

1.6.2. Importancia

Es importante la presente investigación por dos grandes motivos, el primero es que se hace una investigación de una rama del derecho poco conocida y estudiada como es el Derecho Informático, el cual toma cada vez más protagonismo por el crecimiento exponencial que tiene la influencia de la informática en la vida del ser humano y por ende en la sociedad; y el segundo gran motivo es que se investiga parte de una problemática global como son los delitos informáticos, los cuales han venido evolucionando de manera vertiginosa, lo que los hace un problema crítico pues ocasiona toda clase de perjuicios a personas, empresas y gobiernos, por tanto estudios como este resultan valiosos para poder comprender esta problemática y generar soluciones efectivas.

1.6.3. Viabilidad

La investigación fue viable por los siguientes motivos que se señalan a continuación:

- ✓ Se contó con los recursos económicos suficientes para realizar el estudio de manera satisfactoria.
- ✓ Se contó con el acceso necesario a las fuentes de información, como repositorios y bibliotecas para la realización de esta investigación.
- ✓ Se contó con el acceso a las carpetas fiscales archivadas sobre delitos informáticos en el Ministerio Público en Huánuco para su análisis por parte del investigador.

- ✓ Se contó con las autorizaciones necesarias para la aplicación de los instrumentos de investigación en el interior de la sede del Ministerio Público en Huánuco.

1.6.4. Limitaciones

Como limitaciones en el estudio se tiene a los escasos estudios locales y nacionales sobre la problemática de los delitos informáticos que proporcionaran datos objetivos sobre el problema. También se tuvo como limitación que no se pudiera encuestar ni entrevistar a la totalidad de fiscales de las Fiscalías Provinciales Penales Corporativas del distrito fiscal de Huánuco pues muchos de los fiscales se encontraban en diligencias, con licencia o de vacaciones al momento de aplicar la encuesta y guía de entrevista. Finalmente fue una limitación de que no se permitiera sacar copias de los actuados que obran en las carpetas fiscales archivadas pues no se autorizó dicho accionar, lo cual dificultó el análisis de las carpetas por el limitado tiempo que se brindó para revisarlas.

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES TEÓRICOS

Para la presente investigación se ha tenido que hacer una búsqueda minuciosa de bibliografía relacionada al problema y las variables de estudio, para lo cual se tuvo que recurrir a las bibliotecas locales, a bibliotecas en línea y repositorios institucionales de diversas universidades a nivel local, nacional e internacional en búsqueda de estudios objetivos y relevantes; dicha búsqueda que fue muy fructífera, permitió encontrar diversas investigaciones y estudios relacionados al problema de esta investigación o a sus variables, de los cuales se pudo obtener valiosos datos que nos ayudaron en dar mayor sustento teórico al presente trabajo de investigación.

2.1.1. Estudios realizados a nivel internacional

A. **Gonzales Hurtado, Jorge Alexandre. Delincuencia informática: daños informáticos del artículo 264 del código penal y propuesta de reforma. Tesis para obtener el título de doctor en Derecho en la Universidad Complutence de Madrid, Madrid – 2013.**

En esta investigación doctoral que hace un análisis de los delitos informáticos y la legislación española, concluye que aunque a nivel internacional ya existe un marco normativo útil, y que España goza de tener una legislación suficiente en materia de estos delitos informáticos, aún prevalece el problema de las dudas que genera la interpretación de los tipos penales, además de la escasa jurisprudencia que existe, pues el número de casos relacionados a delitos informáticos que se conocen aún son escasos. En esta investigación doctoral que hace un análisis de los delitos informáticos y la legislación española, concluye que aunque a nivel internacional ya existe un marco normativo útil, y que España goza de tener una legislación suficiente en materia de estos delitos informáticos, aún prevalece el problema de las dudas que genera la interpretación de los tipos penales, además de la escasa jurisprudencia que existe, pues el número de casos relacionados a delitos informáticos que se conocen aún son escasos.

B. Medinacelli Diaz, Karina. La necesidad de incorporar en el código penal el tipo penal de falsificación informática. Tesis para optar el grado de licenciado en derecho en la Universidad Mayor de San Andrés, La Paz – 2015.

La investigación aborda el problema de los delitos informáticos preguntándose cuales serían las razones de necesidad para que un tipo penal como la falsificación informática sea incluida en el código penal boliviano, por lo que para responder esta pregunta se plantea como objetivo general identificar la naturaleza y fundamento jurídico de este delito informático. La investigación es del tipo descriptivo-cualitativo, y utiliza métodos como la observación sistemática, el método deductivo, y el método

inductivo, utilizando como técnicas la revisión documental y las entrevistas. De entre las conclusiones, podemos resaltar que la investigadora concluye que el derecho penal y el derecho en su conjunto deben marcar límites en la conducta de los operadores de sistemas informáticos, mediante la tipificación penal de los comportamientos delictivos que pueden derivarse del uso de medios electrónicos, también concluye que la no denuncia de delitos informáticos por las víctimas es a causa de que las víctimas prefieren asumir las consecuencias y ver medidas de prevención en lugar de buscar un proceso judicial, en donde un sistema judicial precario dificulta la planeación de medidas sancionadoras y preventivas adecuadas.

C. **Lemaitre Picado, Roberto. La impunidad de los delitos informáticos en la ciber-sociedad costarricense en ámbito del derecho penal. Tesis para optar el grado de licenciado de en derecho en la universidad de Costa-Rica, San José – 2010.**

La investigación aborda el problema respecto de si el sistema jurídico penal costarricense produce impunidad al presentar insuficiencias en el marco legal del manejo de los delitos informáticos, en un estudio es del tipo cualitativo. De la investigación se puede resaltar que entre sus conclusiones el investigador señala que para comprender los delitos informáticos es necesario conocer las redes informáticas y los equipos informáticos, pues considera que un delito informático no se visualiza correctamente sino se compren el ecosistema donde se desarrolla; también se señala luego del estudio que no hay una definición única de delito informático, lo cual es reflejo de su complejidad; respecto del bien jurídico protegido, el investigador considera que es la información digital contenida en medios informáticos, aunque menciona el concepto de

“apoderamiento sin desapoderamiento” como una característica de los delitos informáticos; finalmente señala que hay una inseguridad jurídica cuando un juez trata de interpretar a su mejor entender, verbos técnicos que se encuentran en los artículos penales sobre delitos informáticos.

D. **Fabian Borghello, Cristian. Seguridad informática: sus implicancias e implementación. Tesis para optar la licenciatura en derecho en la Universidad Tecnológica Nacional, Buenos Aires - 2001.**

   La investigación es presentada como un estudio de análisis sobre la seguridad informática, abordándose como es evidente el tema de los delitos informáticos, en donde el investigador trata de conceptualizar a los delitos informáticos y determinar cuáles son sus características, los tipos, la relación del delincuente y la víctima, así como el tratamiento que se les da en la legislación local e internacional. Entre las conclusiones que se puede resaltar de esta investigación es que el investigador menciona que se adhiere a la idea de que debería haber una legislación internacional unificada que regule el problema de la cibernética y su utilización alrededor del mundo, además para el investigador respecto a los daños que pueden generar de la infiltración a sistemas informáticos, considera que la mejor herramienta para disminuir dichos daños es la capacitación, y no solamente restringir accesos a información.

E. **Organización de las Naciones Unidas. Estudio exhaustivo sobre el delito cibernético. Informe elaborado por la ONU a través de la Oficina de las Naciones Unidad en Drogas y Crimen (United Nations Office on Drugs and Crime), Nueva York – 2013**

   El informe es parte de un estudio realizado por un equipo intergubernamental de expertos de las Naciones Unidas, el objetivo fue

hacer un estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno, en donde se incluyó intercambio de información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional. En el informe es importante resaltar como los estados señalaron a la “capacidad de los agentes de la ley” como un área clave de estrategia nacional sobre delitos cibernéticos, en donde emergió un enfoque concertado sobre establecer la capacidad y capacitación para fiscales, magistrados y jueces, en donde algunos países identificaron como objetivos específicos que “al menos un fiscal que sea responsable exclusivamente de los casos de delito cibernético (...)” o el “crear un grupo de peritos judiciales del sector público y privado para que compartan su experiencia y su conocimiento”.

F. **Garcia Juárez, Ligia Maribel. La investigación de delitos emergentes en internet, su detección y control. Tesis para optar el título y grado académico de licenciada en Investigación Criminal Y Forense en la Universidad Rafael Landívar, Guatemala 2014.**

La investigación abarca los temas de delitos informáticos, la detección de delitos emergentes de internet, y el peritaje informático, con el objetivo de determinar si Guatemala está capacitada para investigación de delitos emergentes de Internet, y como lograr su detección y control. Entre sus conclusiones se puede resaltar que el investigador considera como indispensable y necesaria a correcta instrucción para agentes de investigación de crímenes informáticos, ya que según el investigador son estos quienes tienen bajo su control los elementos o indicios que pueden ser considerados como evidencias y pruebas durante el proceso penal, por

lo que la manipulación de estos debe resguardar su contenido. Además, entre sus recomendaciones el investigador manifiesta que es necesaria la participación del Ministerio Público, pues es el órgano encargado de la persecución penal o bien entidad encargada de velar por el cumplimiento de las normas en materia de delitos informáticos, sugiriendo así que debe de crearse una unidad específica dentro de dicha entidad para el cumplimiento de la ley.

G. **Chauca Acero, Gabriela Cristina. EL PRINCIPIO DE PROPORCIONALIDAD EN LA PREVENCION DE LOS DELITOS INFORMÁTICOS. Tesis para la obtención del título de abogada en la Universidad Regional Autónoma de los Andes. Ibarra-2014.**

La investigación se plantea como objetivo demostrar la importancia de la aplicación del Principio de Proporcionalidad, para la prevención de delitos informáticos cometidos en redes sociales. La investigación de enfoque cualitativo y de tipo descriptivo-propositivo, utiliza como principal instrumento la encuesta. Entre las conclusiones a las que arriba la investigadora encontramos que de acuerdo a la investigadora el desconocimiento del problema de los delitos informáticos es una de las causas de la inseguridad informática que existe, además resalta que en la Código Orgánico Integral Penal de Ecuador conste un capitulo acerca de la Aplicación del Principio de Proporcionalidad en la Prevención de los Delitos Informáticos. Es importante resaltar también que entre las recomendaciones se sugiere que se incentive la formación de los profesionales del derecho en delitos informáticos, ello a través de capacitaciones que sean de iniciativa del Colegio de Abogados.

H. **Zamora Alvizures, José Carlos. Implementación de la informática forense en la obtención de evidencia digital para combatir los delitos informáticos en guatemala. Tesis para para optar al grado académico de Licenciado en Ciencias Jurídicas y Sociales, y los títulos profesionales de abogado y notario en la Universidad de San Carlos de Guatemala, Guatemala – 2012.**

La investigación aborda el fenómeno de los delitos informáticos, en donde el investigador demuestra la hipótesis de que la informática forense permitirá la obtención de evidencia digital para combatir los delitos informáticos en Guatemala, por lo que se plantea como objetivo general establecer el procedimiento jurídico para la implementación de la informática forense. Entre las conclusiones del estudio se puede resaltar que para el investigador es un obstáculo para la persecución penal de los delitos informáticos, la falta de capacitación del Ministerio Publico, de la Policía Nacional Civil y el Instituto Nacional de Ciencias Forense, pues de acuerdo al investigador estos no cuentan con el personal con la preparación necesaria; por tanto es en base a esta conclusión que el investigador sugiere que Es importante que tanto el Ministerio Público, como ente encargado de la persecución e investigación penal, el Instituto Nacional de Ciencias Forenses y la Policía Nacional Civil, como institución auxiliar de la investigación, capaciten a su personal en materia de informática forense, para la investigación de los delitos informáticos, así como también que el Organismo Judicial, como órgano encargado de la administración de justicia, capacite a los jueces, en esta ciencia forense, para conocer y valorar de manera objetiva e imparcial la evidencia digital que se presenta en los procesos penales.

I. **Rincón Ríos, Jarvey. El delito en la cibersociedad y la justicia penal internacional. Tesis para optar el grado de doctor en la Universidad Complutence de Madrid, Madrid – 2015.**

La investigación se fija como objetivo general Proponer la base de una elaboración teórica desde la dogmática penal internacional que permita discutir sobre la necesidad de incluir la investigación y juzgamiento de los delitos informáticos, electrónicos y de las telecomunicaciones en la competencia del Estatuto de Roma. La investigación que es del tipo deductivo concluye que existe la necesidad de buscar un sistema de justicia universal que permita la investigación juzgamiento y sanción de los delitos informáticos o delitos que atentan contra la información y los datos; y también concluye que se hace indispensable que los Estados que se constituyan como partes para la investigación, juzgamiento y sanción de los ciberdelitos, acuerden en una instancia inicial la tipificación de una serie de delitos como ciberdelitos, globales o universales, revistiéndolos de las características técnicas que permiten identificar cuando su comisión ha surgido a través del ciberespacio y de esta forma sobrepasa las barreras del territorio.

J. **Godara, Samiksha. Prevención y control de los delitos informáticos en la india: problemas, temas y estrategias. Una investigación hecha para la Maharshi Dayanand University, Rohtak – 2011.**

El objetivo de este estudio fue tocar todas las facetas importantes que tienen los delitos informáticos en una forma comprensiva, en donde entre sus objetivos se planteó trazar el origen y desarrollo de los delitos informáticos, analizar los principios de jurisdicción de los delitos informáticos, y determinar las iniciativas internacionales que hay para

frenar la amenaza cibernética. La metodología seguida es de un estudio doctrinal, con un análisis comparado del derecho de varios países. El estudio hace observaciones a algunas deficiencias y lagunas normativas que hay en las leyes cibernéticas indias, por lo que el investigador sugiere medidas correctivas para garantizar la prevención y control efectivos de crímenes cibernéticos, tales como: El uso de tecnología encriptada, el desarrollo de la informática forense y las técnicas biométricas, la necesidad de establecer un centro de investigación y desarrollo de delitos informáticos, necesidad de un mecanismo regulador legal universal, necesidad de universalización de la ley cibernética, entre otros.

K. **Imhof, Robert. Los delitos informáticos y el derecho de las telecomunicaciones. Una investigación hecha para la Rochester Institute of Technology, Nueva York – 2010.**

El propósito de la investigación fue perfilar al cibercriminal a través de criminología, el estudio legal de casos y entrevistas profesionales. La conclusión a la cual llega el investigador a través de este estudio es que aunque los delitos informáticos pueden resultar impredecibles, también es cierto que este sigue ciertas tendencias y patrones, de acuerdo a las entrevistas que el investigador hizo, detalla que en todas ellas se mencionó el incremento de ataques cibernéticos foráneos a infraestructuras de red críticas de empresas públicas y privadas; indica también que la motivación de los criminales informáticos es variada pero que en su mayoría se encuentran motivados por un tema económico; un punto de la conclusión de la investigación es que los hackers ven con relativa facilidad perpetrar sus crímenes, siendo que hay una probabilidad baja de ser atrapados, y mucho menos encarcelados, para ellos, esto es

así porque muchas personas no revisan sus ordenadores o siguen las mejores recomendaciones de seguridad, por ello es que las personas que son ignorantes sobre la mejores prácticas de seguridad informática son altamente vulnerables a los ataques.

L. **Leukfeldt, Rutger. El factor humano en el cibercrimen y la ciberseguridad. Una investigación hecha para ELEVEN INTERNATIONAL PUBLISHING. Países Bajos – 2017.**

El objetivo de esta investigación es estimular el estudio del cibercrimen y la ciberseguridad, en donde el factor humano incluye a ofensores, víctimas y actores que desempeñan un papel en la lucha contra el crimen; dentro de la metodología, el investigador se apoya en las consultas, pues este considera que no son necesarias otras técnicas científicas para responder a las preguntas de la investigación. Entre las conclusiones a las que llega el estudio son: Que al estudiar el funcionamiento del sistema de justicia penal con respecto a los delitos informáticos, muestra que la policía, muy aparte de los equipos especializados, no tienen los conocimientos ni habilidades requeridas para manejar efectivamente casos de delitos informáticos; que para hacer intervenciones efectivas, es necesario que la investigación para disuadir a los ciberdelincuentes debe de hacerse con el fin de determinar si tiene sentido aumentar la probabilidad de detección, para lo cual es necesario un conocimiento acerca de las decisiones racionales de ciberdelincuente. Finalmente, el investigador resalta que puede haber otros actores para hacer frente a los ciberdelincuentes, como las asociaciones público-privadas, los proveedores de internet, y ahora incluso empresas como Facebook,

Google, Apple y Microsoft pueden tener un rol en la lucha contra la cibercriminalidad.

M. **Hemraj Saini, Yerra Shankar Rao Y T.C.Panda. Crímenes ciberneticos y sus impactos: un resumen. Una investigation hecha para la International Journal of Engineering Research and Applications (IJERA). 2012.**

La investigación tiene como objetivo investigar los crímenes cibernéticos y su impacto en la sociedad con sus tendencias futuras. El estudio abarca una conceptualización de los delitos informáticos y los tipos de criminales informáticos que hay; por ello al desarrollar las conclusiones, la investigación concluye que la lucha contra estos crímenes se puede clasificar en tres categorías: las leyes cibernéticas, la educación, y la formulación de políticas, que aunque en muchos países no se ha realizado un trabajo significativo en estas, ello no quita de que se deba mejorar el trabajo ya realizado para establecer nuevos paradigmas que nos permitan controlar los ciber ataques.

2.1.2. Estudios realizados a nivel nacional

A. **Vega Aguilar, Jorge Alberto. Los delitos informáticos en el código penal. Tesis para optar el grado académico de magister en Derecho Penal en la Universidad Católica de Santa María, Arequipa – 2010.**

La investigación se había puesto como propósito estudiar los delitos informáticos en el Código Penal, para ello se elaboró un marco histórico de los delitos informáticos, un marco conceptual donde se abarcó los principales términos de lo que el investigador denomina “Ciberespacio”, y un marco teórico en el cual el investigador hizo precisiones sobre los delitos informáticos, las características del delincuente informático, los

bienes jurídicos que resultan afectados por la comisión de estos delitos, y legislación comparada, por lo que en base a todo esto el investigador concluye que los delitos informáticos son plurifensivos, porque afectan diferentes bienes jurídicos, lo cual crea confusión a la hora de realizar la tipificación, agregando además que a la actualidad, tanto jueces como fiscales, cuentan con poco conocimiento y experiencia en el área del Derecho Informático.

B. **Romero Echevarria, Luis Miguel. Marco conceptual de los delitos informáticos. Tesis para optar el grado académico de magister en computación en informática en la Universidad Nacional Mayor de San Marcos.**

   En esta investigación de nivel descriptivo se plantea como objetivo general determinar el factor decisivo que contribuye al mejoramiento de la labor de los operadores de justicia en la investigación y juzgamiento de los delitos informáticos en el Perú. La metodología incluyo la aplicación del método analítico-sintético, el método de la entrevista y el método histórico, valiéndose de técnicas que el investigador menciona como la técnica bibliográfica, la entrevista, y el análisis e interpretación. La principal conclusión que llega el investigador es que se necesita reactualizar constantemente el marco teórico de los delitos informáticos para que se constituya en un instrumento eficaz para los operadores de justicia que intervienen en la lucha con los delitos informáticos en el Perú.

C. **Espinoza Coila, Michael. Derecho Penal Informático: Deslegitimización del poder punitivo en la sociedad de control. Tesis para optar el título profesional de abogado en la Universidad Nacional del Altiplano, Puno – 2017.**

En esta investigación el investigador se aboca del problema de la naturaleza jurídica del Derecho Penal Informático, planteando como hipótesis que el Derecho Penal informático vendría a ser un saber jurídico penal que mediante la interpretación de la ley penal sobre delitos informáticos construye un sistema que limita el poder punitivo y normaliza la sociedad de control cautelando los nuevos espacios de libertad y de privacidad de la población. Por el lado metodológico es una tesis del tipo jurídico dogmático con un diseño cualitativo documental. De la investigación el investigador concluye que efectivamente el derecho Penal Informático es un saber jurídico penal, que mediante la interpretación de leyes penales sobre delitos informáticos propone a los agentes jurídicos un sistema reductor del poder de vigilancia del poder punitivo en la sociedad de control, e impulsar el poder jurídico con el fin de preservar los espacios de libertad y privacidad de las personas. Es importante señalar que el investigador propone la creación de una Fiscalía Especializada en Tecnologías de la Información y Comunicación (TIC).

D. **Parra Perea, Rafael Gustavo. Proyecto legal para un esquema nacional de ciber seguridad. Tesis para optar el grado académico de abogado en la Universidad San Martín de Porres, Lima – 2016.**

El investigador en esta tesis se propone responder tres interrogantes: ¿Cuál es la Diferencia entre Ciber Seguridad y Ciber Defensa?, ¿Por qué la Ciber Seguridad y la Ciber Defensa son de vital importancia para la Defensa del Estado?, ¿Qué busca proteger la Cibersoberanía?. La investigación aplica una metodología exploratoria en base a la afirmación que de que no existían estudios previos en el Perú. Entre sus

conclusiones se puede resaltar que de acuerdo al estudio realizado por el investigador el Ciber Soberania está referida al poder de ejercer soberanía sobre la infraestructura cibernética, que su campo de acción es la protección de información sensible para el estado, y que para que el Estado tenga una adecuada Ciberseguridad necesita de un ordenamiento penal y un mecanismo de persecución de los cibercriminales.

E. **Morales Delgado, Deivid Yuly. La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú. Tesis para optar el título profesional del abogado en la Universidad Señor de Sipán, Pimentel 2016.**

   La investigación se propone explicar la razón de ser de los delitos informáticos, el porqué del uso de la informática computacional para cometer delitos y presentar una propuesta legislativa para el estudio y análisis de la realidad. En el aspecto metodológico, se recurre a la técnica de análisis documental y la técnica del cuestionario. De la investigación se concluye que la influencia de los sistemas informáticos en el Derecho es lo que ha dado lugar a la aparición del Derecho Informático, que existen contradicciones entre las leyes que regulan los delitos informáticos, y que será necesaria la ayuda de la Policía Nacional del Perú para la aprehensión de los delincuentes que cometan delitos informáticos.

F. **Rumiche Pazo, José Alfonso. Sombras de la normatividad que regula el incremento de la ciberdelincuencia en Lima-2015. Tesis para optar el título profesional de abogado en la Universidad Nacional José Faustino Sánchez Carrión. Huacho – 2015.**

En la investigación el investigador se propone determinar si es adecuada la normatividad legal que determina el incremento de la ciberdelincuencia en Lima en el año 2015. Metodológicamente la investigación se presenta como de tipo descriptiva correlacional con enfoque cuantitativo, en donde la población está integrada por miembros de la Policial Nacional del Perú y abogados en lo penal. De las conclusiones se puede resaltar que el investigador si logró determinar que el ejercicio de la actual normatividad que regula la ciberdelincuencia en Lima en el año 2015 contraviene en constantes disyuntivas, y que la falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, por tanto los operadores de justicia deben tener mayores conocimientos en tecnología de la información.

2.1.3. Estudios realizados a nivel local

A. Sequeiros Calderon, Ivett Claritza. Vacíos legales que imposibilitan la sanción de los delitos informáticos en el nuevo código penal peruano. Tesis para optar el Título Profesional de Abogado en la Universidad de Huánuco, Huánuco – 2015.

En esta investigación el objetivo general es determinar qué vacíos legales hay en el Nuevo Código Procesal Penal Peruano y en sus leyes complementarias que imposibilitan la sanción de los delitos informáticos en el Perú; a lo que luego de una labor investigativa no experimental de enfoque cualitativo, en donde se tuvo como población a los fiscales del distrito judicial de Huaura, se concluye que la naturaleza virtual de los delitos informáticos vuelve confusa su tipificación por un poco manejo y conocimiento de esta área.

B. **Romero Ocampo, Meylin del Pilar. Delitos informáticos cometidos a través de redes sociales y su tratamiento en el ministerio público en la ciudad de Huánuco- 2016. Tesis para optar el Título Profesional de Abogado en la Universidad de Huánuco, Huánuco - 2015.**

La investigación trata acerca de determinar cuáles son los delitos informáticos que se cometen en las redes sociales y su tratamiento en el Ministerio Público en Huánuco, así, la tesis concluye que los delitos de: alteración, daño o destrucción de base de datos; atentado a la integridad de datos informáticos; proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos; la Interceptación de datos informáticos; el fraude informático; la suplantación de identidad y el abuso de mecanismos y dispositivos informáticos, son los delitos que tienen mayor frecuencia de un total de 620 procesos, de los cuales el 57.9 fueron archivados, y el 42.1% terminaron en un proceso normal con sentencia dictada.

C. **Ponce Malpartida, Miguel Ángel. Delito informático y acoso sexual de menores de edad regulados por el art. 5 de la ley 30096, en el barrio tunan del distrito de san jerónimo, provincia de huancayo-2016. Tesis para optar el título profesional de abogado en la Universidad de Huánuco, Huánuco – 2017.**

En la investigación se propone como objetivo general determinar de qué forma influye la falta de normatividad y conocimientos sobre Delito Informático para el Acoso sexual de menores de edad, en los pobladores del barrio Tunan en el distrito San Jerónimo de Tunan de la provincia Huancayo -2016. La investigación aplica el método de la inducción-deducción con un diseño transversal descriptivo de tipo correlacional, con

una muestra del tipo probabilística, que incluyó la aplicación de una encuesta a 50 pobladores. Entre las conclusiones, la que más se puede resaltar es que el 62% de los pobladores encuestados tenía un deficiente conocimiento del tema de Delito informático y el acoso sexual a menores de edad, en donde el investigador sugiere como recomendación que se tomen medidas de defensa ante estos delitos por parte del Estado y la Sociedad.

2.2. MARCO HISTÓRICO

2.2.1. Evolución histórica de la formación profesional

La formación profesional a lo largo de la historia ha ido evolucionando progresivamente en todas partes del mundo, desde la antigüedad hasta la época actual ha sido parte incluso del desarrollo humano pues esta se encuentra vinculada a la preparación que debe tener el ser humano para desempeñar diferentes oficios dentro de una sociedad, por lo tanto, revisaremos según etapas históricas como se ha venido dando dicha evolución.

2.2.1.1. En la antigüedad

En la antigüedad desde la aparición del hombre y la formación de los primeros grupos humanos, se vio como el hombre se ocupaba de diversas labores para su supervivencia, desde la recolección de alimentos, la elaboración de herramientas, y la construcción de pequeños campamentos, el hombre desempeñaba todas estas labores por la intuición, pues era fundamental para sobrevivir, como también la observación y la imitación, lo cual permitía que no uno sino todo un grupo humano aprendiera a realizar dichas actividades básicas. Sin embargo el ser humano evolucionó, su forma de vivir y organizar también cambió, y de pequeños grupos humanos nómades evidenciamos como se

construyeron las grandes culturas de la antigüedad, en donde las labores para el crecimiento, mantenimiento y desarrollo de dichos grupos humanos se diversificó, así, vimos como empezaron a aparecer los primeros oficios dentro dichas culturas; por tanto para tener una visión más amplia revisaremos dichos cambios en las principales culturas de la antigüedad.

a) Los egipcios: En el antiguo Egipto, se sabe de la existencia de diferentes oficios que se realizaban, habiendo desde agricultores, artesanos y mineros hasta oficios más avanzados como los de médicos, arquitectos, escribanos y sacerdotes, es en estos últimos en donde se advierte los primeras formas de formación profesional de la historia, y es que por ejemplo para que alguien se desempeñara como médico tenía que seguir cierto proceso de formación o entrenamiento para realizar dicha actividad, y aunque no se podría concebir dicha formación como la formación profesional que ahora conocemos, si nos da luces de cómo fue apareciendo en los albores de la humanidad (Asimov, 1993, p.22).
b) Los griegos: En la antigua Grecia también se evidenció la existencia de diferentes oficios, así también se ha visto la existencia de médicos, arquitectos, artesanos, abogados, etc. Siendo que estos oficios a pesar de que usualmente se transmitían de padres a hijos, también implicaban cierto proceso de entrenamiento previo en donde se les inculcaba los conocimientos que iban a aplicar en determinado oficio; por ello los griegos (como en muchas otras culturas de la época) ya daban los primeros pasos a lo que hoy se conoce como formación profesional.
c) Los romanos: La cultura romana es una de las culturas más representativas del mundo, gozando de una grandeza muy respetada en el mundo antiguo fue también construida de la mano de personas que desempeñaban diversos

oficios que incluso ahora conocemos como profesiones, al igual que en ejemplos anteriores se tiene evidencia de la existencia de arquitectos, abogados, médicos, ingenieros , etc., sin embargo es de resaltarse que para que un ciudadano romano pudiera ejercer alguna profesión, tenía que seguir previamente un proceso educativo que se iniciaba a muy corta edad, y que finalizaba cuando los jóvenes tenían 16 o 17 años, teniendo en ese entonces la opción (generalmente los niños mejor posicionados económicamente) a optar por una carrera pública o como en ese entonces se llamaba “cursos honorum”, o en su defecto optar por ir al ejército (Espinós y Sanchez, 1990, p.14).

2.2.1.2. En la edad media

Durante la edad media podemos ver como muchas de las profesiones que nacieron en la antigüedad se mantuvieron vigentes, y aunque aún con cierta precariedad, se seguía perfeccionando el sistema educativo que preparaba a los hombres para que lleguen a ser profesionales y de este modo ejercer algún oficio, sin embargo la brecha social en la edad media entre ricos y pobres siguió alejando a muchas jóvenes de la posibilidad de ser profesional, y es que recordemos que en la edad media la educación era un privilegio más que un derecho universal, por tanto solo unos pocos accedían a estos conocimientos que les permitiera desempeñar profesiones como las de ingeniero, médico o abogado, por mencionar solo algunos; aun así se sabe que para ser profesional muchos se valieron en su formación sobre todo del método maestro- aprendiz, en donde el maestro se ocupaba de enseñarle todo lo que considerara necesario a su aprendiz antes de que este desempeñara determinada labor, un proceso que tenía como preponderante el aprendizaje por medio de la observación y la imitación.

2.2.1.3. En la Edad Moderna

Con los cambios sociales que vinieron con la edad moderna, la profesionalización de las personas en las nuevas sociedades industriales cobró mayor preponderancia, y es que las exigencias para tener conocimientos profesionales para desempeñar labores dentro de las fábricas (como manipular una máquina) era ahora más importante, así, hablamos en esta época de que se necesitaba ya no solo un conocimiento general sino más profundo que según su nivel de dificultad iba a necesitar un proceso educativo más avanzado, el cual se complementaba con conocimientos profesionales para ejercer determinada profesión, sin embargo es importante anotar que esta impartición de conocimientos profesionales era también bastante limitada, y es que la urgente necesidad de mano de obra en las fábricas hacía que el personal se incorporara luego de recibir breves capacitaciones. Este panorama sin embargo no fue igual en todas las profesiones, y es que las más avanzadas o desarrolladas como la medicina, la ingeniería, la arquitectura, el derecho, etc., gozaban ahora de toda una revolución a nivel de conocimientos que requerían una exigencia intelectual mayor a quienes quisieran desempeñar estos oficios.

En resumen, el cambio que sufre la formación profesional en la edad moderna es sustancial e importante, y lo que más podemos destacar aquí es la aparición en las sociedades industriales (a finales del siglo XIX) de las primeras escuelas de arte y oficios, en donde se enseñaba de forma sistemática y ordenada diversos oficios ocupacionales para el área industrial, agrícola y comercial; las mismas que vendrían a ser un excelente complemento a la labor que ya desempeñaban las universidades en la generación de profesionales en ese entonces (Brunet y Moral, 2017).

2.2.1.4. En la edad contemporánea

En la actualidad la formación profesional ha sufrido diversos cambios, y es que su fuerte relación con la educación ha hecho que evolucione a la par de esta última, por ello ahora se habla por ejemplo de sistemas educativos, en donde jóvenes son instruidos previamente con conocimientos generales, para luego finalizada esta preparación previa puedan iniciar sus formación profesional, ya sea a través de institutos o universidades u otros centros de formación, y aunque estos sistemas varían mucho entre sí, lo cierto es que en esta nueva era la formación profesional tiene una mayor importancia en la sociedad, dada la amplia gama de profesiones que ahora se requieren, implica que se necesita un mayor grupo de personas preparadas con conocimientos más profundos sobre determinadas áreas, por tanto el interés de gobiernos y empresas es ahora mejorar la formación profesional con miras a las exigencias del futuro.

Ahora bien, es importante resaltar que en esta época contemporánea es donde se ha desarrollado más los conceptos sobre formación profesional, por tanto a la pregunta ¿qué es formación profesional?, podemos resaltar que la primera definición hecha por un organismo internacional vino de mano de la Organización Internacional del Trabajo (1970) que en su recomendación Nro. 150 la definía como aquella actividad que “tiene como objeto descubrir y desarrollar aptitudes humanas para una vida productiva y satisfactoria y, en unión con las diferentes formas de educación, mejorar las aptitudes individuales para comprender individual o colectivamente cuanto concierne a las condiciones de trabajo y al medio social, e influir sobre ellos”, dicha definición que resulta algo extensa, es de obligatoria referencia pues es de las definiciones más aceptadas, no solo porque viene de la Organización Internacional del Trabajo, el organismo

más grande a nivel internacional en ocupar asuntos relacionados al trabajo, sino también porque dicha definición provee una idea completa de la formación profesional al hablar de desarrollo de aptitudes individuales. Sin embargo a la actualidad, a la definición que nos da de la Organización Internacional del Trabajo también tenemos la definición que nos provee la Unesco (2016), quienes ahora no solo se ocupan de la formación profesional sino también de la denominada educación y formación técnica y profesional o EFTP en sus siglas en español, que abarca también la formación profesional y se define como aquella parte de la educación que se ocupa de impartir conocimientos y destrezas o capacidades para el mundo del trabajo.

Ahora bien, para tener una mejor visión de esta evolución de la formación profesional y su relación con los nuevos sistemas educativos, es conveniente mencionar a los más representativos actualmente.

A) Sistema de formación profesional en España

Según información que nos brinda el Ministerio de Educación y Formación Profesional en España (2017) en su portal es que esta se encuentra dividida por niveles, y que se resumen a continuación:

- ✓ La formación profesional básica: que son ciclos formativos de dos años para aquellos que no han terminado la Educación Secundaria Obligatoria pero que desean proseguir sus estudios hacia la formación profesional.
- ✓ La formación profesional grado medio: a la cual se accede luego de haber terminado la educación secundaria obligatoria en donde los individuos obtienen al finalizar estos estudios el título de técnico en su titulación.

- ✓ La formación profesional grado superior: entendida como ciclos formativos de grado superior para que el individuo pueda conseguir todas aquellas aptitudes que le permitan adaptarse a situaciones laborales existentes.

B) Sistema de Formación profesional en Alemania

Como bien lo explica Falcón (2015, p.5), Alemania es conocida por su denominado sistema dual de formación profesional, con el cual se busca garantizar que todos sus ciudadanos tengan un formación básica para que puedan insertarse en el mundo laboral; se accede a esta formación dual a través de múltiples vías como son las Berufsfachschule o escuelas de formación profesional, las Fachoberschule que son un tipo de escuela de formación profesional que posibilita a sus estudiante el acceso a la Fachhochschule o universidad de ciencias aplicadas, y finalmente la Fachschule que viene a ser una institución de perfeccionamiento profesional al cual acceden quienes ya tienen una titulación de formación profesional y desempeñan una actividad profesional en relación a un determinada especialidad. Por ello se dice que la dualidad del sistema alemán descansa en los dos elementos que lo sustentan, el primero que vienen a ser las Berufsschule o escuelas de formación profesional y las empresas, en donde la dinámica consiste en que los estudiantes de las escuelas a la vez que asisten a sus clases concurren también a las empresas a laborar.

C) Sistema de formación profesional en China

El sistema de formación profesional en China se caracteriza por ser impartida en cuatro contextos fundamentales (Hernandez, A., y Cascón, R., 2016, p.5):

- ✓ En las escuelas de educación secundaria de nivel inferior.
- ✓ En las escuelas de educación secundaria de nivel superior.

- ✓ Mediante la educación universitaria o de tercer nivel.
- ✓ Mediante la enseñanza de adultos y formación en empresas.

Respecto de este sistema podemos resaltar las bondades que le reconoce la Organización para la Cooperación y el Desarrollo Económicos o OCDE (2017, p.1), entre los más resaltantes esta reconocer el hecho que gracias al sistema se tiene un número creciente de jóvenes que se encuentran en centros profesionales, que gracias al establecimiento de solo 9 años de escolarización casi todos los niños en China finalizan la educación secundaria superior, que el modelo de educación profesional incluye una gran variedad de especializaciones, y que China mantenga el nivel en los centros de formación profesional con los requisitos que requiere en la industria a través de importantes mecanismos que lo garanticen. Sin embargo también la OCDE hace relieve de los desafíos que enfrenta la formación profesional china en base a tres puntos, respecto de la formación en el lugar del trabajo se observa que en China existe una desigual cooperación con los empresarios, así como la escasa presencia de criterios de calidad para la formación en el lugar de trabajo, respecto de los recursos y estándares, se observa que existe un poco dotación de recursos las escuelas de formación profesional en las áreas rurales y provincias pobres, y finalmente respecto de la planificación y coordinación se refiere que china es ineficiente a la hora de satisfacer las necesidades del mercado.

2.2.2. Evolución histórica del derecho informático

Se podría decir que el derecho informático surge a la par de la informática y la cibernética en general, sin embargo, iniciaremos diciendo que dicha concepción no es del todo correcta, para empezar informática y cibernética son dos términos totalmente diferentes:

- ✓ La cibernética es una ciencia multidisciplinaria que apareció por primera vez de la mano de Norbert Wiener a través de su libro “Cybernetics, or Control and Communication in the Animal and the Machine (Cibernética o el control y comunicación en animales y máquinas)”, texto a través del cual proponía la teoría del control y la comunicación entre máquinas y animales (Kubernética, 2017), esto a raíz de una serie de estudios en donde concluía la existencia de mecanismos de control y regulación en hombres, animales y máquinas, como también la conexión entre dichos mecanismos y la transmisión de información. El aporte de Norbert Wiener resultaría fundamental pues a partir de su trabajo se daría nacimiento a las muy conocidas teoría de sistemas, teoría de la información, teorías de la comunicación, etc. Que darían base para otras disciplinas que se desprenderían de la cibernética, entre ellas la informática (Ríos, 1997, p.36).
- ✓ La informática es también considerada una ciencia, pero que se encuentra inmersa dentro de la cibernética como se explicó en el punto anterior, esto en razón de que se apoya en las teorías que nacieron de la mano de la cibernética como son la teoría de la información y la teoría de sistemas, por tanto la principal diferencia será que la ciencia informática se dedica al estudio del tratamiento de la información, sin embargo tenemos que poner en evidencia que el tratamiento de la información históricamente tiene antecedentes mucho más antiguos (Martinez y Garcia, 2000), que parte desde los albores de la humanidad cuando se constituyeron las primeras herramientas de cálculo como el ábaco (5000 a.c.), las calculadoras astronómicas de Stonehenge en Inglaterra, el ábaco mecánico de la edad media, las máquinas de Napier y Schickard para calcular multiplicaciones, la pascalina de Blaise Pascal, etc., hasta llegar aparición primero de la

electrónica, y en base a esta a la era de las computadoras y los lenguajes de programación.

Entonces aclarada la diferencian entre informática y cibernética, toca explicar en qué ha consistido la formación profesional en derecho informático. Como es sabido, la informática que hoy todos conocemos ha estado ligada al uso de los ordenadores, los cuales desde sus primeros momentos (la denominada primera generación) tenían una función meramente experimental y no necesitaba de ninguna regulación especial (entre los años 1940-1050), sin embargo dicho panorama fue cambiando con la aparición de ordenadores de escritorio que ponían al alcance de científicos y negocios (con las computadoras IBM 1401 y IBM 1402) estos novedosos aparatos informáticos que podían recibir, procesar y almacenar información, aunque de forma muy limitada, por ello es que en esta denominada segunda generación de ordenadores (1958) se expandió su uso; ya cuando ingresamos a la denominada tercera generación (1964) con ordenadores como la IBM 360 que fue la pionera de circuitos integrados, nos fuimos acercando al concepto de ordenadores que se tiene actualmente, es por ello que cuando entramos a la cuarta generación tenemos uno de los mayores inventos de ese entonces, y nos referimos al producto que fabricarían Steve Wozniak y Steve Jobs con el primer ordenador Apple, finalmente ya en la quinta generación, que es en la que nos encontramos ahora desde 1991, es la cual en donde se pone bastante énfasis en los chips de alta velocidad (Lopategui, 2017, p.5), los mismos que no solo se perfeccionaron en las computadoras, sino que migraron a otros dispositivos impensados años atrás, como lo son los teléfonos, televisores, relojes, etc. Sin embargo estos ordenadores por si mismos desde su aparición no hubieran tenida mayor relevancia si no fuera por la posibilidad de conectarlos de forma remota desde

cualquier parte del mundo, por ello diremos que buena razón del nacimiento del derecho informático como rama jurídica que regula esta relación entre el derecho y la informático fue a raíz de la aparición de la Internet (Trigo, s.f., p.3), la cual en un principio estaba diseñada para su exclusivo en la defensa de los Estados Unidos de América (un objetivo militar), y que se denominaría inicialmente ARPANET, la cual después de un extenso uso por parte de los militares estadounidense sería dejada de lado parcialmente por los militares, para abrir así las puertas a que civiles pudieran hacer uso de esta red y ampliarla a escala global, sin embargo debemos mencionar que no basto este hecho para que internet se convierta en lo que es hoy, pues se debe de reconocer el trabajo realizado Tim Berners-Lee, un licenciado de la Universidad de Oxford que sería apodado como el padre de la internet por haber desarrollado el tan conocido lenguaje de programación html, así como haber creado los servidores World Wide Web y su primer programa cliente del mismo nombre.

Por tanto con el perfeccionamiento de las computadoras y su interconexión a través del internet, es que tomó relevancia jurídica regular la transmisión y procesamiento de los datos en este entorno informático, apareciendo así el derecho informático, siendo que el término fue acuñado por primera vez en 1970 por el Dr. Wilhelm Steinmüller de la Universidad de Ratisbona de Alemania como “Rechtsinformatik”; sin embargo el control normativo de este mundo informático ha resultado complicado, esto en razón de que no se ha podido lograr consensos para crear un marco normativo internacional sólido que regule la informática, siendo que actualmente encontramos normas especiales en cada país que intentan regularla, normas que repasaremos más adelante en esta investigación, aun así es importante recordar que aunque no exista un marco normativo global que regule la informática, ello no ha implicado que se pasara por alto el riesgo

de que se pueda hacer un uso abusivo de esta ciencia y sus disciplinas, por tanto es que se tiene normas que protegen los derechos humanos de las personas; así, relacionando dichas normas al ámbito informático debemos hacer referencia a las normas que regulan el derecho a la privacidad de las personas, un punto delicado y polémico pues se dice que la privacidad se ha encontrado en riesgo desde que aparecieron los entornos informáticos, por tanto veamos históricamente cual ha sido la protección que se le ha dado a este derecho a a nivel internacional:

- ✓ La Declaración Universal de los Derechos Humanos (1948, p.3) protege la privacidad a través de su artículo 12 que dice: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.”.
- ✓ El Pacto Internacional de Derechos Civiles y Políticos (1976, p.7), que también protege la privacidad de las personas a través de su artículo 17 que dice: “Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.”.
- ✓ En Europa también protegen la privacidad de las personas a través del Convenio para la Protección de los Derechos Humanos y de Las Libertades Fundamentales (1950, p.11) que en su artículo 8 nos dice “Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.”.
- ✓ La Convención Americana sobre Derechos Humanos (1969, p.6), que a través del artículo 11 protege también la privacidad: “Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia,

en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación."

- ✓ La Declaración Internacional sobre los Datos Genéticos Humanos (2003, p.7), que también se ocupó de proteger la privacidad a través de su artículo 14: "Los Estados deberían esforzarse por proteger la privacidad de las personas y la confidencialidad de los datos genéticos humanos asociados con una persona, una familia o, en su caso, un grupo identificables, de conformidad con el derecho interno compatible con el derecho internacional relativo a los derechos humanos.".
- ✓ La resolución de Naciones Unidas titulada "El derecho a la privacidad en la era digital" (2015, p.3), en donde en esencia se reafirma que el derecho a la privacidad es aquel del cual "nadie debe ser objeto de injerencias arbitrarias o ilícitas en su vida privada, su familia, su domicilio o su correspondencia, y el derecho a la protección de la ley contra tales injerencias, establecidos en el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos", y que por tanto afirma que "los derechos de las personas, incluido el derecho a la privacidad, también deben estar protegidos en Internet".

Es importante agregar a este desarrollo histórico, de que en el mundo la preocupación por el derecho informático ha hecho de que se realicen eventos de talla mundial para tratar la regulación de la informática, así tenemos a la Primera Fase de la Cumbre Mundial sobre la Sociedad de la Información desarrollada en Ginebra en el año 2003, en la cual participaron los miembros de la Organización de las Naciones Unidas, y la Segunda Fase de la Cumbre Mundial sobre la Sociedad de la Información en donde se trató el tema de la gobernanza de la Internet. Finalmente, también debemos hacer referencia en

este subcapítulo al histórico convenio sobre cibercriminalidad o también conocido como Convenio de Budapest firmado el 23 de noviembre del 2001, el cual fue el primer esfuerzo conjunto a nivel global para hacer frente a la nueva amenaza de la seguridad mundial como son los delitos informáticos, sin embargo detallaremos el contenido del convenio más adelante en esta investigación.

2.2.3. Evolución histórica de los delitos informáticos

La posibilidad de la existencia de delitos informáticos hizo su aparición histórica desde el momento en que la informática digitalizó datos, para almacenarlos, transmitirlos o procesarlos; dicho momento que ocurrió a mediados del siglo XX con el nacimientos de las denominadas ciencias de la computación (entre otras disciplinas), despertó el interés de muchos criminales con conocimientos avanzados de informática, pues a medida en que pasaba el tiempo la aplicación de la informática iba ampliándose, abarcando cada vez más información de personas, empresas, instituciones e incluso gobiernos, por tanto los criminales o también llamados cibercriminales (por interactuar en entornos virtuales) idearon formas en cómo aplicar la informática para manipular dichos datos, ya sea para almacenarlos o transmitirlos sin autorización, hasta modificarlos e incluso destruirlos; dicha aplicación maliciosa de la informática ha ido evolucionando en el transcurso del tiempo, que como veremos a continuación se manifiesta ahora de muchas formas.

2.2.3.1. Virus Informáticos

Históricamente la primera concepción o idea sobre los delitos informáticos estuvo muy ligada al desarrollo de los virus, pues son una de las principales herramientas que utilizan los criminales informáticos; los virus que son parte

fundamental en la historia de los delitos informáticos, fue concebida inicialmente por John Louis Von Neumann (Erquiaga, s.f., p.1), un científico húngaro famoso por ser uno de los matemáticos más importantes de la historia moderna por sus aportes en la física cuántica, la economía, la estadística, la cibernética, y las ciencias de la computación, es así que este famoso científico escribiría en el año de 1948 el artículo titulado “Teoría y organización de autómatas complejos”, un texto que hablaba acerca de la capacidad de crear programas que pudiesen tomar el control de otros, dicho trabajo sería más adelante perfeccionado por Arthur Burks, un matemático norteamericano que publicaría su aporte a través del libro “Teoría de auto-reproducción autómata”.

Ya por los años de la posguerra, en el año de 1959 en los laboratorios de Bell Computer se desarrollaría el denominado precursor de los virus informáticos a través de un juego llamado CoreWar, el cual fue desarrollado por Robert Thomas Morris, Douglas McIlory y Víctor Vysottsky, quienes basándose en la teoría de Von Neumann hacían que dos programas escritos en un pseudo-lenguaje de programación denominado RedCode batallaran entre sí, en donde el ganador era aquel que lograba ocupar la memoria de su oponente. Hasta este momento ya se venían ensayando una de las herramientas más sofisticadas que utilizan los criminales informáticos.

Fue hasta el año de 1972 en que se creó el primer virus llamado Creeper, el cual logró infectar una máquina de la empresa IBM de la mano de Robert Thomas Morris, un profesor asociado en el Instituto Tecnológico de Massachusetts; dicho virus mostraba de forma periódica el mensaje "I'm a creeper...catch me if you can!" (soy una enredadera, ¡atrápame si puedes!), siendo que para eliminar este virus fue necesario crear el primer software de antivirus denominado Reaper, el cual eliminaba al virus Creeper.

Con la creación del primer virus, se fueron concibiendo otras ideas de malware, así en el año de 1975 un escritor británico llamado John Brunner (2012) concebiría la primera idea de un gusano informático a través de su obra “El jinete de la onda de shock”, el cual era parte de lo que el describía como una sociedad construida alrededor de lo que hoy conocemos con Internet.

En el año de 1984 ya se daba cuenta a través de un foro de debates de internet denominado BIX BBS de la propagación de software malicioso que estaba infectando las computadoras, lo cual daría pie a que el científico computacional americano Fred Cohen (1984) realizara en su tesis titulada “Computer Viruses - Theory and Experiments” la primera definición de virus informático, lo cual le dio a dicho autor el apodo del padre de los virus. Es importante aquí señalar que para Fred Cohen los virus informáticos eran una amenaza, pues en una entrevista dada al portal de noticias British Broadcasting Corporation (2009), uno de los colegas de Fred Cohen llamado Len Adleman relataba lo siguiente “Fred se me acercó y me dijo que había descubierto un tipo nuevo de amenaza informática, y empezó a describirme lo que ahora denominamos virus”.

En el año de 1989 se conocería por primera vez al virus responsable de una de las primeras infecciones a escala intercontinental, afectando a Europa y Estados Unidos, dicho virus que se conocería como Dark Avenger tenía la capacidad de infectar una computadora con solo abrir o copia un ejecutable, para luego corromper e incluso destruir los datos, dejando tras de sí en los archivos un mensaje que decía “Eddie lives... somewhere in time!” (¡Eddie vive en algún lugar del tiempo!).

En el año de 1990 se crea el primer virus polifórmico de manos de Mark Washburn, el virus llamado “1260” tenía la capacidad de modificar con algoritmos polifórmicos su código malicioso para evitar así ser detectado, y en el año de 1995 aparece el virus “Concept” el cual da inicio a una clase de virus denominados macro, es en este año también en que aparecen virus específicamente programados para infectar ordenadores con el sistema operativo Windows 95.

En el año de 1998 los virus siguen evolucionando hasta tener ahora no solo la capacidad de infectar el software de las computadoras, sino también el hardware, a tal punto que pueden incluso dañarlo, esto se demostró con el virus Chernobyl que no eliminaba información, sino también sobrescribía la BIOS y perjudicaba el funcionamiento de una computadora, se infectaron millones de computadoras en todo el mundo, y causado daños por millones de dólares también.

En 1999 se empieza a conocer los virus anexados a correos electrónicos como el virus Melissa y Bubbleboy, siendo el más infeccioso este último pues lograba infectar una computadora con solo mostrar un mensaje escrito en lenguaje HTML.

En el 2001 se conoce por primera vez el virus Nimda, un virus que también se diseminaba a través de correos electrónicos y que tenía el objetivo de recuperar libretas de direcciones de correos electrónicos luego de infectar una computadora, dicho virus cobro mucha relevancia pues se esparció en la red pocos días después del ataque a las Torres Gemelas en los Estados Unidos.

En el 2012 se conoce un nuevo tipo de malware mucho más sofisticado que afecta computadoras en todo el mundo, conocidos como rasomware en donde

los criminales informáticos “secuestran” partes del sistema que tenga información valiosa, para luego pedir una recompensa o rescate que le permita a la víctima tener acceso nuevamente a dicha información.

2.2.3.2. Delitos informáticos contra el patrimonio

Aunque los virus son parte importante para cometer delitos informáticos, es importante también señalar que en la historia no se ha necesitado hacer uso de este tipo de software para cometer delitos informáticos, pues se tienen registro de casos de fraude informático en el mundo donde los criminales los cometieron aprovechando sus conocimientos en informática. A continuación, haremos un repaso de los más emblemáticos.

- ✓ En el año de 1988, Armand Devon Moore se hizo famoso al ser responsable del mayor caso de malversación de fondos en Chicago, en donde Armand convenció a personal que trabajaba en la entidad bancaria First National Bank a robar a la entidad a través de trasferencias electrónicas aprovechando el acceso a los equipos de la empresa que estos tenían, se sabe que se traspasaron más de 70 millones de dólares en solo 60 minutos.
- ✓ En el año de 1993 cuatro ejecutivos de una empresa de combustibles de Florida en Estados Unidos llamada Value Rent a Car, cometieron un fraude en perjuicio de unos 47 000 consumidores de la empresa cargando consumos extra a las facturas de los clientes a través de programas de cómputo. Se sabe que a cada cliente se le defraudo entre 2 y 15 dolares.
- ✓ En el año de 1994 se supo también de otro fraude millonario cometido por Vladimir Levin en contra de la famosa entidad bancaria Citibank, en donde través de la irrupción a la red de la empresa de manera remota, logro robar cerca de 3,7 millones de dólares en solo unas pocas semanas.

- ✓ En el año de 1999 se tiene registro del delito de fraude informático cometido por Maxim Kovalchuk, a quien se le acuso de robar 300 000 número de tarjeta de crédito, y que utilizaría para realizar una operación de saqueo de dinero que había en dichas tarjetas a través de una operación coordinada internacional con otros delincuentes de Rusia y Ucrania.

Sin embargo, muy aparte de estos casos emblemáticos de fraude informático que ha habido en el mundo, también tenemos en la historia reciente del Perú antecedentes de delitos informáticos con características similares:

- ✓ En el año 2009, un alto ejecutivo de una entidad bancaria en Lima fue acusado de integrar una banda criminal, en la cual aprovechando el puesto clave que tenía, en el transcurso de varios meses había sustraído ilegalmente con ayuda de sus cómplices los intereses de varias cuentas de ahorro de clientes para transferirlas a cuentas de terceros a nombre de mujeres que la misma banda de había ocupado de reclutar, por un monto aproximado de un millón ochocientos mil soles. El caso salió a la luz luego de que una de las mujeres denunciara ser víctima de extorsión y amenazas luego de poner en conocimiento dicho fraude. (La República, 2009).
- ✓ En el año 2009, un contador público fue detenido por la División de Investigación de Delitos de Alta Tecnología por apropiarse de más de medio millón de soles; dicho dinero fue sustraído de una empresa de carga y transportes de nombre Transporting, en donde el contador haciendo uso programas informáticos que le permitían obtener información reservada, obteniendo así las claves y contraseñas de los gerentes de la empresa para cometer el hecho delictivo (El Comercio, 2009).

- ✓ En el año 2017, se reportó que una ex trabajadora del Banco de Credito había confesado haber manipulado la base de datos del banco para realizar 13 transferencias por un monto total de un millón seiscientos noventa y nueve mil dólares, todo ello a través de un pequeño dispositivo que le había entregado una ex compañera del mismo banco, según refirió en su confesión (América TV, 2017).

2.2.3.3. Delitos informáticos contra la libertad sexual

Las redes informáticas son uno de los mayores medios por los cuales se atenta contra la libertad sexual de las personas, sobre todo de menores de edad a través de las redes de pornografía infantil, así, en el mundo se tienen antecedentes que dan evidencia de redes informáticas que trafican con este tipo de información:

- ✓ En el año 2011, se reportó el descubrimiento de la red internacional de pedofilia más grande del mundo hasta ese momento, dicho reporte que vino desde la Oficina Europea de Policía daba cuenta que dicha red que operaba desde internet contaba con aproximadamente 70 000 miembros que operaban en más de 30 países alrededor del mundo (Russia Today, 2011).
- ✓ En el año 2012, se dio noticia de una red internacional de pedofilia en la que operaban individuos de más de siete países alrededor del mundo, se detendrían cerca de 43 individuos, los cuales poseían dentro de sus computadoras decenas de miles de imágenes de pornografía infantil que iban a ser distribuidos en esta red criminal; es importante adicionar que la noticia fue realzada en su momento por el hecho en que los agentes de investigación de Estados Unidos se apoyarían en el seguimiento de uno oso de peluche para dar con la red criminal (RPP, 2012).

- ✓ En el año 2017, en una operación conjunta de la policía española, la Ameripol y la Interpol, se desmanteló una red internacional de pedofilia que funcionaba a través del aplicativo de comunicación informática “Whatsapp”, en pedófilos de habla hispana intercambiaban pornografía infantil a través de dicha aplicación, fueron detenidas 38 personas provenientes de más de 15 países (Publimetro, 2017).

2.2.3.4. Delitos informáticos contra la intimidad

Debido a que mucha información personal o reservada se encuentra digitalizada en la red, muchos criminales aprovechan dicha ventaja para tratar de acceder a dicha información privada, en donde valiéndose de sus conocimientos en informática, logran obtener toda clase de datos sensibles de sus víctimas, ya sea para traficar con estos en la red, extorsionar al propietario de dichos archivos, etc. A continuación citaremos algunos casos relevantes en donde se atentó contra la intimidad de las personas por medios informáticos:

- ✓ En el año 2012, se hizo noticia del hackeo de varias cuentas de Twitter de famosos, desde futbolistas hasta cantantes, en donde el criminal informático aprovechando el acceso a las cuentas privadas dejó mensajes en su nombre (ABC, 2012).
- ✓ En el año 2014, se supo de un hackeo masivo a varías actrices norteamericanas aprovechando una falla de seguridad en el servicio de almacenamiento en la nube Icloud, en donde un hacker luego de obtener acceso a dichos archivos privados, se contactaba aparentemente con las afectadas y les pedía dinero a cambio de no difundir las imágenes por Internet, siendo que entre las actrices más afectadas al momento de salir

la noticia fue Jennifer Lawrence, de quien el hacker estuvo negociando sus archivos privados (El Universal, 2014).

- ✓ En el año 2017, se tuvo noticia de un hackeo que afectó a miles de famosos que tenían cuentas en Instagram, y es que se reportó que cibercriminales habían tenido acceso ilegal a más de 6 millones de cuentas, en donde habrían recopilado información sensible como direcciones de correo electrónico y número de teléfono (ABC, 2017).

2.2.3.5. Delitos informáticos contra la seguridad nacional

Se tienen antecedentes de delitos informáticos que se cometieron en agravio de gobiernos de diversas naciones, en donde los cibercriminales atentaron contra la seguridad nacional a través de diversos ataques que mencionaremos a continuación:

- ✓ En el año 2010, el mundo veía con asombro uno de los mayores filtros de información clasificada a través del portal Wikileaks, en donde se divulgaría muchos de los abusos que se cometieron en las operaciones militares que desplegó Estados Unidos en Irak (El Mundo, 2010), dicha filtración aunque fue saludada en su momento porque ponía en relieve múltiples abusos a los derechos humanos cometidos en Irak, no quita que también haya sido uno de los delitos informáticos más sensibles que se vio en los Estados Unidos pues se filtraron miles de documentos de categoría clasificada.
- ✓ En el año 2012, se hizo noticia del hackeo de la página del FBI a mano de cibercriminales del grupo Anonymous que realizaron dicho acto delictivo en represalia del cierre de una página de almacenamiento en la nube llamada Megaupload, dicho hackeo que resultó histórico sería el principal

ataque que haría que el grupo de cibercriminales Anonymous se hiciera popular (Univisión, 2012).

- ✓ En el año 2013, se hizo noticia de Edward Snowden, un ex agente de la NSA de los Estados Unidos de América, que filtraría información ultra secreta sobre herramientas de vigilancia mundial que tendría el gobierno norteamericano, así como el espionaje a decenas de gobiernos extranjeros alrededor del mundo (El Pais, 2013), dicha filtración que es considerada por su magnitud como la mayor filtración de información ultra secreta de los Estados Unidos, fue suficiente para que fuera perseguido como traidor, siendo que a la fecha se encuentra asilado en Rusia.
- ✓ En el año 2015, se denunció que cibercriminales chinos habrían robado la información de millones de funcionarios norteamericanos para obtener a través de ellos datos sensibles o secretos, pues entre los afectados se encontraban aparentemente funcionarios de la CIA y otras agencias federales importantes de los Estados Unidos (La Prensa, 2015).
- ✓ En el 2016, se denunció públicamente uno de los mayores escándalos de hacking en el mundo pues se reportó que aparentemente hackers rusos habrían alterado las elecciones en los Estados Unidos, en dicho caso que fue investigado por la CIA, se concluyó que había habido una interferencia ilegal vía ataques cibernéticos en la elección presidencial de dicho país, en donde el objetivo era afectar a la candidata del partido demócrata Hillary Clinton; trascendió que aparentemente dicho ataque habría sido ordenado desde el gobierno Ruso (British Broadcasting Corporation, 2016).

2.3. MARCO CONCEPTUAL

2.3.1. La formación profesional en derecho informático

Luego de haber repasado los antecedentes de la formación profesional y el derecho informático, podemos definirlo como el conjunto de competencias en esta rama del derecho para su aplicación en el desempeño profesional; dicha definición ha resultado del análisis de la esencia de lo que se entiende ahora por formación profesional, pues como se repasó en los antecedentes esta ya no se encuentra relacionada solo con la transmisión de conocimientos, sino también con las competencias, que son entendidas como aquel conjunto de características individuales que permiten que una persona se desempeñe óptimamente en su trabajo, por tanto partiendo de esta premisa de que el profesional debe dominar una serie de competencias, es que ahora se exige a los profesionales del derecho dominar competencias básicas como el dominar sistemas jurídicos, conocer las fuentes del derecho, aplicar los principios del estado constitucional de derecho, aplicar los derechos fundamentales, conocer la estructura y funcionamiento del estado y sus instituciones, aplicar la argumentación jurídica, entre otras competencias que le permitan en suma resolver casos en el desempeño de su profesión, por tanto si nos trasladamos al campo que nos ocupa como es el derecho informático, este también exige una serie de competencias que el investigador ha visto a bien identificar son:

- ✓ La aplicación de las fuentes del derecho informático, pues como se sabe cada rama jurídica tiene sus propias fuentes y es necesario conocerlas, por tanto alguien que domine esta competencia es capaz de identificar las fuentes jurídicas del derecho informático, analizar dichas fuentes, y utilizarlas al momento de argumentar algún escrito o documento en el desempeño de la profesión de abogado.

- ✓ La aplicación de conceptos jurídicos de derecho informático, que implica básicamente que identifique en primer lugar los conceptos de derecho informático, analice dichos conceptos y los utilice en su argumentación cuando se ocupe de resolver problemas jurídicos de derecho informático.
- ✓ La aplicación del ordenamiento jurídico de derecho informático, pues recordemos que esta rama del derecho ha estado renovando su ordenamiento jurídico, no solo en el Perú a través de normas que regulan la informática, sino también en el extranjero pues la regulación de la informática aun ocupa un lugar central en la agenda de muchos países de América y Europa.
- ✓ La resolución de problemas en el ámbito del derecho informático, pues recordemos que no solo se trata de transmitirse conocimiento teórico de esta rama sino también saber usarlo para la resolución de problemas, por tanto para resolver problemas en este campo del derecho es necesario identificar dichos problemas, analizar dichos problemas de derecho informático, y finalmente plantear soluciones a dichos problemas.
- ✓ La aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional, que implica identificar el uso de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional, analizar dicho uso, y finalmente utilizar la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional.

2.3.1.1. Teorías del derecho informático

a) La teoría de los sistemas en el derecho informático

Como se sabe, dentro de los pilares teóricos de la informática en general encontramos a la teoría de los sistemas, planteada por Ludwig von Bertalanffy,

quien nos hablaba de una "teoría de los sistemas de control basada en la comunicación (transferencia de información) entre sistema y medio circundante, y dentro del sistema, y el control (retroalimentación) del funcionamiento del sistema en consideración del medio)"(como se cita en Fix, p.42), así, la teoría de los sistemas se constituye como el pilar de la cibernética, que como recordaremos es la ciencia que se encarga de estudio análogo del sistema o también conocido como teoría general del sistema (Rios, 1997,p.37), y por tanto también pilar de la informática, que como dice Villazán (2010, p.8) es: "la ciencia de la información, un conjunto de conocimientos que permiten el tratamiento automático de la información". Por tanto no es de extrañarse que en el campo jurídico del derecho informático, sea necesario comprender primero la teoría de los sistemas, pues el entorno en el que vivimos actualmente es uno completamente informatizado, y ello es gracias a la aplicación de dicha teoría por medio de la informática.

b) La teoría de la información en el derecho informático

Al igual que la teoría de los sistemas, la teoría de la información propuesta por Claude E. Shannon y Warren Weaver a finales de la década de los años 1940, es otro de los pilares de la informática y por ende un referente teórico dentro del derecho informático, así, Vico (2011, p.83) nos menciona que: "la teoría de la información tiene objetivo orientar y situar el conocimiento en torno a la comunicación, con una dirección concreta específica para investigar la información", por lo tanto, en esta nueva era de la información, podríamos asumir que necesidad de determinar, con la máxima precisión, la capacidad de los diferentes sistemas de comunicación para transmitir información (Correa, 2013).

2.3.1.2. Derecho Informático

Se sabe que el término derecho informático o “Rechtsinformatik” fue acuñado por primera vez por el doctor Dr. Wilhelm Steinmüller, un académico Universidad de Ratisbona de Alemania en el año de 1970. De acuerdo a Téllez Valdés (2008, p.26) lo define como “la rama de las ciencias jurídicas que contempla la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática)”, para Zaballos Pulido (2013, p.41) se define como “la aplicación del conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y las comunicaciones y que tiene por objeto la aplicación de las Tecnologías de la Información al Derecho”, para Velasco Melo (2008, p.5) el derecho informático nace del estudio de las relaciones entre las Tecnologías de la Información y las Comunicaciones y el derecho.

En suma, el derecho informático es para el investigador una rama de las ciencias jurídicas que se ocupa de englobar todo un conjunto de normas, principios, doctrina y jurisprudencia destinadas a regular el uso, desarrollo y expansión de la informática. Es importante resaltar que no es lo mismo derecho informático que Informática Jurídica, debido a que el primero está relacionado al tema normativo, y la segunda a la aplicación de la informática en el derecho.

2.3.1.2.1. Relación entra el derecho y la informática

Cuando tratamos acerca de la relación entre el derecho y la informática, es tratar acerca del problema que ha traído el uso expandido y generalizado de la informática, un problema complejo que ha sido analizado desde diferentes perspectivas y enfoques, sin embargo Olivera (s.f.) nos señala de que esta relación tiene dos líneas de estudio bien diferenciadas: la primera relativa a la aplicación de la informática en el tratamiento de la información jurídica, y la segunda respecto de los aspectos normativos derivados del uso de la

informática. Es aquí en donde encontramos los fundamentos para la división entre lo que se conoce como Derecho informático, que será materia de estudio en esta investigación, y la informática jurídica, que es una rama independiente íntimamente relacionada a la primera, que, aunque relacionada a la informática, guardas sus diferencias con el derecho informático.

2.3.1.2.2. Fuentes del derecho informático

Cuando se habla acerca de fuentes del derecho sabemos que esto se refiere a todo ese conjunto de factores que dan origen al derecho y por ende a las normas, en donde trasladando esta idea general advertimos que en el derecho informático se identifica también las fuentes de donde emana su contenido, por lo que siguiendo la división tradicional de las fuentes del derecho, esta rama admitiría dos clases de fuentes: las fuentes materiales y las fuentes formales, de las fuentes formales podríamos decir que son todo ese conjunto de factores y condiciones que hubo en la sociedad desde la aparición de la informática para dar origen a lo que hoy conocemos como derecho informático, y como fuentes formales consideraríamos a todo ese conjunto procesos, procedimientos o modos de carácter formal que producen normas jurídicas (), así en el derecho informático podemos considerar las siguientes fuentes formales:

a) Legislación: El derecho informático tiene como primera fuente a la ley y por ende a la legislación en esta materia, pues desde el siglo XX se ha visto el desarrollo de leyes de derecho informático en diferentes países incluyendo al Perú, lo cual fue estimulado mediante el desarrollo de marco jurídico internacional de derecho informático compuesto por tratados y convenios internacionales.

b) La jurisprudencia: El derecho informático también reconoce como fuente a la jurisprudencia, es decir todo ese conjunto de fallos y sentencias dictadas por los tribunales de justicia en materia de derecho informático, los cuales son de observancia obligatoria,

c) La doctrina: Que viene a ser las opiniones y puntos de vista de los juristas de reconocido prestigio, también se considera como fuente del derecho informático pues a la fecha ya se cuentan con gran variedad de publicaciones de derecho informático de vital importancia.

d) Los principios generales del derecho: como se sabe el derecho como ciencia posee todo un conjunto de principios que son universales, que dan razón y sustento a los sistemas jurídicos, estas ideas centrales del derecho constituyen la base teórica de los ordenamientos jurídicos, por tanto, el derecho informático los reconoce como fuente dichos principios fueron considerados para dar sustento jurídico a todo ese marco normativo que rodea al derecho informático.

e) La costumbre: Conocida como la fuente más antigua del derecho, se puede considerar también como fuente del derecho informático, pues aquí se considera a las normas jurídicas que, aunque no están escritas son impuestas por su uso reiterado; por tanto tomando en cuenta que el derecho informático es una rama jurídica reciente y de naturaleza transversal pues abarca a otras ramas jurídicas que también consideran a la costumbre, es que también se le puede considerar como una de sus fuentes jurídicas.

2.3.1.2.3. Relación del derecho informático con otras ramas jurídicas

De acuerdo a Lambias Lozano (2013, p.57), el derecho informático se relaciona con otras ramas del derecho como se detallará a continuación.

a) Con el derecho constitucional: el derecho informático se relaciona con esta rama del derecho público pues las normas de derecho informático han sido emanadas en base a la constitución de los diferentes estados, siendo además que dentro del derecho constitucional se encuentra la estructura y órganos fundamentales de un estado, temas a tomar en cuenta a la hora de comprender como es que se desenvuelve la norma jurídica en derecho informático.
b) Con el derecho penal: pues el derecho informático también considera la sanción de diversas conductas hechas a través de medios informáticos contra bienes jurídicos protegidos, dando nacimiento a una nueva sub rama del derecho informático y el derecho penal denominada Derecho Penal Informático, en donde los objetos de estudio vienen a ser los delitos informáticos o también llamados ciberdelitos.
c) Con el derecho civil: La relación se funda en la aparición de los denominados contratos electrónicos, que básicamente consiste en la posibilidad de que las personas puedan realizar contratos a través de dispositivos informáticos y la Internet, estos contratos, que pueden estar referidos a bienes o servicios vienen siendo perfeccionados tecnológicamente a la par del desarrollo de la informática, y jurídicamente a la par del desarrollo de normas que regulan dichos contratos, normas de derecho informático en el ámbito civil.
d) Con el derecho procesal: El derecho informático tiene íntima relación con el derecho procesal pues a lo largo de los años se vienen automatizando a través de la informática los proceso, sean estos penales, civil, laborales, administrativos, etc., esta automatización al ser necesario regularlas trajo

como consecuencia el nacimiento de normas de derecho informático en el ámbito procesal.

e) Con el derecho comercial: El derecho informático se vincula con esta rama por la aparición del comercio electrónico, entendido como la posibilidad de realizar actos de compra y venta de bienes y servicios a través de dispositivos electrónicos y la internet. Dicho comercio electrónico como es natural ha sido necesario regularlo, dando nacimiento a normas de derecho informático dentro del campo del derecho comercial.

f) Con el derecho laboral: La vinculación aquí se funda en dos puntos concretos, el primero es que ahora tanto empleadores como empleados hacen uso de la informática, ya sea para mejorar sus comunicaciones, para hacer más eficientes sus labores, o para mejorar los vínculos labores dentro de las entidades, el segundo punto está relacionado al hecho de que muchas empresas se desenvuelven en entornos completamente virtuales, cambiando la forma en cómo interactúan empleadores y trabajadores dentro de las entidades; por tanto debido a la incorporación de la informática en el derecho laboral, es que se da lugar al nacimiento de normas de derecho informático orientadas a regular esta área.

2.3.1.2.4. Informática jurídica

Como se mencionó en el inciso anterior, de la relación del derecho y la informática nace la informática jurídica, que de acuerdo a Guibourg (s.f., p.791) es aquella que: “Se refiere a los métodos informáticos aplicados al campo del derecho”. Por tanto, dentro del campo del Derecho Informático conviene conocer y estudiar la informática jurídica, pues la informática se ha ido implementando y expandiendo en la administración de justicia, para aparentemente, servir de ayuda para agilizar los procesos, tanto dentro y fuera de las instituciones público

o privadas, en un intento de estar a la vanguardia con las nuevas tecnologías y sacar provecho de estas.

2.3.1.2.5. Informática forense

De acuerdo al Buró Federal de Investigaciones (FBI en sus siglas en inglés) de los Estados Unidos de América, se define a la informática forense de la siguiente manera: "…la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional." (Como se cita en Canedo, p.82) por tanto es en base a esta definición que tenemos lo expresado por Sebastián (2009, p.3) al decirnos que es: "el proceso de identificar, preservar, analizar y presentar evidencia digital, de manera que esta sea legalmente aceptable". Por tanto, queda en relieve, que al estar ligada la informática forense con la seguridad informática, tiene entonces ambas una relación directa para el tratamiento de los delitos informáticos, pues es esta disciplina la que se encarga de lidiar con las pruebas y las evidencias relativas a estos casos.

2.3.1.2.6. Protección de datos personales

La protección de los datos personales es un área de estudio dentro del derecho informático que nace a raíz de la necesidad regular la información personal en un entorno informatizado como es el actual, así, los datos personales de a acuerdo a Comisión Europea (2018) vendrían a ser: "cualquier información relativa a una persona física viva identificada o identificable", dicho concepto guarda mucha similitud con el que nos brinda el Ministerio de Justicia y Derechos Humanos del Perú (2014, p.4) estableciendo que los datos personales son "cualquier información que permite identificar a una persona" especificando más

adelante que “(…)El nombre, los apellidos, la fecha de nacimiento, la dirección del domicilio, la dirección de correo electrónico, el número de teléfono, el número de RUC, el número de la placa del vehículo, la huella digital, el ADN, una imagen, el número del seguro social, etc. son datos que identifican a una persona, ya sea directa o indirectamente”, así, en este campo del derecho informático se estudiará la regulación del tratamiento de los datos personales, los derechos del titular de los datos personales, las obligaciones de los bancos de datos personales, así como el régimen jurídico de los datos personales y los órganos competentes que intervienen la protección de los datos personales.

2.3.1.2.7. Protección jurídica de software

Dentro del campo de la informática, se sabe que está dividido la composición de los ordenadores o computadoras en hardware y software, el primero relativo a los componentes físicos del aparato, y el segundo relativo al conjunto de programas que se ejecutan a través del mismo, el hardware por su naturaleza física goza de tutela legal, sin embargo el software, por su naturaleza no-física, representó en su momento un reto para los juristas del derecho darle una debida protección jurídica, es así que este también es un campo en el que entra a tallar el derecho informático. El software es entendido más allá de solo ser considero un conjunto de programas, así, tenemos definiciones como las de Lapenne (2011, p.2.) que nos dice que el software es: “un conjunto de instrucciones escritas que, al ser implementadas e interpretadas por una computadora -hardware- producen cierto resultado”, a esta definición la podemos complementar con la de Elliot (s.f., p.1.) que lo nos dice lo siguiente: “Podemos mencionar que el software es un conjunto de instrucciones organizadas lógicamente (pues siguen una secuencia) y codificadas (porque se utiliza un lenguaje de programación para su desarrollo)

y que tienen como fin resolver un problema o situación específica del usuario. Estas instrucciones interpretan la información dada por el usuario a la computadora (por medio del teclado). Si comparamos nuestro organismo con una computadora, nos encontraríamos con que el software es el cerebro del cuerpo humano".

2.3.1.2.8. Protección jurídica de base de datos

Las bases de datos también son objeto de estudio del derecho informático, según Gómez (2013, p.8), son entendidos como: "una colección de datos interrelacionados y un conjunto de programas para acceder a dichos de datos", por lo que a partir de este concepto se le define a las bases de datos como un conjunto de programas utilizados para definir, administrar y procesar una base de datos y sus aplicaciones (Gómez (2013, p.8); por tanto, y dada la función que cumplen las bases de datos, estos gozan también de una tutela jurídica dirigida a su protección, de por ejemplo, potenciales atacantes, que aprovechando sus conocimientos en informática, pueden infiltrarse en estos sistemas para el robo sistemático de información.

2.3.1.2.9. Comercio electrónico

El comercio electrónico también entra dentro del marco del estudio del derecho informático, entendiéndose como tal de acuerdo a la Organización Mundial del comercio como la producción, distribución, comercialización, venta y entrega de bienes y servicios por medios electrónicos (Nieto, s.f.,p.12). Por lo tanto al apoyarse en los medios electrónicos, se relaciona íntimamente con el derecho informático, pues dicho comercio necesita de una regulación adecuada, atendiendo a su naturaleza especial, por lo que será necesario estudiar todo ese marco normativo que regula esta nueva forma de transacción comercial en la

que las partes interactúan electrónicamente en lugar de por intercambio o contacto físico directo (León, 1998, como se cita en Nieto, s.f., p.12).

2.3.2. La persecución penal de delitos informáticos

2.3.2.1. Persecución penal de un delito

Entendida como la función del Ministerio Público de perseguir el delito, en donde se abarca desde la investigación la investigación de casos de delitos informáticos, la acusación penal a los responsables y la prueba de la responsabilidad penal de los acusados en el proceso penal; por ello, Peláez Bardales (2011, p.31) nos dice respecto de la persecución del delito: “Es objetivo primordial de la Fiscalía de la Nación que se desarrollen investigaciones de mayor eficacia, identificándose plenamente al autor o autores del delito, las circunstancias de su comisión y la futura imposición de la pena que corresponda”. Además es importante mencionar que el Ministerio Público en el Perú, persigue el delito también a través de políticas de prevención y líneas de acción directa, en lo que ellos denominan la “Persecución estratégica del delito”, y que según Van (Van, 1999, como se cita en Escuela del Ministerio Público, 2010, p.13) sería: “las políticas, medidas y técnicas, fuera de los límites del sistema de justicia penal, dirigidas a reducir las diversas clases de daños producidos por actos ilícitos definidos por el Estado”.

Entonces entenderemos como persecución penal de un delito, a la función que desempeña por mandato constitucional el Ministerio Público para perseguir todas aquellas conductas sancionadas por la ley penal al ser estas hechos típicos, antijurídicos y culpables.

Ahora bien, conceptualizado el significado de perseguir penalmente un delito, toca ahora revisar cómo es que se cumple dicha función en el proceso penal.

a) Las funciones que cumplen las fiscalías penales corporativas

En la persecución del delito un rol importante y fundamental es el que cumplen las fiscalías provinciales penales corporativas en el Perú (y las fiscalías mixtas), que son los que en primera instancia asumen, analizan y evalúan las denuncias y expedientes que se ingresan al Ministerio Público, por tanto, las funciones que deben cumplir dichas fiscalías son:

- ✓ La función de coordinación, en se seleccionen y distribuyan los casos a los despachos de acuerdo a criterios de decisión temprana o de investigación.
- ✓ La función de decisión temprana, que implica que los fiscales promuevan salidas alternativas desde que se encuentran en la etapa de investigación según sea posible en cada caso, lo cual implica la posibilidad de realizar una negociación para aplicar el principio de oportunidad y los denominados acuerdos reparatorios.
- ✓ La función de investigar, lo cual implica que actue con objetividad e independencia de criterio, de manera que se recabe información relevante y elementos de convicción que cumplan con los requisitos de pertinencia, conducencia, y utilidad.
- ✓ La función de liquidar los casos que vienen del sistema procesal antiguo.

b) Las etapas del proceso penal

El proceso penal actual se rige en función al vigente nuevo código procesal penal, el cual se encuentra enmarcado dentro del sistema acusatorio moderno, en el cual se reconocen las siguientes etapas:

- La investigación preparatoria, que se caracteriza por ser la etapa en la cual el fiscal dirige la investigación, solicita medidas coercitivas según sea el caso, y reúne los medios de prueba, dicha etapa tiene como finalidad reunir los elementos de convicción, de cargo y de descargo, que permitan al fiscal si es que formulará acusación. La investigación la dirige el mismo fiscal con apoyo de la policía que puede realizar diligencias de investigación que ayuden al esclarecimiento de los hechos. En esta etapa la corresponde al juez de investigación preparatoria autorizar que se constituyan las partes, pronunciarse sobre las medidas que limiten derechos o de protección, resolver excepciones, cuestiones previas y prejudiciales en caso se formularan. Esta etapa a su vez se divide en dos partes, la primera denominada investigación preliminar, en donde se realizan las diligencias preliminares por un plazo de 60 días, en la cual el fiscal determina si es necesario pasar a la etapa de investigación preparatoria; la segunda parte que viene a ser la investigación preparatoria propiamente dicha es aquella en donde el fiscal dispone que se realicen diligencias de investigación que considere pertinentes y útiles, dicha etapa que puede durar desde 120 días naturales y ser prorrogada hasta 60 días, si en caso se trata de un caso complejo son 8 meses y si los hechos delictivos fueran perpetrados por una organización criminal el plazo es de 36 meses. En etapa si vencido el plazo el fiscal no al concluyera, las partes pueden solicitar al juez de investigación preparatoria que disponga la conclusión.
- La etapa intermedia

  Esta etapa que inicia luego de que el fiscal concluye la investigación preparatoria se caracteriza por el hecho de que aquí el fiscal cumple con

el rol de presentar la acusación o solicitar el sobreseimiento, mientras que el juez se ocupa de escuchar al fiscal y las partes en las audiencias, y realizar una función de control sobre lo que solicite el fiscal. En esta etapa es importante mencionar que en caso el fiscal decidiera formular acusación, el juez de investigación preparatoria es el que convoca a una audiencia en donde se debate la procedencia o admisibilidad de cada una de las cuestiones planteadas, así como la pertinencia de las pruebas ofrecidas.

- El juicio oral

  Esta que es la etapa principal y de mayor importancia en el proceso, es en la cual se decide sobre la culpabilidad o inocencia del imputado, en donde el juez penal se encarga de dirigir el debate en el cual el fiscal sustenta la acusación y el abogado sustenta la defensa de su patrocinado. Esta etapa que está regida por los principios de oralidad, publicidad, inmediación y contradicción, se encuentra comprendida en los alegatos preliminares, la actuación probatoria, los alegatos finales, la deliberación y la sentencia. Es importante resaltar que en esta etapa es el juez penal o el presidente del juzgado colegiado quien dirige el juicio y ordena los actos necesarios para su desarrollo, en donde debe garantizar el ejercicio pleno de la acusación y de defensa de cada una de las partes.

c) Políticas de prevención y líneas de acción directa

Según el propio Ministerio Público menciona que “debe ir más allá de sus conocidas funciones de persecución penal, para pasar a implementar medidas preventivas que acerquen la institución a la ciudadanía y al mismo tiempo, la puesta en marcha de estas medidas les permite obtener información clave para hacer frente al delito a nivel nacional.”, y es que como sabemos el Ministerio

Público es un organismo que cumple un rol protagónico no solo en la persecución del delito sino también de su prevención, por tanto se encuentra en la imperiosa necesidad de implementar políticas de prevención y líneas de acción directa para enfrentar al problema de los delitos en el Perú, y es que el Ministerio Público reconoce que la sola aplicación de la norma jurídica no es suficiente, por ello mencionan que “Combatir el delito sólo con la aplicación estricta de la ley no viene dando los resultados esperados, de modo que el Ministerio Público, además de cumplir sus funciones de persecución penal, considera necesario evaluar el delito y los factores que lo causan, con el fin de enfrentar a la criminalidad también en sus raíces y origen”. Es así que en razón de estos fundamentos que el Ministerio Público implementó en el año 2008 el Programa de persecución estratégica del delito, en donde se incluyeron justamente líneas de acción para acortar el distanciamiento que hay entre la comunidad y los operadores del sistema de justicia, logrando a través de ello una estrecha colaboración con la ciudadanía para combatir los fenómenos delictivos.

d) Los actos de investigación en el proceso penal

Como sabemos dentro del proceso penal peruano se reconoce toda una serie de actuaciones para que sean realizadas durante las diligencias preliminares como en la investigación preparatoria, dichas actuaciones sirven para indagar las circunstancias que comprueben la imputación o se exima de responsabilidad penal al imputado, lo que se busca aquí es obtener los elementos de convicción, así como información relevante que ayuden a acreditar los hechos, identificar los autores, etc. Dichas actuaciones que pueden ser practicadas por la policía nacional del Perú, el fiscal, siendo que en algunos

casos requiere que se tenga una autorización judicial. A continuación, mencionaremos las actuaciones que reconoce nuestro ordenamiento jurídico:

- **Actuaciones que realiza la policía**

  Las cuales son realizadas de por sí o por disposición fiscal sobre las personas o sobre las cosas, constituyen indagaciones para encontrar las evidencias del delito, al imputado o a una persona prófuga. Aquí se reconoce dos actos, la retención que es restringir la libertad de las personas temporalmente de moverse del lugar de donde se realizan las pesquisas, y el registro de personas, que consiste en practicar una revisión de las personas que se considera pueden ocultar bienes relacionados al delito.

- **Actuaciones que requiere confirmación judicial**

  Estas actuaciones que se realizan en el supuesto que en el momento de la intervención no se tenga una orden judicial por lo que el fiscal debe solicitar la confirmación judicial, en este tipo de actuaciones tenemos al aseguramiento de documentos privados, que consiste en asegurar un documento sin examinar su contenido, el aseguramiento de documentos contables y administrativos, el examen corporal urgente, la exhibición forzosa o incautación de bienes en caso de flagrancia o peligro inminente y la clausura o vigilancia de local e inmovilización de cosas muebles.

- **Realizadas previa autorización judicial**

  Aquí encontramos a todas las actuaciones que para ser ejecutadas necesitan que previamente haya una orden expresa del juez de investigación preparatoria, aquí encontramos las siguientes actuaciones: incautación de documentos privados; el examen corporal; el allanamiento; la exhibición forzosa e incautación de bienes en propiedad, posesión, administración, tenencia o afín; interceptación e incautación postal, cartas, pliegos, valores,

telegramas y otros; la intervención, grabación o registro de comunicaciones telefónicas, radiales y otros; el levantamiento del secreto bancario; levantamiento de la reserva tributaria; clausura o vigilancia de local e inmovilización de cosas y muebles.

- **Actuaciones por disposición fiscal**

  Aquí encontramos las siguientes actuaciones: la video vigilancia, fotos, imágenes y otras técnicas de observación; la exhibición e incautación de actuaciones y documentos no privados, la circulación y entrega vigilada de bienes delictivos y el agente encubierto.

2.3.2.2. Delito informático

Se denomina así a todos aquellos delitos que afectan sistemas o datos informáticos u otros bienes jurídicos de relevancia penal mediante la utilización de las TIC's. Ahora bien, respecto del término "delito informático", en el mundo también se le suele llamar delito cibernético o cyberdelito, sin embargo a efectos de la presente investigación, se usará el término de delitos informáticos debido a dos motivos, el primero debido a que es el término más usado tanto a nivel de la doctrina como de las investigaciones llevadas a cabo en Sudamérica y España, y en segundo lugar porque es el término que emplea nuestra legislación para referirse a este tipo de delitos, y es que si bien es cierto el término de "delito cibernético" (del término en ingles cybercrime) es también usado, la misma Naciones Unidas a través de su informe relativo a los delitos informáticos señala que a nivel de legislación comparada, la mayoría de países usa el término de Delitos informáticos y no de Delitos cibernéticos: "Los enfoques de definición evidenciados en los instrumentos nacionales, internacionales y regionales nutren el método adoptado por este Estudio. Este Estudio no busca 'definir' el delito cibernético per se. En lugar de ello describe una lista o 'canasta' de actos que

podrían constituir al delito cibernético. (…)Por ello, probablemente es mejor no considerar el término 'delito cibernético' como un término legal técnico.". Debido a estas razones, y para no generar confusión en la investigación, es que se dará prioridad al término de "delitos informáticos".

2.3.2.3. El bien jurídico protegido en delitos informáticos

El tema del bien jurídico protegido en los delitos informáticos, es un tema de debate en la doctrina nacional e internacional, pues no ha logrado un consenso respecto al mismo, por ejemplo Hugo (2014, p.11) como algunos autores nos dice que "el bien jurídico tutelado en este tipo de delitos informáticos es el patrimonio, desde la perspectiva del derecho a la propiedad que tiene el sujeto pasivo a su base de datos informáticos y/o al adecuado funcionamiento de un sistema informático.", y por otro lado tenemos lo que nos dice el jurista Villavicencio Terreros (2014, p.288): "el bien jurídico tutelado en los delitos informáticos se concibe en los planos de manera conjunta y concatenada; en el primero se encuentra la información de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y en el segundo plano, los demás bienes afectados a través de este tipo de delitos como son la indemnidad sexual, intimidad, etcétera", con estos dos ejemplos se puede ver que no todos ven en la información el bien jurídico protegido, para otros en realidad no se habla de un solo bien jurídico protegido, sino que los delitos actualmente tienen la característica de ser pluriofensivos, es decir, que lesionan o ponen en riesgo varios bienes jurídicos.

2.3.2.4. Clasificación de delitos informáticos

Existen múltiples modalidades en las que se cometen delitos informáticos, por lo que se han producido intentos por clasificarlos, así por ejemplo Hugo (2014,

p.4) clasifica a los delitos informáticos o delitos cibernéticos, de la siguiente forma:

- Fraudes cometidos mediante manipulación de computadoras, que incluiría la manipulación de datos de entrada, de programas y de datos de salida.
- Falsificaciones informáticas, que incluye la alteración de datos computarizados, o la alteración de documentos físicos a través de medios computarizados.
- Daños o modificaciones de programas o datos computarizados: que incluiría el sabotaje informático, acceso no autorizado a servicios informáticos, acceso no autorizado a sistemas informáticos, y la reproducción no autorizada de programas.

De otro lado Télles Valdéz (2008, p.190) nos brinda otra clasificación más amplia sobre los delitos informáticos, dividiéndolos en primer lugar como instrumento o medio y como fin u objetivo:

a) Como instrumento o medio

En esta categoría encontramos a todas aquellas conductas delictivas que usan a la informática como un medio para ser cometidas, ello ya sea a través de computadoras u otros dispositivos electrónicos, incluyendo también programas de software. Aquí como ejemplo podemos tener a los delitos de falsificación de documentos o la sustracción de información confidencial.

b) Como fin u objetivo

Que abarcaría a todas aquellas las conductas delictivas que están orientadas contra un ordenador o un dispositivo electrónico informático, ya sea por ejemplo para afectar datos o sistemas informáticos; en este caso es que se tiene como ejemplos la programación de malware para bloquear un sistema

informático, la destrucción de datos informáticos, o el atentando contra el hardware de equipos informáticos dañándolos o alterando su funcionamiento.

Ahora bien, las Organización de las Naciones Unidas también han previsto una clasificación de los delitos informáticos (Télles, 2008, p.193) en la cual se agrupa los delitos informáticos de la siguiente forma:

a) Fraudes cometidos mediante la manipulación de computadoras

Que incluiría delitos de manipulación de datos de entrada, es decir de sustracción de datos, un delito relativamente común que no necesitaría de conocimientos técnicos en informática. También se incluiría aquí a delitos como la manipulación de programas, en donde el delincuente informático modifica programas utilizando conocimientos técnicos especializados, así como delitos que implican la manipulación de datos de salida, en donde por ejemplo se altera las instrucciones de un ordenador de un cajero en la fase de adquisición de datos para obtener información sensible de una tarjeta de crédito.

b) Falsificaciones informáticas

Que puede darse de dos formas, la primera que consiste en alterar los documentos almacenados en una computadora, y la segunda que consiste en usar computadoras para realizar la falsificación de documentos.

c) Daños o modificaciones de programas o datos computarizados

Aquí encontraríamos a los muy conocidos virus, que son programas especialmente para programados para propagarse luego de ingresar en un sistema informático, así como también al sabotaje informático, que consiste en borrar, suprimir o modificar sin autorización las funciones o datos contenidos dentro de una computadora u otro aparato electrónico.

d) Falsificaciones informáticas

Aquí encontramos a aquellos delitos que implican la reproducción total o parcial de programas informático, lo cual genera cuantiosas pérdidas materiales a los propietarios del programa.

2.3.2.5. Tipos de delitos informáticos

En conformidad a nuestro código penal peruano y la ley de delitos informáticos 30096 y su modificatoria que se encuentran vigentes, presentamos a continuación los delitos informáticos que nuestro ordenamiento penal reconoce, así como las modalidades en que estos son cometidos:

A) Delitos contra datos informáticos

Tipificado en la ley N° 30096 “Ley de delitos informáticos” que en su artículo 3 señala que “El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.” Este tipo penal es uno que sanciona el acceso o manipulación ilícita a datos informáticos, ya sea para modificarlos, borrarlos, o alterar su accesibilidad, y es que como se puede advertir se puede encontrar hasta cinco verbos rectores diferentes para cometer ese ilícito, siendo que cada uno de ellos nos lleva a pensar que la clasificación que tendría este delito sería de mera actividad; por tanto un ejemplo sencillo de ingreso de información se produciría en el caso de que alguien ingresará información errónea de una persona dentro de un sistema informático bancario para obtener algún beneficio económico, en el caso del verbo “borrar” ejemplo sería cuando personal informático de una entidad elimina información sobre un ilícito que haya

cometido de modo que no se halle evidencias de lo que hizo, para el caso del verbo “deteriorar” si nos trasladamos a un plano físico sería cuando alguna persona en su afán de eliminar evidencia de un acto ilícito que cometió a través de una computadora, decidiera incendiar el ordenador y eliminar así los datos informáticos contenidos en el disco duro, ahora para el verbo “alterar” un ejemplo práctico sería cuando a un archivo de texto se le modificará su contenido una vez ingresado al sistema de una entidad luego de burlar la seguridad que dicho sistema posea, finalmente para el verbo “suprimir” o “hacer inaccesible” se tendría como ejemplo cuando una persona con los conocimientos informáticos suficientes altera el código de un archivo de texto generado a través del programa Word para que ninguna otra persona más tenga acceso al mismo.

Ahora bien, afectar datos informáticos pueden o no requerir conocimientos avanzados en computación, y es que según se requiera existen formas de incrementar la seguridad de datos informáticos, sin embargo, los criminales informáticos ven otras maneras de acceder a estos, datos, al respecto Acurio (s.f, p.25) nos menciona algunas otras modalidades en que se afectan datos informáticos:

- ✓ Los virus informáticos, que como se explicó en los antecedentes son una forma de software malicioso que una vez que infectan un ordenador tienen a replicarse y reproducirse en todo el sistema, buscando modificar o destruir datos, así como enviarlos a terceros con información confidencial de la computadora atacada.
- ✓ Los gusanos informáticos, que muy similares a los virus infectan los ordenadores en busca de modificar o destruir datos, se diferencian de los virus en su complejidad, y pueden causar estragos como modificar un

sistema informático para enviar por ejemplo continuamente dinero de una cuenta bancaria sin autorización del propietario.

- ✓ El uso de bombas lógicas (logic bombs), el cual se logra a través del uso de virus, en donde se programa la modificación o incluso destrucción de datos informáticos, es una modalidad que exige conocimientos avanzados de informática y es difícil de detectar.
- ✓ El uso de llaves maestras (superzapping), en donde a través del diseño de programas informáticos avanzados se logra crear una especie de llave maestra informática que permite a su creador acceder a cualquier archivo de una computadora, con el objetivo de alterar dichos archivos o eliminarlos.

B) Delitos contra sistemas informáticos

Tipificados también en la ley N° 30096 “Ley de delitos informáticos” y que fue modificado por la ley N° 30171 que en su artículo 4 señala que “El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de la libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa”. En este tipo penal se debe precisar dos puntos, el primero implica que el inutilizar un sistema informático parcial o totalmente, que impida a otros su acceso o que entorpezca o imposibilite su funcionamiento es un accionar que no todos pueden realizar pues requiere de conocimiento avanzados de informática en las cuales no solo se conozca el sistema a vulnerar, sino también su funcionamiento, y falencias en seguridad que este pueda tener, así como herramientas de software y hardware que permitan afectar el funcionamiento del sistema. El segundo punto es clasificar a este delito como un delito de resultado, pues es necesario que el sistema informático se encuentre efectivamente inutilizado parcial o totalmente.

La afectación a un sistema informático también se puede lograr de múltiples formas, al respecto Acurio (s.f., p. 27) nos menciona otras modalidades para afectar sistemas informáticos:

- ✓ Ataques de denegación de servicio (DDOS), que consisten en dejar inutilizable por un periodo de tiempo un sistema informático, impidiendo su acceso a los usuarios que hagan uso de dicho sistema, siendo que desentendiendo de la magnitud del ataque informático se podrá solucionar, y es que ataques masivos pueden llegar a requerir más tiempo de lo usual para que el sistema regresa a su estado normal.

C) Delitos contra la libertad sexual

Tipificados también en la ley N° 30096 “Ley de delitos informáticos” que en su artículo 5 señala que “El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.”, dicha norma penal establece una agravante también en su segundo párrafo “Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.”. Este tipo penal que se describe en la ley no necesita siempre de conocimientos avanzados de informática, y es que los pedófilos generalmente solo necesitarán hacer uso de sistemas informáticos para poder compartir el contenido pornográfico ilegal con otros criminales.

D) Delitos contra la intimidad y el secreto de las comunicaciones

De acuerdo a la ley N° 30096 “Ley de delitos informáticos”, nos dice en su artículo 7 que “El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.”.

E) Delitos contra el patrimonio

Siendo que aquí encontraremos al delito de fraude informático, el cual según la ley N° 30096 en su artículo 8 es aquel en el cual “El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.”. Siendo que se establece más adelante la agravante si el patrimonio afectado es del estado, siendo en tal caso una pena privativa de libertad no menor de cinco ni mayor de diez años y de ochenta ha ciento cuarenta días multa. Ahora bien, Acurio (s.f., p.23) nos menciona las modalidades que existen para cometerse fraudes informáticos:

- ✓ Los datos falsos (data diddling), que consiste en el ingreso de datos falsos a un sistema con el fin de producir un resultado favorable, este tipo de modalidad también es conocida como manipulación de datos de entrada.
- ✓ Manipulación de datos a través de caballos de troya, y es que los caballos de troya son archivos que incluyen en su interior todo tipo de virus y gusanos

informáticos que buscan altererar un sistema informático, por lo cual es muy usado también para realizar fraudes informáticos.

- ✓ La técnica del Salami (Salami Technique), que consite en alterar un sistema informático para realizar pequeñas transacciones financieras de las cuentas de la víctima, de forma repetitiva de modo que no sean fáciles de detectar, siendo que todo el dinero recaudado va a cuentas de terceros.
- ✓ Manipulación de datos de salida, que es lo que usualmente se veía en la clonación de tarjetas de crédito o débito robadas, en donde se alterando sistemas informáticos se obtenía la información contenida en las tarjetas.
- ✓ La fuga de datos (Data Leakage), que consiste en la copia y divulgación no autorizada de datos con propiedad intelectual, un delito muy común en estos días pues no necesita de conocimientos avanzados en informática.

F) Delitos contra la fe publica

En estos delitos informáticos encontramos a la suplantación de identidad, la misma que también se sanciona según el artículo 9 de la ley N° 30096 “Ley de delitos informáticos” que nos dice “El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.”. Según Acurio (s.f., p.23) aquí también se puede encontrar modalidades delictivas que atentan contra la fe pública:

- ✓ Las falsificaciones informáticas, que consiste en alterar datos informáticos para su uso ilegal, dichas falsificaciones que se pueden lograr desde el uso de programas informáticos resulta una modalidad delictiva que no necesita

de muchos conocimientos en informático, lo cual eso sí, depende de la complejidad del archivo que se va a falsificar.

- ✓ El phishing, que es la modalidad en la cual se roba la identidad de una persona a través del uso de programas informáticos ilegales también conocidos como malware, con los cuales se obtiene información personal como números de tarjeta de crédito, contraseñas, información de cuentas en sistemas informáticos, etc.

2.4. MARCO JURÍDICO

El marco de la presente investigación inicia por la legislación internacional que hay en materia informática, así como la legislación nacional que también se ha desarrollado al respecto, por tanto, se hará un repaso punto por punto a cada una de las normas que se encuentran vigentes en materia informática a la fecha:

2.4.1. Marco jurídico internacional

A nivel internacional encontramos un marco normativo que regula el derecho informático, entre los más importantes tenemos:

A. La convención sobre la propiedad intelectual de Estocolmo

Convenio firmado en Estocolmo y en donde se estableció la Organización Mundial de la Propiedad Intelectual el 14 de julio de 1967; dicha organización en el año de 1971 paso pasó a ser parte de uno de los organismos especializados de la Organización de las Naciones Unidas tiene dos objetivos que son: fomentar la protección de la propiedad intelectual en todo el mundo, y el segundo asegurar la cooperación entre las naciones en materia de propiedad intelectual.

B. La convención para la protección y producción de fonogramas de 1971

Dicho convenio que fue adoptado en Ginebra en el año de 1971 estableció la obligación de proteger a los que producían fonogramas de copias sin el consentimiento del productor, de que dichas copias no se importen ni se distribuyan al público, es así que aquí tenemos a la organización mundial de la propiedad intelectual como la encargada de administrar este convenio conjuntamente con la Organización Internacional del Trabajo y la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

C. La convención relativa a la distribución de programas y señales.

Este convenio firmado en Bruselas en el año de 1974 establece la obligación de los estados contratantes de tomar medidas adecuadas para impedir que, en su territorio o desde él, se distribuyan sin autorización señales portadoras de programas transmitidas por satélite. se considera que una distribución carece de autorización si no ha sido autorizada por el organismo - por lo general, un organismo de radiodifusión - que ha decidido el contenido del programa. sin embargo, no se aplican las disposiciones del convenio cuando la distribución de señales se efectúa desde satélites de radiodifusión directa.

D. El convenio de Budapest sobre la Cibercriminalidad

El Convenio sobre ciberdelincuencia firmado en el año 2001 en Budapest, también conocido como el Convenio de Budapest sobre ciberdelincuencia o simplemente como Convenio Budapest, es el primer convenio internacional que buscó hacer frente a los delitos informáticos mediante la coordiación de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las países firmantes . Dicho convenio elaborado por el Consejo de Europa en

Estrasburgo, con la participación activa de los estados observadores de Canadá, Japón y China.

En el convenio se definieron diez delitos informáticos entre los que se puede resaltar los siguiente: acceso ilícito, interceptación ilícita, ataque a la integridad de datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático, los delitos relacionados con la pornografía infantil, delitos relacionados contra la propiedad intelectual y de derechos afines.

Asimismo, en dicho convenio, se expusieron temas de derecho procesal como la preservación de los datos informáticos; la preservación y divulgación parcial de los datos de tráfico: la orden de producción, búsqueda y la incautación de datos informáticos, la recolección en tiempo real del tráfico de datos y la interceptación de datos de contenido.

Además, el Convenio contiene una disposición sobre un tipo específico de acceso transfronterizo a los datos informáticos almacenados que no requieren asistencia mutua y prevé también la creación de una red para garantizar una asistencia rápida entre las partes que firmaron el acuerdo, es importante agregar que a la fecha el Perú no es parte de dicho acuerdo.

2.4.2. Marco jurídico nacional

A nivel nacional encontramos un marco normativo que regula el derecho informático, entre las normas más importantes tenemos:

A. Sobre delitos informáticos

- **La ley N° 30096:** Los delitos informáticos son actualmente sancionados a través una ley especial como la ley N° 30096 “Ley de Delitos

Informáticos", que está conformado por siete capítulos estructurados de la siguiente manera: finalidad y objeto de la ley (Capítulo I), delitos contra datos y sistemas informáticos (Capítulo II), delitos informáticos contra la indemnidad y libertad sexual (Capítulo III), delitos informáticos contra la intimidad y el secreto de las comunicaciones (Capítulo IV), delitos informáticos contra el patrimonio (Capítulo V), delitos informáticos contra la fe pública (Cap. VI), disposiciones comunes (Cap. VII).

B. Sobre el comercio electrónico

- **La Ley Nº 27291:** que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica.
- **El TLC Perú/USA:** que cuenta con un capítulo referido al de comercio electrónico.
- **El TLC Perú/Canadá:** que cuenta con un capítulo referido al de comercio electrónico.
- **El TLC Perú/Singapur:** que cuenta con un capítulo referido al de comercio electrónico.
- **El TLC Perú/Corea del Sur:** que cuenta con un capítulo referido al de comercio electrónico.

C. Sobre el control de contenidos

- **La Ley Nº 28119:** que prohíbe el acceso de menores de edad a páginas web de contenido pornográfico.
- **La Ley N° 28681**: que regula la comercialización, consumo y publicidad de bebidas alcohólicas
- **La Ley Nº 29139:** que modifica la Ley Nº 28119, que prohíbe el acceso de menores de edad a páginas web de contenido pornográfico.

D. Sobre la propiedad intelectual

- **TLC Perú/USA:** que cuenta con un capítulo de propiedad intelectual.
- **TLC Perú/China:** que cuenta con un capítulo de propiedad intelectual.
- **TLC Perú/Costa Rica:** que cuenta con un capítulo sobre propiedad intelectual.
- **TLC Perú/Guatemala:** que cuenta con un capítulo sobre propiedad intelectual.
- **TLC Perú/Corea del Sur:** que cuenta con un capítulo sobre propiedad intelectual
- **TLC Perú/Japón:** que cuenta con un capítulo sobre propiedad intelectual.
- **TLC Perú/Panamá:** que cuenta con un Capítulo sobre propiedad intelectual.
- **TLC Perú/Comunidad Europea:** que cuenta con un capítulo sobre propiedad intelectual.

E. Sobre la protección de datos

- **La Ley Nº 27489:** que regula las centrales privadas de información de riesgos y de protección al titular de la Información.
- **La Ley Nº 27863:** que modifica varios artículos de la ley que regula las centrales privadas de información de riesgos y de protección al titular de la información;
- **La Ley Nº 27697:** que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional.
- **El Decreto Legislativo N° 991:** que modifica la Ley Nº 27697, que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional;

- **La Directiva Nº 005-2009/COD-INDECOPI:** del funcionamiento del registro de números telefónicos y direcciones de correo electrónico excluidos de ser destinatarios de publicidad masiva - Registro "Gracias... No Insista":
- **La Ley Nº 29733:** de Protección de Datos Personales.

F. Sobre la seguridad de la información

- **La Resolución Ministerial Nº 197-2011-PCM:** que establece fecha límite para que las diversas entidades de la administración pública implementen el plan de seguridad de la información dispuesto en la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información".
- **La Resolución Ministerial Nº 129-2012-PCM:** que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática.

G. Sobre las firmas digitales

- **La Ley 27269, de Firmas Digitales:** esta norma fue modificada por la Ley 27310 para permitir que pudieran ser incorporados los certificados digitales de origen extranjero.
- **El Decreto Supremo Nº 052-2008-PCM:** reglamento de la Ley de Firmas y Certificados Digitales.
- **El Decreto Supremo Nº 105-2012-PCM:** que fija disposiciones para facilitar la puesta en marcha de la firma digital y modifica el DS Nº 052-2008-PCM (Reglamento de la Ley de Firma). Esta norma busca acelerar los procesos de adopción de la firma digital en el e-gov.

H. Sobre los tributos

- **La RS Nº 333-2010/SUNAT:** que aprueba la nueva versión del PDT Planilla Electrónica, Formulario Virtual Nº 0601; la RS 344-2010-SUNAT para la implementación del sistema de embargo por medios telemáticos ante las empresas que desempeñan el rol adquiriente en los Sistemas de Pago mediante Tarjetas de Crédito y/o Débito.

I. Sobre el SPAM

- **Ley N° 28493**: que regula el uso del correo electrónico comercial no solicitado (SPAM). A la fecha solo ha existido un único caso que ha llegado a su fin.
- **El Decreto Supremo 031-2005-MTC:** que aprueba el Reglamento de la Ley 28493, que regula el envío del correo electrónico comercial no solicitado (SPAM).

J. Sobre la sociedad de la información

- **El Decreto Supremo 031-2006-PCM:** Que aprueba Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana. Versión 1.0;
- **El Decreto Supremo 066-2011-PCM:** que aprueba el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0".

K. Sobre la ciberdefensa

- **La Resolución Ministerial Nº 873-2004-DE-SG**: sobre la política de informática del sector Defensa.
- **El DS 069-2011-PCM:** que crea el Portal de Información de Datos Espaciales del Perú (GEOIDEP).

L. Sobre el voto electrónico

- **La Ley 29603:** que autoriza a la ONPE a emitir las Normas Reglamentarias para la implementación gradual y progresiva del Voto Electrónico.
- **El Decreto Supremo 211-2010-J/ONPE**: sobre el reglamento del voto electrónico.

M. Sobre el software

- **La Ley Nº 28612:** que norma el uso, adquisición y adecuación del software en la administración pública. Denominada también Ley de Neutralidad Tecnológica en la Adquisición de Software.

N. Sobre el hábeas data

- **La Ley Nº 29904:** sobre la promoción de la banda ancha y construcción de la red dorsal nacional de fibra óptica.

O. Sobre la interoperabilidad

- **El Decreto Supremo Nº 083-2011-PCM:** que crea la plataforma de interoperabilidad del Estado – PIDE.

P. Sobre nombres de dominio

- **La RJ 207-2002-INEI:** sobre las normas técnicas para la asignación de nombres de dominio de las entidades de la administración pública.

Q. Sobre el gobierno electrónico

- **La Resolución Ministerial 085-2012-PCM:** referido al Plan de Acción del Perú para su incorporación a la Sociedad de Gobierno Abierto.

R. Sobre el expediente digital

- **La RA 414-2010-CE-PJ:** que aprueba el Procedimiento de Formalización del Expediente Digital en la Nueva Ley Procesal del Trabajo.

S. Sobre la factura electrónica

- **La Resolución Ministerial 0188-2010-Sunat: l**a norma amplía el Sistema de Emisión Electrónica a la Factura y documentos vinculados a esta.

T. Sobre la accesibilidad

- **La Ley Nº 28530:** de promoción de acceso a Internet para personas con discapacidad y de adecuación del espacio físico en cabinas públicas de internet.

U. Sobre la gestión pública

- **La Ley Nº 27419:** sobre notificación por correo electrónico.
- **El Decreto Supremo 059-2004-PCM:** que fija disposiciones relativas a la administración del "Portal del Estado Peruano".
- **El Decreto Supremo 032-2006-PCM**: que crea el portal de servicios al ciudadano y empresas.
- **La Resolución Ministerial Nº 274-2006-PCM:** sobre la estrategia nacional de gobierno electrónico.
- **La Resolución Ministerial Nº 282-2005-PCM**: que aprueba los "Lineamientos para la Implantación Inicial del Sistema Electrónico de Adquisiciones y Contrataciones del Estado (SEACE)".
- **Ley N! 27806 de transparencia y acceso a la información pública:** que crea portales de acceso a la información pública de las entidades públicas. Luego, el DS Nº 072-2003-PCM reglamenta la norma.
- **La RJ Nº 088-2003-INEI**: sobre las normas para el uso del servicio de correo electrónico en las entidades de la administración pública.
- **La Ley Nº 27291:** que modifica el Código Civil, permitiendo la utilización de los medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica.

2.5. DEFINICIÓN DE TÉRMINOS BÁSICOS

Bienes jurídicos: Se entiende como bienes jurídicos a todos aquellos bienes materiales o inmateriales que son protegidos por el Estado en merito a la constitución política.

Datos informáticos: Se entiende como datos informáticos a la información que se almacena en un ordenador, que es manipulada a través de diferentes algoritmos de programación, y que se puede transmitir entre dispositivos a través de las redes de la informática como el INTERNET.

Delitos informáticos: Se denomina así a todos aquellos delitos que afectan sistemas o datos informáticos u otros bienes jurídicos de relevancia penal mediante la utilización de las Tecnologías de la información y la comunicación.

Derecho informático: El derecho informático es la rama de las ciencias jurídicas que se ocupa de englobar todo un conjunto de normas, principios, doctrina y jurisprudencia destinadas a regular el uso, desarrollo y expansión de la informática.

Formación profesional en Derecho Informático: Es el conjunto de competencias en derecho informático para su aplicación en el desempeño profesional.

Persecución penal de delitos informáticos: Es la función del Ministerio Público de perseguir penalmente todos aquellos delitos que afectan sistemas o datos informáticos u otros bienes jurídicos de relevancia penal mediante la utilización de las Tecnologías de la Información y las comunicaciones.

Sistemas informáticos: Se entiende como sistema informático a todo aquel sistema informatizado que permite almacenar y procesar información, a través

de una actividad que interrelaciona el hardware, software y personal a cargo del manejo de dicho sistema.

Tecnologías de la información y la comunicación: Se denomina así a todo el conjunto de tecnologías que se utilizan dentro de las ciencias de la computación para manipular o gestionar información, esto incluye desde ordenadores hasta programas informáticos, que permiten convertir, almacenar, administrar, y transmitir la información; por ello es que a las “Tecnologías de la información y la comunicación”, se les considera como herramientas para la búsqueda de información, o como medio para la comunicación e interacción social.

CAPÍTULO III

MARCO METODOLÓGICO

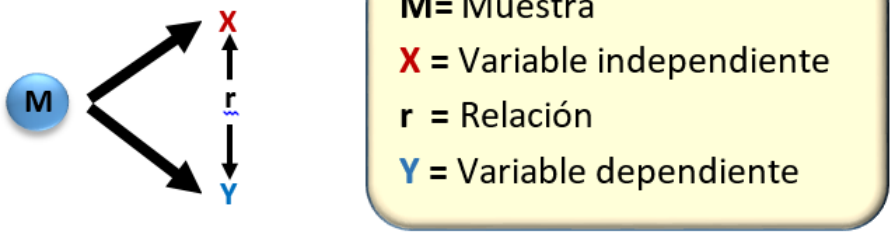
3.1. TIPO DE INVESTIGACIÓN

La presente investigación, en base al problema, objetivos e hipótesis planteados, se determinó como un estudio descriptivo correlacional en base a los siguientes fundamentos:

- ✓ Descriptivo: Porque se describió todos los componentes principales del fenómeno que se va a estudiar.
- ✓ Correlacional: Porque la finalidad general de la investigación fue determinar la relación que existe entre las dos variables, en este caso la formación en derecho informático y la persecución de delitos informáticos, pues como nos dice Hernandez Sampieri (2014, p.92): “Este tipo de estudios tiene como finalidad conocer la relación o grado de asociación que exista entre dos o más conceptos, categorías o variables en una muestra o contexto en particular”.

3.2. DISEÑO Y ESQUEMA DE INVESTIGACIÓN

Debido a que estuvimos frente a una investigación no experimental, el diseño de la investigación fue transaccional o transversal, en donde la recolección de datos fue en un único momento.



3.3. POBLACIÓN Y MUESTRA

3.3.1. POBLACIÓN

La presente investigación tuvo como población a los operadores jurisdiccionales del distrito judicial de Huánuco, específicamente a los fiscales provinciales penales, pues son ellos quienes en primera instancia tienen a su cargo los casos de delitos informáticos.

También se tuvo como población a los casos archivados de delitos informáticos que fueron tramitados en el Ministerio Público.

CANTIDAD	UBICACIÓN	TEMPORALIDAD
72 fiscales	Fiscalías Provinciales Penales Corporativas de Huánuco	Del 1 de julio al 31 de julio del 2018
24 Carpetas Fiscales archivadas de Delitos Informáticos	Fiscalías Provinciales Penales Corporativas de Huánuco	Del 02 de enero al 31 de diciembre del 2017

3.3.2. Muestra

Para la presente investigación corresponde tomar una muestra intencional del tipo probabilístico, siendo los siguientes:

Para análisis de contenido (carpetas fiscales), se determinó los siguientes:

Carpetas fiscales de Delitos Informáticos de las Fiscalías Provinciales Penales Corporativas de Huánuco.	12

Para encuesta (cuestionarios), se determinó los siguientes:

Fiscales de las Fiscalías Provinciales Penales Corporativas de Huánuco.	41

3.4. DEFINICIÓN OPERATIVA DE LOS INSTRUMENTOS DE RECOLECCIÓN DE DATOS

3.4.1. Lista de cotejo

Instrumento que fue preparado por el investigador para obtener información sobre los actos realizados por los fiscales de las fiscalías provinciales penales corporativas de Huánuco en aplicación del derecho del derecho informático.

3.4.2. Cuestionario

Que estuvo compuesto por un conjunto de preguntas, preparadas previamente, sobre los aspectos que le interesarán a la investigación, los cuales serán extraídos de las variables que estarán sujetas a medición. El cuestionario fue elaborado teniendo en cuento los objetivos de la investigación para que sea

contestado por los fiscales titulares de las Fiscalías Provinciales Penales Corporativas del distrito judicial de Huánuco.

3.4.3. Guías de entrevista

Que estuvo compuesto por un conjunto de preguntas, preparadas previamente, sobre los aspectos que le interesarán a esta investigación, los cuales fueron extraídos de las variables que estuvieron sujetas a medición.

TÉCNICA	INSTRUMENTO	FUENTE
Análisis de documentos	Matriz de análisis de datos	Carpetas fiscales de delitos informáticos
Encuesta	Cuestionario	Fiscales titulares de las Fiscalías Provinciales Penales Corporativas del distrito judicial de Huánuco
Entrevistas	Guías de entrevista	Fiscales titulares de las Fiscalías Provinciales Penales Corporativas del distrito judicial de Huánuco

3.5. TECNICAS DE RECOJO, PROCESAMIENTO Y PRESENTACIÓN DE DATOS

3.5.1. Edición y depuración de datos

En esta primera fase se precisaron y verificaron que todos los ítems estén resueltos (completados); determinando que los datos obtenidos sean legibles, claros y precisos.

3.5.2. Categorización de datos

En esta segunda fase los datos se categorizaron para su tabulación, análisis e interpretación.

3.5.3. Tabulación

En esta tercera fase, los datos luego de estar ordenados cuantitativamente (de modo que pueda realizarse su conteo delimitado en el número de casos) se transfirieron a tablas que facilitarán su tratamiento sistemático.

3.5.4. Presentación de datos

Los resultados obtenidos del trabajo de campo fueron presentados a través de gráficos y/o cuadros, para lo cual se hizo uso de programas informáticos como el Excel el SPSS, de modo que se pudiera sustentar que se ha alcanzado el propósito de la investigación.

CAPÍTULO IV

RESULTADOS

4.1. ANÁLISIS E INTEPRETACIÓN DE ENCUESTAS APLICADAS

La información que se presenta a continuación fue obtenida a través de la aplicación del instrumento denominado cuestionario, en el cual se formularon un total de 14 preguntas cerradas (con alternativas “Si” y “No”) que fueron respondidas por los Fiscales que laboran en las Fiscalías Provinciales Penales Corporativas de Huánuco, siendo que se planteó la aplicación de 72 cuestionarios.

Luego de aplicación de los cuestionarios se tuvo que por limitaciones de tiempo solo se pudo obtener una muestra de 41 fiscales encuestados, los cuales compartían el perfil cualitativo de que ocupaban el cargo de fiscal, y el perfil cuantitativo de que el 40% eran fiscales provinciales titulares y un 60% fiscales adjuntos.

Pregunta N° 01: En la fiscalía donde labora ¿se investigaron casos sobre la presunta comisión delitos informáticos en el año 2017?

Objetivo: Identificar si en la fiscalía donde labora se investigaron casos sobre la presunta comisión delitos informáticos en el año 2017.

CUADRO N° 01

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	23	60,5	60,5	60,5
	Sí	15	39,5	39,5	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 01

INTERPRETACIÓN: Un 39.47% de los encuestados ha manifestado que en la fiscalía en donde labora sí se han investigado casos sobre la presunta comisión de delitos informáticos, mientras que un 60.53% manifestó que en la fiscalía donde laboran no se han investigado casos sobre la presunta comisión de delitos informáticos.

ANÁLISIS: Aunque el índice de comisión de delitos informáticos en Huánuco es bajo, ello no quita que casi un 40% de los fiscales ya se hayan topado con casos de delitos informáticos, y si se toma en consideración que dichos índices

aumentos es más que probable que en un futuro la totalidad de los fiscales se topen con casos de delitos informáticos.

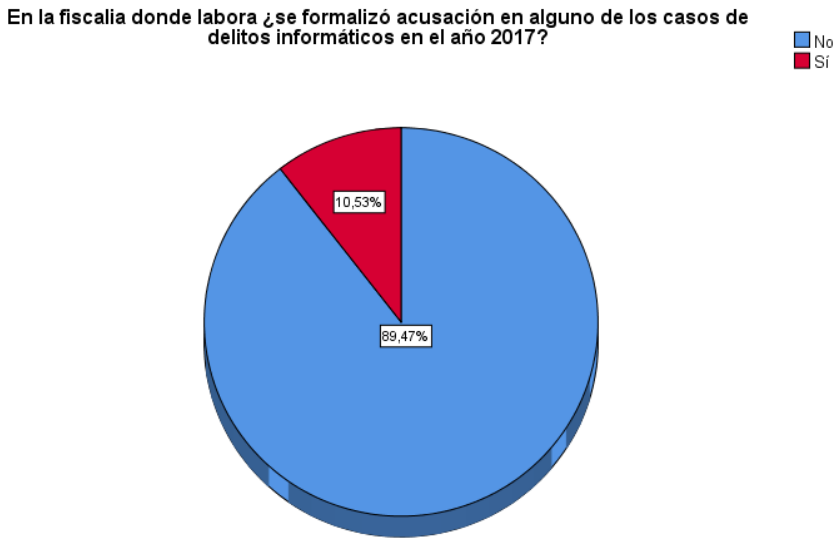
Pregunta N° 02: En la fiscalía donde labora ¿se formalizó acusación en alguno de los casos de delitos informáticos en el año 2017?

Objetivo: Identificar si en la fiscalía donde labora se formalizó acusación en alguno de los casos de delitos informáticos en el año 2017.

CUADRO N° 02

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	34	89,5	89,5	89,5
	Sí	4	10,5	10,5	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 02



INTERPRETACIÓN: El 10.53% de los encuestados ha manifestado que en la fiscalía en donde labora sí se formalizó acusación en algunos de los casos de delitos informáticos que tuvieron a su cargo en el año 2017, mientras que el 89.47% manifestó que no se formalizó acusación.

ANÁLISIS: El bajo porcentaje de encuestados que manifestó haber formalizado acusación en casos de delitos informáticos se explica en base al hecho de que los casos que logran pasar a la etapa de investigación preparatoria es mínima.

Pregunta N° 03: En la fiscalía donde labora ¿se logró probar la responsabilidad penal de los acusados en alguno de los casos de delitos informáticos en el año 2017?

CUADRO N° 03

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	36	94,7	94,7	94,7
	Sí	2	5,3	5,3	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 03

INTERPRETACIÓN: El 5.26% de los encuestado manifestaron que en las fiscalías donde laboran se logró probar la responsabilidad penal de los acusados en algunos de los casos de delitos informáticos en el año 2017, mientras que el 94.74% de los encuestados manifestaron que no se logró probar la responsabilidad penal de los acusados.

ANÁLISIS: Se debe de resaltar que aun con todas las limitaciones que tienen los fiscales en Huánuco para investigar los delitos informáticos, un porcentaje de los fiscales manifestara que en el año 2017 lograron probar la responsabilidad penal de sujetos acusados de cometer estos delitos.

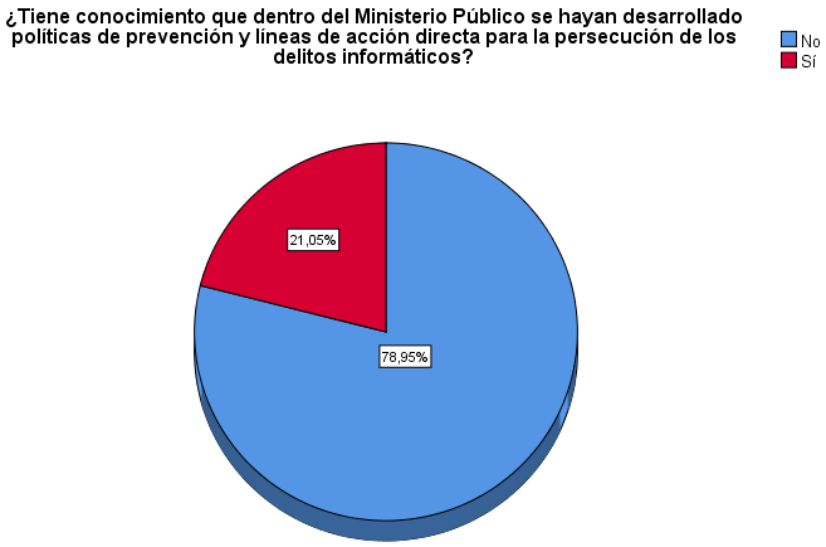
Pregunta N° 04: ¿Tiene conocimiento que dentro del Ministerio Público se hayan desarrollado políticas de prevención y líneas de acción directa para la persecución de los delitos informáticos?

Objetivo: Determinar si tiene conocimiento que dentro del Ministerio Público se hayan desarrollado políticas de prevención y líneas de acción directa para la persecución de los delitos informáticos.

CUADRO N° 04

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	30	78,9	78,9	78,9
	Sí	8	21,1	21,1	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 04



INTERPRETACIÓN: El 21.05% de los encuestados manifestaron que sí tienen conocimiento que dentro del Ministerio Público se hayan desarrollado políticas

de prevención y líneas de acción directa para la persecución de los delitos informáticos, mientras que un 78.95% manifestaron que no tienen conocimiento que dentro del Ministerio Público se hayan desarrollado políticas de prevención y líneas de acción directa al respecto.

ANÁLISIS: Dentro del Ministerio se desarrollan políticas de prevención y líneas de acción directa para la persecución del delito, lo cual implica que dentro de estas políticas se incluyen a los delitos informáticos, sin embargo, como se pudo observar en la encuesta, un alto índice de fiscales desconocen dichas políticas de prevención o líneas directas de acción.

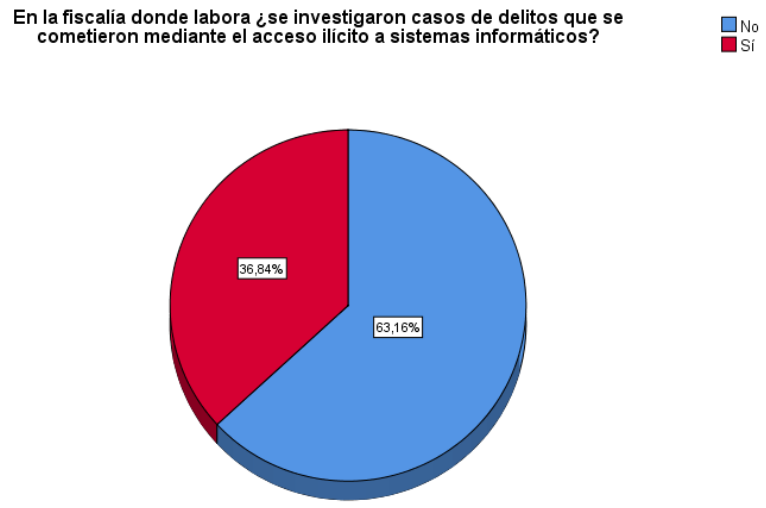
Pregunta N° 05: En la fiscalía donde labora ¿se investigaron casos de delitos que se cometieron mediante el acceso ilícito a sistemas informáticos?

Objetivo: Identificar si en la fiscalía donde labora se investigaron casos de delitos que se cometieron mediante el acceso ilícito a sistemas informáticos.

CUADRO N° 05

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	24	63,2	63,2	63,2
	Sí	14	36,8	36,8	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 05



INTERPRETACIÓN: El 36.84% de los encuestados manifestaron que en las fiscalías donde laboran si se investigaron delitos que fueron cometidos mediante el acceso ilícito a sistemas informáticos, mientras que el 63.16 % manifestaron que en la fiscalía donde laboran no se investigaron delitos que fueran cometidos mediante el acceso ilícito a sistemas informáticos

ANÁLISIS: El resultado obtenido se puede explicar en el hecho de que muchos de los delitos informáticos que se investigan en el Ministerio Público tienen involucrados a entidades bancarias o instituciones públicas o privadas, en donde los criminales suelen acceder ilícitamente a los sistemas informáticos.

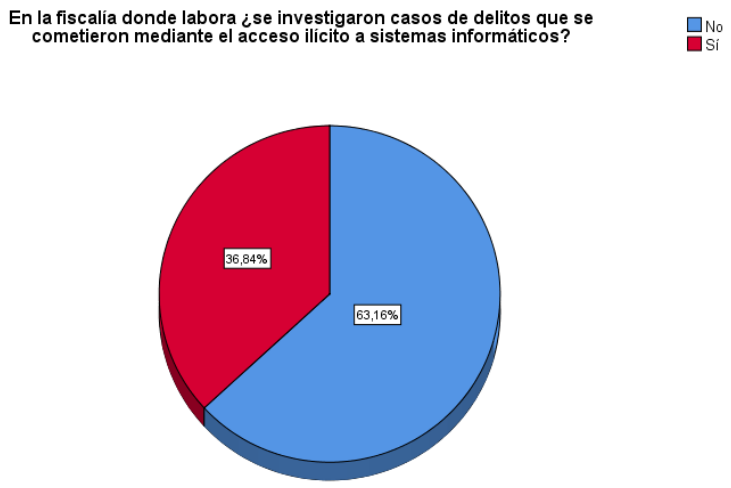
Pregunta N° 06: En la fiscalía donde labora ¿se investigaron casos de delitos que se cometieron mediante el atentado a la integridad de los sistemas informáticos?

Objetivo: Identificar si en la fiscalía donde labora se investigaron casos de delitos que se cometieron mediante el atentado a la integridad de los sistemas informáticos.

CUADRO N° 06

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	24	63,2	63,2	63,2
	Sí	14	36,8	36,8	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 06



INTERPRETACIÓN: El 36.84% de los encuestados manifestaron que en las fiscalías donde laboran si se investigaron delitos que fueron cometidos mediante el acceso ilícito a sistemas informáticos, mientras que el 63.16 % manifestaron que en la fiscalía donde laboran no se investigaron delitos que fueran cometidos mediante el acceso ilícito a sistemas informáticos.

ANÁLISIS: El resultado obtenido se puede explicar en el hecho de que muchos de los delitos informáticos que se investigan en el Ministerio Público tienen involucrados a entidades bancarias o instituciones públicas o privadas, en donde los criminales suelen acceder ilícitamente a los sistemas informáticos.

Pregunta N° 07: En la fiscalía donde labora ¿se investigaron casos de delitos que se cometieron mediante el atentado a la integridad de los sistemas informáticos?

Objetivo: Identificar si en la fiscalía donde labora se investigaron casos de delitos que se cometieron mediante el atentado a la integridad de los sistemas informáticos.

CUADRO N° 07

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	28	73,7	73,7	73,7
	Sí	10	26,3	26,3	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 07

INTERPRETACIÓN: El 26.32% de los encuestados manifestaron que en la fiscalías donde laboran si se investigaron casos de delitos que atentaron a la integridad de los sistemas informáticos, mientras que un 73.68% manifestaron que no investigaron casos de delitos que atentaron a la integridad de los sistemas informáticos.

ANÁLISIS: El resultado que se ha obtenido tiene sus explicación en el hecho de que quienes conocen a un nivel avanzado la informática pueden terminar afectando la integridad de sistemas informáticos, y por lo respondido por los fiscales se evidencia que casos con estas características ya se han estado produciendo en el distrito fiscal de Huánuco.

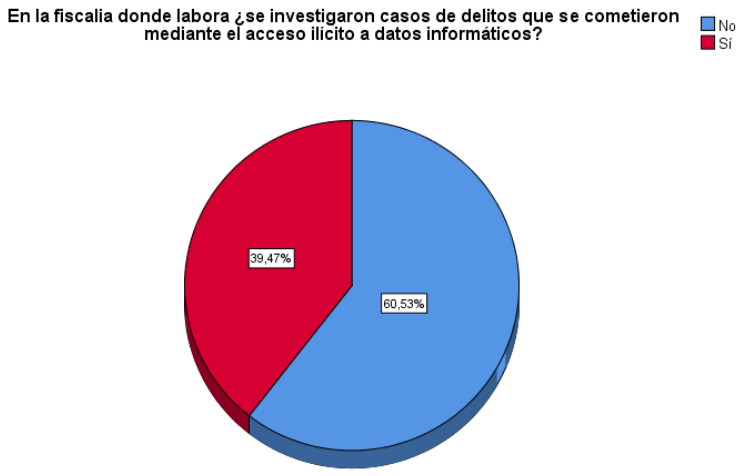
Pregunta N° 08: En la fiscalía donde labora ¿se investigaron casos de delitos que se cometieron mediante el acceso ilícito a datos informáticos?

Objetivo: Identificar si en la fiscalía donde labora se investigaron casos de delitos que se cometieron mediante el acceso ilícito a datos informáticos.

CUADRO N° 08

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	23	60,5	60,5	60,5
	Sí	15	39,5	39,5	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 08



INTERPRETACIÓN: El 39.47% de los encuestados manifiesta que en la fiscalía donde labora sí se investigaron casos de delitos que se cometieron mediante el acceso ilícito a datos informáticos, mientras que el 60.53% manifestó que no se investigaron casos de delitos que se cometieron mediante el acceso ilícito a datos informáticos.

ANÁLISIS: El resultado obtenido se explica en el hecho de que actualmente para la comisión de algunos delitos se accede ilegalmente a los datos informáticos de las personas, empresas o instituciones, ello con el objetivo de obtener información privada y hacer un uso ilegal de la misma.

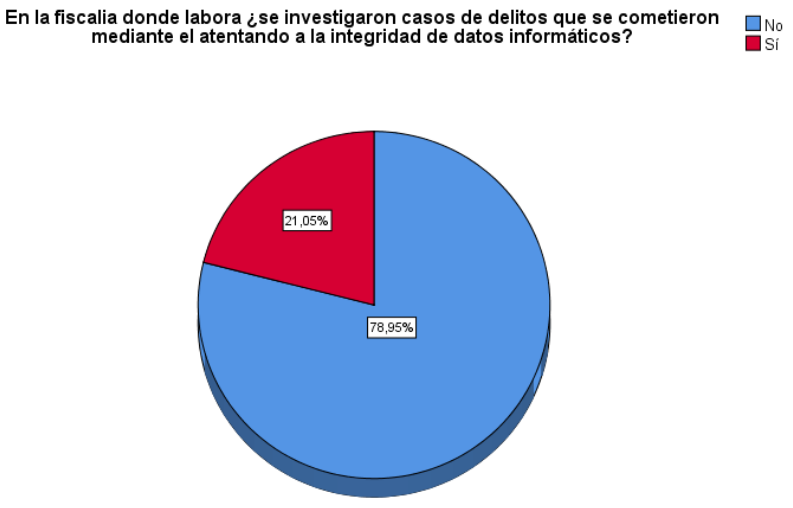
Pregunta N° 09: En la fiscalía donde labora ¿se investigaron casos de delitos que se cometieron mediante el atentando a la integridad de datos informáticos?

Objetivo: Identificar si en la fiscalía donde labora se investigaron casos de delitos que se cometieron mediante el atentando a la integridad de datos informáticos.

CUADRO N° 09

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	30	78,9	78,9	78,9
	Sí	8	21,1	21,1	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 09



INTERPRETACIÓN: El 21.05% de los encuestados manifestaron que en la fiscalía donde laboran sí se investigaron casos de delitos que se cometieron mediante el atentado a la integridad de datos informáticos, mientras que el 78.95% de los encuestados manifestaron que en la fiscalía donde laboran no se investigaron casos de delitos que se cometieron mediante el atentado a la integridad de datos informáticos.

ANÁLISIS: Aunque el resultado obtenido es menor, sí evidencia que en Huánuco ya se han estado produciendo casos en los que se atenta la integridad de datos informáticos, lo cual recordemos se produce cuando se altera o elimina datos informáticos.

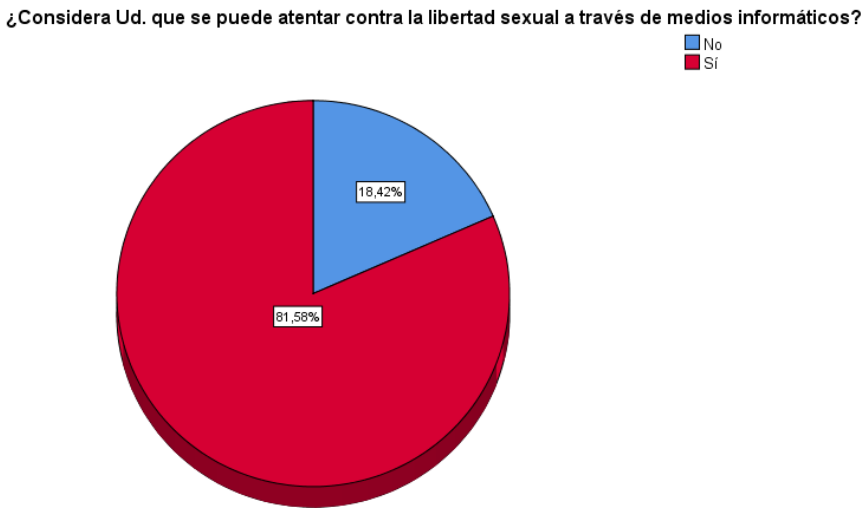
Pregunta N° 10: ¿Considera Ud. que se puede atentar contra la libertad sexual a través de medios informáticos?

Objetivo: Determinar si se puede atentar contra la libertad sexual a través de medios informáticos.

CUADRO N° 10

¿Considera Ud. que se puede atentar contra la libertad sexual a través de medios informáticos?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	7	18,4	18,4	18,4
	Sí	31	81,6	81,6	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 10



INTERPRETACIÓN: El 81.58% de los encuestados manifestó que sí se puede atentar contra la libertad sexual a través de medios informáticos, mientras que un 18.42% manifestó que no se puede atentar contra la libertad sexual a través de medios informáticos.

ANÁLISIS: La pregunta que se formuló en este ítem fue hecha en base a vigente ley de delitos informáticos que protege este bien jurídico, por lo que del resultado obtenido se puede advertir que la mayoría de los fiscales respondieron correctamente al manifestar que si se puede atentar contra la libertad sexual por medios informáticos.

Pregunta N° 11: ¿Considera Ud. que se puede atentar contra la intimidad a través de medios informáticos?

Objetivo: Determinar si se puede atentar contra la intimidad a través de medios informáticos.

CUADRO N° 11

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	7	18,4	18,4	18,4
	Sí	31	81,6	81,6	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 11

INTERPRETACIÓN: El 94.74% de los encuestado manifestaron que sí se puede atentar contra la intimidad a través de medio informáticos, mientras que un 5.26% de los encuestados manifestaron que no se puede atentar contra la intimidad a través de medio informáticos.

ANÁLISIS: La pregunta que se formuló en este ítem también fue hecha en base a vigente ley de delitos informáticos que protege este bien jurídico, por lo que del resultado obtenido se puede advertir que la amplia mayoría de los fiscales respondieron correctamente al manifestar que si se puede atentar contra la intimidad por medios informáticos.

Pregunta N° 12: ¿Considera Ud. que se puede atentar contra la seguridad pública a través de medios informáticos?

Objetivo: Determinar si se puede atentar contra la seguridad pública a través de medios informáticos.

CUADRO N° 12

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	7	18,4	18,4	18,4
	Sí	31	81,6	81,6	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 12

INTERPRETACIÓN: El 81.58% de los encuestados manifestaron que sí se puede atentar contra la seguridad pública a través de medios informáticos, mientras que un 18.42% de los encuestados manifestaron que no se puede atentar contra la seguridad pública a través de medios informáticos.

ANÁLISIS: La pregunta que se formuló en este ítem también fue hecha en base a vigente ley de delitos informáticos que protege este bien jurídico, por lo que del resultado obtenido se puede advertir que la amplia mayoría de los fiscales respondieron correctamente al manifestar que si se puede atentar contra la seguridad pública por medios informáticos.

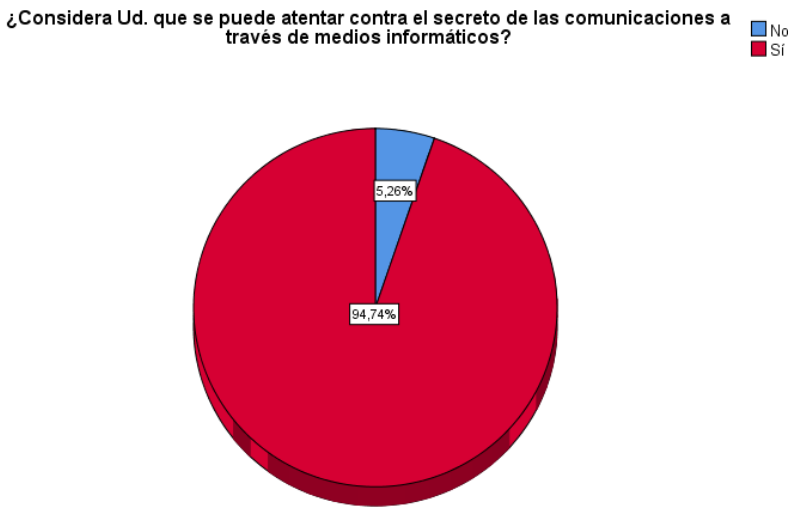
Pregunta N° 13: ¿Considera Ud. que se puede atentar contra el secreto de las comunicaciones a través de medios informáticos?

Objetivo: Determinar si se puede atentar contra el secreto de las comunicaciones a través de medios informáticos.

CUADRO N° 13

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	2	5,3	5,3	5,3
	Sí	36	94,7	94,7	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 13



INTERPRETACIÓN: El 94.74% de los encuestados manifestaron que sí se puede atentar contra el secreto de las comunicaciones a través de medios informáticos, mientras que el 5.26% de los encuestados manifestaron que no se puede atentar contra el secreto de las comunicaciones a través de medios informáticos.

ANÁLISIS: La pregunta que se formuló en este ítem también fue hecha en base a vigente ley de delitos informáticos que protege este bien jurídico, por lo que del resultado obtenido se puede advertir que la amplia mayoría de los fiscales respondieron afirmativamente, al manifestar que si se puede atentar contra el secreto de las comunicaciones a través de medios informáticos.

Pregunta N° 14: ¿Considera Ud. que se puede atentar contra el patrimonio a través de medios informáticos?

Objetivo: Determinar si se puede atentar contra el patrimonio a través de medios informáticos.

CUADRO N° 14

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	3	7,9	7,9	7,9
	Sí	35	92,1	92,1	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 14

INTERPRETACIÓN: El 92.11% de los encuestados manifestaron que sí se puede atentar contra el patrimonio a través de medios informáticos, mientras que el 7.89% de los encuestados manifestaron que no se puede atentar contra el patrimonio a través de medios informáticos.

ANÁLISIS: La pregunta que se formuló en este ítem también fue hecha en base a vigente ley de delitos informáticos que protege este bien jurídico, por lo que del resultado obtenido se puede advertir que la amplia mayoría de los fiscales respondieron afirmativamente, al manifestar que si se puede atentar contra el patrimonio a través de medios informáticos.

Pregunta N° 15: ¿Considera Ud. que se puede considerar como delito informático a todos aquellos delitos que utilicen las Tecnologías de la Información y las Comunicaciones para su comisión?

Objetivo: Determinar si se puede considerar como delito informático a todos aquellos delitos que utilicen las Tecnologías de la Información y las Comunicaciones para su comisión.

CUADRO N° 15

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	15	39,5	39,5	39,5
	Sí	23	60,5	60,5	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 15

4.2. ANALISIS E INTERPRETACIÓN DE LAS GUÍAS DE ENTREVISTA

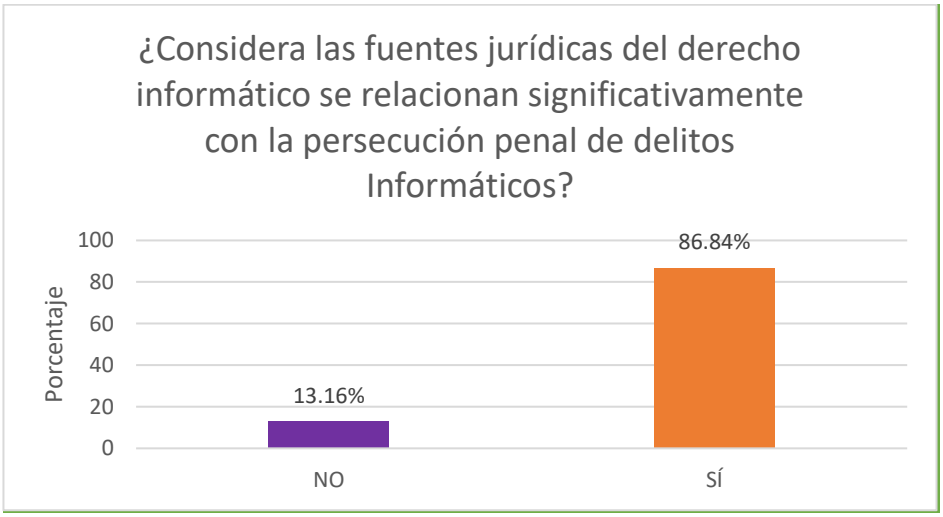
Pregunta N° 01: ¿Considera las fuentes jurídicas del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos?

Objetivo: Determinar si consideran las fuentes jurídicas del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos

CUADRO N° 16

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	5	13,2	13,2	13,2
	SÍ	33	86,8	86,8	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 16



INTERPRETACIÓN: El 86.84% de los encuestados consideró las fuentes jurídicas del derecho informático se relacionan significativamente con la persecución penal de delitos Informáticos, mientras que el 13.16% consideró que las fuentes jurídicas del derecho informático no se relacionan significativamente con la persecución penal de delitos Informáticos.

ANÁLISIS: Los resultados evidencian que efectivamente las fuentes jurídicas del derecho informático se relacionan significativamente con la persecución penal de delitos Informáticos, y es que debemos recordar que el derecho informático al ser una rama autónoma del derecho posee también fuentes jurídicas propias que el profesional del derecho debe conocer pues de estos se emana la norma jurídica en derecho informático.

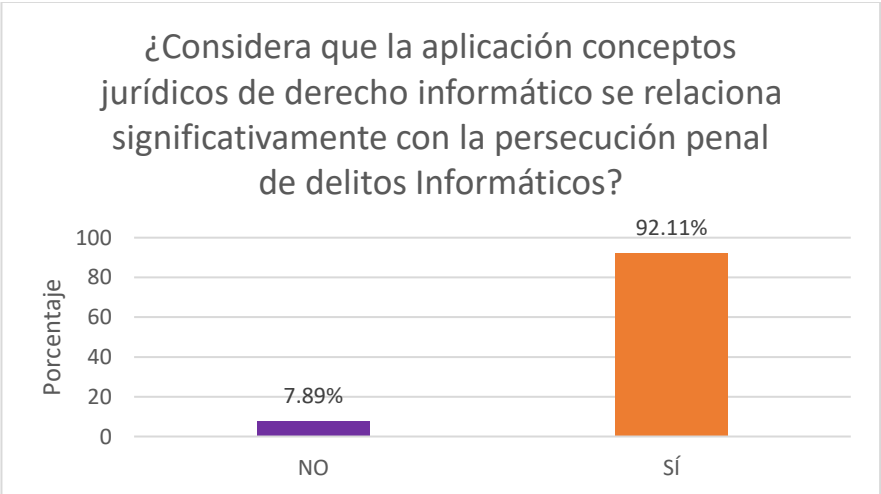
Pregunta N° 02: ¿Considera que la aplicación conceptos jurídicos de derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos?

Objetivo: Determinar si la aplicación conceptos jurídicos de derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos.

CUADRO N° 17

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	3	7,9	7,9	7,9
	SÍ	35	92,1	92,1	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 17



INTERPRETACIÓN: El 92,11% de los encuestados consideró que la aplicación conceptos jurídicos de derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos, mientras que el 7,89% consideró que la aplicación conceptos jurídicos de derecho informático no se relaciona significativamente con la persecución penal de delitos Informáticos.

ANÁLISIS: Los resultados evidencian que la aplicación conceptos jurídicos de derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos, y es que recordemos el derecho informático tiene conceptos jurídicos propios que son necesarios que el profesional del derecho debe conocer.

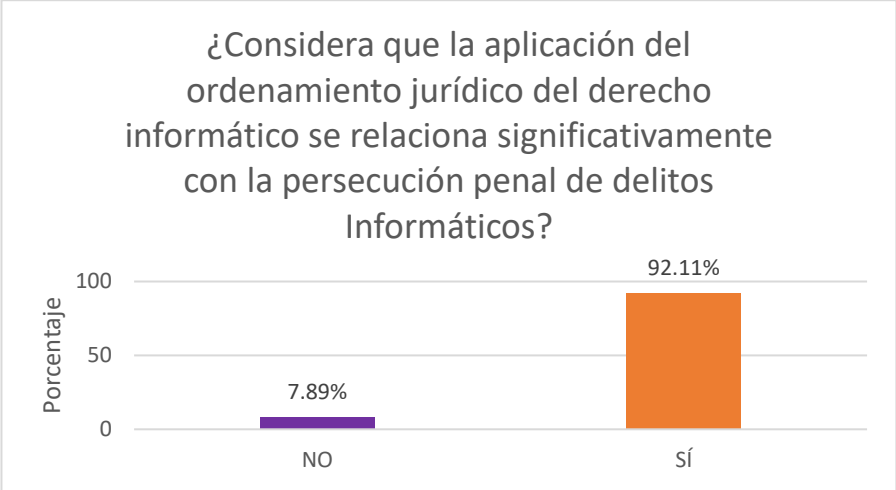
Pregunta N° 03: ¿Considera que la aplicación del ordenamiento jurídico del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos?

Objetivo: Determinar si la aplicación del ordenamiento jurídico del derecho informático se relaciona significativamente con la persecución penal de delitos informáticos.

CUADRO N° 18

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	3	7,9	7,9	7,9
	SÍ	35	92,1	92,1	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 18



INTERPRETACIÓN: El 92.11% de los encuestados consideró que la aplicación del ordenamiento jurídico del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos, mientras que el 7.89% consideró que la aplicación del ordenamiento jurídico del derecho informático no se relaciona significativamente con la persecución penal de delitos Informáticos.

ANÁLISIS: Los resultados evidencian la aplicación del ordenamiento jurídico del derecho informático sí se relaciona significativamente con la persecución penal de delitos Informáticos, y es que recordemos que al tener un ordenamiento jurídico propio hace que sea sustancial su debida comprensión y aplicación, más aún cuando se trata de delitos informáticos.

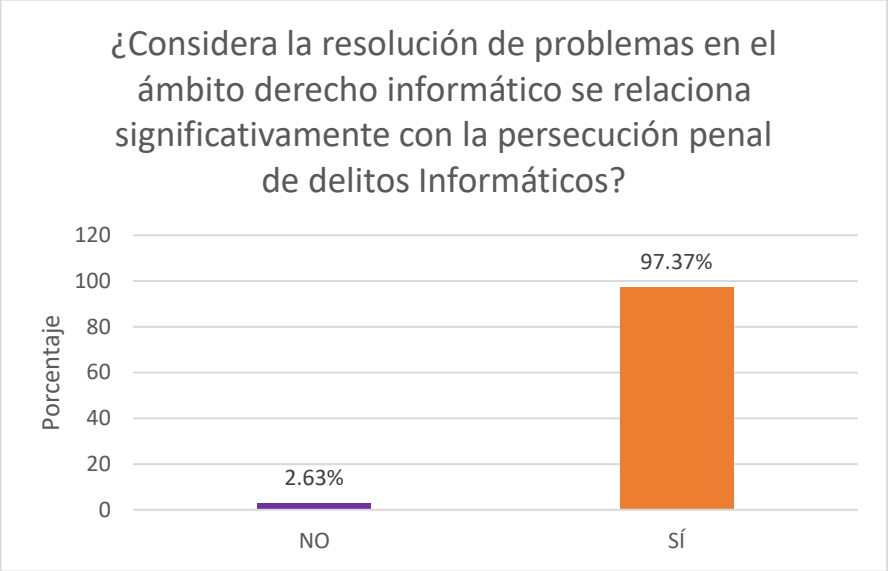
Pregunta N° 04: ¿Considera la resolución de problemas en el ámbito derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos?

Objetivo: Determinar si la resolución de problemas en el ámbito derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos.

CUADRO N°19

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	1	2,6	2,6	2,6
	SÍ	37	97,4	97,4	100,0
	Total	38	100,0	100,0	

GRÁFICO N°19



INTERPRETACIÓN: El 97.37% de los encuestados consideró que la resolución de problemas en el ámbito derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos, mientras que un 2.63% consideró la resolución de problemas en el ámbito derecho informático no se relaciona significativamente con la persecución penal de delitos Informáticos.

ANÁLISIS: Los resultados son contundentes en este punto, y es que recordemos que a medida que la informática se integre más en la vida del ser humano, será más grande la amenaza de que los criminales informáticos atenten contra otros bienes jurídicos protegidos a través de medios informatizados, por tanto, es necesario que el profesional del derecho esté preparado para la resolución de problemas en el ámbito derecho informático, lo cual incluye a los delitos informáticos.

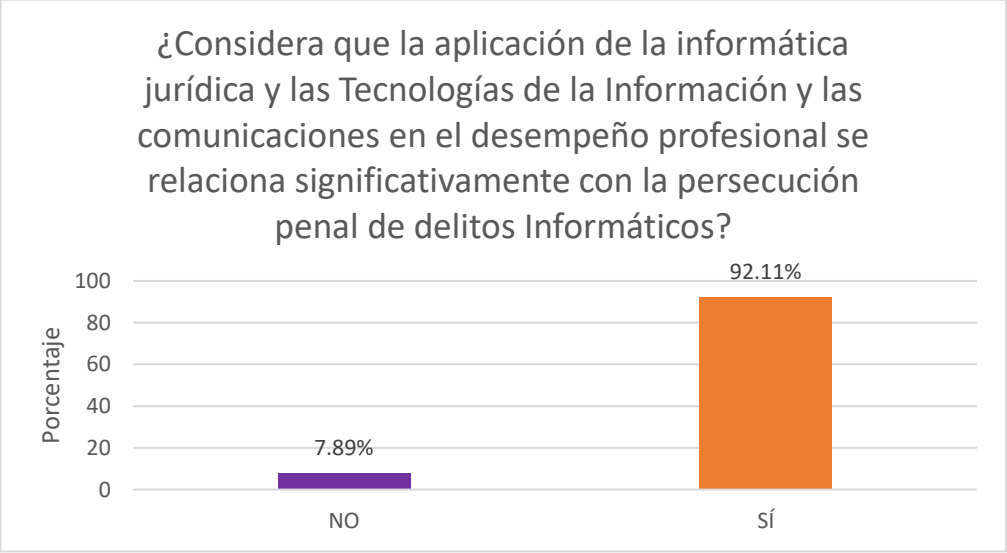
Pregunta N° 05: ¿Considera que la aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional se relaciona significativamente con la persecución penal de delitos Informáticos?

Objetivos: Determinar si la aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional se relaciona significativamente con la persecución penal de delitos Informáticos.

CUADRO N° 20

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	3	7,9	7,9	7,9
	SÍ	35	92,1	92,1	100,0
	Total	38	100,0	100,0	

GRÁFICO N° 20



INTERPRETACIÓN: El 92.11% de los encuestados consideró que la aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional se relaciona significativamente con la persecución penal de delitos Informáticos, mientras que un 7.89% consideró la aplicación de la informática jurídica y las Tecnologías de la

Información y las comunicaciones en el desempeño profesional no se relaciona significativamente con la persecución penal de delitos Informáticos.

ANÁLISIS: Los resultados son contundentes pues como se sabe los delitos informáticos se desarrollan a la par de las Tecnologías de la Información y las Comunicaciones, por tanto en la medida que las Tecnologías de la Información y las Comunicaciones se desarrollen y evolucionen también lo harán los delitos informáticos, por lo que conocer el uso de la informática jurídica como también de las tecnologías de la información y las comunicaciones puede resultar fundamental a la hora de perseguir delitos informáticos.

4.3. PRESENTACIÓN DE RESULTADOS DE ANÁLISIS DE ESTUDIO DE CARPETAS FISCALES ARCHIVADAS

Para la presentación de los resultados del análisis de estudio de las carpetas fiscales archivadas de delitos informáticos en el distrito fiscal de Huánuco, se ha tenido que recurrir a la elaboración de una lista de cotejo, en donde a través de diversos indicadores se ha podido evaluar las diversas competencias en derecho informático que han evidenciado los fiscales en estos casos.

Por tanto, en esta lista de cotejo se evaluaron los siguientes indicadores a un total de 12 de carpetas fiscales archivadas de delitos informáticos en el distrito fiscal de Huánuco:

- ✓ Identificación de las fuentes de derecho informático
- ✓ Análisis de las fuentes de derecho informático
- ✓ Argumentación utilizando las fuentes de derecho.
- ✓ Identificación de los conceptos jurídicos de derecho informático.
- ✓ Análisis de los conceptos jurídicos de derecho informático.
- ✓ Argumentación utilizando conceptos jurídicos de derecho informático.

- ✓ Identificación el ordenamiento jurídico del derecho informático.
- ✓ Análisis el ordenamiento jurídico en derecho informático
- ✓ Argumentación en base al ordenamiento jurídico en derecho informático.
- ✓ Identificación problemas del ámbito del derecho informático
- ✓ Análisis problemas del ámbito del derecho informático
- ✓ Planteamiento de soluciones con fundamentos a problemas del ámbito del derecho informático.
- ✓ Identificación del uso de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional.
- ✓ Análisis del uso de la informática jurídica y las Tecnologías de la Información y las comunicaciones
- ✓ Utilización de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional.

N°	DIMENSIONES / INDICADORES / ITEMS — CARPETAS FISCALES ARCHIVADAS	Aplicación de las fuentes del derecho informático						Aplicación conceptos jurídicos de derecho informático						Aplicación del ordenamiento jurídico del derecho informático						Resolución de problemas en el ámbito derecho informático						Aplicación de la informática jurídica y las TIC's					
		Identifica las fuentes de derecho informático		Analiza la fuentes de derecho informático		Argumenta utilizando las fuentes de derecho.		Identifica los conceptos jurídicos de derecho informático.		Analiza los conceptos jurídicos de derecho informático.		Argumenta utilizando conceptos jurídicos de derecho informático.		Identifica el ordenamiento jurídico del derecho informático.		Analiza el ordenamiento jurídico en derecho informático		Argumenta en base al ordenamiento jurídico en derecho informático.		Identifica problemas del ámbito del derecho informático		Analiza problemas del ámbito del derecho informático		Plantea soluciones con fundamentos a problemas del ámbito del derecho informático		Identifica el uso de la informática jurídica y las TIC's		Analiza el uso de la informática jurídica y las TIC's		Utiliza la informática jurídica y las TIC's	
		Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No
01	N° DE CARPETA: 427-2017 FISCALÍA: 1° FPPC	X		X		X		X			X	X		X		X		X			X		X		X		X		X		X
02	N° DE CARPETA: 724-2017 FISCALÍA: 1° FPPC	X		X		X		X		X		X		X			X	X		X			X		X	X		X		X	
03	N° DE CARPETA: 232-2017 FISCALÍA: 2° FPPC	X			X	X		X		X		X		X		X		X			X		X		X		X		X		X
04	N° DE CARPETA: 1790-2017 FISCALÍA: 2° FPPC		X		X		X	X			X	X		X			X		X		X		X		X		X		X		
05	N° DE CARPETA: 201-2017 FISCALÍA: 5° FPPC	X		X		X		X		X		X		X		X		X		X		X		X			X		X		X
06	N° DE CARPETA: 773-2017 FISCALÍA: 5° FPPC	X			X	X		X			X	X		X			X	X		X		X		X		X		X		X	
07	N° DE CARPETA: 1202-2017		X		X		X	X		X		X		X		X		X			X		X		X	X		X		X	

	FISCALÍA: 5° FPPC																														
08	N° DE CARPETA: 1318-2017 FISCALÍA: 5° FPPC		X		X		X		X		X		X		X		X		X		X		X		X		X		X		X
09	N° DE CARPETA: 1813-2017 FISCALÍA: 5° FPPC		X		X		X		X	X		X		X		X		X		X		X			X		X		X		X
10	N° DE CARPETA: 594-2017 FISCALÍA: 6° FPPC		X		X		X	X			X	X		X		X		X		X		X			X		X		X		X
11	N° DE CARPETA: 831-2017 FISCALÍA: 6° FPPC		X		X		X		X		X		X		X		X		X		X		X		X		X		X		X
12	N° DE CARPETA: 835-2017 FISCALÍA: 6° FPPC		X		X		X		X		X		X		X		X		X		X		X		X		X		X		X
TOTAL:		**5**	**7**	**3**	**9**	**5**	**7**	**8**	**4**	**5**	**7**	**9**	**3**	**9**	**3**	**6**	**6**	**8**	**4**	**5**	**7**	**5**	**7**	**2**	**10**	**5**	**7**	**4**	**8**	**4**	**8**

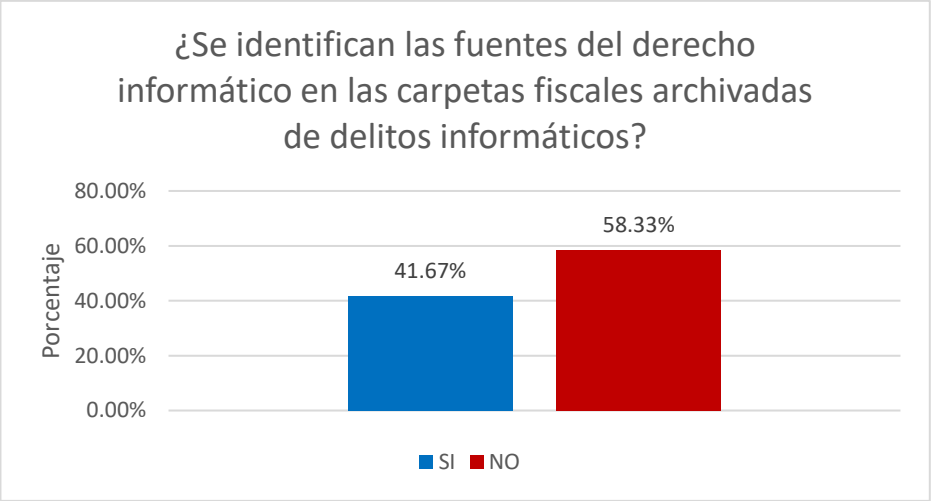
Pregunta N° 01: ¿Se identifican las fuentes jurídicas de derecho informático en las carpetas fiscales archivadas de delitos informáticos?

Objetivo: Determinar si se identifican las fuentes jurídicas de derecho informático en las carpetas fiscales archivadas de delitos informáticos.

CUADRO N° 21

		FRECUENCIA	PORCENTAJE	PROCENTAJE VALIDO	PORCENTAJE ACUMULADO
VÁLIDO	NO	7	58.33	58.33	58.33
	SÍ	5	41.67	41.67	100.00
	TOTAL	12	100.00	100.00	

GRÁFICO N° 21



INTERPRETACIÓN: En el 41.67% de las carpetas fiscales archivadas de delitos informáticos sí se identificaron las fuentes del derecho informático, mientras que el 58.33% de las carpetas fiscales archivadas de delitos informáticos no se identificaron las fuentes jurídicas de derecho informático.

ANÁLISIS: En más de la mitad (58.33%) de las carpetas fiscales archivadas no se advirtió la identificación de las fuentes jurídicas del derecho informático, sin embargo, un porcentaje aún importante (41.67%) si identificaron las fuentes jurídicas del derecho informático, siendo la legislación la fuente jurídica más identificada.

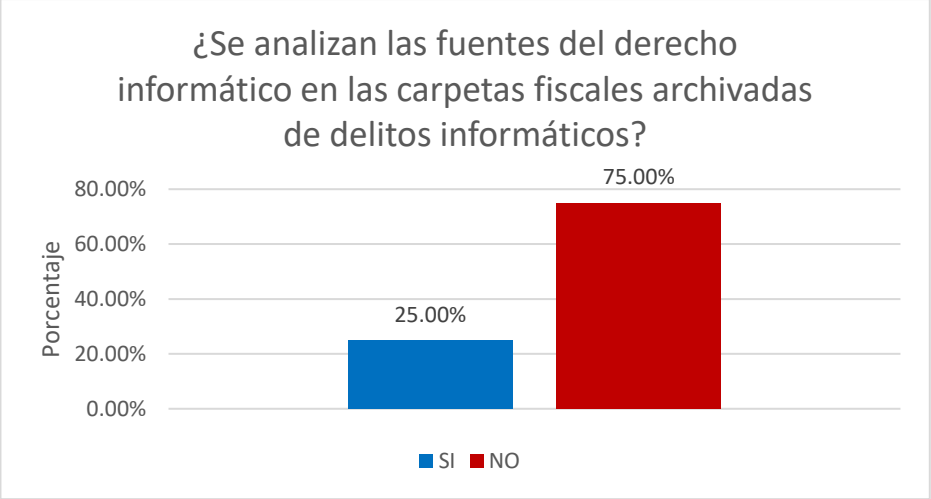
Pregunta N° 02: ¿Se analizan las fuentes jurídicas de derecho informático en las carpetas fiscales archivadas de delitos informáticos?

Objetivo: Determinar si se analiza las fuentes de derecho informático en las carpetas fiscales archivadas de delitos informáticos.

CUADRO N° 22

		FRECUENCIA	PORCENTAJE	PROCENTAJE VALIDO	PORCENTAJE ACUMULADO
VÁLIDO	NO	9	75.00	75.00	75.00
	SÍ	3	25.00	25.00	100.00
	TOTAL	12	100.00	100.00	

GRÁFICO N° 22



INTERPRETACIÓN: En el 25.00 % de las carpetas fiscales archivadas de delitos informáticos sí se analizaron las fuentes del derecho informático, mientras que el 75.00 % de las carpetas fiscales archivadas de delitos informáticos no se analizaron las fuentes jurídicas de derecho informático.

ANÁLISIS: La mayoría de las carpetas fiscales archivadas (75%) no se advirtió el análisis de las fuentes jurídicas del derecho informático, sobretodo de la legislación en delitos informáticos que como se mencionó en el punto anterior fue la fuente más identificada.

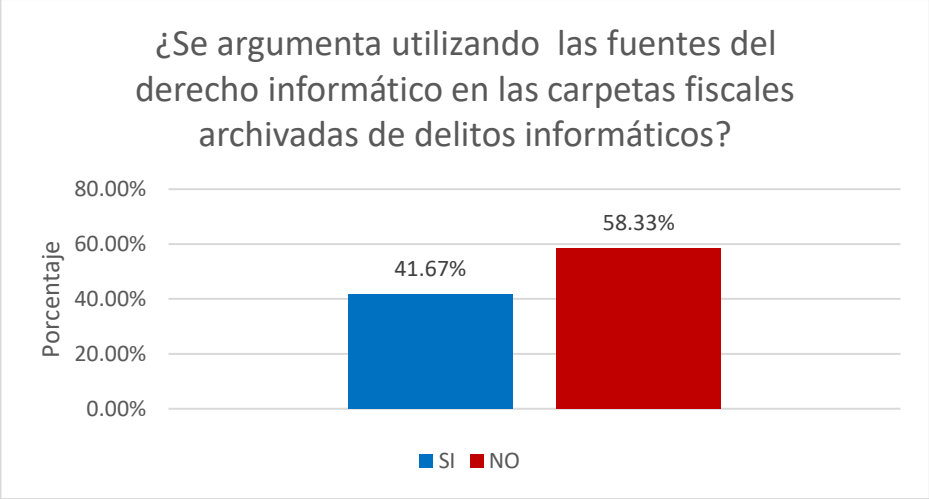
Pregunta N° 03: ¿Se argumenta utilizando las fuentes de derecho informático en las carpetas fiscales archivadas de delitos informáticos?

Objetivo: Determinar si se argumenta utilizando las fuentes de derecho informático en las carpetas fiscales archivadas de delitos informáticos.

CUADRO N° 23

		FRECUENCIA	PORCENTAJE	PROCENTAJE VALIDO	PORCENTAJE ACUMULADO
VÁLIDO	NO	7	58.33	58.33	58.33
	SÍ	5	41.67	41.67	100.00
	TOTAL	12	100.00	100.00	

GRÁFICO N° 23



INTERPRETACIÓN: En el 41.67 % de las carpetas fiscales archivadas de delitos informáticos sí se argumentó utilizando las fuentes del derecho informático, mientras que el 58.33 % de las carpetas fiscales archivadas de delitos informáticos no se argumentó utilizando las fuentes de derecho informático.

ANÁLISIS: Buena parte de las carpetas fiscales archivadas (58.33%) no se advirtió el análisis de las fuentes del derecho informático, sobretodo de la legislación actual en delitos informáticos que como se mencionó en el punto anterior fue la fuente más identificada.

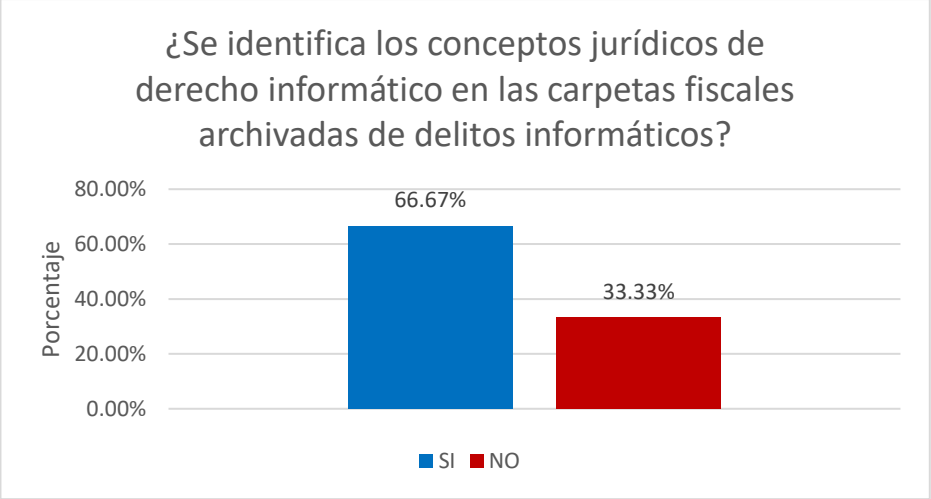
Pregunta N° 04: ¿Se identifica los conceptos jurídicos de derecho informático en las carpetas fiscales archivadas de delitos informáticos?

Objetivo: Determinar si se identifican los conceptos jurídicos de derecho informático en las carpetas fiscales archivadas de delitos informáticos.

CUADRO N° 24

		FRECUENCIA	PORCENTAJE	PROCENTAJE VALIDO	PORCENTAJE ACUMULADO
VÁLIDO	NO	4	33.33	33.33	33.33
	SÍ	8	66.67	66.67	100.00
	TOTAL	12	100.00	100.00	

GRÁFICO N° 24



INTERPRETACIÓN: En el 66.67% de las carpetas fiscales archivadas de delitos informáticos sí se identificaron los conceptos jurídicos de derecho informático, mientras que el 33.33% de las carpetas fiscales archivadas de delitos informáticos no se identificaron los conceptos jurídicos de derecho informático.

ANÁLISIS: En el derecho informático como se ha mencionado en las bases teóricas tiene una serie de conceptos jurídicos propios que se deben de saber identificar, así tenemos que en más de la mitad (66.67%) de carpetas fiscales archivadas sí se identificaron dichos conceptos.

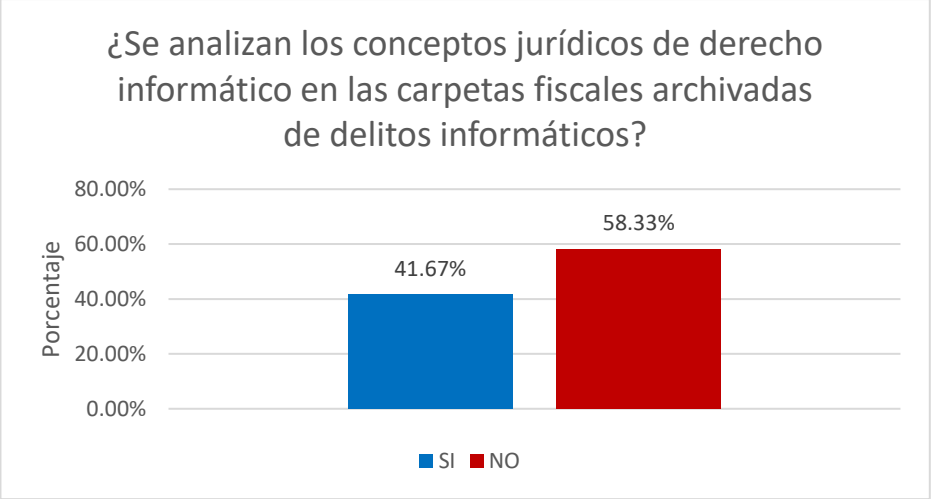
Pregunta N° 05: ¿Se analizan los conceptos jurídicos de derecho informático en las carpetas fiscales archivadas de delitos informáticos?

Objetivo: Determinar si se analizan los conceptos jurídicos de derecho informático en las carpetas fiscales archivadas de delitos informáticos.

CUADRO N° 25

		FRECUENCIA	PORCENTAJE	PROCENTAJE VALIDO	PORCENTAJE ACUMULADO
VÁLIDO	NO	7	58.33	58.33	58.33
	SÍ	5	41.67	41.67	100.00
	TOTAL	12	100.00	100.00	

GRÁFICO N° 25



INTERPRETACIÓN: En el 41.67% de las carpetas fiscales archivadas de delitos informáticos sí se analizaron los conceptos jurídicos de derecho informático, mientras que el 58.33% de las carpetas fiscales archivadas de delitos informáticos no se analizaron los conceptos jurídicos de derecho informático.

ANÁLISIS: Luego de identificado los conceptos jurídicos que hay en el campo del derecho informático es necesario que estos sean analizados, así tenemos que en más de la mitad (58.33%) de las carpetas fiscales archivadas no se analizaron dichos conceptos.

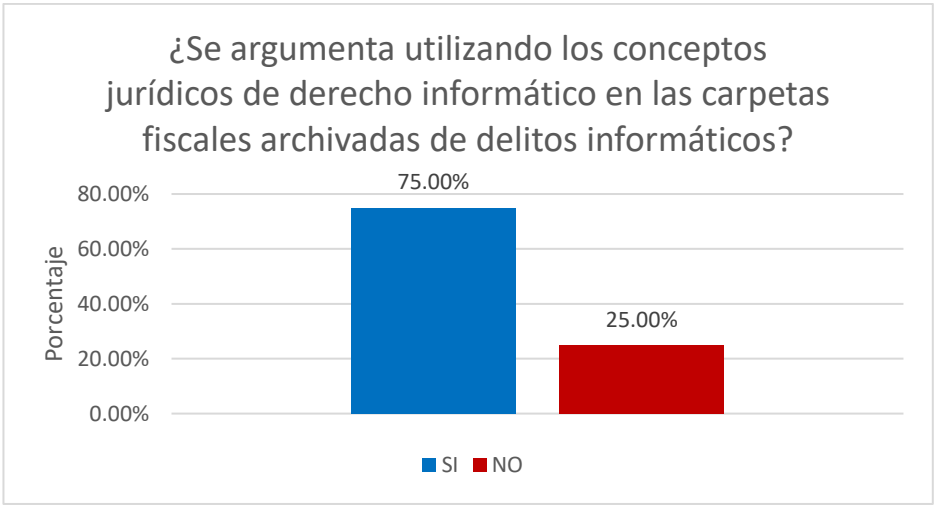
Pregunta N° 06: ¿Se argumenta utilizando los conceptos jurídicos de derecho informático en las carpetas fiscales archivadas de delitos informáticos?

Objetivo: Determinar si se argumenta utilizando los conceptos jurídicos de derecho informático en las carpetas fiscales archivadas de delitos informáticos.

CUADRO N° 26

		FRECUENCIA	PORCENTAJE	PROCENTAJE VALIDO	PORCENTAJE ACUMULADO
VÁLIDO	NO	3	25.00	25.00	25.00
	SÍ	9	75.00	75.00	100.00
	TOTAL	12	100.00	100.00	

GRÁFICO N° 26



INTERPRETACIÓN: En el 75.00% de las carpetas fiscales archivadas de delitos informáticos sí se argumentó utilizando los conceptos jurídicos de derecho informático, mientras que el 25.00% de las carpetas fiscales archivadas de delitos informáticos no se argumentó utilizando los conceptos jurídicos de derecho informático.

ANÁLISIS: Lo que se pretendía evaluar aquí es si los conceptos luego de identificados y analizados eran utilizados para elaborar argumentos jurídicos, así tenemos que en más de la mitad (75.00%) de las carpetas fiscales archivadas sí se argumentó utilizando conceptos jurídicos de derecho informático.

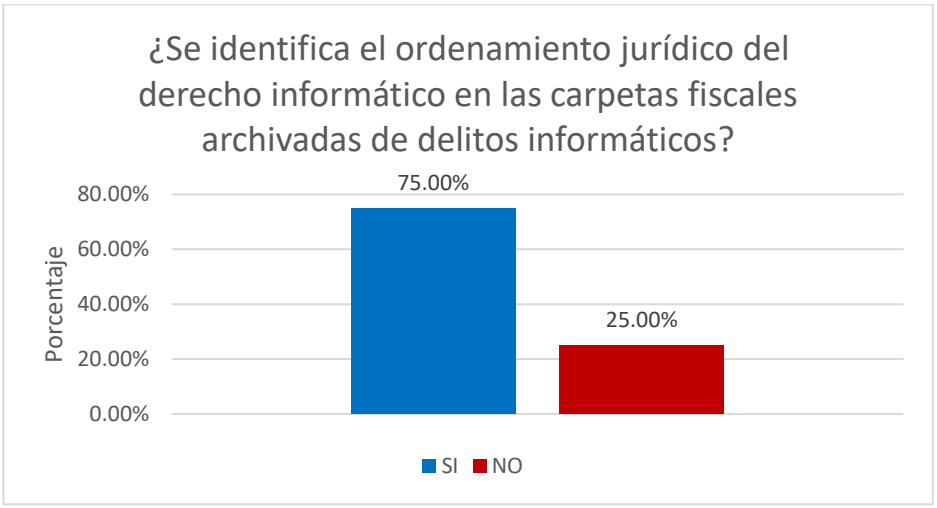
Pregunta N° 07: ¿Se identifica el ordenamiento jurídico del derecho informático en las carpetas fiscales archivadas de delitos informáticos?

Objetivo: Determinar si se identifica el ordenamiento jurídico del derecho informático en las carpetas fiscales archivadas de delitos informáticos.

CUADRO N° 27

		FRECUENCIA	PORCENTAJE	PROCENTAJE VALIDO	PORCENTAJE ACUMULADO
VÁLIDO	NO	3	25.00	25.00	25.00
	SÍ	9	75.00	75.00	100.00
	TOTAL	12	100.00	100.00	

GRÁFICO N° 27



INTERPRETACIÓN: En el 75.00% de las carpetas fiscales archivadas de delitos informáticos sí se identificó el ordenamiento jurídico del derecho informático, mientras que el 25.00% de las carpetas fiscales archivadas de delitos informáticos no se identificó el ordenamiento jurídico del derecho informático.

ANÁLISIS: Como se sabe, el derecho informático pose un ordenamiento jurídico propio que es necesario conocer y saber aplicar, por ello en primer lugar se debe saber identificar dicho ordenamiento, por lo cual en base a los resultados obtenidos vemos que en más de la mitad (75.00%) de las carpetas fiscales archivadas si se identificó el ordenamiento jurídico que rodea al derecho informático.

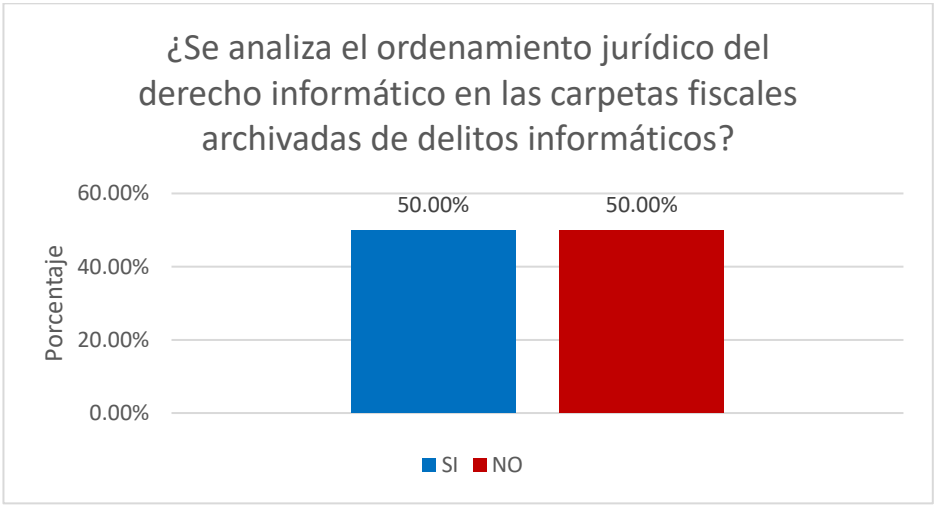
Pregunta N° 08: ¿Se analiza el ordenamiento jurídico del derecho informático en las carpetas fiscales archivadas de delitos informáticos?

Objetivo: Determinar si se analiza el ordenamiento jurídico del derecho informático en las carpetas fiscales archivadas de delitos informáticos.

CUADRO N° 28

		FRECUENCIA	PORCENTAJE	PROCENTAJE VALIDO	PORCENTAJE ACUMULADO
VÁLIDO	NO	6	50.00	50.00	50.00
	SÍ	6	50.00	50.00	100.00
	TOTAL	12	100.00	100.00	

GRÁFICO N° 28



INTERPRETACIÓN: En el 50.00% de las carpetas fiscales archivadas de delitos informáticos sí se analizó el ordenamiento jurídico del derecho informático, mientras que el 50.00% de las carpetas fiscales archivadas de delitos informáticos no se analizó el ordenamiento jurídico del derecho informático.

ANÁLISIS: Luego de haberse identificado el ordenamiento jurídico del derecho informático, es necesario evaluar ahora si se realizó algún análisis de dicho ordenamiento, por lo cual en base a los resultados obtenidos vemos que existe una paridad si se analizó o no el ordenamiento jurídico que rodea al derecho informático.

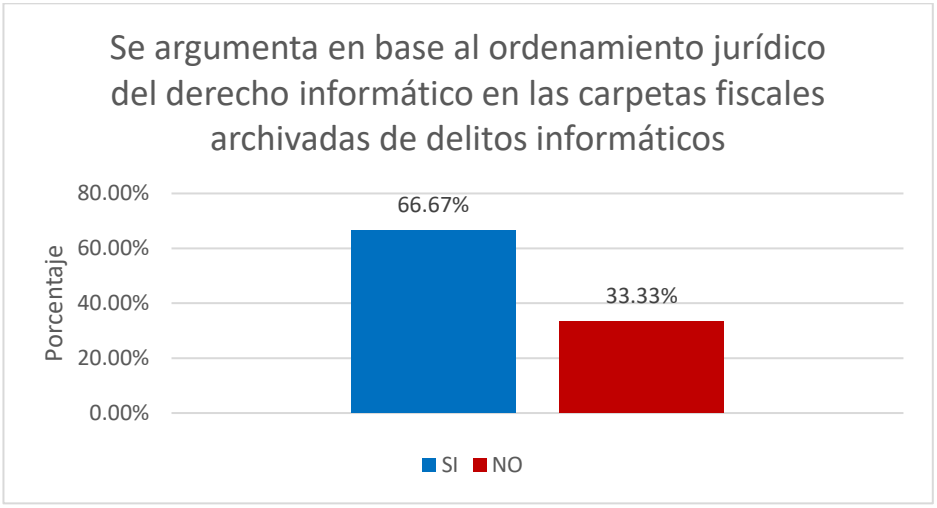
Pregunta N° 09: ¿Se argumenta en base al ordenamiento jurídico del derecho informático en las carpetas fiscales archivadas de delitos informáticos?

Objetivo: Determinar si se argumenta en base al ordenamiento jurídico del derecho informático en las carpetas fiscales archivadas de delitos informáticos.

CUADRO N° 29

		FRECUENCIA	PORCENTAJE	PROCENTAJE VALIDO	PORCENTAJE ACUMULADO
VÁLIDO	NO	4	33.33	33.33	33.33
	SÍ	8	66.67	66.67	100.00
	TOTAL	12	100.00	100.00	

GRÁFICO N° 29



INTERPRETACIÓN: En el 66.67% de las carpetas fiscales archivadas de delitos informáticos sí se argumentó en base al ordenamiento jurídico del derecho informático, mientras que el 33.33% de las carpetas fiscales archivadas de delitos informáticos no se argumentó en base al ordenamiento jurídico del derecho informático.

ANÁLISIS: Luego de realizarse el análisis es importante evaluar también si se ha hecho argumentos en base al ordenamiento jurídico del derecho informático, en donde base a los resultados vemos que un porcentaje superior (66.67%) de carpetas fiscales archivadas evidenciaron que sí se argumentó en base al ordenamiento jurídico del derecho informático.

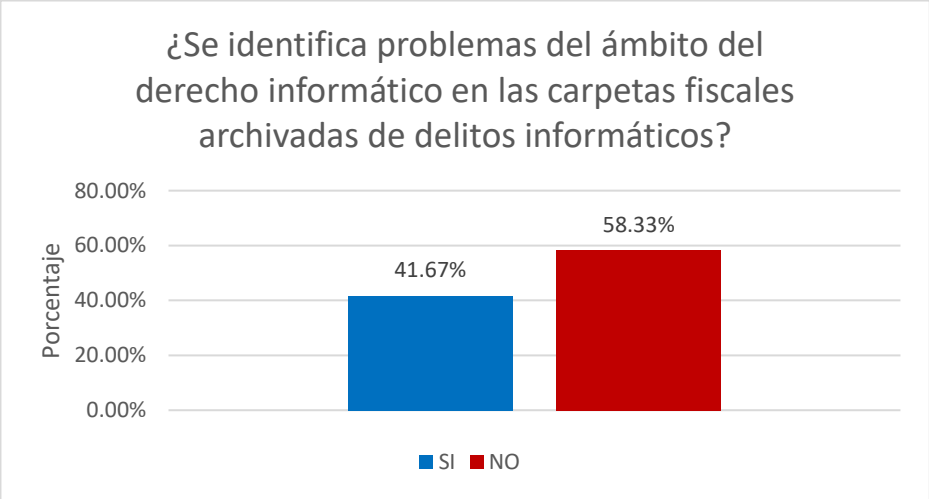
Pregunta N° 10: ¿Se identifica problemas del ámbito del derecho informático en las carpetas fiscales archivadas de delitos informáticos?

Objetivo: Determinar si se identifica problemas del ámbito del Derecho informático en las carpetas fiscales archivadas de delitos informáticos.

CUADRO N° 30

		FRECUENCIA	PORCENTAJE	PROCENTAJE VALIDO	PORCENTAJE ACUMULADO
VÁLIDO	NO	7	58.33	58.33	58.33
	SÍ	5	41.67	41.67	100.00
	TOTAL	12	100.00	100.00	

GRÁFICO N° 30



INTERPRETACIÓN: En el 41.67% de las carpetas fiscales archivadas de delitos informáticos sí se identificó problemas del ámbito del derecho informático, mientras que el 58.33% de las carpetas fiscales archivadas de delitos informáticos no se identificó problemas del ámbito del derecho informático.

ANÁLISIS: En este punto el objetivo era evaluar si se estaba advirtiendo los problemas enmarcadas dentro del ámbito del derecho informático en las carpetas fiscales archivadas, por tanto, en base a los resultados vemos que un porcentaje superior (58.33%) de carpetas fiscales archivadas evidenciaron que no se identificó problemas del ámbito del derecho informático.

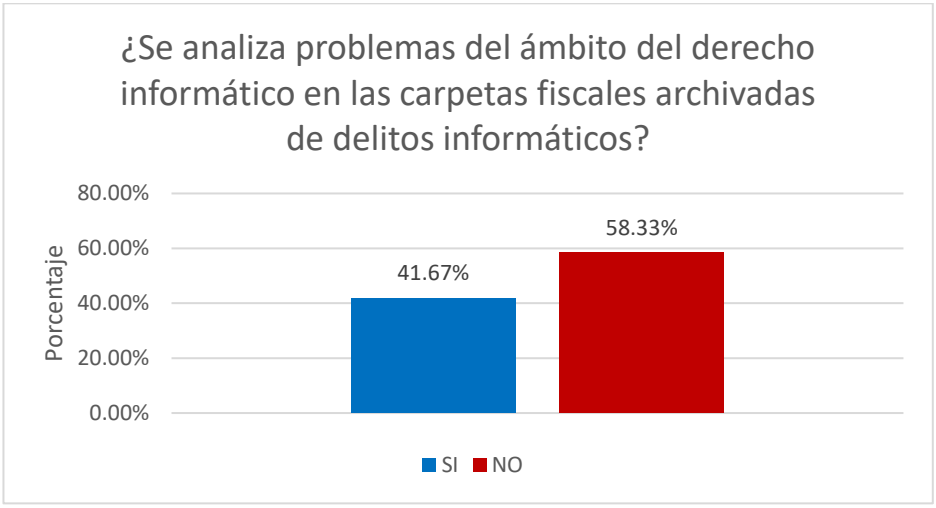
Pregunta N° 11: ¿Se analiza problemas del ámbito del derecho informático en las carpetas fiscales archivadas de delitos informáticos?

Objetivo: Determinar si se analiza problemas del ámbito del Derecho informático en las carpetas fiscales archivadas de delitos informáticos.

CUADRO N° 31

		FRECUENCIA	PORCENTAJE	PROCENTAJE VALIDO	PORCENTAJE ACUMULADO
VÁLIDO	NO	7	58.33	58.33	58.33
	SÍ	5	41.67	41.67	100.00
	TOTAL	12	100.00	100.00	

GRÁFICO N° 31



INTERPRETACIÓN: En el 41.67% de las carpetas fiscales archivadas de delitos informáticos sí se analizó problemas del ámbito del derecho informático, mientras que el 58.33% de las carpetas fiscales archivadas de delitos informáticos no se analizó problemas del ámbito del derecho informático.

ANÁLISIS: En este punto el objetivo era evaluar si luego de identificarse los problemas estos eran analizados, por tanto, en base a los resultados vemos que un porcentaje superior (58.33%) de carpetas fiscales archivadas evidenciaron que no se analizó problemas del ámbito del derecho informático.

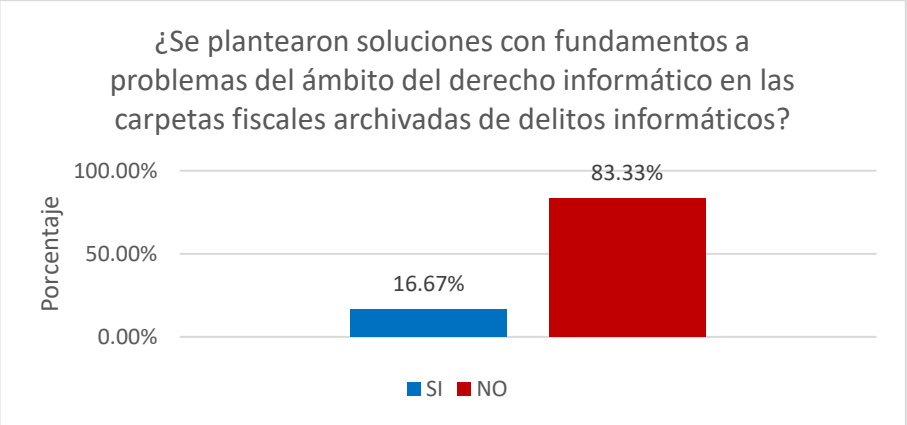
Pregunta N° 12: ¿Se plantearon soluciones con fundamentos a problemas del ámbito del derecho informático en las carpetas fiscales archivadas de delitos informáticos?

Objetivo: Determinar si se plantearon soluciones con fundamentos a problemas del ámbito del derecho informático en las carpetas fiscales archivadas de delitos informáticos.

CUADRO N° 32

9		FRECUENCIA	PORCENTAJE	PROCENTAJE VALIDO	PORCENTAJE ACUMULADO
VÁLIDO	NO	10	83.33	83.33	83.33
	SÍ	2	16.67	16.67	100.00
	TOTAL	12	100.00	100.00	

GRÁFICO N° 32



INTERPRETACIÓN: En el 16.67% de las carpetas fiscales archivadas de delitos informáticos sí se plantearon soluciones con fundamentos a problemas del ámbito del derecho informático, mientras que el 83.33% de las carpetas fiscales archivadas de delitos informáticos no se plantearon soluciones con fundamentos a problemas del ámbito del derecho informático.

ANÁLISIS: Identificados y analizados los problemas, toca ahora identificar si en las carpetas fiscales se han planteado soluciones a dichos problemas, por tanto, en base a los resultados vemos que un porcentaje superior (83.33%) de carpetas fiscales archivadas evidenciaron que no se plantearon soluciones con fundamentos a problemas del ámbito del derecho informático.

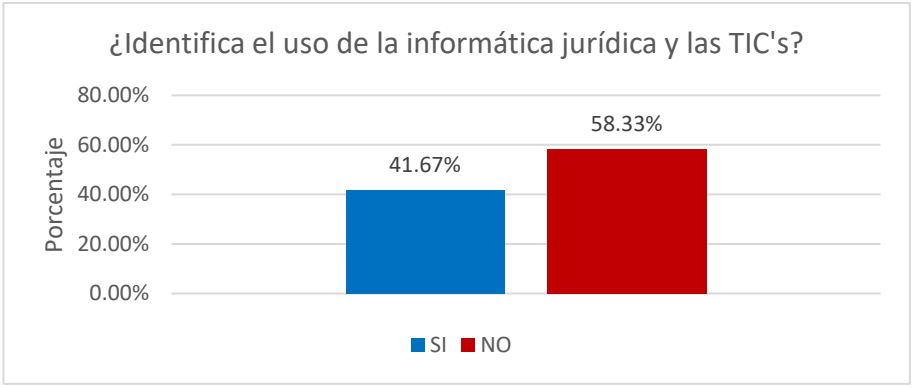
Pregunta N° 13: ¿Se Identifica el uso de la informática jurídica y las Tecnologías de la Información y las Comunicaciones en las carpetas fiscales archivadas de delitos informáticos?

Objetivo: Determinar si se identifica el uso de la informática jurídica y las Tecnologías de la Información y las Comunicaciones en las carpetas fiscales archivadas de delitos informáticos.

CUADRO N° 33

		FRECUENCIA	PORCENTAJE	PROCENTAJE VALIDO	PORCENTAJE ACUMULADO
VÁLIDO	NO	7	58.33	58.33	58.33
	SÍ	5	41.67	41.67	100.00
	TOTAL	12	100.00	100.00	

GRÁFICO N° 33



INTERPRETACIÓN: En el 41.67% de las carpetas fiscales archivadas de delitos informáticos sí se identificó el uso de la informática jurídica y las Tecnologías de la Información y las Comunicaciones, mientras que el 53.33% de las carpetas fiscales archivadas de delitos informáticos no se identificó el uso de la informática jurídica y las Tecnologías de la Información y las Comunicaciones.

ANÁLISIS: Dentro de la persecución de delitos informáticos es importante evaluar si se ha identificado el uso de la informática jurídica y las Tecnologías de la Información y las Comunicaciones pues son áreas del derecho informático, por tanto, en base a los resultados vemos que un porcentaje superior (53.33%) de las carpetas fiscales archivadas de delitos informáticos no se identificó el uso de la informática jurídica y las Tecnologías de la Información y las Comunicaciones.

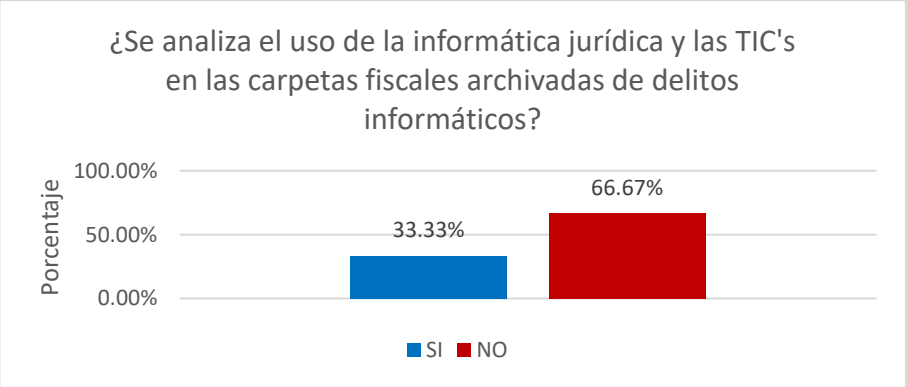
Pregunta N° 14: ¿Se analiza el uso de la informática jurídica y las Tecnologías de la Información y las Comunicaciones en las carpetas fiscales archivadas de delitos informáticos?

Objetivo: Determinar si se analiza el uso de la informática jurídica y las Tecnologías de la Información y las Comunicaciones en las carpetas fiscales archivadas de delitos informáticos.

CUADRO N° 34

		FRECUENCIA	PORCENTAJE	PROCENTAJE VALIDO	PORCENTAJE ACUMULADO
VÁLIDO	NO	8	66.67	66.67	66.67
	SÍ	4	33.33	33.33	100.00
	TOTAL	12	100.00	100.00	

GRÁFICO N° 34



INTERPRETACIÓN: En el 33.33% de las carpetas fiscales archivadas de delitos informáticos sí se analizó el uso de la informática jurídica y las Tecnologías de la Información y las Comunicaciones, mientras que el 66.67% de las carpetas fiscales archivadas de delitos informáticos no se analizó el uso de la informática jurídica y las Tecnologías de la Información y las Comunicaciones.

ANÁLISIS: Luego que se identifica el uso de la informática jurídica y las Tecnologías de la Información y las Comunicaciones es necesario que se analice dicho uso, por tanto, en base a los resultados vemos que un porcentaje superior (66.67%) de las carpetas fiscales archivadas de delitos informáticos no se analizó el uso de la informática jurídica y las Tecnologías de la Información y las Comunicaciones.

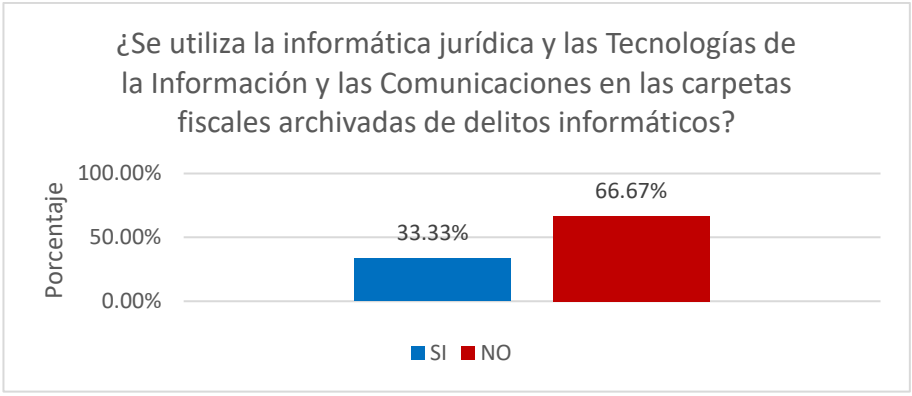
Pregunta N° 14: ¿Se utiliza la informática jurídica y las Tecnologías de la Información y las Comunicaciones en las carpetas fiscales archivadas de delitos informáticos?

Objetivo: Determinar si se utiliza la informática jurídica y las Tecnologías de la Información y las Comunicaciones en las carpetas fiscales archivadas de delitos informáticos.

CUADRO N° 34

		FRECUENCIA	PORCENTAJE	PROCENTAJE VALIDO	PORCENTAJE ACUMULADO
VÁLIDO	NO	8	66.67	66.67	66.67
	SÍ	4	33.33	33.33	100.00
	TOTAL	12	100.00	100.00	

GRÁFICO N° 34



INTERPRETACIÓN: En el 33.33% de las carpetas fiscales archivadas de delitos informáticos sí se utilizó la informática jurídica y las Tecnologías de la Información y las Comunicaciones, mientras que el 66.67% de las carpetas fiscales archivadas de delitos informáticos no se utilizó la informática jurídica y las Tecnologías de la Información y las Comunicaciones.

ANÁLISIS: Si se ha identificado el uso de la informática jurídica y las Tecnologías de la Información y las Comunicaciones y se analizado dicho uso, lo que toca ahora es identificar si se ha hecho uso finalmente de ambos campos del derecho informático, por tanto, en base a los resultados vemos que un porcentaje superior (66.67%) de las carpetas fiscales archivadas de delitos informáticos sí se utilizó la informática jurídica y las Tecnologías de la Información y las Comunicaciones.

CAPÍTULO V

DISCUSIÓN DE RESULTADOS

5.1. CONTRASTACIÓN DE LA INVESTIGACIÓN CON LOS ANTECEDENTES TEÓRICOS

En este punto comparamos los resultados que se habían obtenido en el capítulo anterior con las investigaciones previas que ha habido acerca del problema y que se incorporaron en esta investigación, con el objetivo principal y fundamental de explicar semejanzas o diferencias que pudieran advertirse entre estas y los resultados obtenidos:

5.1.1. Antecedentes teóricos internacionales

- ✓ Del trabajo de investigación realizado por Jorge Alexandre Gonzales Hurtado (2013) titulado: “Delincuencia informática: daños informáticos del artículo 264 del código penal y propuesta de reforma”, en el cual se concluía que España goza de tener una legislación suficiente en materia de delitos informáticos, pero que mencionaba la prevalencia del problema sobre la interpretación de los tipos penales, tenemos que decir que dicha conclusión

comparativamente hablando también se ha podido advertir en esta investigación, y es que aunque el Perú ya sanciona penalmente los delitos informáticos a través de la ley N° 30096 y su modificatoria, el problema de la interpretación de los tipos penales también es recurrente.

- ✓ Del trabajo de investigación realizado por Karina Medinacelli Díaz (2015) titulado: “La necesidad de incorporar en el código penal el tipo penal de falsificación informática.”, en dicha investigación se concluía que el derecho penal y el derecho en su conjunto deben marcar límites en la conducta de los comportamientos delictivos que pueden derivarse del uso de medios electrónicos, también concluye que la no denuncia de delitos informáticos por las víctimas es a causa de que las víctimas prefieren asumir las consecuencias y ver medidas de prevención en lugar de buscar un proceso judicial, al respecto podemos decir que en la presente investigación también se ha podido corroborar lo mencionado en este estudio hecho en Bolivia, pues en el Perú también se necesita mejorar las medidas de prevención para delitos informáticos pues estos se encuentran en constante evolución y cambio, en donde no bastará solo tener legislación penal que este a la par de estos cambios, sino también de toda un política de prevención que la complemente.
- ✓ Del trabajo de investigación de Roberto Lemaitre Picado (2010) titulado: “La impunidad de los delitos informáticos en la ciber-sociedad costarricense en ámbito del derecho penal”, que concluye que es necesario conocer sobre redes informáticas y equipos informáticos para comprender el ecosistema en donde se desarrollan los delitos informáticos, y que existe cierta inseguridad jurídica cuando un juez trata de interpretar a su entender verbos técnicos que se encuentran en artículos penales de delitos informáticos; al respecto

podemos decir que a través del presente trabajo de investigación también se ha podido corroborar ambas conclusiones, y es que los delitos informáticos al desarrollarse en medios informáticos implican que quien quiera comprenderlos deba entender en primer lugar conceptos de informática (como redes y equipos informáticos), como también de la terminología técnico-jurídica que hay alrededor de la tipificación de estos delitos, los cuales necesitarán que quien los interprete tenga cierto grado de preparación para entender bien la ley penal en materia de delitos informáticos e incluso de derecho informático en general.

- ✓ Del trabajo de investigación de Cristian Fabián Borghello titulado:" Seguridad informática: sus implicancias e implementación.", se concluye primero que debería de haber una legislación internacional unificada que regule el problema de la cibernética, y en segundo lugar concluye que la mejor herramienta para disminuir los daños por infiltración a sistemas informáticos es la capacitación, y no solamente restringir el acceso a la información; al respecto de esta investigación podemos decir que través de la presente investigación se ha corroborado la necesidad de una legislación unificada en materia de la informática, pues permitiría atacar problemas como la cibercriminalidad de manera más puntual y eficiente, y segundo lugar respecto a la capacitación podemos mencionar que concordamos en que la preparación a través de la capacitación puede llegar a ser crucial para prevenir delitos informáticos.
- ✓ Del informe de la Organización de las Naciones UNIDAS (2013) titulado: "Estudio exhaustivo sobre el delito cibernético", se resalta la "capacidad de los agentes de la ley" como un área clave de estrategia nacional sobre delitos informáticos, en donde se emergió un enfoque concertado sobre la

capacitación de fiscales, magistrados y jueces; al respecto podemos decir que la presente investigación concuerda con dicho tema pues la preparación que puedan tener los operadores de justicia es clave cuando se trata de investigar y sancionar delitos de esta naturaleza.

- ✓ De la investigación hecha por Ligia Maribel García Juarez (2014) titulada "Estudio exhaustivo sobre el delito cibernético", que concluye que es indispensable y necesaria a correcta instrucción para agentes de investigación de crímenes informáticos, debemos mencionar que esta investigación concuerda con dicha conclusión pues se ha corroborado la necesidad de que en el Perú exista un Ministerio Público y una Policía Nacional preparados para investigar delitos informáticos.
- ✓ De la investigación de Gabriela Cristina Chauca Acero (2014) titulado: "El principio de proporcionalidad en la prevención de los delitos informáticos", se concluye que el desconocimiento del problema de los delitos informáticos es una de las causas de la inseguridad informática que existe, al respecto debemos mencionar que en este estudio se ha podido corroborar dicha conclusión a través del estudio de las carpetas fiscales archivadas sobre delitos informáticos, en donde se puso de relieve el problema del desconocimiento que hay alrededor de la problemática de los delitos informáticos.
- ✓ De la investigación de José Carlos Zamora Alvizures (2012) titulado:" Implementación de la informática forense en la obtención de evidencia digital para combatir los delitos informáticos en Guatemala.", dicha investigación concluye que es un obstáculo para la persecución penal de los delitos informáticos, la falta de capacitación del Ministerio Publico, de la Policía Nacional Civil y el Instituto Nacional de Ciencias Forense, pues de acuerdo

al investigador estos no cuentan con el personal con la preparación necesaria, al respecto podemos decir que hemos corroborado en parte dicha afirmación al tener como estudio al fiscalías provinciales penales corporativas de Huánuco, en donde el personal no contaba con la preparación necesaria para perseguir delitos informáticos.

- ✓ De la investigación de Jarvey Rincón Ríos titulado: “El delito en la cibersociedad y la justicia penal internacional”, esta concluye afirmando la necesidad de buscar un sistema de justicia universal que permita la investigación juzgamiento y sanción de los delitos informáticos o delitos que atentan contra la información y los datos; al respecto podemos mencionar que en la presente investigación a través de la revisión teórica también se ha podido advertir dicha necesitad pues los delitos informáticos están revestidos de características técnicas como su internacionalización que los hacen más dífilas de perseguir y sancionar.
- ✓ De la investigación hecha por Samiksha Godara (2011) titulado: “Prevención y control de los delitos informáticos en la india: problemas, temas y estrategias”, se concluye que es necesario el uso de la tecnología encriptada, el desarrollo de la informática forense y las técnicas biométricas, así como la necesidad de establecer un centro de investigación y desarrollo de delitos informáticos en la India; al respecto podemos mencionar que esta investigación concuerda con la aplicación de medidas preventivas de este tipo que ayuden a combatir el problema de la criminalidad informática.
- ✓ De la investigación hecha por Robert Imhof (2010) titulada: “Los delitos informáticos y el derecho de las telecomunicaciones.”, esta concluye que ue los hackers ven con relativa facilidad perpetrar sus crímenes, siendo que hay una probabilidad baja de ser atrapados, y mucho menos encarcelados; al

respecto la presente investigación también concuerda con dicha conclusión pues se ha advertido que el desconocimiento en informática y derecho informático puede llevar a crearse cierto ambiente de impunidad para los cibercriminales.

- ✓ De la investigación hecha por Leukfeldt Rutger (2017) titulado “El factor humano en el cibercriminal y la ciberseguridad”, se concluye que estudiar el funcionamiento del sistema de justicia penal con respecto a los delitos informáticos, muestra que la policía, muy aparte de los equipos especializados, no tienen los conocimientos ni habilidades requeridas para manejar efectivamente casos de delitos informáticos; al respecto a través de la presente investigación hemos podido concordar con dicha conclusión de este estudio internacional, pues en el Perú a pesar de la Policía Nacional del Perú cuenta con una división especializada en delitos informáticos, esta no se encuentra ni mucho menos preparada enfrentar al problema de los delitos informáticos, una realidad que también a través del presente estudio hemos podido corroborar en el Ministerio Público.
- ✓ De la investigación hecha por Hemraj Saini, Yerra Shankar Rao Y T.C.Panda (2012) titulada “ Crímenes cibernéticos y sus impactos: un resumen.”, esta concluye que se puede clasificar en tres categorías: las leyes cibernéticas, la educación, y la formulación de políticas, que aunque en muchos países no se ha realizado un trabajo significativo en estas, ello no quita de que se deba mejorar el trabajo ya realizado para establecer nuevos paradigmas que nos permitan controlar los ciber ataques; al respecto podemos decir que la presente investigación concuerda con dicha conclusión pues es necesario tener una legislación eficaz para enfrentar los delitos informáticos, una

política educativa que incida en la prevención de dichos actos delictivos, así como la formulación de políticas públicas que aborden el tema también.

5.1.2. Antecedentes teóricos nacionales

- ✓ De la investigación hecha por Jorge Alberto Vega Aguilar (2010) titulado “Los delitos informáticos en el código penal.”, se concluye que delitos informáticos son plurifensivos, porque afectan diferentes bienes jurídicos, lo cual crea confusión a la hora de realizar la tipificación, agregando además que a la actualidad, tanto jueces como fiscales, cuentan con poco conocimiento y experiencia en el área del Derecho Informático; al respecto debemos mencionar que la presente investigación concuerda con dicha conclusión, pues a través del desarrollo del marco teórico se ha podido advertir como los delitos informáticos afectan múltiples bienes jurídicos, corroborándose además que el desconocimiento en torno al derecho informático en jueces y fiscales es un problema que puede llegar a dificultar la persecución de delitos informáticos.
- ✓ De la investigación hecha por Luis Miguel Romero Echevarría (2005) titulado: “Marco conceptual de los delitos informáticos”, La principal conclusión que llega el investigador es que se necesita reactualizar constantemente el marco teórico de los delitos informáticos para que se constituya en un instrumento eficaz para los operadores de justicia que intervienen en la lucha con los delitos informáticos en el Perú; al respecto la presente investigación concuerda pues a la fecha que se realizó dicha investigación (2005) el marco conceptual de los delitos informáticos ha tenido toda una serie de variaciones pues estos han seguido evolucionando con el paso del tiempo.
- ✓ De la investigación hecha por Michael Espinoza Coila (2017) titulada “Derecho penal informático: deslegitimización del poder punitivo en la

sociedad de control", el investigador concluye que efectivamente el derecho Penal Informático es un saber jurídico penal, que mediante la interpretación de leyes penales sobre delitos informáticos propone a los agentes jurídicos un sistema reductor del poder de vigilancia del poder punitivo en la sociedad de control, e impulsar el poder jurídico con el fin de preservar los espacios de libertad y privacidad de las personas; al respecto debemos mencionar que esta investigación concuerda en cuanto la importancia que tiene la interpretación de las leyes penales sobre delitos informáticos.

- ✓ De la investigación hecha por Rafeel Gustavo Parra Perea (2016) titulado: "Proyecto legal para un esquema nacional de ciber seguridad", se concluye que para que el Estado tenga una adecuada Ciberseguridad necesita de un ordenamiento penal y un mecanismo de persecución de los cibercriminales; respecto a dicha conclusión a través de la presente investigación concordamos pues la necesidad de un ordenamiento legal acorde a la realidad en delitos informáticos es crucial en la persecución de los cibercriminales.
- ✓ De la investigación de Deivid Yuly Morales Delgado (2016) titulado: "La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú", se concluye que la influencia de los sistemas informáticos en el Derecho es lo que ha dado lugar a la aparición del Derecho Informático, que existen contradicciones entre las leyes que regulan los delitos informáticos, y que será necesaria la ayuda de la Policía Nacional del Perú para la aprehensión de los delincuentes que cometan delitos informáticos; al respecto debemos mencionar que también se concuerda con dicha conclusión pues se necesita revisar la actual legislación penal en materia de delitos informáticos pues no está resultando

eficaz para combatir la cibercriminalidad, así como la importancia del rol que cumple la policía nacional del Perú en la persecución de los delitos informáticos, lo cual implica que se haga mayor énfasis en la preparación deben tener los policías para enfrentar esta problemática.

- ✓ De la investigación de José Alfonso Rumiche Pazo (2015) titulado: "Sombras de la normatividad que regula el incremento de la ciberdelincuencia en Lima-2015", se concluye que el investigador si logró determinar que el ejercicio de la actual normatividad que regula la ciberdelincuencia en Lima en el año 2015 contraviene en constantes disyuntivas, y que la falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, por tanto los operadores de justicia deben tener mayores conocimientos en tecnología de la información; al respecto la presente investigación concuerda con dicha conclusión pues se ha advertido la importancia en la preparación de los operadores jurídicos en derecho informático para poder combatir la ciberdelincuencia.

5.1.3. Antecedentes teóricos locales

- ✓ De la investigación de Ivett Clariza Sequeiros Calderón (2015) titulado "Vacíos legales que imposibilitan la sanción de los delitos informáticos en el nuevo código penal peruano.", se concluye que la naturaleza virtual de los delitos informáticos vuelve confusa su tipificación por el poco manejo y conocimiento que hay en esta área; al respecto podemos mencionar que a través del presente estudio se ha podido corroborar que hay ciertas deficiencias en la legislación penal sobre los delitos informáticos que no se han podido superar y que implican la necesidad de que se revise dicha normatividad.

- ✓ De la investigación de Meylin del Pilar Romero Ocampo (2016) titulado "Delitos informáticos cometidos a través de redes sociales y su tratamiento en el ministerio público en la ciudad de Huánuco- 2016.", se concluye que los delitos de: alteración, daño o destrucción de base de datos; atentado a la integridad de datos informáticos; proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos; la Interceptación de datos informáticos; el fraude informático; la suplantación de identidad y el abuso de mecanismos y dispositivos informáticos, son los delitos que tienen mayor frecuencia; al respecto debemos mencionar que aunque la presente investigación no verificó los datos que se proporcionan en esta tesis, si se puede concordar de que dichos delitos son actualmente los delitos informáticos más comunes.
- ✓ De la investigación de Miguel Ángel Ponce Malpartida (2017) titulado: "Delito informático y acoso sexual de menores de edad regulados por el art. 5 de la ley 30096, en el barrio tunan del distrito de san jerónimo, provincia de huancayo-2016.", se concluye que 62% de los pobladores encuestados tenía un deficiente conocimiento del tema de Delito informático y el acoso sexual a menores de edad; la presente investigación concuerda con dicho resultado pues el problema del desconocimiento de delitos informáticos es una problemática generalizada que se replica incluso en el departamento de Huánuco, como en otros departamentos del Perú, lo cual como se ha mencionado en la presente investigación promueve cierto ambiente de impunidad para los cibercriminales pues aprovechan dicho conocimiento, pues muchas de las víctimas de delitos informáticos inclusive no denuncian hechos relacionados a delitos informáticos pues desconocen del tema.

5.2. CONTRASTACIÓN DE LA HIPÓTESIS

5.2.1. HIPÓTESIS GENERAL

Paso 1. Redacción de la hipótesis

Ho (nula) : No Existe relación directa entre la formación profesional en derecho informático y la persecución penal de delitos informáticos.

H1 (alterna) : Existe relación directa entre la formación profesional en derecho informático y la persecución penal de delitos informáticos.

Paso 2. Definir el porcentaje de error

α = 0.05 = 5%

Paso 3. Elección de la prueba

Objetivo comparativo

		PRUEBAS NO PARAMETRICAS			PRUEBAS PARAMETRICAS
		Nominal Dicotómica	Nominal Politómica	Ordinal	Numérica
Estudio Transversal Muestras Independientes	Un grupo	X^2 Bondad de ajuste Binomial	X^2 Bondad de ajuste	X^2 Bondad de ajuste	T de Student (una muestra)
	Dos grupos	X^2 Bondad de ajuste Corrección de Yates Test exacto de Fisher	X^2 Bondad de Homogeneidad	U de Mann-Withney	T de Student (muestras independientes)
	Más de dos grupos	X^2 Bondad de ajuste	X^2 Bondad de ajuste	H Kruskal-Walls	ANOVA con un factor (INTERsujetos)
Estudio Longitudinal Muestras relacionadas	Dos medidas	Mc. Nemar	Q de Cochran	Wilcoxon	T de Student (muestras relacionadas)
	Más de dos medidas	Q de Cochran	Q de Cochran	Wilcoxon	ANOVA para medidas repetidas (INTRAsujetos)

Decisión:

Nuestra investigación se desarrolla tomando datos categóricos (No paramétricos) en una sola oportunidad (Estudio Transversal) y en Muestras Independientes, teniendo en cuenta el cuadro de objetivo

comparativo, la prueba estadística usada fue la X^2 Bondad de ajuste (chi cuadrada).

Paso 4. Construcción de la tabla de contingencia empleando el software PASW 24 (SPSS)

VARIABLE 1		%
SI	83	46%
NO	97	54%
TOTAL	180	100%

VARIABLE 2		%
SI	295	53%
NO	263	47%
TOTAL	558	100%

Tabla cruzada La formación profesional en derecho informático*Persecución penal de delitos Informáticos				
Recuento				
		Persecución penal de delitos Informáticos		Total
		no	si	
La formación profesional en derecho informático	no	47	7	54
	si	0	46	46
Total		47	53	100

Paso 5. Decisión estadística

Pruebas de chi-cuadrado					
	Valor	df	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	75,542[a]	1	,000		
Corrección de continuidad[b]	72,088	1	,000		
Razón de verosimilitud	96,616	1	,000		
Prueba exacta de Fisher				,000	,000
Asociación lineal por lineal	74,786	1	,000		
N de casos válidos	100				

Vemos que:		
P- valor = 0,000	<	α = 0.05
Dado que el nivel de significancia es menor que 0.05 rechazamos la hipótesis nula y aceptamos la hipótesis alterna. **Conclusión:** Existe relación directa entre la formación profesional en derecho informático y la persecución de delitos informático		
Criterio para decidir: Si la probabilidad obtenida P-valor ≤ α, se rechaza Ho (Se acepta H1) Si la probabilidad obtenida P-valor > α, se rechaza la H1 (Se acepta Ho)		

5.2.2. HIPÓTESIS ESPÉCIFICA 01

Paso 1. Redacción de la hipótesis

Ho (nula) : La aplicación de las fuentes jurídicas del derecho informático no se relacionan con la función del Ministerio Público de perseguir penalmente delitos informáticos.

H1 (alterna) : La aplicación de las fuentes jurídicas del derecho informático se relacionan significativamente con la función del Ministerio Público de perseguir penalmente delitos informáticos.

Paso 2. Definir el porcentaje de error

α = 0.05 = 5%

Paso 3. Elección de la prueba

		PRUEBAS NO PARAMETRICAS			PRUEBAS PARAMETRICAS
		Nominal Dicotómica	**Nominal Politómica**	**Ordinal**	**Numérica**
Estudio Transversal **Muestras Independientes**	**Un grupo**	**X^2 Bondad de ajuste** Binomial	**X^2 Bondad de ajuste**	**X^2 Bondad de ajuste**	**T de Student** (una muestra)
	Dos grupos	**X^2 Bondad de ajuste** Corrección de Yates Test exacto de Fisher	**X^2 Bondad de Homogeneidad**	**U de Mann-Withney**	**T de Student** (muestras independientes)
	Más de dos grupos	**X^2 Bondad de ajuste**	**X^2 Bondad de ajuste**	**H Kruskal-Walls**	**ANOVA** con un factor (INTERsujetos)
Estudio Longitudinal **Muestras relacionadas**	**Dos medidas**	**Mc. Nemar**	**Q de Cochran**	**Wilcoxon**	**T de Student** (muestras relacionadas)
	Más de dos medidas	**Q de Cochran**	**Q de Cochran**	**Wilcoxon**	**ANOVA** para medidas repetidas (INTRAsujetos)

Decisión:

Nuestra investigación se desarrolla tomando datos categóricos (No paramétricos) en una sola oportunidad (Estudio Transversal) y en Muestras Independientes, teniendo en cuenta el cuadro de objetivo comparativo, la prueba estadística usada fue la X^2 Bondad de ajuste (chi cuadrada).

Paso 4. Construcción de la tabla de contingencia empleando el software PASW 24 (SPSS)

DIMENSION 1		%
SI	13	36%
NO	23	64%
TOTAL	36	100%

VARIABLE 2		%
SI	295	53%
NO	263	47%
TOTAL	558	100%

Tabla cruzada Aplicación de las fuentes jurídicas del derecho informático*Persecución penal de delitos Informáticos

Recuento

		Persecución penal de delitos Informáticos		
		no	si	Total
Aplicación de las fuentes jurídicas del derecho informático	no	47	17	64
	si	0	36	36
Total		47	53	100

Paso 5. Decisión estadística

Pruebas de chi-cuadrado

	Valor	df	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	49,882[a]	1	,000		
Corrección de continuidad[b]	46,978	1	,000		
Razón de verosimilitud	64,175	1	,000		
Prueba exacta de Fisher				,000	,000
Asociación lineal por lineal	49,383	1	,000		
N de casos válidos	100				

Vemos que:		
P- valor = 0,000	<	α = 0.05
Dado que el nivel de significancia es menor que 0.05 rechazamos la hipótesis nula y aceptamos la hipótesis alterna. **Conclusión:** La aplicación de las fuentes jurídicas del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos.		
Criterio para decidir: Si la probabilidad obtenida P-valor ≤ α, se rechaza Ho (Se acepta H1) Si la probabilidad obtenida P-valor > α, se rechaza la H1 (Se acepta Ho)		

5.2.3. HIPÓTESIS ESPÉCIFICA 02

Paso 1. Redacción de la hipótesis

Ho (nula) : La aplicación de conceptos jurídicos de derecho informático no se relaciona significativamente con la persecución penal de delitos Informáticos.

H1 (alterna) : La aplicación de conceptos jurídicos de derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos.

Paso 2. Definir el porcentaje de error

α = 0.05 = 5%

Paso 3. Elección de la prueba

		PRUEBAS NO PARAMETRICAS			PRUEBAS PARAMETRICAS
		Nominal Dicotómica	**Nominal Politómica**	**Ordinal**	**Numérica**
Estudio Transversal **Muestras Independientes**	**Un grupo**	**X^2 Bondad de ajuste** Binomial	**X^2 Bondad de ajuste**	**X^2 Bondad de ajuste**	**T de Student** (una muestra)
	Dos grupos	**X^2 Bondad de ajuste** Corrección de Yates Test exacto de Fisher	**X^2 Bondad de Homogeneidad**	**U de Mann-Withney**	**T de Student** (muestras independientes)
	Más de dos grupos	**X^2 Bondad de ajuste**	**X^2 Bondad de ajuste**	**H Kruskal-Walls**	**ANOVA** con un factor (INTERsujetos)
Estudio Longitudinal **Muestras relacionadas**	**Dos medidas**	**Mc. Nemar**	**Q de Cochran**	**Wilcoxon**	**T de Student** (muestras relacionadas)
	Más de dos medidas	**Q de Cochran**	**Q de Cochran**	**Wilcoxon**	**ANOVA** para medidas repetidas (INTRAsujetos)

Decisión:

Nuestra investigación se desarrolla tomando datos categóricos (No paramétricos) en una sola oportunidad (Estudio Transversal) y en Muestras Independientes, teniendo en cuenta el cuadro de objetivo comparativo, la prueba estadística usada fue la X^2 Bondad de ajuste (chi cuadrada).

Paso 4. Construcción de la tabla de contingencia empleando el software PASW 24 (SPSS)

DIMENSION 2		%
SI	295	53%
NO	263	47%
Total	558	100%

VARIABLE 2		%
SI	22	61%
NO	14	39%
TOTAL	36	100%

Tabla cruzada Aplicación conceptos jurídicos de derecho informático*Persecución penal de delitos Informáticos				
Recuento				
		Persecución penal de delitos Informáticos		Total
		no	si	
Aplicación conceptos jurídicos de derecho informático	no	39	0	39
	si	8	53	61
Total		47	53	100

Paso 5. Decisión estadística

Pruebas de chi-cuadrado					
	Valor	df	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	72,096[a]	1	,000		
Corrección de continuidad[b]	68,650	1	,000		
Razón de verosimilitud	90,865	1	,000		
Prueba exacta de Fisher				,000	,000
Asociación lineal por lineal	71,375	1	,000		
N de casos válidos	100				

Vemos que:		
P- valor = 0,00	<	α = 0.05
Dado que el nivel de significancia es menor que 0.05 rechazamos la hipótesis nula y aceptamos la hipótesis alterna. **Conclusión:** La aplicación de conceptos jurídicos de derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos.		
Criterio para decidir: Si la probabilidad obtenida P-valor ≤ α, se rechaza Ho (Se acepta H1) Si la probabilidad obtenida P-valor > α, se rechaza la H1 (Se acepta Ho)		

5.2.4. HIPÓTESIS ESPÉCIFICA 03

Paso 1. Redacción de la hipótesis

Ho (nula) : La aplicación del ordenamiento jurídico del derecho informático no se relaciona significativamente con la persecución penal de delitos Informáticos.

H1 (alterna) : La aplicación del ordenamiento jurídico del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos.

Paso 2. Definir el porcentaje de error

$$\alpha = 0.05 = 5\%$$

Paso 3. Elección de la prueba

		PRUEBAS NO PARAMETRICAS			PRUEBAS PARAMETRICAS
		Nominal Dicotómica	**Nominal Politómica**	**Ordinal**	**Numérica**
Estudio Transversal **Muestras Independientes**	**Un grupo**	**X^2 Bondad de ajuste** Binomial	**X^2 Bondad de ajuste**	**X^2 Bondad de ajuste**	**T de Student** (una muestra)
	Dos grupos	**X^2 Bondad de ajuste** Corrección de Yates Test exacto de Fisher	**X^2 Bondad de Homogeneidad**	**U de Mann-Withney**	**T de Student** (muestras independientes)
	Más de dos grupos	**X^2 Bondad de ajuste**	**X^2 Bondad de ajuste**	**H Kruskal-Walls**	**ANOVA** con un factor (INTERsujetos)
Estudio Longitudinal **Muestras relacionadas**	**Dos medidas**	**Mc. Nemar**	**Q de Cochran**	**Wilcoxon**	**T de Student** (muestras relacionadas)
	Más de dos medidas	**Q de Cochran**	**Q de Cochran**	**Wilcoxon**	**ANOVA** para medidas repetidas (INTRAsujetos)

Decisión:

Nuestra investigación se desarrolla tomando datos categóricos (No paramétricos) en una sola oportunidad (Estudio Transversal) y en Muestras Independientes, teniendo en cuenta el cuadro de objetivo comparativo, la prueba estadística usada fue la X^2 Bondad de ajuste (chi cuadrada).

Paso 4. Construcción de la tabla de contingencia empleando el software PASW 24 (SPSS)

DIMENSION 3		%
SI	23	64%
NO	13	36%
TOTAL	36	100%

VARIABLE 2		%
SI	295	53%
NO	263	47%
TOTAL	558	100%

Tabla cruzada Aplicación del ordenamiento jurídico del derecho informático*Persecución penal de delitos Informáticos

Recuento

		Persecución penal de delitos Informáticos		
		no	si	Total
Aplicación del ordenamiento jurídico del derecho informático	no	36	0	36
	si	11	53	64
Total		47	53	100

Paso 5. Decisión estadística

Pruebas de chi-cuadrado

	Valor	df	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	63,431[a]	1	,000		
Corrección de continuidad[b]	60,150	1	,000		
Razón de verosimilitud	79,537	1	,000		
Prueba exacta de Fisher				,000	,000
Asociación lineal por lineal	62,797	1	,000		
N de casos válidos	100				

Vemos que:		
P- valor = 0,000	<	α = 0.05
Dado que el nivel de significancia es menor que 0.05 rechazamos la hipótesis nula y aceptamos la hipótesis alterna. **Conclusión:** La aplicación del ordenamiento jurídico del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos.		
Criterio para decidir: Si la probabilidad obtenida P-valor ≤ α, se rechaza Ho (Se acepta H1) Si la probabilidad obtenida P-valor > α, se rechaza la H1 (Se acepta Ho)		

5.2.5. HIPÓTESIS ESPÉCIFICA 04

Paso 1. Redacción de la hipótesis

Ho (nula) : La resolución de problemas en el ámbito derecho informático no se relaciona significativamente con la persecución penal de delitos Informáticos.

H1 (alterna) : La resolución de problemas en el ámbito derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos.

Paso 2. Definir el porcentaje de error

α = 0.05 = 5%

Paso 3. Elección de la prueba

		PRUEBAS NO PARAMETRICAS			PRUEBAS PARAMETRICAS
		Nominal Dicotómica	**Nominal Politómica**	**Ordinal**	**Numérica**
Estudio Transversal **Muestras Independientes**	**Un grupo**	**X^2 Bondad de ajuste** Binomial	**X^2 Bondad de ajuste**	**X^2 Bondad de ajuste**	**T de Student** (una muestra)
	Dos grupos	**X^2 Bondad de ajuste** Corrección de Yates Test exacto de Fisher	**X^2 Bondad de Homogeneidad**	**U de Mann-Withney**	**T de Student** (muestras independientes)
	Más de dos grupos	**X^2 Bondad de ajuste**	**X^2 Bondad de ajuste**	**H Kruskal-Walls**	**ANOVA** con un factor (INTERsujetos)
Estudio Longitudinal **Muestras relacionadas**	**Dos medidas**	**Mc. Nemar**	**Q de Cochran**	**Wilcoxon**	**T de Student** (muestras relacionadas)
	Más de dos medidas	**Q de Cochran**	**Q de Cochran**	**Wilcoxon**	**ANOVA** para medidas repetidas (INTRAsujetos)

Decisión:

Nuestra investigación se desarrolla tomando datos categóricos (No paramétricos) en una sola oportunidad (Estudio Transversal) y en Muestras Independientes, teniendo en cuenta el cuadro de objetivo comparativo, la prueba estadística usada fue la X^2 Bondad de ajuste (chi cuadrada).

Paso 4. Construcción de la tabla de contingencia empleando el software PASW 24 (SPSS)

DIMENSION 4		%
SI	12	33%
NO	24	67%
TOTAL	36	100%

VARIABLE 2		%
SI	295	53%
NO	263	47%
	558	100%

Tabla cruzada Resolución de problemas en el ámbito derecho informático*Persecución penal de delitos Informáticos

Recuento

		Persecución penal de delitos Informáticos		
		no	si	Total
Resolución de problemas en el ámbito derecho informático	no	47	16	63
	si	0	37	37
Total		47	53	100

Paso 5. Decisión estadística

Pruebas de chi-cuadrado

	Valor	df	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	52,081[a]	1	,000		
Corrección de continuidad[b]	49,130	1	,000		
Razón de verosimilitud	66,871	1	,000		
Prueba exacta de Fisher				,000	,000
Asociación lineal por lineal	51,561	1	,000		
N de casos válidos	100				

Vemos que:		
P- valor = 0,000	<	α = 0.05
Dado que el nivel de significancia es menor que 0.05 rechazamos la hipótesis nula y aceptamos la hipótesis alterna. **Conclusión:** La resolución de problemas en el ámbito derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos.		
Criterio para decidir: Si la probabilidad obtenida P-valor ≤ α, se rechaza Ho (Se acepta H1) Si la probabilidad obtenida P-valor > α, se rechaza la H1 (Se acepta Ho)		

5.2.6. HIPÓTESIS ESPÉCIFICA 05

Paso 1. Redacción de la hipótesis

Ho (nula) : La aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional no se relaciona significativamente con la persecución penal de delitos Informáticos.

H1 (alterna) : La aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional se relaciona significativamente con la persecución penal de delitos Informáticos.

Paso 2. Definir el porcentaje de error

α = 0.05 = 5%

Paso 3. Elección de la prueba

		PRUEBAS NO PARAMETRICAS			PRUEBAS PARAMETRICAS
		Nominal Dicotómica	**Nominal Politómica**	**Ordinal**	**Numérica**
Estudio Transversal **Muestras Independientes**	**Un grupo**	**X² Bondad de ajuste** Binomial	**X² Bondad de ajuste**	**X² Bondad de ajuste**	**T de Student** (una muestra)
	Dos grupos	**X² Bondad de ajuste** Corrección de Yates Test exacto de Fisher	**X² Bondad de Homogeneidad**	**U de Mann-Withney**	**T de Student** (muestras independientes)
	Más de dos grupos	**X² Bondad de ajuste**	**X² Bondad de ajuste**	**H Kruskal-Walls**	**ANOVA** con un factor (INTERsujetos)
Estudio Longitudinal **Muestras relacionadas**	**Dos medidas**	**Mc. Nemar**	**Q de Cochran**	**Wilcoxon**	**T de Student** (muestras relacionadas)
	Más de dos medidas	**Q de Cochran**	**Q de Cochran**	**Wilcoxon**	**ANOVA** para medidas repetidas (INTRAsujetos)

Decisión:

Nuestra investigación se desarrolla tomando datos categóricos (No paramétricos) en una sola oportunidad (Estudio Transversal) y en Muestras Independientes, teniendo en cuenta el cuadro de objetivo comparativo, la prueba estadística usada fue la X^2 Bondad de ajuste (chi cuadrada).

Paso 4. Construcción de la tabla de contingencia empleando el software PASW 24 (SPSS)

DIMENSION 5		%
SI	13	36%
NO	23	64%
TOTAL	36	100%

VARIABLE 2		%
SI	295	53%
NO	263	47%
TOTAL	558	100%

Tabla cruzada Aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional*Persecución penal de delitos Informáticos

Recuento

		Persecución penal de delitos Informáticos		
		no	si	Total
Aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional	no	47	17	64
	si	0	36	36
Total		47	53	100

Paso 5. Decisión estadística

Pruebas de chi-cuadrado

	Valor	df	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	49,882[a]	1	,000		
Corrección de continuidad[b]	46,978	1	,000		
Razón de verosimilitud	64,175	1	,000		
Prueba exacta de Fisher				,000	,000
Asociación lineal por lineal	49,383	1	,000		
N de casos válidos	100				

Vemos que:		
P- valor = 0,000	<	α = 0.05
Dado que el nivel de significancia es menor que 0.05 rechazamos la hipótesis nula y aceptamos la hipótesis alterna. **Conclusión:** La aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional se relaciona significativamente con la persecución penal de delitos Informáticos.		
Criterio para decidir: Si la probabilidad obtenida P-valor ≤ α, se rechaza Ho (Se acepta H1) Si la probabilidad obtenida P-valor > α, se rechaza la H1 (Se acepta Ho)		

5.3. APORTE CIENTÍFICO DE LA INVESTIGACIÓN

El aporte científico de esta investigación es que se da una respuesta aplicando el método científico a un problema de investigación muy importante y poco estudiado como es el de la formación profesional en derecho informático, a través del cual se está brindando datos que el investigador considera valiosos para futuros estudios sobre este y otros problemas de investigación relacionados, y es que como se ha mencionado en el capítulo sobre la presentación de resultados, aquí se ha aplicado una encuesta sobre el problema de los delitos informáticos a un número importante de fiscales que laboran en el Ministerio Público, en donde muchos de ellos ya habían estado investigando casos sobre delitos informáticos, por lo tanto para cualquier investigador que a futuro desee conocer la realidad sobre este problema en Huánuco probablemente encuentre útil los resultados que aquí se han obtenido, de igual manera es que es importante el análisis que se han hecho a las carpetas fiscales archivadas sobre delitos informáticos, pues facilitan el trabajo a los investigadores jurídicos que deseen conocer cómo es que han estado investigando los fiscales en casos de

delitos informáticos, de modo que puedan ahondar más en las casusas de los resultados obtenidos, pues como se ha advertido los fiscales de las Fiscalías Provinciales Penales Corporativas del distrito fiscal de Huánuco han demostrado no tener los suficientes conocimientos sobre derecho informático o delitos informáticos. Finalmente, el aporte de esta investigación se encuentra desde el plano pedagógico pues tentativamente el investigador en base a sus propios conocimientos y de la revisión de las bases teóricas ha señalado cuáles deberían ser las competencias con las que debe contar el profesional que tiene formación en derecho informático, competencias de las cuales evidentemente se puede ampliar su estudio y perfeccionar su aplicación.

CONCLUSIONES

- Se concluye que existe una relación significativa entre la aplicación de las fuentes jurídicas del derecho informático con la persecución penal de delitos informáticos, en razón de que el derecho informático cuenta con fuentes jurídicas propias que el abogado con formación profesional en derecho informático debe de conocer, pues en el desempeño de su profesión necesitará dominar la aplicación de dichas fuentes jurídicas para poder hacer frente a los nuevos problemas que viene trayendo la informática a la sociedad, por lo cual dicha competencia se reviste de mayor importancia cuando el profesional del derecho labora en un organismo como el Ministerio Público, el cual se ocupa de la persecución penal de los delitos informáticos en el Perú.
- Se concluye que existe una relación significativa entre la aplicación de los conceptos jurídicos del derecho informático y la persecución penal de delitos informáticos, por cuanto en el desempeño profesional del abogado es necesario conocer los conceptos y definiciones propias de esta rama del derecho.
- Se concluye que existe una relación significativa entre la aplicación del ordenamiento jurídico del derecho informático y la persecución penal de delitos informáticos, esto en razón de que el derecho informático cuenta con un ordenamiento jurídico propio compuesto por normas que regulan la informática, el cual incluye normas penales que sancionan los delitos informáticos.
- Se concluye que existe una relación significativa entre la resolución de problemas en el ámbito derecho informático y la persecución penal de delitos Informáticos, en razón que desde la aparición de la informática se

han ido presentando numerosos problemas relacionados al ámbito jurídico que el profesional del derecho debe saber identificar y analizar, así como el plantear soluciones fundamentadas que permitan resolver dichos problemas en el desempeño de su profesión, sobre todo si labora en un organismo como el Ministerio Público que no solo se ocupa de perseguir los delitos informáticos sino también de prevenirlos.

- Se concluye que existe una relación significativa entre la aplicación de la informática jurídica y las Tecnologías de la Información y las Comunicaciones con la persecución penal de delitos informáticos, por cuanto ambas áreas son parte importante del derecho informático, y juegan en este siglo XXI un rol preponderante en la vida del profesional del derecho, el cual debe mantenerse constantemente actualizado en las nuevas aplicaciones que tiene la informática jurídica, así como el de conocer también las aplicaciones de las Tecnologías de la Información y las Comunicaciones, las cuales vienen evolucionando de manera acelerada a cada momento con nuevas invenciones, ya sea para que las aplique para mejorar su desempeño como profesional, como también para identificar posibles aplicaciones maliciosas que se pueden derivar en la comisión de delitos informáticos.
- Finalmente se concluye que efectivamente existe una relación directa entre la formación profesional en derecho informático y la persecución penal de delitos informáticos, por cuanto se han podido corroborar satisfactoriamente las hipótesis específicas que se plantearon, hallándose en cada una de ellas una correlación significativa, lo cual nos lleva afirmar que se ha podido cumplir con el objetivo general de esta investigación que era determinar la relación entre estas dos variables de estudio.

RECOMENDACIONES

- Se recomienda que las universidades con facultades de derecho brinden mayor importancia a la formación profesional en derecho informático de sus estudiantes, por cuanto se necesita tener abogados preparados para los retos que traerá la informática en el futuro, teniéndose una perspectiva más visionaria de lo que será el abogado del futuro, el cual se desenvolverá en un ambiente completamente informatizado dominado por el derecho informático.
- Se recomienda que se revise el actual ordenamiento jurídico penal sobre delitos informáticos, por cuanto desde su modificatoria no se han hecho mayores aportes que nos permitan tener un cuerpo normativo penal actualizado a las nuevas modalidades de comisión de estos delitos.
- Se recomienda al Ministerio Público y al Poder Judicial realizar con mayor frecuencia capacitaciones y talleres sobre derecho informático, y por ende sobre delitos informáticos, para mitigar en cierta medida el desconocimiento que hay acerca de esta nueva rama del derecho y su temática.
- Se recomienda al Estado Peruano elaborar políticas de prevención sobre delitos informáticos, y es que se sabe que la sola norma penal no es suficiente para prevenir la comisión de un delito, por cuanto es necesario que dicho cuerpo normativo se encuentre acompañado de todo un conjunto de políticas de prevención.
- Se recomienda finalmente a toda la comunidad jurídica a que se investigue más los temas que contiene el derecho informático, pues existen escasas investigaciones sobre múltiples aspectos jurídicos sobre esta nueva del derecho alrededor del mundo. De igual manera se

recomienda a los investigadores jurídicos que se ocupan del estudio del derecho penal, hacer mayor énfasis en la investigación de los delitos informáticos, los cuales al estar en constante evolución necesitan ser estudiados con mayor profundidad y análisis.

REFERENCIAS BIBLIOGRÁFICAS

Acurio, S. (s.f.). Delitos informáticos: Generalidades. Washington, Estados Unidos: OEA.

Aladro Vico, Eva. (2011). La Teoría de la Información ante las nuevas tecnologías de la comunicación. Madrid, España: Universidad Complutense de Madrid.

Asamblea General de las Naciones Unidas. (1948). Declaración Universal de Derechos Humanos. París, Francia.

Asamblea General de las Naciones Unidas. (1976). Pacto Internacional de Derechos Civiles y Políticos. Nueva York, Estados Unidos.

Asimov, Isaac. (1993). Historia de los egipcios. Madrid, España: Alianza Editorial S.A.

Brunet, I. y Moral, D. (2017). Origen, contexto, evolución y futuro de la Formación Profesional. Cataluña, España: Universitat Rovira i Virgili.

Brunner, J. (2012). El jinete de la onda de shock. Reino Unido: Editorial Gigamesh.

Canedo Estrada, Alex. (2010). La informática forense y los delitos informáticos. Medellín, Colombia: Corporación Universitaria Americana.

Canedo Estrada, Alex. (2010). La informática forense y los delitos informáticos. Medellín, Colombia: Corporación Universitaria Americana.

Chauca Acero, G. (2014). El principio de proporcionalidad en la prevención de los delitos informáticos (tesis de pregrado). Universidad Regional Autónoma de los Andes, Ecuador.

Concejo de Europa. (1950). Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Roma, Italia.

Correa Villa, Mauricio. (2017). Fundamentos de la teoría de la información. Medellín, Colombia: Instituto Tecnológico Metropolitano.

Elliot Segura, Aldo. (s.f.). Aspectos Jurídicos y Técnicos sobre el Software. Lima, Perú: Universidad San Martín de Porres.

Erquiaga, M. (s.f.). Botnets: Mecanismos de Control y de propagación. Buenos Aires, Argentina: Universidad Nacional de la Plata.

Escuela del Ministerio Público. (2010). La persecución estratégica del delito. Lima, Perú: Ministerio Público.

Espinós, J. y Sánchez, M. (1990). Así vivían los romanos. Madrid, España: Editorial Anaya.

Espinoza Coila, M. (2017). Derecho penal informático: deslegitimización del poder punitivo en la sociedad de control. Universidad Nacional del Altiplano, Puno.

Fabian Borghello, C. (2001). Seguridad informática: sus implicancias e implementación (tesis de pregrado). Universidad Tecnológica Nacional, Argentina.

Falcón, J. (2015). El sistema dual de formación profesional alemán. Sau Paulo, Brasil: Universidad de las Palmas de Gran Canaria.

Fix Fierro, Hector. (1996). Informática y documentación jurídica. Ciudad de México, México: Universidad Autónoma de México.

Garcia Juárez, L. (2014). La investigación de delitos emergentes en internet, su detección y control (tesis de pregrado). Universidad Rafael Landívar, Guatemala.

Godara, Samiksha. (2011). Prevención y control de los delitos informáticos en la india: problemas, temas y estrategias. Maharshi Dayanand University, India.

Gómez Fuentes, María del Carmen. (2013). Bases de Datos. Ciudad de México, México: Universidad Autónoma Metropolitana.

Gonzales Hurtado, J. (2013). Delincuencia informática: daños informáticos del artículo 264 del código penal y propuesta de reforma (tesis de doctorado). Universidad Complutence de Madrid, Madrid.

Guibourg, Ricardo A. (s.f.). Informática Jurídica. Ciudad de México, México: Universidad Autónoma de México.

Hemraj Saini, Yerra Shankar Rao y T.C.Panda. (2012). Crímenes ciberneticos y sus impactos: Un resumen. International Journal of Engineering Research and Applications.

Hernandez, A., y Cascón, R. (2016). Un análisis comparativo de los sistemas de formación profesional en Extremo Oriente: los casos de China, Taiwán, Corea del Sur y Japón. Cataluña, España: Revista Internacional de Organizaciones.

Hugo Vizcardo, Silfredo Jorge. (2014). Tipificación de los Delitos Informáticos Patrimoniales en la nueva ley de Delitos Informáticos N°30096. Lima, Perú: Universidad Nacional Mayor de San Marcos.

Imhof, Robert. (2010). Los delitos informáticos y el derecho de las telecomunicaciones. Rochester Institute of Technology, Estados Unidos.

Lapenne, Juan. (2011). Protección Jurídica del Software. Montevideo, Uruguay: Fox & Lapenne.

Lemaitre Picado, R. (2010). La impunidad de los delitos informáticos en la cibersociedad costarricense en ámbito del derecho penal (tesis de pregrado). Universidad de Costa-Rica, Costa Rica.

Leukfeldt, Rutger. (2017). El factor humano en el cibercrimen y la ciberseguridad. Eleven International Publishing, Holanda.

Martinez, R., y Garcia, A. (2000). Breve historia de la informática. Madrid, España: Universidad Politécnica de Madrid.

Medinacelli Diaz, K. (2015). La necesidad de incorporar en el código penal el tipo penal de falsificación informática (tesis de pregrado). Universidad Mayor de San Andrés, La Paz.

Ministerio de Justicia y Derechos Humanos (2014). El Derecho Fundamental a la Protección de Datos Personales. Lima, Perú: Ministerio de Justicia y Derechos Humanos.

Morales Delgado, D. (2016). La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú (tesis de pregrado). Universidad Señor de Sipán, Pimentel.

Nieto. P. (s.f.). Nociones generales sobre el comercio electrónico. Lima, Perú: Universidad San Martín de Porres.

Olivera, Noemí L. (s.f.). Estado de la cuestión en la relación entre derecho e informática. La Plata, Argentina: Universidad Nacional de la Plata.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2017). La Enseñanza y Formación Técnico Profesional en América Latina y el Caribe. Una perspectiva regional hacia 2030. Buenos Aires, Argentina: UNESCO.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2016). Estrategia para la Enseñanza y Formación Técnica y Profesional. Buenos Aires, Argentina: UNESCO.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2003). Declaración Internacional sobre los Datos Genéticos Humanos. París, Francia.

Organización de las Naciones Unidas. (2013). Estudio exhaustivo sobre el delito cibernético. Nueva York, Estados Unidos.

Organización de los Estados Americanos. (1969). Convención Americana sobre Derechos Humanos. San José, Costa Rica.

Parra Perea, R (2016). Proyecto legal para un esquema nacional de ciber seguridad (tesis de pregrado). Universidad San Martín de Porres, Lima.

Pélaez Bardales, José Antonio. (2011). Seguridad ciudadana: Un enfoque integral. Lima, Perú: Ministerio Público.

Ponce Malpartida, M. (2016) Delito informático y acoso sexual de menores de edad regulados por el art. 5 de la ley 30096, en el barrio Tunan del distrito de San Jerónimo, provincia de Huancayo (tesis de pregrado). Universidad de Huánuco, Huánuco.

Rayón, M., y Gómez, J. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. Anuario Jurídico y Económico Escurialense. Madrid, España: Universidad Complutense de Madrid.

Rincón Ríos, J. El delito en la cibersociedad y la justicia penal internacional (tesis de doctorado). Universidad Complutence de Madrid, España.

Ríos Estavillo, Juan José. (1997). Derecho e informática en México. Informática jurídica y derecho de la informática. Ciudad de México, México: Universidad Autónoma de México.

Ríos, J. (1997). Derecho e informática en México : informática jurídica y derecho de la informática. Ciudad de México, México: Universidad Autónoma de México.

Romero Echevarria, L. (2005). Marco conceptual de los delitos informáticos (tesis de maestría). Universidad Nacional Mayor de San Marcos, Lima.

Romero Ocampo, M. (2016). Delitos informáticos cometidos a través de redes sociales y su tratamiento en el ministerio público en la ciudad de Huánuco (tesis de pregrado). Universidad de Huánuco, Huánuco.

Rumiche Pazo, J. (2015). Sombras de la normatividad que regula el incremento de la ciberdelincuencia en Lima (tesis de pregrado). Universidad Nacional José Faustino Sánchez Carrión, Huacho.

Sebastián, G. (2009). Jornadas de Seguridad Informática: Informática forense. Neuquen, Argentina: Poder Judicial de la Provincia de Neuquen.

Sequeiros Calderón, I. (2015). Vacíos legales que imposibilitan la sanción de los delitos informáticos en el nuevo código penal peruano (tesis de pregrado). Universidad de Huánuco, Huánuco.

Téllez Valdéz, J. (2008). Derecho informático. Ciudad de México, México: Universidad Autónoma de México.

Trigo, V. (s.f.). Historia y evolución de internet. Madrid, España: Autores Científico-Técnicos y Académicos.

Vega Aguilar, J. (2010). Los delitos informáticos en el código penal (tesis de maestría). Universidad Católica de Santa María, Arequipa.

Velasco Melo, A. (2008). El derecho informático y la gestión de la seguridad de la información. Barranquilla, Colombia: Universidad del Norte de Barranquilla.

Villavicencio Terreros, Felipe. (s.f.). Delitos Informáticos en la Ley 30096 y la Modificación De La Ley 30071. Lima, Perú: Universidad San Martín de Porres.

Villazán Olivarez, Francisco José. (2010). Informática I. Michoacán, México: Universidad Michoacana de San Nicolás de Hidalgo.

Zaballos Pulido, E. (2013). La protección de datos personales en España: evolución normativa y criterios de aplicación. Madrid, España: Universidad Complutense de Madrid.

Zamora Alvizures, J. (2012). Implementación de la informática forense en la obtención de evidencia digital para combatir los delitos informáticos en Guatemala (tesis de pregrado). Universidad de San Carlos de Guatemala, Guatemala.

WEBSITE

AméricaTV. (22 de Octubre de 2013). *Gobierno promulgó polémica ley de delitos informáticos pese a críticas*. Recuperado de

Publimetro. (19 de mayo de 2017). Estos son los 8 delitos cibernéticos más comunes. (19 de mayo del 2017). Publimetro. Recuperado de https://publimetro.pe/actualidad/noticia-estos-son-8-delitos-ciberneticos-mas-comunes-interactivo-60268

Radio Programas del Perú. (25 de Octubre de 2013). *Expertos critican nueva ley de delitos informáticos*. Obtenido de https://rpp.pe/peru/actualidad/expertos-critican-nueva-ley-de-delitos-informaticos-noticia-642465.

Organización Internacional del Trabajo. (2017). R150 - Recomendación sobre desarrollo de los recursos humanos. Recuperado de https://www.ilo.org/dyn/normlex/es/f?p=NORMLEXPUB:55:0:::55:P55_TYPE,P55_LANG,P55_DOCUMENT,P55_NODE:REC,es,R150,/Document

Ministerio de Educación y Formación Profesional. (2018). Formación Profesional. Recuperado de https://www.mecd.gob.es/educacion/mc/lomce/fp.html

Kubernética. (2017). La cibernética de Norbert Wiener. Recuperado de http://www.santiagokoval.com/2017/01/09/la-cibernetica-de-norbert-wiener/

Lopategui, E. (2017). Manejo de la información y uso de la computadora. Recuperado de http://www.saludmed.com/EGIC1000/pdf/Ciencias_de_la_Computadora.pdf

British Broadcasting Corporation. (2009). Cómo se hizo el primer virus informático. Recuperado de https://www.bbc.com/mundo/internacional/2009/11/091119_1524_primer_virus_pea

La República. (2009). Millonario fraude contra usuarios de banco. Recuperado de https://larepublica.pe/sociedad/415814-millonario-fraude-contra-usuarios-de-banco

El Comercio. (2009). Contador robó más de 500 mil soles por Internet de la empresa donde trabajaba. Recuperado de http://archivo.elcomercio.pe/sociedad/lima/contador-robo-mas-500-mil-soles-internet-empresa-donde-trabajaba-noticia-329587

America TV. (2017). Los Olivos: ex trabajadora de banco confesó millonario robo informático. Recuperado de

https://www.americatv.com.pe/noticias/actualidad/detienen-mujer-acusada-intentar-robar-millones-soles-banco-n281741

Russia Today. (2011). Descubren la red internacional de pedofilia más grande del mundo. Recuperado de https://actualidad.rt.com/actualidad/view/24769-Descubren-red-internacional-de-pedofilia-mas-grande-del-mundo

Radio Programas del Perú. (2012). Conejito de peluche propició caída de red de pedófilos. Recuperado de https://rpp.pe/lima/actualidad/conejito-de-peluche-propicio-caida-de-red-de-pedofilos-noticia-508787

Publímetro. (2017). Desmantelan gigantesca red internacional de pedofilia por WhatsApp: cuatro chilenos arrestados. Recuperado de https://www.publimetro.cl/cl/noticias/2017/07/12/desmantelan-gigantesca-red-internacional-pedofilia-whatsapp-cuatro-chilenos-arrestados.html

ABC. (2012). Hackean las cuentas de Twitter de varios famosos. Recuperado de https://www.abc.es/20120830/estilo-gente/abci-hacker-twitter-famosos-201208301623.html

El Universal. (2014). Todo sobre el caso de las famosas desnudas. Recuperado de http://archivo.eluniversal.com.mx/computacion-tecno/2014/hackean-a-los-famosos-por-dinero-93992.html

ABC. (2017). El «hackeo» a Instagram afectó a mil famosos, entre ellos Emilia Clarke, Lady Gaga o Floyd Mayweather. Recuperado de https://www.abc.es/tecnologia/redes/abci-hackeo-instagram-afecto-famosos-entre-ellos-emilia-clarke-lady-gaga-o-floyd-mayweather-201709041221_noticia.html

El Mundo. (2010). Wikileaks difunde nuevos vídeos sobre abusos de EEUU en Irak. Recuperado de

https://www.elmundo.es/elmundo/2010/10/26/internacional/1288122604.html

Univisión. (2012). Anonymous hackeó sitio de FBI en represalia a cierre de Megaupload. Recuperado de https://www.univision.com/noticias/tecnologia/anonymous-hackeo-sitio-de-fbi-en-represalia-a-cierre-de-megaupload

El País. (2013). Las revelaciones de Edward Snowden, un seísmo planetario. Recuperado de https://elpais.com/internacional/2013/10/21/actualidad/1382360394_562353.html

La Prensa. (2015). Hackeo a computadoras del gobierno de Estados Unidos es: "potencial catástrofe en términos de contraespionaje". Recuperado de https://www.prensa.com/mundo/Hackeo-computadoras-Unidos-catastrofe-contraespionaje_0_4230327135.html

British Broadcasting Corporation. (2016). Cómo fue el 'hackeo' de piratas informáticos de Rusia durante las elecciones de Estados Unidos. Recuperado de https://www.bbc.com/mundo/noticias-internacional-38350244

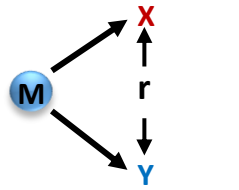
Comisión Europea. (2018).¿Qué son los datos personales?. Recuperado de https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es

ANEXOS

ANEXO "A"

MATRIZ DE CONSISTENCIA (ESTRUCTURA ANALÍTICA)

MATRIZ DE CONSISTENCIA

PROBLEMA	OBJETIVOS	HIPOTESIS	MARCO TEORICO	CUADRO DE OPERACIONALIZACIÓN DE VARIABLES			INDICADORES	MARCO METODOLÓGICO	
GENERAL	**GENERAL**	**GENERAL**	**ANTECEDENTES**	**VARIABLES**	**CONCEPTUALES**	**DIMENSIONES**		**TIPO**	Cuantitativo-no experimental
¿Cuál es la relación que existe entre *la formación profesional en derecho informático* **y** *la persecución penal de delitos informáticos* **en las Fiscalías Provinciales Penales del distrito fiscal de Huánuco en el año 2017**?	Determinar la **relación** que existe entre **la formación profesional en derecho informático y la persecución penal de delitos informáticos** en las Fiscalías Provinciales Penales del distrito fiscal de Huánuco.	Existe una relación directa entre la formación profesional en derecho informático y la persecución de delitos informático.	*SEQUEIROS CALDERON , "Vacíos legales que imposibilitan la sanción de los delitos informáticos en el nuevo Código Penal Peruano-2015", UDH, Lima, 2016. * ROMERO ECHEVARRIA, "Marco conceptual de los delitos informáticos", UNMSM, LIMA, 2005.	La formación profesional en derecho informático	Conjunto de competencias en derecho informático para su aplicación en el desempeño profesional.	Aplicación de las fuentes jurídicas del derecho informático	-Identifica las fuentes de derecho informático. - Analiza las fuentes de derecho informático - Argumenta utilizando las fuentes de derecho.	**NIVEL**	Investigación descriptiva.
						Aplicación conceptos jurídicos de derecho informático	- Identifica los conceptos jurídicos de derecho informático. - Analiza los conceptos jurídicos de derecho informático. - Argumenta utilizando conceptos jurídicos de derecho informático.	**ENFOQUE**	Investigación de enfoque cuantitativo
						Aplicación del ordenamiento jurídico del derecho informático	- Identifica el ordenamiento jurídico del derecho informático. - Analiza el ordenamiento jurídico en derecho informático - Argumenta en base al ordenamiento jurídico en derecho informático.	**DISEÑO**	DESCRIPTIVO TRANSACCIONAL
						Resolución de problemas en el ámbito derecho informático	- Identifica problemas del ámbito del derecho informático - Analiza problemas del ámbito del derecho informático - Plantea soluciones con fundamentos a problemas del ámbito del derecho informático	**ESQUEMA**	 **M=** Muestra **X** = Variable independiente **r** = Relación **Y** = Variable dependiente
						Aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional	- Identifica el uso de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional. - Analiza el uso de la informática jurídica y las Tecnologías de la Información y las comunicaciones - Utiliza la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional.		
ESPECÍFICO	**ESPECÍFICO**	**ESPECÍFICO**	**BASES TEÓRICAS**	Persecución penal de delitos Informáticos	Es la función del Ministerio Público de perseguir penalmente todos aquellos delitos que afectan	- Función del Ministerio Público de perseguir penalmente delitos informáticos.	-Investiga la presunta comisión de delitos informáticos. -Formula acusación contra los que cometen delitos informáticos. -Prueba en el proceso penal la responsabilidad penal de los acusados de delitos informáticos. - Se desarrollan políticas de prevención y líneas de acción	**POBLACIÓN**	**Operadores Jurisdiccionales:** 72 Fiscales de las Fiscalías Provinciales
PE1: ¿La aplicación de las fuentes jurídicas del derecho informático se relaciona	**OE1:** Determinar si la aplicación de las fuentes jurídicas del derecho informático se	**HE1:** La aplicación de las fuentes jurídicas del derecho informático se relaciona	- La teoría de los sistemas de Ludwig von Bertalanffy. - La teoría de la información de						

ANEXO "A"

MATRIZ DE CONSISTENCIA (ESTRUCTURA ANALÍTICA)

significativamente con la persecución penal de delitos Informáticos? **PE2:** ¿La aplicación conceptos jurídicos de derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos? **PE3:** ¿La aplicación del ordenamiento jurídico del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos? **PE4:** ¿La resolución de problemas en el ámbito derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos? **PE5:** ¿La aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño	relaciona significativamente con la persecución penal de delitos Informáticos. **OE2:** Determinar si la aplicación de conceptos jurídicos de derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos. **OE3:** Determinar si la aplicación del ordenamiento jurídico del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos. **OE4:** Determinar si la resolución de problemas en el ámbito derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos. **OE5:** Determinar si la aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el	significativamente con la persecución penal de delitos Informáticos. **HE2** La aplicación de conceptos jurídicos de derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos. **HE3:** La aplicación del ordenamiento jurídico del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos. **HE4:** La resolución de problemas en el ámbito derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos. **HE5:** La aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño	Claude E. Shannon. - La teoría de los delitos informáticos.		sistemas o datos informáticos u otros bienes jurídicos de relevancia penal mediante la utilización de las Tecnologías de la Información y las comunicaciones	- Persecución penal de Delitos que afectan a sistemas informáticos. - Persecución penal de Delitos que afectan datos informáticos. - Persecución penal de Delitos que afectan otros bienes jurídicos protegidos. - Persecución penal de Delitos que utilizan las Tecnologías de la Información y las comunicaciones.	directa para la persecución de los delitos informáticos. - Comisión de delitos mediante el acceso ilícito a sistemas informáticos. - Comisión de delitos mediante el atentado a la integridad de los sistemas informáticos. - Comisión de delitos mediante el acceso ilícito a datos informáticos. - Comisión de delitos mediante el atentando a la integridad de datos informáticos. - Delitos que atentan contra la libertad sexual a través de medios informáticos. - Delitos que atentan contra la intimidad a través de medios informáticos. - Delitos que atentan contra la seguridad pública a través de medios informáticos. - Delitos que atentan contra la secreto de las comunicaciones a través de medios informáticos. - Delitos que atentan contra el patrimonio a través de medios informáticos. - Delitos en donde utilizan las Tecnologías de la Información y las Comunicaciones para su comisión.	**MUESTRA** **TÉCNICAS** **INSTRUMENTOS**	Penales Corporativas de Huánuco. **Carpetas fiscales archivadas:** 12 **No probabilístico** **Fiscales de las Fiscalías Provinciales Penales Corporativas:** 38 **Carpetas fiscales de Delitos Informáticos de las Fiscalías Provinciales Penales Corporativas de Huánuco:** 26 ➢ **Análisis documental** ➢ **La encuesta** ➢ **La entrevista** ➢ **Matriz de análisis de datos** ➢ **Cuestionario** ➢ **Guía de entrevista**

ANEXO “A”

MATRIZ DE CONSISTENCIA (ESTRUCTURA ANALÍTICA)

profesional se relaciona significativamente con la persecución penal de delitos Informáticos?	desempeño profesional se relaciona significativamente con la persecución penal de delitos Informáticos.	profesional se relaciona significativamente con la persecución penal de delitos Informáticos.							

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CUESTIONARIO

INSTRUCCIONES:

- ✓ Lea detenidamente cada una de las preguntas y responda con la verdad.
- ✓ Conteste marcando con un aspa (X) la valoración que otorgue a cada una de las interrogantes.
- ✓ No debe dejar de marcar ninguna de las preguntas, en caso de duda, pregunte al evaluador.

Tabla de valoración:

1 = SI 2 = NO

RUBROS	PREGUNTAS	RESPUESTAS	
		1	2
2	En la fiscalia donde labora ¿se investigaron casos sobre la presunta comisión delitos informáticos en el año 2017?		
	En la fiscalia donde labora ¿se formalizó acusación en alguno de los casos de delitos informáticos en el año 2017?		
	En la fiscalia donde labora ¿se logró probar la responsabilidad penal de los acusados en alguno de los casos de delitos informáticos en el año 2017?		
	¿Tiene conocimiento que dentro del Ministerio Público se hayan desarrollado políticas de prevención y líneas de acción directa para la persecución de los delitos informáticos?		
3	En la fiscalía donde labora ¿se investigaron casos de delitos que se cometieron mediante el acceso ilícito a sistemas informáticos?		
	En la fiscalía donde labora ¿se investigaron casos de delitos que se cometieron mediante el atentado a la integridad de los sistemas informáticos?		
4	En la fiscalia donde labora ¿se investigaron casos de delitos que se cometieron mediante el acceso ilícito a datos informáticos?		
	En la fiscalia donde labora ¿se investigaron casos de delitos que se cometieron mediante el atentando a la integridad de datos informáticos?		
5	¿Considera Ud. que se puede atentar contra la libertad sexual a través de medios informáticos?		
	¿Considera Ud. que se puede atentar contra la intimidad a través de medios informáticos?		
	¿Considera Ud. que se puede atentar contra la seguridad pública a través de medios informáticos?		
	¿Considera Ud. que se puede atentar contra el secreto de las comunicaciones a través de medios informáticos?		
	¿Considera Ud. que se puede atentar contra el patrimonio a través de medios informáticos?		
6	¿Considera Ud. que se puede considerar como delito informático a todos aquellos delitos que utilice las Tecnologías de la Información y las Comunicaciones para su comisión?		

MUCHAS GRACIAS POR SU COLABORACIÓN.

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

GUÍA DE ENTREVISTA

INSTRUCCIONES:

- ✓ LEER DETENIDAMENTE.
- ✓ MARCAR CON UN ASPA (X) LA VALORACIÓN QUE CONSIDERE CONVENIENTE.
- ✓ NO DEJAR EN BLANCO NINGUNA RESPUESTA, EN CASO DE DUDA PREGUNTAR AL ENTREVISTADOR.

N°	PREGUNTA	RESPUESTA	
		SI	NO
1	¿Considera las fuentes jurídicas del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos?		
2	¿Considera que la aplicación conceptos jurídicos de derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos?		
3	¿Considera que la aplicación del ordenamiento jurídico del derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos?		
4	¿Considera la resolución de problemas en el ámbito derecho informático se relaciona significativamente con la persecución penal de delitos Informáticos?		
5	¿Considera que la aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional se relaciona significativamente con la persecución penal de delitos Informáticos?		

MUCHAS GRACIAS POR SU COLABORACIÓN.