

UNIVERSIDAD DE HUANUCO
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
ESCUELA ACADÉMICO PROFESIONAL DE DERECHO Y
CIENCIAS POLÍTICAS



TESIS

**EFICACIA DE LA LEY DE DELITOS INFORMÁTICOS
EN EL DISTRITO JUDICIAL DE HUÁNUCO 2017.**

**PARA OPTAR EL TÍTULO PROFESIONAL DE
ABOGADO**

TESISTA:

HERRERA URSUA, Lesly Monica

ASESOR:

Dr. PONCE E INGUNZA, Félix

HUÁNUCO - PERÚ

2018



UNIVERSIDAD DE HUÁNUCO
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
Ciclo de Asesoramiento para la Tesis Profesional



RESOLUCIÓN N° 061-2018-DCATP-UDH
Huánuco, 28 de mayo de 2018

Visto la Resolución N°179-2017-DCATP-UDH de fecha 18 de diciembre de 2017 que declara **APROBAR** el Proyecto de Investigación intitulado **"EFICACIA DE LA LEY DE DELITOS INFORMATIVOS EN EL DISTRITO JUDICIAL DE HUANUCO 2017"**, presentado por la Bachiller **Lesly Mónica HERRERA URSUA**;

CONSIDERANDO:

Que, el Art. 14° numeral 1 del Reglamento de Grados y Títulos del Programa Académico de Derecho y Ciencias Políticas vigente para el caso determina las diversas modalidades al cual el Graduando puede acogerse para obtener el Título Profesional de Abogado.

Que, mediante Resolución N°587-2015-R-CU-UDH de fecha 29 de mayo de año 2015 se aprobó el ciclo de Asesoramiento para la tesis profesional- CATP/DERECHO del Programa Académico de Derecho y Ciencias Políticas, en atención al Art. 31 del Reglamento General de Grados y Títulos de la UDH;

Que, mediante Oficio N°033-2017-UDH/FD-CATP/FPel. De fecha 07 de diciembre del 2017, el Dr. Felix Ponce e Ingunza Asesor del Proyecto de Investigación **"EFICACIA DE LA LEY DE DELITOS INFORMATIVOS EN EL DISTRITO JUDICIAL DE HUANUCO 2017"**, aprueba el informe final de la Investigación;

Que, en cumplimiento al Art. 31 del Reglamento de Grados y Títulos del Programa Académico de Derecho y CC.PP vigente para el caso y a mérito del documento de visto y habiendo el Bachiller previamente presentado los tres ejemplares de la referida Tesis debidamente espiralados, es pertinente emitir la Resolución de Jurado y señalar fecha y hora para su Sustentación;

Estando a lo dispuesto en el Art. 44° de la Nueva Ley Universitaria N° 30220; Inc. n) del Art. 44° del Estatuto de la Universidad de Huánuco; Reglamento de Grados y Títulos aprobado con Resolución N° 466-2016-R-CU-UDH del 23 de mayo de 2016 y la facultad que indique;

SE RESUELVE:

Artículo Primero.- DESIGNAR al Jurado Calificador para examinar al Bachiller en Derecho y Ciencias Políticas, doña **Lesly Mónica HERRERA URSUA**, para obtener el Título Profesional de **ABOGADO** por la modalidad de Trabajo de Investigación Científica (Tesis), llevado a cabo en el Ciclo de Asesoramiento para la Tesis profesional; a los siguientes docentes:

Mg. Eli Carbajal Alvarado	: Presidente
Abg. Hugo Peralta Baca	: Secretario
Mg. Mariella C. Garay Mercado	: Vocal



UNIVERSIDAD DE HUÁNUCO
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
Ciclo de Asesoramiento para la Tesis Profesional



RESOLUCIÓN N° 061-2018-DCATP-UDH
Huánuco, 28 de mayo de 2018

Artículo Segundo.- Señalar el día viernes 01 de junio de 2018 a horas 8.00 a.m. dicha Sustentación, en la Sala de Simulación de Audiencias Judiciales de la Universidad de Huánuco, sito en el 4to. Edificio 1er. Piso de la ciudad universitaria La Esperanza

Artículo Tercero.- Difúndase publicando e invitando a la comunidad académica para que presencien dicha sustentación.

Regístrese, comuníquese y archívese.



UNIVERSIDAD DE HUÁNUCO

Uladislao Escobedo Acosta Dr. D.
DECANO DE LA FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

UNIVERSIDAD DE HUÁNUCO
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

Mg. FERNANDO PORCINO BARRUETA
DIRECTOR DEL CATP

DISTRIBUCIÓN: Vice. Rect. Académico, Fac. Derecho, Of. Mat. Y Reg. Acad..f. Exp. Interesado, archivo





**ACTA DEL PROCESO DE CALIFICACIÓN POR LA MODALIDAD DE PRESENTACION
Y SUSTENTACION DE UNA TESIS**

En la ciudad de Huánuco, siendo las 8.00 horas del día 01 del mes de Junio del año dos mil dieciocho se reunieron en el Salón de Audiencia los miembros Ratificados del Jurado Examinador, designados por Resolución N°061-2018-DCATP - UDH del 28 de mayo de 2018, al amparo de la nueva Ley Universitaria N° 30220 inc "n" del Art. 44 del Estatuto de la Universidad de Huánuco, Reglamento de Grados y Títulos, para proceder por la modalidad de Presentación y Sustentación de una Tesis del Graduado **Lesly Mónica HERRERA URSUA** la postulante al Título de Abogado, procedió a la exposición de la Tesis, absolviendo las interrogantes que le fueron formuladas por los miembros designados del Jurado, de conformidad con las respectivas disposiciones reglamentarias; realizado el exposición, el Jurado procedió a la calificación.

JURADOS CALIFICADORES

PUNTAJE

Mg. Eli Carbajal Alvarado	Presidente	<u>15</u>
Abg. Hugo Peralta Baca	Secretario	<u>16</u>
Mg. Mariella C. Garay Mercado	Vocal	<u>16</u>

CALIFICATIVO : 16 DIESEISES
En números En letras

RESULTADO Aprobado por unanimidad


Mg. Eli Carbajal Alvarado
Presidente


Abg. Hugo Peralta Baca
Secretario


Mg. Mariella C. Garay Mercado
Vocal

DEDICATORIA

Este informe final de la investigación realizada por mi persona va dedicado; a mi familia, en especial a mi madre, por su incondicional apoyo, su comprensión y todo su amor, y gracias a ella pude hacer posible este sueño tan anhelado.

AGRADECIMIENTOS

A DIOS por la vida, salud y fortaleza, A la universidad de Huánuco, por permitirnos aprender los conocimientos y facilitarnos acceder al estudio, A los maestros por brindarnos e impartirnos todos sus conocimientos a lo largo de la carrera, con mucha tolerancia y paciencia; y por último a todas las personas que colaboraron de una manera desinteresada para la factibilidad de esta investigación.

ÍNDICE

DEDICATORIA	5
AGRADECIMIENTOS	6
RESUMEN.....	9
ABSTRACT	10
INTRODUCCIÓN.....	11
CAPÍTULO I	12
PROBLEMA DE INVESTIGACIÓN.....	12
1.1 Descripción del problema	12
1.2 Formulación del problema.....	13
1.2.1 Problema general:	13
1.2.2 Problemas específicos.....	13
1.3 Objetivo general.....	13
1.4 Objetivos específicos.....	13
1.5 Justificación de la investigación.....	14
1.6 Limitaciones de la investigación.....	14
1.7 Viabilidad de la investigación	14
CAPÍTULO II	15
MARCO TEÓRICO	15
2.1 Antecedentes de la investigación.....	15
2.2 Bases teóricas.....	19
2.2.1 Delitos Informáticos.	19
2.2.2 Características de los delitos informáticos.....	20
2.2.3 Clasificación de los delitos informáticos.....	21
2.2.3.1 Según la Actividad Informática.	21
2.2.3.2 Según el Instrumento, Medio o Fin u Objetivo.....	24
2.2.3.3 Según actividades delictivas graves.	25
2.2.4 Clasificación de acuerdo con las Naciones Unidas.....	26
2.2.5 Regulación Jurídica Nacional e Internacional.....	27
2.2.5.1 Regulación Jurídica en el Perú.	27
2.2.5.2 Regulación Jurídica Internacional.....	30
2.2.6 Formas de Control.	32
2.2.6.1 Preventivo	32
2.2.6.2 Correctivo.....	33
2.2.7 Impacto de los delitos informáticos	33
2.2.7.1 Impacto a nivel General.....	33

2.2.7.2	Impacto a nivel Social.....	33
2.2.7.3	Impacto en la esfera judicial	34
2.3	Definiciones conceptuales.	34
2.4	Hipótesis.....	35
2.4.1	Hipótesis general.....	35
2.4.2	Hipótesis específicas	35
2.5	Variables	35
2.5.1	Variable de estudio	35
2.6	Operacionalización de variable (Dimensiones e Indicadores).....	36
CAPÍTULO III		37
METODOLOGÍA DE LA INVESTIGACIÓN		37
3.1	Tipo de investigación	37
3.1.1	Enfoque.....	37
3.1.2	Alcance o nivel.....	37
3.1.3	Diseño	37
3.2	Población y muestra.....	38
3.2.1	Población.....	38
3.2.2	Muestra	38
3.3	Técnicas e instrumentos para la recolección de datos	38
3.3.1	Para la recolección de datos	38
3.3.2	Para la presentación de datos	39
3.3.3	Para el análisis e interpretación de los datos.....	39
CAPÍTULO IV		40
RESULTADOS		40
4.1	Procesamiento de datos.....	40
4.2	Contrastación de hipótesis.....	53
4.2.1	Hipótesis general.....	53
4.2.2	Hipótesis específicos	53
CAPÍTULO V		55
DISCUSIÓN DE RESULTADOS		55
5.1	Análisis de los resultados.....	55
CONCLUSIONES		57
RECOMENDACIONES		58
REFERENCIAS BIBLIOGRÁFICAS		60
ANEXOS		61

RESUMEN

En los últimos tiempos el avance de la tecnología es inminente en todo el mundo, con ello el incremento de una nueva forma de criminalidad; donde las computadoras nos ofrecen diversas formas sofisticadas de infringir la ley. Ante ello se debe legislar una norma, que, regulen todas estas conductas infractoras; y paralelamente asegurar la eficacia de la misma, razón por lo cual se ha desarrollado esta investigación, denominada “**Eficacia de la ley de delitos informáticos en el distrito judicial de Huánuco 2017**”, cuyo objetivo general es demostrar el nivel de eficacia de la ley de delitos informáticos en el distrito judicial de nuestra ciudad durante el presente año. Entre otros objetivos que se muestran en el capítulo uno de esta investigación.

La presente investigación es del tipo básico, solo se buscó ampliar y profundizar los conocimientos científicos acerca de la realidad estudiada, con un enfoque mixto, porque se utilizaron ambos enfoques, cualitativo y cuantitativo, con un alcance descriptivo, y, un diseño descriptivo simple donde se buscó y recogió información respecto al objeto de estudio.

La técnica utilizada para el procesamiento de datos fueron los cuadros estadísticos, con el modelo pastel, donde se observa diez cuadros con sus respectivos informes de cada pregunta encuestada, debajo de ellas los gráficos que ilustran con porcentajes la información procesada.

De los resultado obtenidos llegamos a seis conclusiones, la primera conclusión a la que se llegó con esta investigación es que el nivel de eficacia de la ley de delitos informáticos en el distrito judicial de Huánuco es baja, segundo, que no existen juzgados especializados para estos delitos informáticos, tercero, no existe un área de logística para la investigación de estos delitos informáticos, cuarto, es evidente que tanto jueces como fiscales no tienen ninguna capacitación en estos temas, entre otras conclusiones que se muestran al final de esta investigación.

PALABRAS CLAVES: Delitos informáticos, eficacia.

ABSTRACT

In recent times the advance of technology is imminent worldwide, with it the increase of a new form of criminality; where computers offer us sophisticated ways to break the law. In view of this, a regulation must be legislated, which regulates all these infringing conducts; and in parallel to ensure the effectiveness of the same, which is why this research has been developed, called "Efficacy of the law of computer crimes in the judicial district of Huánuco 2017", whose general objective is to demonstrate the level of effectiveness of the law of computer crimes in the judicial district of our city during this year. Among other objectives that are shown in chapter one of this research.

The present investigation is of the basic type, it only sought to expand and deepen the scientific knowledge about the studied reality, with a mixed approach, because both qualitative and quantitative approaches were used, with a descriptive scope, and, a simple descriptive design where we searched and collected information regarding the object of study.

The technique used for the data processing was the statistical tables, with the pastel model, where ten tables with their respective reports of each question surveyed are observed, below them the graphs that illustrate the processed information with percentages.

From the results obtained we reached six conclusions, the first conclusion that came with this research is that the level of effectiveness of the law of cybercrime in the judicial district of Huánuco is low, second, there are no specialized courts for these cybercrimes, fourth, it is clear that both judges and prosecutors have no special training in these subjects, among other conclusions that are shown at the end of this investigation.

KEY WORDS: Computer crimes, efficiency.

INTRODUCCIÓN

El impacto de la tecnología y su avance en todos los ámbitos es impresionante y a su vez desafiante para todos legisladores de cada Estado, esto porque en la actualidad la informática está presente en casi todas las áreas de la vida de las personas y la mayoría de las instituciones desplazaron el uso manual de realizar sus actividades por los sistemas tecnológicos, así también algunas personas con conocimientos avanzados en estas se perfilan día a día para hacer de las suyas en el ciberespacio. Por ello nos atrevemos a afirmar que este avance trajo consigo comportamientos infractores, nunca antes pensado, que llevan a la desesperación al legislador al tipificarlos, al fiscal al perseguirlos y al juez al aplicarlos, quienes en esa desesperación por resolver este mal que aqueja a nuestra sociedad crean leyes ambiguas, que no regulan o tipifican bien los comportamientos típicos delincuenciales, que resultan ser ineficaces frente a la realidad que se vive en la actualidad.

A raíz de todo lo descrito líneas arriba, la presente investigación se enfocó en la eficacia que tiene la ley de delitos informáticos en el distrito judicial de Huánuco en el presente año.

En el primer capítulo de esta investigación abarcó todo acerca de este problema tales como el planteamiento de la misma, formulación, justificación, los objetivos que hemos logrado con su estudio, el segundo capítulo comprenden todas las generalidades respecto al tema a investigar, es decir conceptos realizados por distintos autores, características, clasificaciones, efectos, la regulación jurídica desde un ámbito nacional e internacional, entre otras propias del tema (delitos informáticos). En el tercer capítulo se presentó la metodología que se ha utilizado para llevar a cabo la presente investigación, el cuarto los resultados obtenidos, en el quinto la discusión de dichos resultados; y, por último las conclusiones que hemos llegado con todo lo estudiado, así como la bibliografía que se ha tomado como referencia.

CAPÍTULO I

PROBLEMA DE INVESTIGACIÓN

1.1 Descripción del problema

El avance de la tecnología es inminente en nuestro país. El cual influye en la vida de casi todas las personas naturales como jurídicas existentes en nuestro Estado; el progreso de la informática es importante para el desarrollo de nuestro país, porque se encuentra inmersa en todos los servicios públicos que este brinda. El propósito no es describir el avance y progreso de la tecnología informática sino la problemática creciente con ella, que a raíz de su avance se han producido una serie de comportamientos ilícitos la cual denominaremos “**delitos informáticos**”. En nuestro país a medida que va avanzando la informática paralelo a ella también avanza el uso indebido de ésta, y a los que incurren en estas malas artes se les denomina delincuentes informáticos, quienes, en la mayoría de veces, logran burlar a la ley sin dejar documento alguno que compromete su culpabilidad cometida desde una computadora, cuenta electrónica, virus que congelan y borran todos los datos de algún disco duro, que contiene alguna información económica para ser sustraída; estos son algunos delitos que se han visto en nuestro país y en nuestra región. Estos delincuentes informáticos son tan diversos o dispersos como sus delitos. No debemos pasar por alto que Huánuco también es una ciudad en progreso y desarrollo; tanto que la tecnología informática se encuentra al alcance de la mayoría de sus habitantes sin hacer distinción. En los últimos años se ha percibido de manera acelerada y creciente conductas delictivas en el ámbito tecnológico, lo cual solo era propio de nuestra capital.

Los llamados dispositivos hackers son colocados en algunos cajeros automáticos que copian toda la información del usuario para luego ser sustraído por los delincuentes informáticos. Son algunos de los ejemplos que podemos citar los cuales vienen aconteciendo en nuestra ciudad, sin mencionar que esto se podrá agravar si no se pone un límite a ese flagelo que azota cada día a nuestra localidad; es decir, hoy son dispositivos hackers en los cajeros automáticos, mañana programas especiales para codificar cada tarjeta bancaria y las de crédito en bandas magnéticas. Siendo

afectados no solo los empresarios de nuestra ciudad, sino también la mayoría de personas que utilizan estas tarjetas.

En la actualidad, existe una ley que sanciona, sin embargo estas conductas delictivas no han cesado hasta el presente año, las cuales siguen con mucha ferocidad y en reiteradas veces, razón por la cual se cuestiona la eficacia de la ley de delitos informáticos. Podría ser que dicha ley necesita una mayor difusión y mayor rigidez, entre otras soluciones, que iremos proponiendo a lo largo de la investigación. ¿Entonces frente a esta problemática como no preocuparse por la seguridad de nuestros ciudadanos huanuqueños?

1.2 Formulación del problema

1.2.1 Problema general:

¿Cuál es el nivel de eficacia de la ley de los delitos informáticos en el Distrito Judicial de Huánuco 2017?

1.2.2 Problemas específicos

- ¿Existen vacíos legales en la ley de los delitos informáticos que se administra en el Distrito Judicial de Huánuco 2017?
- ¿Cuál es el porcentaje de denuncias de delitos informáticos que obran en las fiscalías penales del Distrito Judicial de Huánuco 2017?
- ¿Cuál es la diferencia entre la ley de los delitos informáticos que se administra en el Distrito Judicial de Huánuco 2017 con otras legislaciones internacionales?

1.3 Objetivo general

Demostrar el nivel de eficacia de la ley de los delitos informáticos en el Distrito Judicial de Huánuco 2017.

1.4 Objetivos específicos

- a. Identificar los vacíos legales en la ley de los delitos informáticos que se administra en el Distrito Judicial de Huánuco 2017.

- b. Determinar el porcentaje de denuncias de delitos informáticos que obran en las fiscalías penales del Distrito Judicial de Huánuco 2017.
- c. Analizar las diferencias de la ley de los delitos informáticos que se administra en el Distrito Judicial de Huánuco 2017 con otras legislaciones internacionales.

1.5 Justificación de la investigación

Con el desarrollo de las ciencias aplicadas se han mostrado nuevos casos de conductas delictivas que para el contexto jurídico imposibilitando demasiadas veces su sanción, porque superan a la realidad por no estar acorde la actualidad tecnológica.

Y estos nuevos delincuentes con conocimientos específicos, deberían ser investigados con mayor inteligencia, lo que nos indica que a raíz de su incremento tanto el persecutor del delito como el que apoya en su investigación, no se encuentran capacitados para ello, lo que desemboca en impunidad delictiva.

Por ello la presente investigación sirvió para identificar el nivel de eficacia que tiene la ley de los delitos informáticos en nuestro Distrito Judicial, y a su vez con su estudio nos permitió aportar soluciones a esta controversial problemática.

1.6 Limitaciones de la investigación

Las limitaciones en esta investigación fue la muestra de estudio dado que a la hora de la encuesta fue dificultosa y poco accesibles para obtener dicha información, debido a que los sujetos de muestra por el trabajo que ostentan no disponen de tiempo libre.

Otra de las limitaciones fue la escasa bibliografía o material de estudio que se puede recopilar acerca de este tema; ya que por ser una cuestión reciente, aun no se han profundizado investigaciones.

1.7 Viabilidad de la investigación

Este proyecto fue viable investigar porque contamos con todos los recursos necesarios para el estudio, tales como materiales, recursos económicos, disponibilidad de tiempo, empeño y entusiasmo para llevarlo a cabo.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes de la investigación

- **2016, Ivett Claritza Sequeiros Calderon, “Vacíos legales que imposibilitan la sanción de los delitos informáticos en el nuevo Código Penal peruano 2015”**, Ya que los delitos informáticos se cometen virtualmente, estos pueden ser confusos en su tipificación, y, a esta se suma la escasa información adecuada y aplicación en la inspección de aquellas. Causal para dar presencia de algunas lagunas legales que dificultan el castigo de estas conductas infractoras. Como es el caso del comercio electrónico, claro ejemplo como estos delitos se presentan de manera diversa, por lo cual es necesario crear un instrumento legal efectivo que ayude al combate directo de estos.

Estos tipos de infracciones no deben impedir que el usuario se prive de todo lo que proporcionan las tecnologías de por ello se debe trazar todo un desafío a los profesionales de la informática, cuyo fin únicamente sea otorgar seguridad a los usuarios de estas tecnologías.

- **Costa Rica 2015, Ever Francisco Sanchez Azofeifa, “Desarrollo de la prueba en Delitos Informáticos y uso de documentos electrónicos”**, Los delitos informáticos son tan difíciles que requiere para su comisión a personas con conocimientos especializados en los mismos, es decir un conocimiento muy desarrollado de los sistemas de software y hardware. Dentro de la legislación de Costa Rica para la configuración de estas conductas infractoras deben de seguir una valoración muy estricta, para que estas puedan ser comprobables ante juicio.

De la investigación al Poder Judicial realizada por el autor sus datos estadísticos fueron existen denunciase investigaciones en contra de estos delitos, pero la tasa de éxito en ser probadas son mínimas, a razón de 1.6 % al 2.2 % de los casos llega a sentencia final. A esto debemos sumarle que muchas de las víctimas no llegan a denunciar estos hechos delictivos por miedo a dañar su reputación como garantes de los datos.

Concluyendo entonces es forzoso entonces que el operador del derecho se llene de todos estos nuevos conocimientos para afrontar este delitos surgente con la tecnología.

- **Madrid 2013, Jorge Alexandre González Hurtado. “Delincuencia Informática: Daños informáticos del artículo 264 del Código Penal y propuesta de Reforma”.** La conclusión final que se extrae de la elaboración de este instrumento de investigación, es que la legislación española respecto a los delitos de daños informáticos debería ser reformulada desde nuevos principios integradores. Porque su diseño arroja algunas dudas de interpretación, y en cuanto a jurisprudencia aun los casos presentados ante los tribunales son escasos.

Se tiene presente que los legisladores españoles anticiparon la nueva problemática aparecida, pero no se ha tomada esa ventaja para decretar normas precisas, sino seriamente engorrosas. Si bien se ha comenzado con la iniciativa de resguardar a la colectividad de nuevos tipos de delincuencia, es necesario hacerlo con la máxima efectividad.

Para esto es obligatorio establecer medidas concretas tanto en el campo nacional e internacional, donde todos se comprometan a completar lo establecido y mejorarlo también para frenar la ola delincencial producidas en el mundo cibernético pero con mayor énfasis en el ámbito penal.

- **2013, Eduardo André Ramos Rodríguez “Delitos Informáticos y Computacionales”.** El delito informático es el que daña un ajeno beneficio colectivo, un nuevo bien jurídico penal, es decir afecta la información o que dañe un sistema de tratamiento de la información. En cambio los delitos computacionales son un nuevo medio para cometer otros delitos como por ejemplo el hurto. Estas conductas infractoras generan desconfianza tanto de usuarios como nuevas empresas en utilizar los métodos tecnológicos o ampliar métodos de información para optimizar o prestar su fabricación.

➤ **Salamanca 2012, Andrea de Cea Jiménez “*los delitos en las redes sociales: aproximación a su estudio y clasificación*”,**

Esta investigación desarrolló de manera profunda las clasificaciones documentales, tanto que se pudo elaborar una clasificación especializada lográndose elaborar una representación clara y concisa. Existe un número superior de este tipo de delitos, como ejemplo tenemos a las redes sociales cuyos elementos más resaltantes son: el muro, los mensajes privados; etc. Paralelo a ello, existen otros que están presentes pero no son importantes para nosotros, como la publicidad, los juegos, etc. a través de las cuales se cometen estos delitos y los usuarios no se dan cuenta. En base a lo descrito anteriormente, se debe decir que existen más formas de llevar a cabo cada uno de estos delitos. Mayormente estos delitos podrían ser evitados por la propia víctima si ésta sería más responsable con la información privada que expone en sus cuentas sociales, también si antes de hacer uso de alguna aplicación por lo menos leyera los términos y condiciones de estas o se certificara que en realidad existe.

➤ **2012, Juan Carlos Alburquerque Quiroz “*Delitos informáticos en el Perú*”,** se puede afirmar que los delitos informáticos en el Perú, son todas aquellas gestiones y quehaceres utilizados por una persona o grupo de personas que en pleno uso de sus facultades físicas y mentales y, mediante el uso incorrecto de cualquier canal informático o telemático incitan una lesión a cualquier persona natural o jurídica.

Estas conductas dañinas son muy sofisticadas, tanto que presentan dificultades a la hora de ser comprobadas, por ser de carácter técnico, las cuales provocan cuantiosas pérdidas económicas, las cuales en su mayoría llegan a ser impunes por todas las características descritas y por falta de ley que otorgue el derecho que sean sancionados aquellos infractores que incurren en estas malas artes.

Por lo cual se requiere adecuar y actualizar la ley peruana en forma permanente para incorporar aquellos delitos donde utilicen las Tecnologías de Información y Comunicaciones.

- **2011, Juan David Rodríguez Arbeláez, “Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación”**, En Colombia no existe una ley precisa que sancionen estos delitos cometidos a través de las redes sociales, la cuales vienen afectando a toda una sociedad completa.
Entonces la preocupación por aplacar la comisión de estos delitos no solo está en palabras, sino que estas deben ser acciones tales como políticas criminales destinadas a la prevención cuya base sea el uso correcto de las redes sociales, para así minimizar riesgos, por ello es fundamental fomentar una cultura que conlleve a las personas a protegerse en este espacio digital. Y la dación de esas nuevas normas deberían contener las posibles vulneraciones a los derechos constitucionales para que las personas puedan tener opciones y medios dónde acudir para denunciar y protegerse frente a cualquier delito en las redes sociales.

- **2002, Ángel Alfonso Arata Salinas, “Las Nuevas Tecnologías de la Información y la problemática Jurídica del comercio electrónico”**, Se infiere que, el progreso de las tecnologías dirigidas a acciones comerciales, ha llevado al uso de tecnologías con capacidad artificial incorporada, y para determinar su alcance, hay que determinar la naturaleza jurídica del comercio electrónico, es decir sus particularidades. Para ello es necesario plantear propuestas que normen el comercio electrónico donde se contemplen los elementos esenciales en cuanto a la forma y al fondo de la contratación mediante el uso de soportes informáticos, Donde el profesional del derecho debe ser consiente que la estabilidad jurídica es un elemento vital en el perfeccionamiento del intercambio comercial y económico en cualquier parte del mundo.
Lo que vendría a ser un reto y respuesta del derecho peruano brindar estabilidad jurídica en cuanto al tema del comercio electrónico para poder generar confianza y su uso masivo en beneficio de todos los peruanos.

- **2001, Cristian F Borghello, “seguridad informática: Sus Implicancias e Implementación”**, en estos tipos de delitos la ley no solo debe buscar la forma de castigo, sino algo mucho más importante como lograr probar

el delito. Lo que a la realidad esto viene siendo un inconveniente muy grande a la hora de legislar por el carácter inmaterial de la información.

Es decir un delito es un delito no menoscabará su característica si este se cometió por un medio tecnológico o no, y para que este problema tenga un final diferente se deben crear con inmediatez mecanismos de legislación a la velocidad con la cual avanza esta nueva forma de delinquir.

Otra salida a este problema es la unificación de todos los países a los postulados de la ONU en cuanto a este tema, para generar una legislación internacional que regulen la problemática de la cibernética y su utilización tan generalizada en el mundo.

2.2 Bases teóricas

2.2.1 Delitos Informáticos.

Es toda aquella acción anti jurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

Los delitos informáticos son actividades ilícitas que:

- Se configuran mediante el uso de computadoras, procedimientos informáticos entre otros puntos de conexión de las comunicaciones (el tratamiento de la información científica es el medio o vía para realizar un delito); o
- Tienen por objetivo principal provocar menoscabos, incitar pérdidas o paralizar el uso de sistemas informáticos (delitos informáticos).

Los también conocidos Ciberdelitos, lo que señala Téllez, son maneras inversas a los beneficios de las personas en que se tiene a los sistemas computacionales como herramienta o fin (concepto atípico) y las conductas atípicas, contrarias a ley y culpables en que se tiene a los ordenadores como instrumento o fin (concepto típico).

Algunos autores y entidades lo definen del presente modo: (citado por **VIEGA RODRÍGUEZ** María José. *“Un nuevo desafío jurídico. Los delitos informáticos”*. Integrante de la Comisión de Derecho Informático y Tecnológico de la Asociación de Escribanos del Uruguay)

Para la **Universidad de México** que ha elaborado un artículo sobre este tema define a los delitos informáticos como: "son todas las acciones ilícitas merecibles totalmente de ser castigadas por el derecho penal, para todas las personas que manejan de manera indebida cualquier instrumento informático".

- **Jijena Leiva** los describe así: "toda acción típica, antijurídica y culpable, que para su realización se usan los ordenadores computacionales afectando a la información contenida en un ordenador tecnológico.
- **María José Viega Rodríguez:** lo precisa como "toda conducta ilícita, condenada por el derecho penal, que para su consumación se utilizan los medios informáticos, productos de las nuevas tecnologías, ya sea como utensilio para la comisión del delito o como fin en sí mismo, afectando los datos informáticos contenidos en un sistema".
- Y por último para **la Organización para la Cooperación Económica y el Desarrollo (OECD)** lo conceptualiza como: "cualquier acción humana, no ética, o no aprobada, que comprende el procesamiento automático de datos y la transmisión de las mismas".

2.2.2 Características de los delitos informáticos

Entre las principales características se mencionan las siguientes:

- Son acciones criminales de cuello blanco, por ello para que se configure la comisión de estas, tendrían que ser un concluyente número de personas con ciertos conocimientos específicos en temas computacionales e informáticos.
- Son conductas ocupacionales porque al tener el tiempo ocupado las víctimas, estos bandidos aprovechan estos espacios para cometer sus actos delincuenciales.
- Son acciones de oportunidad puesto que se beneficia del avance tecnológico que emerge en la actualidad para tener conocimientos especializados en estos temas y así lograr lo cometido, ya que las víctimas son abundantes por el uso de estas tecnologías.
- Provocan graves y cuantiosos desfalcos económicos, ya que en su mayoría generan "beneficios" mayores de cinco cifras a aquellos que los realizan.

- Ofrecen la comisión fácil de tiempo y espacio debido a que estos delitos son cometidos en diminutos espacios de tiempo por no decir en un abrir y cerrar de ojos y además para su realización no es necesaria la presencia física.
- Los casos presentados actualmente son extensos, pero lo preocupante son las escasas denuncias de estas, debido a la falta de regulación, debido a la falta de regulación en el fuero internacional penal.
- Son muy rebuscados y respectivamente frecuentes en el dominio militar.
- Presentan grandiosos problemas para su demostración, por su representación técnica.
- En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposos o imprudenciales.
- Ofrecen a los menores de edad facilidades para su comisión.
- Estos se están expandiendo cada vez con más frecuencia, por lo que merece mayor atención en cuanto a una regulación jurídica en el ámbito internacional

2.2.3 Clasificación de los delitos informáticos

2.2.3.1 Según la Actividad Informática.

a. Sabotaje informático. La palabra sabotaje informático se entiende como todas aquellas diligencias encaminadas a provocar daños en el hardware o en el software de un sistema. Los procesos manipulados para provocar estragos en los sistemas computacionales son de índole múltiple las cuales se han ido desarrollando hacia metodologías cada vez más sofisticadas y de difícil detección. Esencialmente, se puede apreciar dos grandes casos: las primeras, son conductas diseñadas a producir destrucciones físicas y, por el otro, las técnicas diseñadas a provocar desastres lógicos.

b. Conductas dirigidas a causar daños físicos. Como denota el párrafo anterior el primer caso comprende todo tipo de gestiones predestinadas a la pérdida «física» del hardware y el software de un ordenador sistemático (por ejemplo: causar quemaduras o explosiones, empotrar piezas de aluminio

dentro de un ordenador para generar cortocircuitos, verter café o agentes cáusticos en los equipos, etc. En general, estas acciones pueden ser examinadas, desde el punto de vista jurídico, en forma análoga a los comportamientos similares de destrucción física de otra clase de objetos previstos típicamente en el delito de daño.

c. Conductas dirigidas a causar daños lógicos. Bien visto el primer caso, ahora analizaremos el segundo caso, entonces ésta relacionado específicamente con la técnica informática, es decir se refiere a las conductas que generan estragos lógicos, comprendase, todas aquellas acciones que producen, como resultado, la pérdida, ocultación, o alteración de datos contenidos en un ordenador lógico.

d. Fraude a través de computadoras. Estas diligencias radican en la maniobra ilícita, en las cuales se crean datos falsos o la transformación de datos o procesos contenidos en sistemas informáticos, estos son desarrolladas con el fin de obtener ganancias indebidas.

e. Copia ilegal de software y espionaje informático. Aquí abarcan las conductas destinadas a obtener datos, de manera falsificada, de una computadora. Estas conductas son comunes, en especial con el apropiamiento de datos de investigaciones, listas de clientes, balances, etc. En la mayoría de las situaciones presentadas el centro del apoderamiento es el mismo programa de computación (software) que suele tener un importante valor económico. Las cuales detallamos a continuación:

- **Infracción de los derechos de autor:** La definición de los conceptos de copia, comercialización, transferencia y comunicación pública de los programas de ordenador utilizando la red ha provocado diversos criterios a nivel jurisprudencial. Lo que nos hace denotar que no hay unanimidad a la hora de sentenciar dichos actos.

- **Infracción del Copyright de bases de datos:** a decir verdad no preexiste una defensa equivalente de las bases de datos en los países que tienen acceso a Internet. El método de protección más habitual es el contractual: el propietario del sistema permite que los beneficiarios realicen "descargar" de los programas o aplicaciones contenidos en el sistema, pero impide la réplica de estos datos o la copia masiva de información.

f. *Uso ilegítimo de sistemas informáticos ajenos.* Este modo operandi radica en utilizar sin autorización alguna las computadoras y los programas contenidos en ellas que sean ajenos. Estas conductas atípicas son perpetrados comúnmente por los empleados de alguna empresa o institución que se encuentran a cargo de los sistemas de procesamiento de datos que estas entidades utilizan para el funcionamiento privado propias de su ejercicio laboral. Con la comisión de estos hechos, lo único que se produce es un menoscabo perjudicial para la economía de estas empresas, también el pago del alquiler de estos sistemas los cuales son usados por ellas.

g. *Delitos informáticos contra la privacidad.* Es el conjunto de conductas que de una u otra forma pueden dañar el ámbito de privacidad e intimidad de una persona perteneciente a una sociedad, ya sea con la obtención de esta de forma acumulativa para luego ser difundidas indebidamente, todos aquellos datos contenidos en un ordenador lógico. Esta normativización está referida para todas aquellas personas que sin estar autorizadas a ellas, se apoderen, utilicen o modifiquen, toda esta información confidencial en agravio de otra a quien pertenece esa información, tales como datos reservados muy personales o familiares, todas contenidos en sistemas informáticos. A continuación pasaremos a detallar las agravantes por la divulgación de ficheros las cuales son:

- El carácter de los datos: ideología, religión, creencias, salud, origen racial y vida sexual.
- Las circunstancias de la víctima: menor de edad o incapaz.

2.2.3.2 Según el Instrumento, Medio o Fin u Objetivo.

Según, TELLEZ VALDEZ da una clasificación a estos actos delincuenciales, de acuerdo a dos razones:

a. Como instrumento o medio. En esta clase se encuentra las acciones criminales que tienen como medio de comisión a las computadoras, para dar más claridad a estos mostramos unos ejemplos:

- Adulteración de documentos vía digital (tarjetas de crédito, cheques, etc.)
- Desviación de los activos y pasivos en los casos contable de las empresas.
- Premeditación y simulación de delitos comunes (robo, homicidio, fraude, etc.)
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- Uso no autorizado de programas de cómputo.
- Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
- Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- Acceso a áreas informatizadas en forma no autorizada.
- Intervención en las líneas de comunicación de datos o teleproceso.

b. Como fin u objetivo. En esta clase, se encuentran las conductas delincuenciales cuyas víctimas son las computadoras, accesorios o programas como entidad física, como por ejemplo:

- Programación de instrucciones que producen un bloqueo total al sistema.
- Destrucción de programas por cualquier método
- Daño a la memoria.
- atentado físico contra la máquina o sus accesorios.
- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.)

2.2.3.3 Según actividades delictivas graves.

Vistos todos los delitos mencionados líneas arriba, solo nos queda decir que el internet tiene un lado oscuro el cual facilita y permite la comisión de ciertos actos muy peligrosos como son:

- Terrorismo: a través de las cuales cierto grupo de terroristas envían mensajes anónimos con el único fin de amedrentar a la población remitiendo en estos mensajes sus planes de acción a nivel internacional, y con la existencia de ciertos programas que ocultan la identidad del difusor de dichos mensajes estos grupos terroristas son impunes. Y al quedar impune los materiales difundidos vía internet, que no solo queda en amenazas, de hecho, se han detectado mensajes con instrucciones para la fabricación de material explosivo.
- Narcotráfico: Así como en el caso de terrorismo se han dado mensajes donde se difunden fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
- Espionaje: no obstante todo lo mencionado han surgido casos donde facinerosos han logrado acceder a sistemas no autorizados tales como los sistemas gubernamentales, también acciones como apropiación de correo electrónico del servicio secreto de un país, entre otros actos que podrían ser calificados de espionaje si estos actos fuesen realizados por otro gobierno.

- Espionaje industrial: Así como el espionaje propiamente dicho y descrito un párrafo arriba, también se han producido casos donde se han apropiado de los sistemas operativos de grandes empresas, usurpando diseños industriales, fórmulas, sistemas de fabricación, etc. Las cuales han sido aprovechadas posteriormente en empresas competidoras o estas se han divulgado sin ninguna autorización.
- Otros delitos: con las mismas opciones y facilidades que brinda el internet para la comisión de los otros delitos graves vistos con anterioridad, también pueden cometerse algunos delitos tales como; como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro acto delincuenciales que pueda ser traído de la vida real al ciberespacio o viceversa.

2.2.4 Clasificación de acuerdo con las Naciones Unidas.

Según el anual de las Naciones Unidas para la prevención y control de delitos informáticos señala que si el problema aparece en el fuero internacional, se engrandecen los obstáculos y las escaseces, por cuanto los delitos informáticos constituyen una nueva forma de delito transnacional y su combate requiere una eficaz cooperación internacional concertada. Ante ello la ONU resume la falta de acuerdo internacional en cuanto a estos tipos de infracciones de la siguiente manera:

- Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
- Falta de especialización de los policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
- No armonización entre las diferentes leyes procesales nacionales referentes a la investigación de los delitos informáticos.
- Carácter transnacional de múltiples delitos cometidos mediante el uso de computadoras.

- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

2.2.5 Regulación Jurídica Nacional e Internacional.

2.2.5.1 Regulación Jurídica en el Perú.

LEY N° 30096

LEY DE DELITOS INFORMÁTICOS

CAPÍTULO II

Delitos contra datos y sistemas informáticos

Artículo 2. Acceso ilícito

El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa. Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado.

Artículo 3. Atentado contra la integridad de datos informáticos

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

Artículo 4. Atentado contra la integridad de sistemas informáticos

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

CAPÍTULO III

Delitos informáticos contra la indemnidad y libertad sexuales

Artículo 5. Propositiones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

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

CAPÍTULO IV

Delitos informáticos contra la intimidad y el secreto de las comunicaciones

Artículo 6. Tráfico ilegal de datos

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

Artículo 7. Interceptación de datos informáticos

El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia. La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.

CAPÍTULO V

Delitos informáticos contra el patrimonio

Artículo 8. Fraude informático

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

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

CAPÍTULO VI

Delitos informáticos contra la fe pública

Artículo 9. Suplantación de identidad

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

CAPÍTULO VII

Disposiciones comunes

Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

Artículo 11. Agravantes

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

1. El agente comete el delito en calidad de integrante de una organización criminal.
2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.
3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.
4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

2.2.5.2 Regulación Jurídica Internacional

- **Argentina.** En Argentina sancionó el 4 de junio de 2008 la Ley 26.388 (promulgada de hecho el 24 de junio de 2008) que modifica el Código Penal a fin de incorporar al mismo diversos delitos informáticos, tales como la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.
- **Uruguay.** El Estado uruguayo aprobó en el año 2007 la **ley N° 18.237** denominada EXPEDIENTE ELECTRÓNICO cuyo único artículo autoriza el uso de expediente electrónico, de documento electrónico, clave informática simple, firma electrónica, firma digital y domicilio electrónico constituido en todos los procesos judiciales y administrativos que se tramitan ante el Poder Judicial, con idéntica eficacia jurídica y valor probatorio que sus equivalentes convencionales. Donde los delitos informáticos no son de tratamiento específico por la legislación uruguaya, puesto que no existe una ley de ilícitos informáticos (no puede haber delito sin ley previa, estricta y escrita que lo determine - principio de legalidad-),

ni tampoco un título específico relativo a los mismos en el Código Penal uruguayo.

- **Colombia.** En Colombia el 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “De la Protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales. En Colombia existen instituciones de educación como UNICOLOMBIA que promueven capacitaciones en temas relacionados con Delitos Informáticos, el mejor manejo y uso de la prueba digital, establecer altos estándares científicos y éticos para Informáticos Forenses, Llevar a cabo investigación y desarrollo de nuevas tecnologías y los métodos de la ciencia del análisis forense digital e Instruir a los estudiantes en diversos campos específicos sobre nuevas tecnologías aplicadas a la informática Forense, la investigación científica y el proceso tecnológico de las mismas.
- **España.** En España, los delitos informáticos son un hecho sancionable por el Código Penal, estas sanciones se recogen en la Ley Orgánica 10/1995, de 23 de noviembre en el BOE número 281, de 24 de noviembre de 1995. A la hora de proceder a su investigación, debido a que una misma acción puede tener consecuencias en diferentes fueros, comenzará la investigación aquel partido judicial que primero tenga conocimiento de los hechos delictivos cometidos a través de un medio informático, si durante el transcurso de la investigación, se encuentra al autor del delito y pertenece a otro partido judicial, se podrá realizar una acción de inhibición a favor de este último para que continúe con la investigación del delito.
- **México.** En México los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática son hechos sancionables por el Código

Penal Federal en el título noveno capítulo I y II. El artículo 167 fr.VI del Código Penal Federal sanciona con prisión y multa al que intencionalmente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos.

- **Venezuela.** El 30 de octubre de 2001 la Asamblea Nacional formulo la Ley Especial contra los Delitos Informáticos donde se decreta, a través de 32 Artículos, como se protege a todos los sistemas y tecnologías de información en Venezuela, cuáles son los delitos relacionados con estos y que sanciones se aplican en cada delito específico.

2.2.6 Formas de Control.

2.2.6.1 Preventivo

Este tipo de ilícitos requieren un control necesario, por no encontrarse en la actualidad una adecuada protección jurídica, por lo mismo tanto los empresarios como entre otras instituciones a manera de institución han tomado algunas medidas para protegerse frente a estos actos ilícitos. Las cuales servirían mucho al momento de elaborar una legislación para frenar este delito.

Entre las cuales están:

- Elaboración de un examen psicométrico previo al ingreso e áreas de sistemas en las empresas.
- Inclusión de cláusulas especiales en los contratos de trabajo con el personal informático que así lo requiera por el tipo de labores a realizar.
- Establecimiento de un código ético de carácter interno en las empresas.
- Adopción de estrictas medidas en el acceso y control de las áreas informáticas de trabajo.
- Capacitación adecuada del personal informático, a efecto de evitar actitudes negligentes.
- Identificación y, en su caso, segregación de personal informático descontento.

- Rotación en el uso de acceso al sistema.

2.2.6.2 Correctivo

Este tipo de control podrán ser aplicados cuando ya exista un conjunto de normas que regulen todos estos ilícitos penales de manera concreta, ya que una adecuada legislación no solo traería efectos correctivos sino que a su vez preventivos, de tal forma que se reducirían de una manera muy notable estos ilícitos que tanto mal causan a los interesados individuales y sociales.

2.2.7 Impacto de los delitos informáticos

2.2.7.1 Impacto a nivel General

Hoy en día los usuarios online superan los 200 millones, lo que es un incremento muy significativo comparado con los 26 millones en el año 1995. Es que la tecnología nos han facilitado muchas cosas, entre ellas comprar, vender, realizar pagos, consultar a nuestros médicos entre muchas acciones que nos facilitan las redes para nuestro obrar cotidiano sin tener que acudir personalmente a las instituciones que brindan este servicio. Por lo cual las personas que cometen estos delitos son tan diversos, y tan escurridizos para ley, que en reiteradas ocasiones pasan desapercibidos a través de las fronteras, ocultarse tras incontables enlaces o simplemente desvanecerse sin dejar documento alguno que pueda indicar rastro de ellos. Como se observa son diversas formas el modus operandi de estos delincuentes, que no solo van en esconder pruebas delictivas, también pueden sabotear la computadoras, manipular datos, mandar virus que dañen programas cibernéticos, etc. u sin fin de accionares ilícitos.

2.2.7.2 Impacto a nivel Social

Este hecho ha provocado en la sociedad que esta sea cada vez más desconfiada a la hora de utilizar estas tecnologías informáticas, las cuales hemos advertido en los párrafos anteriores que es de mucho beneficio para un buen desarrollo social en general.

Entonces este hecho viene afectando una nueva forma de negociación, hasta el punto que podría menguar el comercio electrónico por la falta de apoyo por parte de la población en general.

Las personas que cometen estos delitos son aquellas que tienen ciertos conocimientos especiales en tecnología, quienes día tras día vienen

perfeccionando sus actos delictivos para realizar sus actos delictivos, cuyas víctimas no solo son personas naturales, sino que su mira ahora está mucho más alto como lo es el ámbito empresarial y global. Por lo cual aquellas personas que no tienen conocimientos básicos tecnología, serán siempre blanco fácil para estos malhechores, entonces es necesario contar con algo de conocimiento en este campo para no ser víctimas de ellos. Por ello el componente clave para hacerle frente a este mal es la educación a la población en cuanto a tecnología informática, para que de esta manera ellos no sean engañados y manipulados de manera sencilla.

2.2.7.3 Impacto en la esfera judicial

A raíz del crecimiento de estos delitos, también ha surgido la preocupación de muchos países por legislar estas conductas antijurídicas que están dañando la seguridad de las personas pertenecientes a sus respectivos Estados, estos números países han promulgado leyes para regular esta situación creciente, también actualizaron leyes obsoletas, para que aquellos delitos considerados tradicionales, sean a su vez considerados ilegales en el mundo virtual.

Algunos países cuentan con un grupo especializado en la investigación de estos delitos, como lo son; la Oficina de Investigaciones especiales de la Fuerza Aérea de los Estados Unidos, los Investigadores del Internet de Australia, grupos que son especialistas en el recojo de pruebas.

2.3 Definiciones conceptuales.

- a. **Eficacia.** Capacidad para alcanzar lo que se anhela.
- b. **Ley.** Regla o norma que regulan las conductas de una sociedad, para que esta se encuentre armonizada, cuyo carácter es de obligatorio cumplimiento por quienes pertenecen a esa sociedad.
- c. **Informática.** Información creada y procesada automáticamente a través de un dispositivo electrónico computacional.
- d. **Delito.** Toda conducta ya sea por voluntad propia o imprudencias contrarias al orden legal establecido en una sociedad. (En esencia, acción + típica + antijurídica + culpable)
- e. **Delitos Informáticos.** Toda acción típica antijurídica y culpable cometidos a través de un dispositivo electrónico o computacional,

afectando bienes jurídicos protegidos por la ley como; la integridad, confidencialidad, etc.

2.4 Hipótesis.

2.4.1 Hipótesis general

El nivel de eficacia de la ley de delitos informáticos en el Distrito Judicial de Huánuco, es muy baja, porque siguen incrementándose su infracción por las penas benignas.

2.4.2 Hipótesis específicas

- a. Existen vacíos legales que dificultan la sanción de estos delitos en la ley de delitos informáticos que administra el Distrito Judicial de Huánuco, porque su regulación no es precisa y existen ambigüedades.
- b. El porcentaje de denuncias que obran en las fiscalías penales del Distrito Judicial de Huánuco es un 10% porque las denuncias en su mayoría son archivadas por falta de elementos de convicción.
- c. La diferencia entre la Ley de Delitos Informáticos que se administra en el Distrito Judicial de Huánuco con otras leyes internacionales que sancionan el mismo ilícito penal es que estas últimas son precisas y no existen ambigüedades.

2.5 Variables

2.5.1 Variable de estudio

Delitos informáticos

2.6 Operacionalización de variable (Dimensiones e Indicadores)

VARIABLE	DIMENSIONES	INDICADORES
1. Delitos informáticos	- Regulación legislativa. - Eficacia en el cumplimiento. - Reincidencia.	- Existencia de normas legales para tratar los delitos informáticos. - Regulación de sanciones para los infractores - Atención a las víctimas de delitos informáticos - Celeridad en los procesos - Sanción a los infractores - Denuncias archivadas - Causales de reincidencia - Acciones tomadas contra los reincidentes

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Tipo de investigación

La presente investigación es del tipo básico, “no tiene propósitos aplicativos inmediatos, pues sola busca ampliar y profundizar el caudal de conocimientos científicos acerca de la realidad” (CARRASCO: 2007, p. 43); este tipo de investigación constituye su objeto de estudio las teorías científicas, las mismas que las analiza para perfeccionar sus contenidos.

3.1.1 Enfoque

Mixto, porque se utilizaron de ambos enfoques cualitativo y cuantitativo. “Este tipo de enfoque se caracteriza por utilizar cinco fases similares y relacionadas entre sí; llevan a cabo la observación y evaluación de fenómenos, establecen suposiciones o ideas como consecuencias de la observación, prueban y demuestran el grado de las ideas, revisan las suposiciones sobre la base de pruebas o del análisis y por ultimo proponen nuevas observaciones y evaluaciones para modificar, esclarecer las suposiciones para generar otras” (HERNÁNDEZ: 2003, p.5).

3.1.2 Alcance o nivel

Descriptiva porque consiste en describir un fenómeno o situación mediante el estudio del mismo. “Es decir nos refiere sobre las características, cualidades internas y externas, propiedades y rasgos esenciales de los hechos y fenómenos de la realidad en un momento o tiempo” (CARRASCO: 2007, p. 42)

3.1.3 Diseño

Investigación descriptiva simple. En relación al nivel, buscaremos y recogeremos la información respecto al objeto de estudio y no buscando relacionar ni controlar variables, sino simplemente obtener información para agrandar los conocimientos. “En este tipo de diseño no podemos suponer la influencia de variables extrañas, nos limitamos a recoger la información que nos proporciona la situación” (SÁNCHEZ: 1984, p. 61).

El diseño de este trabajo de investigación descriptiva simple se esquematiza de la siguiente forma:

M

O

Donde:

M: muestra.

O: información que se recogerá de la muestra.

3.2 Población y muestra

3.2.1 Población

La población de estudio de la presente investigación estuvo conformada por los jueces y fiscales del Distrito Judicial de Huánuco.

3.2.2 Muestra

Por ser una población muy extensa y poco accesible solo se tomó 30 a razón de 15 jueces y 15 fiscales del distrito judicial de Huánuco y esta muestra se ha establecido por la técnica muestral **no aleatoria**, por las siguientes razones. Siendo muy extensa y dispersa la población y poco accesible por el tiempo ocupado que manejan se tomó ese número de muestra a criterio propio y conveniencia de la investigación.

3.3 Técnicas e instrumentos para la recolección de datos

3.3.1 Para la recolección de datos

- **Técnica**

La encuesta; se encuestó a los sujetos de muestra, para así obtener la información de manera directa, para analizarlo de acuerdo a los objetivos.

El fichaje; se utilizó esta técnica de manera interna para realizar algunas anotaciones importantes a lo largo de la investigación.

- **Instrumentos**

Cuestionario; se utilizaron cuestionarios con preguntas cerradas dicotómicas, para aplicarlos a los integrantes de la muestra.

Fichas textuales y fichas bibliográficas, se utilizaron estas dos tipos de fichas, la primera para realizar anotaciones extensas de la investigación, la segunda para tomar las citas bibliográficas o los autores que se tomaron para el desarrollo de la misma.

3.3.2 Para la presentación de datos

Se procesaron todos los datos recolectados, en tablas estadísticas no probabilísticas, ya que al ser una investigación mixta, se trabajó con los porcentajes de los datos obtenidos. Para lo cual se utilizó el programa IBM SPSS STATISTICS 23.

3.3.3 Para el análisis e interpretación de los datos

Los datos obtenidos fueron interpretados y analizados en relación a los objetivos que se planteó en la investigación y según al marco teórico del mismo el cual sirvió como fundamento.

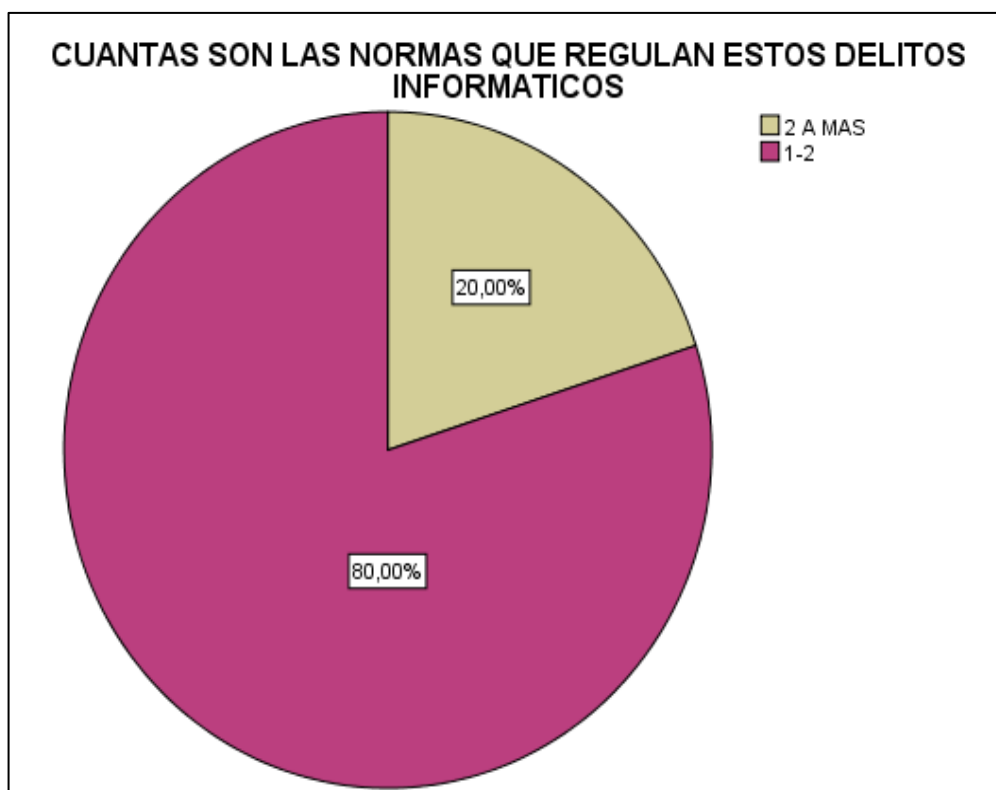
CAPÍTULO IV RESULTADOS

4.1 Procesamiento de datos

CUADRO N° 1

Normas que regulan los delitos informáticos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	2 A	6	18,8	20,0	20,0
	MAS				
	1-2	24	75,0	80,0	100,0
	Total	30	93,8	100,0	
Perdido	Sistema	2	6,3		
s					
Total		32	100,0		



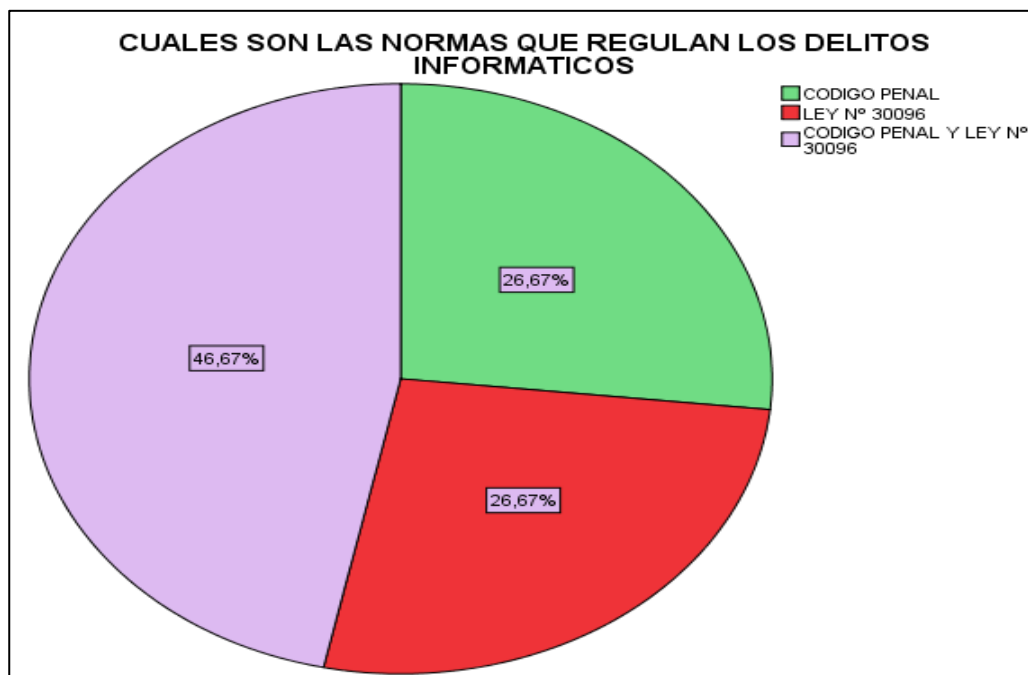
Interpretación

Del total de encuestados, 6 (20%), dicen que son de 2 a más las normas vigentes que regulan los delitos informáticos; en cambio 24 (80%) que solo existen de 1 a 2 normas vigentes.

CUADRO N° 2

Clases de normas que regulan los delitos informáticos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	CODIGO PENAL	8	25,0	26,7	26,7
	LEY N° 30096	8	25,0	26,7	53,3
	CODIGO PENAL Y LEY N° 30096	14	43,8	46,7	100,0
	Total	30	93,8	100,0	
Perdidos	Sistema	2	6,3		
Total		32	100,0		



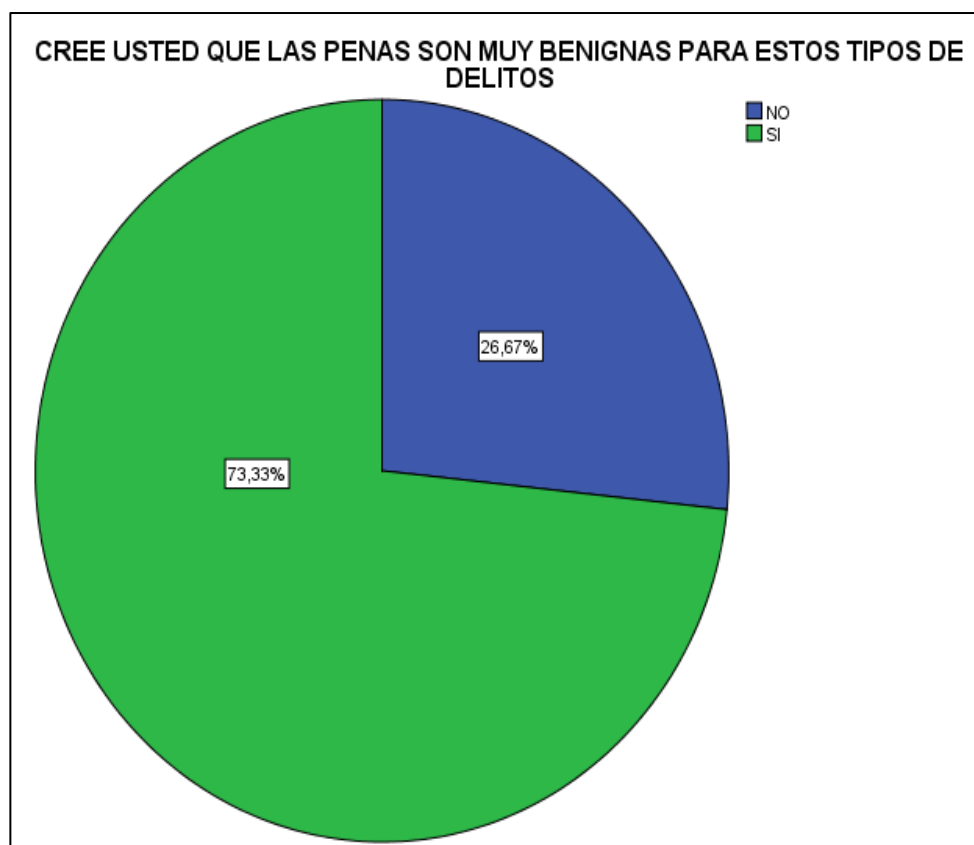
Interpretación

En lo referente a cuales son las normas que regulan los delitos informáticos del total de encuestados un 46, 67 % respondieron que es la Ley N° 30096 la que la regula, un 26, 67% que es el Código penal que la regula, y, un 26,67% ambas, es decir el Código Penal y la ley 30096.

CUADRO N°3

Cree que las penas son muy benignas para estos delitos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	8	25,0	26,7	26,7
	SI	22	68,8	73,3	100,0
	Total	30	93,8	100,0	
	Sistema				
Perdido		2	6,3		
s					
Total		32	100,0		



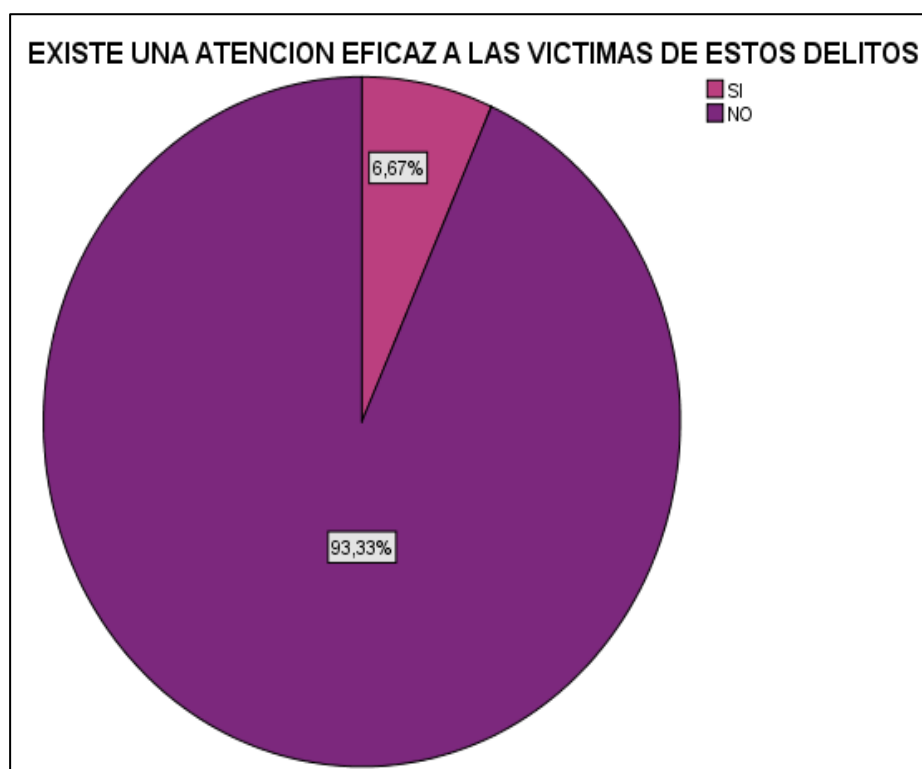
Interpretación

Respecto a que si las penas son muy benignas para estos tipos de delitos del total de encuestados un 73, 33% respondieron que sí, creían que eran muy benignas; y, un 26, 67% dijeron que no eran muy benignas.

CUADRO N° 4

Atención eficaz a las víctimas de delitos informáticos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	2	6,3	6,7	6,7
	NO	28	87,5	93,3	100,0
	Total	30	93,8	100,0	
Perdido	Sistema	2	6,3		
s					
Total		32	100,0		



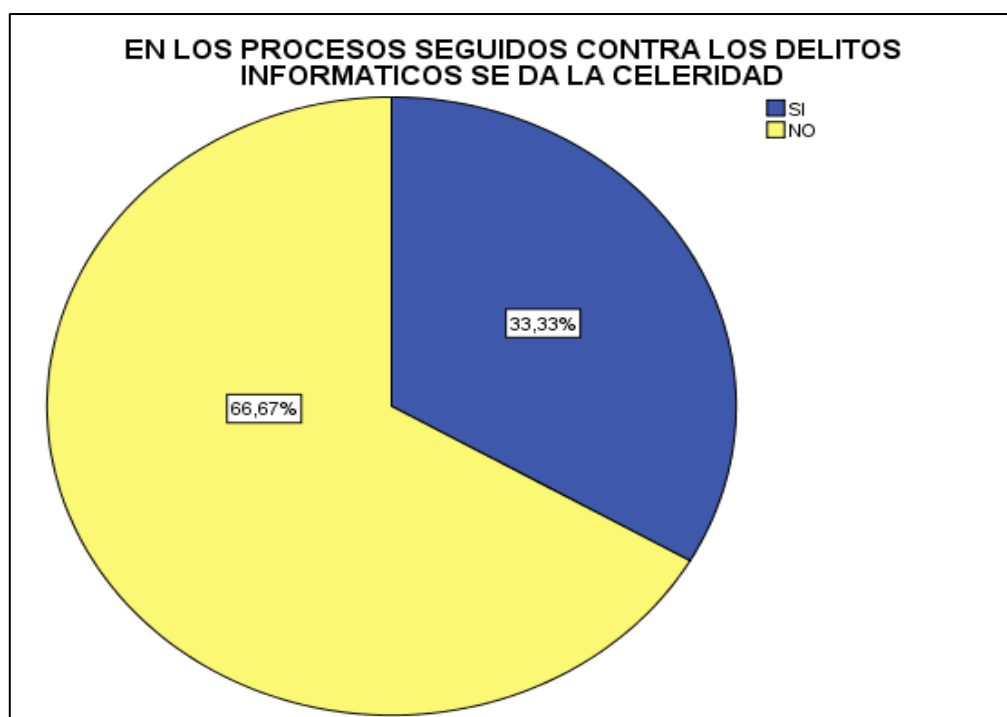
Interpretación

En cuanto a esta pregunta del total de encuestados un 93, 33% dijeron que no existe una atención eficaz a las víctimas de estos delitos, y, un 6, 67% que sí.

CUADRO N° 5

Celeridad en los procesos seguidos contra los delitos informáticos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	10	31,3	33,3	33,3
	NO	20	62,5	66,7	100,0
	Total	30	93,8	100,0	
Perdidos	Sistemas	2	6,3		
Total		32	100,0		

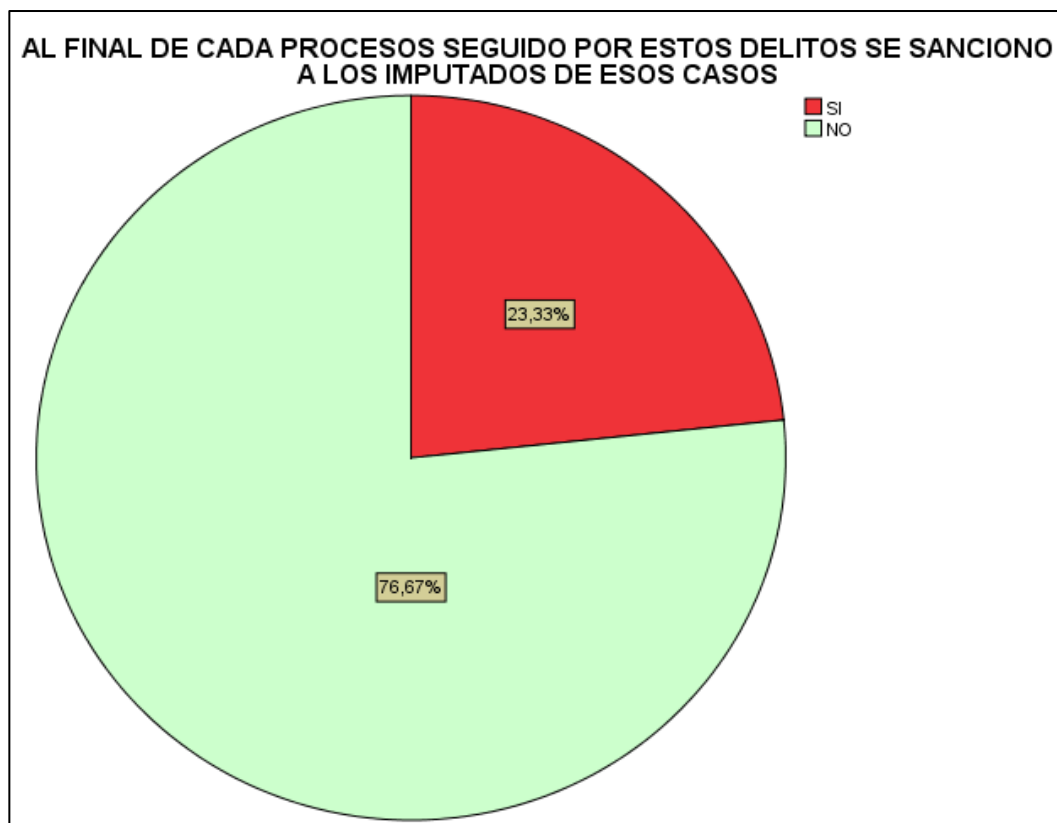


Interpretación

En cuanto a esta interrogante del total de encuestados un 66, 67% dieron respuesta negativa, es decir a que no existe celeridad en estos procesos seguidos contra los delitos informáticos, y, un 33, 33% que si existía celeridad en estos procesos.

CUADRO N° 6
Sanción a los imputados por los delitos informáticos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	7	21,9	23,3	23,3
	NO	23	71,9	76,7	100,0
	Total	30	93,8	100,0	
Perdido	Sistema	2	6,3		
s					
Total		32	100,0		



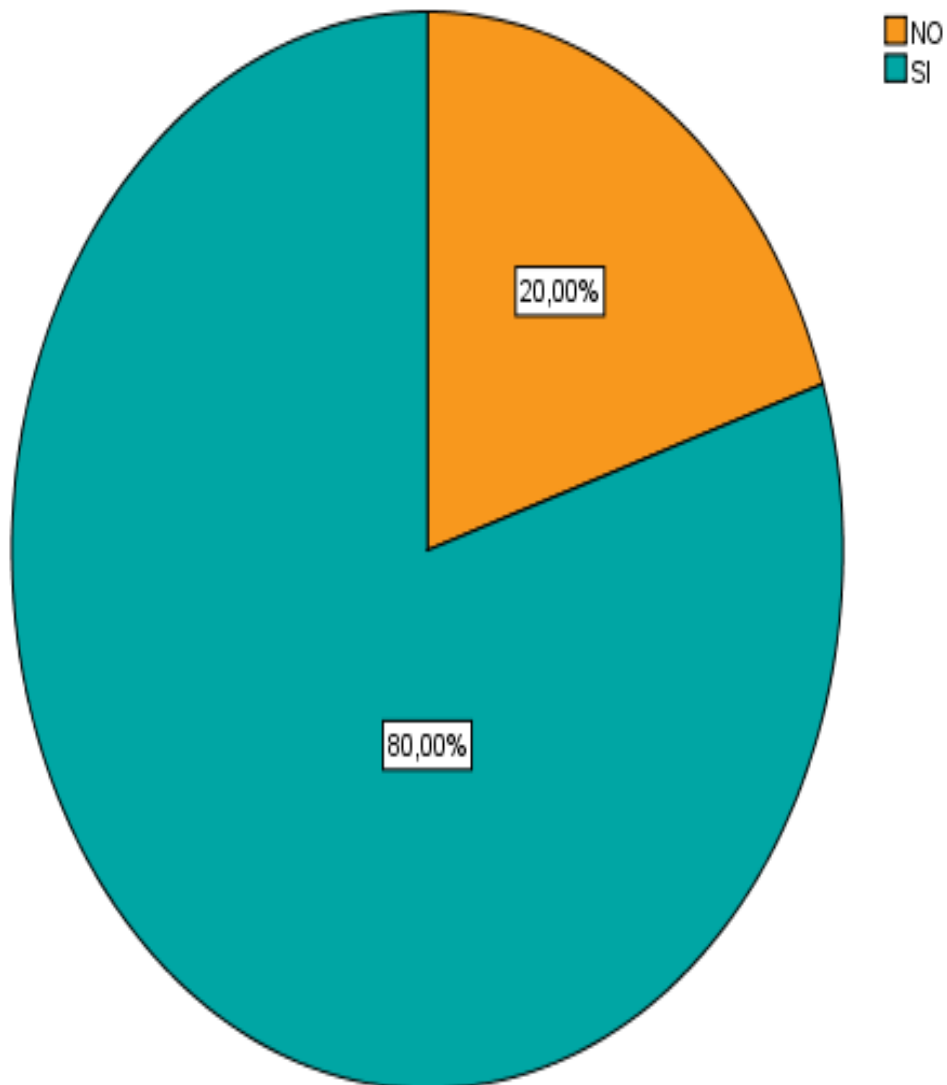
Interpretación

Respecto a esta pregunta del total de encuestados un 76, 67% dicen que no se sancionaron a los imputados de estos casos, y, un 23, 33% que si se sancionaron.

CUADRO N° 7
Archivamiento de denuncias sobre delitos informáticos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	6	18,8	20,0	20,0
	SI	24	75,0	80,0	100,0
	Total	30	93,8	100,0	
Perdido	Sistema	2	6,3		
Total		32	100,0		

SE ARCHIVAN MUCHAS DENUNCIAS SOBRE ESTOS CASOS DE DELITOS INFORMATICOS



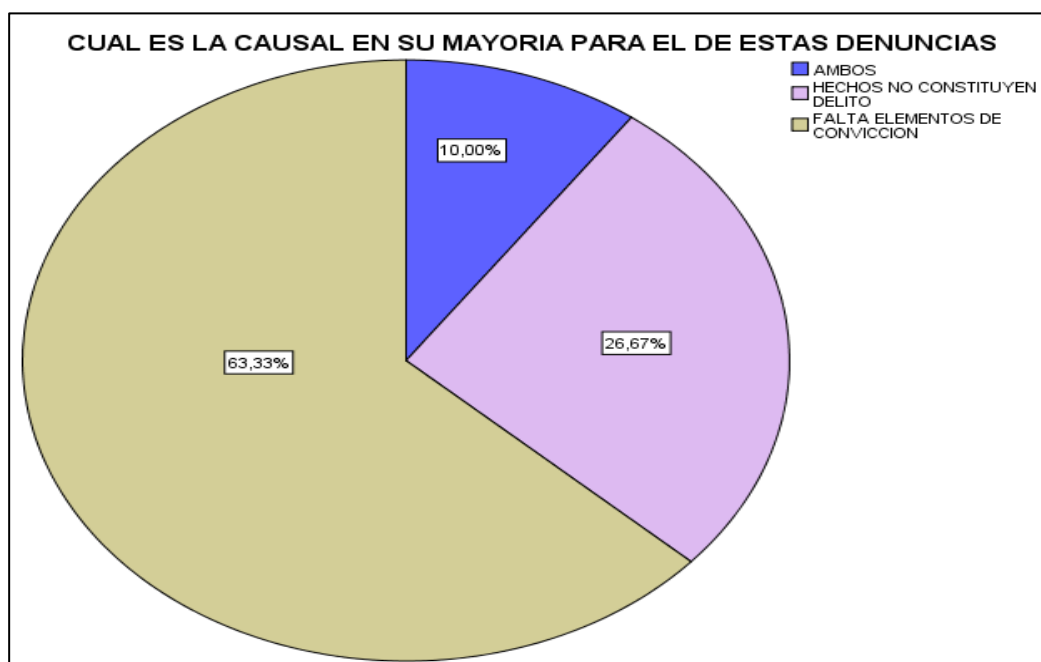
Interpretación

En cuanto a que si muchas denuncias se archivan sobre estos casos de delitos informáticos del total de encuestados un 80% refieren que sí, y, un 20% que no se archivan.

CUADRO N° 8

Causal para el archivamiento de denuncias

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	AMBOS	3	9,4	10,0	10,0
	HECHOS NO CONSTITUYEN DELITO	8	25,0	26,7	36,7
	FALTA ELEMENTOS DE CONVICCION	19	59,4	63,3	100,0
	Total Sistema	30	93,8	100,0	
Perdidos		2	6,3		
Total		32	100,0		



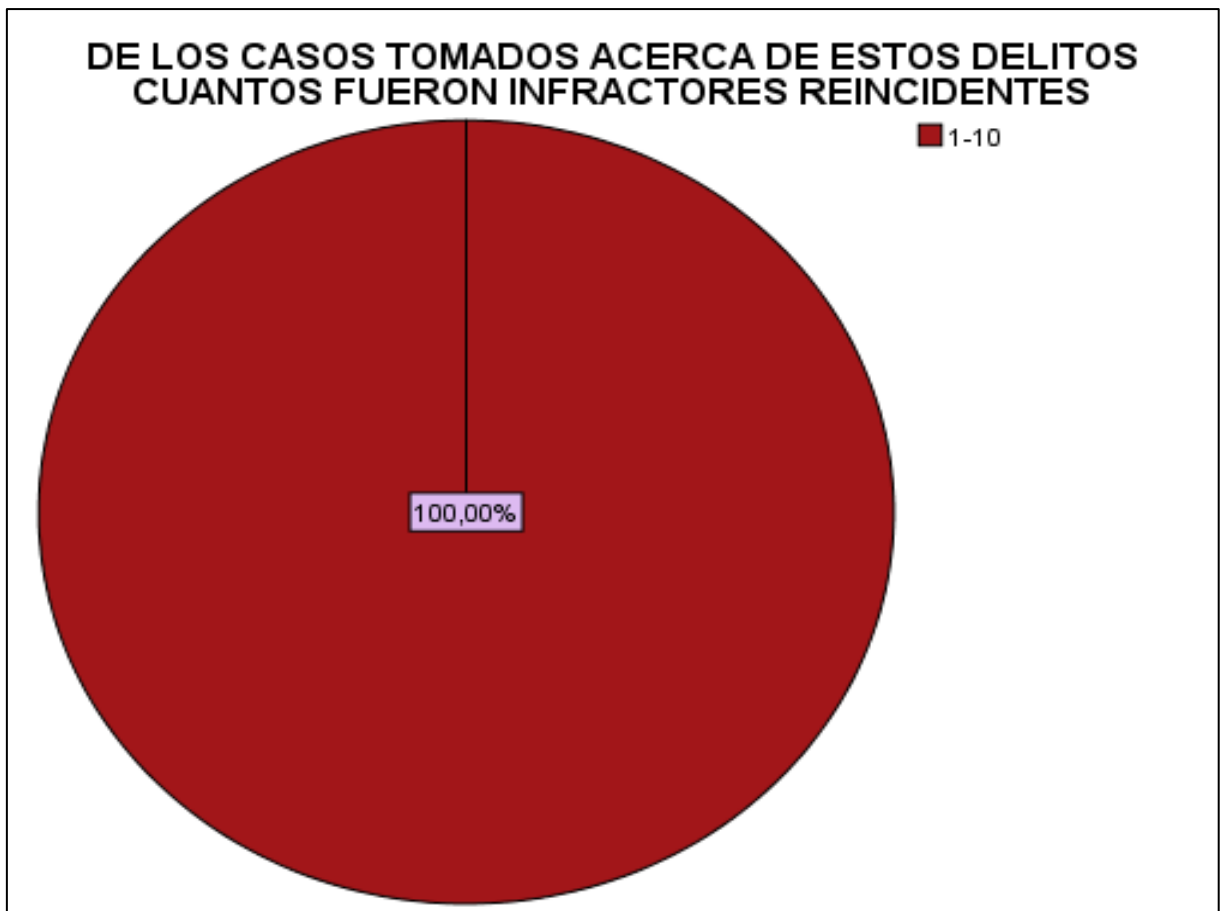
Interpretación

Del total de encuestados un 63, 33% dijeron que la causal frecuente para el archivamientos de estos denuncias es que en los casos presentados faltan elementos de convicción, un 26, 67% que los hechos presentados no constituyen delito, y, por último un 10% ambos causales concurren para que se archiven las mismas.

CUADRO N° 9

Infractores reincidentes en delitos informáticos

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido 1-10	30	93,8	100,0	100,0
Perdido Sistema	2	6,3		
Total	32	100,0		



Interpretación

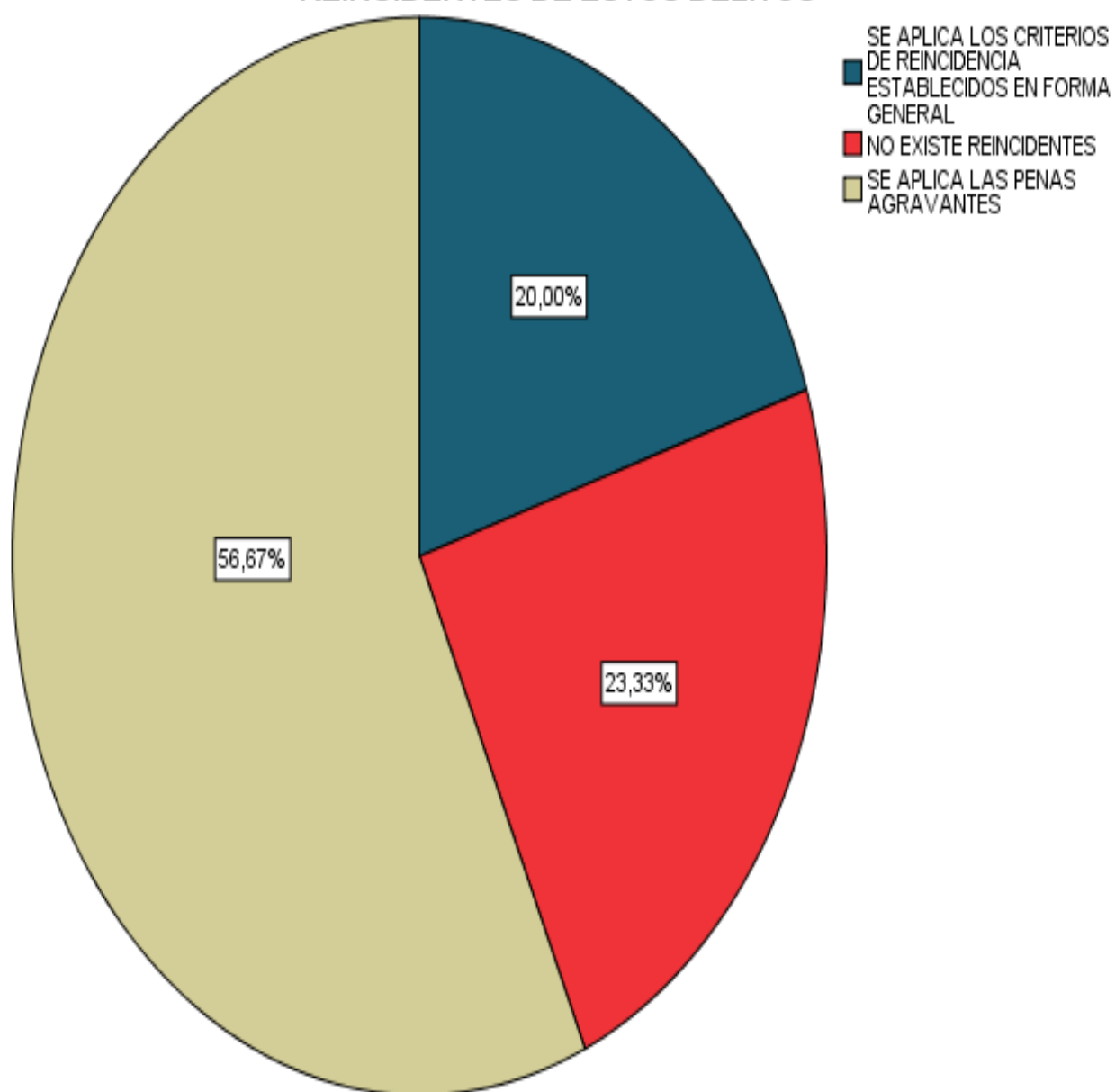
Respecto a esta interrogante, todos los encuestados, es decir un 100% respondieron unánimemente que son de 1 a 10 los infractores reincidentes que se dan en estos tipos de delitos.

CUADRO N° 10

Acciones que se toman en su despacho para tratar a los reincidentes de delitos informáticos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	-SE APLICA LOS CRITERIOS DE REINCIDENCIA ESTABLECIDOS EN FORMA GENERAL	6	18,8	20,0	20,0
	-NO EXISTE REINCIDENTES	7	21,9	23,3	43,3
	-SE APLICA LAS PENAS AGRAVANTES	17	53,1	56,7	100,0
	Total	30	93,8	100,0	
	Sistema	2	6,3		
Perdidos					
Total		32	100,0		

QUE ACCIONES SE TOMAN EN SU DESPACHO PARA TRATAR A LOS REINCIDENTES DE ESTOS DELITOS



Interpretación

Por último respecto a que acciones se tomaban en sus despacho para tratar a los reincidentes un 57, 67% dijeron que se aplica las penas agravantes, 23, 33% dijo que no existen reincidentes en su despacho, y un 20, 00% dijo que se aplican los criterios de reincidencia establecidos de forma general para todos los delitos.

4.2 Contrastación de hipótesis

4.2.1 Hipótesis general

Hg. El nivel de eficacia de la ley de delitos informáticos en el Distrito Judicial de Huánuco, es muy baja, porque siguen incrementándose su infracción por las penas benignas.

Los datos obtenidos de la encuesta, nos indica que en realidad la ley N° 30096 ley de delitos informáticos que se administra en el distrito judicial de Huánuco es ineficaz, primero porque su tipificación no es precisa, segundo la ley no está debidamente implementada, y al no existir la parte logística o instrumentos adecuados para su investigación no puede ser perseguible tal delito.

En cuanto a que si las penas son benignas de los resultados obtenidos podemos indicar que si son benignas dichas penas aplicadas para estos tipos de delitos.

4.2.2 Hipótesis específicos

H1. Existen vacíos legales que dificultan la sanción de estos delitos en la ley de delitos informáticos que administra el Distrito Judicial de Huánuco, porque su regulación no es precisa y existen ambigüedades.

En base a los resultados obtenidos de la encuesta podemos indicar que efectivamente, existen, vacíos legales que dificultan la sanción de estos delitos, esto al no ser precisos en la tipificación de los hechos delictivos, razón por la cual en el Distrito Judicial de Huánuco al momento de ver estos casos, no optan por aplicar la ley N° 30096, sino las del Código Penal, adecuando las conductas infractoras con las que se tipifican en el Código y no con las que deberían ser regulados por dicha ley.

H2. El porcentaje de denuncias que obran en las fiscalías penales del Distrito Judicial de Huánuco es un 10% porque las denuncias en su mayoría son archivadas por falta de elementos de convicción.

Según a la encuesta realizada un 80% manifestó que si se archivan las denuncias en los despachos fiscales, a razón de, un 63, 33% porque faltan elementos de convicción para formalizar las denuncias, esto no porque los fiscales no sepan realizar su trabajo, sino, que al no contar con los instrumentos tecnológicos avanzados para su investigación, les dificulta continuar con la

misma para realizar la denuncia formalmente ante un magistrado; un 26, 67% porque los hechos denunciados ante los fiscales, no constituyeron delito, dado que la ley al no tipificar precisamente las conductas infractoras, dejando así vacíos legales imposibilitan la sanción de las mismas.

H3. La diferencia entre la Ley de Delitos Informáticos que se administra en el Distrito Judicial de Huánuco con otras leyes internacionales que sancionan el mismo ilícito penal es que estas últimas son precisas y no existen ambigüedades

Según a la investigación realizada externamente, para dar respuesta a esta hipótesis, se indican las siguientes diferencias:

Con **Estados Unidos**; este país no solo es adelantado en tecnología, sino también en las leyes y para corroborar ello, con la dación del **Acta Federal de Abuso Computacional** (18 U.S.C. Sec. 1030) que modificó al **Acta de Fraude y Abuso Computacional de 1986**. Este país no se preocupa en definir lo que es un delito informático, ellos optan por describir el acto para no dar cabida a estos delitos, lo que lo diferencia con nuestra legislación, tipificando lo presente y no previniendo en un futuro, otra de las diferencias es que en cuanto a sus penas estipuladas en la ley estadounidense es que ello son más severos para aquellos que actúan con dolo, a quienes se les impone una pena mínima de 10 años, hecho que también lo diferencia con nuestra legislación nacional al contar en su ley con penas no tan drásticas, cuyas penas van desde un mínimo de 1 año y un máximo de 10 años.

Con **ALEMANIA**, este país sancionó, el espionaje de datos, fraude informático, sabotaje informático y la alteración de datos en 1986 con la ley denominada **Contra la Criminalidad Económica**. Conductas típicas que no se encuentran incluidas en nuestra legislación.

Con **AUSTRIA, GRAN BRETAÑA y HOLANDA**, estos últimos tres países penalizan el hacking, preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio) así como la puesta en circulación de virus, regulación que no se encuentra en la Ley N° 30096.

CAPÍTULO V

DISCUSIÓN DE RESULTADOS

5.1 Análisis de los resultados

Según a la contratación de los resultados se establece que la ley de delitos informáticos que se administra en el distrito judicial de Huánuco es ineficaz, primero porque su tipificación no es precisa, segundo la ley no está debidamente implementada, y al no existir la parte logística o instrumentos adecuados para su investigación, la persecución y sanción de este delito es muy complicado por no decir imposible.

Otro de los temas de gran preocupación es que al no ser precisa esta ley, y no regular todas las conductas infractoras, los delincuentes informáticos tienen una salvedad, quedando impunes frente a sus actos delictivos, esto porque las políticas criminológicas acerca de este delito planteadas en nuestra legislación peruana se encuentran desfasados en cuanto a una realidad tecnológica actual, lo que se evidencia en la falta de preparación para su persecución legal por parte de las entidades persecutoras de estos delitos. Lo que genera una gran preocupación para toda la población.

De los resultados obtenidos de la encuesta también se observa que, la mayoría de fiscales, no adecuan correctamente el tipo penal, esto porque se han dado casos como violación a la intimidad por redes sociales, y fue adecuado al tipo penal de coacción, como se puede observar no se ajustó correctamente al tipo penal que corresponde para estos delitos sino, un artículo de delitos comunes del Código Penal, lo cual denota la mala adecuación que hace el persecutor del delito frente a un hecho delictivo que merece un trato especial según la ley dada para estos delitos, pero al no ser precisa esta ley, provoca ambigüedad y confusión a los operadores de justicia. Y así otros casos particulares, a las cuales no se dieron el tratamiento adecuado, a la actualidad, en nuestra ciudad existe desconocimiento en los despachos tanto judiciales como fiscales respecto a este tema desafiante para el derecho, esto porque no se ha difundido, ni profundizado estos conocimientos.

Sabemos que todo lo concerniente a la tecnología es un campo nuevo para muchas personas, dada la naturaleza virtual de los delitos informáticos resulta

difícil su tratamiento y a su vez su tipificación. Lo cierto es que si no se actúa con inmediatez, y no buscamos alternativas nuevas de soluciones frente a este mal social, los delincuentes mejores preparados en este campo nos seguirán llevando la delantera, burlando todos los estándares propuestos para todos estos casos de delitos cibernéticos.

CONCLUSIONES

- La primera conclusión a la que se abordó con esta investigación es que la ley de delitos informáticos que se administra en el distrito judicial de Huánuco, tiene un nivel bajo de eficacia, esto a raíz de su imprecisión al regular la conducta infractoras.
- Segundo, que no existen Juzgados especializados para la aplicación de la ley antes mencionada, lo cual viene causando mucha confusión en los administradores de justicia.
- Tercero, no existe un área de logística, para la investigación de estos delitos, ni capacitaciones para su tratamiento especial, cuando estos se presenten.
- Cuarto, es evidente que tanto los fiscales como jueces no tienen ninguna capacitación especial en estos temas, razón por la que se dejan de sancionar dichos delitos como tales; dándoles un proceso distinto a lo de su naturaleza.
- Estos delitos en nuestra ciudad aun no son frecuentes, tanto a nivel fiscal como judicial.

RECOMENDACIONES

- Si bien se observa a lo largo de esta investigación que la ley muestra las inconsistencias en la tipificación de las conductas esto puede llevar a mostrar una imagen “simbólica” de la intervención penal en esta materia; ya que tenemos una ley regulando esta problemática jurídica y social, lo que debemos hacer para mejorarla es implementarla correctamente de acuerdo a las necesidades de las mismas. Tomando el ejemplo estadounidense, tipificando acciones futuras, así prevendremos y estaremos un paso más adelante que la criminalidad.
- Es evidente que al no existir una capacitación adecuada, ni los instrumentos requeridos para investigar estos delitos, se debe promover con prontitud un área especializada con estos, tales como: perito especializados, máquinas a la vanguardia de la tecnología, que permitan la rápida y eficaz intervención al infractor.
- Y para hacer efectivo lo anterior, se debe implementar un Juzgado especializado en delitos informáticos para el correcto proceso, con la celeridad debida en la atención a las víctimas de estos delitos.
- Es importante también que tomemos el ejemplo de Colombia donde existe una institución especializada en este tema, que brinda constantes capacitaciones en este área para los administradores de justicia, lo cual sería muy beneficioso imitar para que de este modo nos encontremos prevenidos frente a estos nuevos hechos delincuenciales, y así mismo darles un tratamiento correcto desde su investigación, hasta la obtención de una sanción eficazmente sancionadora.
- Y por último, algunos países han tomado la magnífica idea de unirse a unos tratados internacionales que unifican las leyes en cuanto a estos tipos de delitos, estos empiezan desde una definición legal de dichas conductas delictivas, así ,mismo la especialización que deberían tener los policías para investigar estos casos, los fiscales y demás administradores de justicia para hacer efectiva una sanción, la instauración de tratados que permitan la extradición de estos infractores de la ley para que de esta manera la sanción traspase fronteras poniéndolas como ejemplo de sanción efectiva para todos aquellos infractores que piensan que tras

actuar detrás de una computadora quedaran impunes frente a sus hechos delincuenciales. Esta sería una medida muy eficaz para nuestro Estado para prevenir males futuros como la dación de delitos muy graves que pondrían en una inseguridad total a nuestra sociedad.

REFERENCIAS BIBLIOGRÁFICAS

- BRAMONT, L (2000). “Delitos Informáticos”, en Revista Peruana de Derecho CALDERON, L. (2010). “Delitos informáticos” y Derecho Penal”, México, Ubijus.
- CAMACHO, L (1997). “El delito informático”, Madrid, Gráficas Condor.
- Diario Oficial El Peruano.
- Durand (2002) “Los delitos informáticos en el Código Penal Peruano” en revista Peruana de Ciencias Penales. N° 11, Lima.
- FERNÁNDEZ (2002) “Los delitos informáticos”, Editorial Juristas, Enero.
- MORANT (2003). “Protección penal de la intimidad frente a las nuevas tecnologías”, Valencia Ed. Práctica de Derecho, 2003.
- VALDÉS T (2003). “Derecho Informático”, 3^{era} ed., Ed. Mac Graw Hill, México,.
- ORTS (2001). “Delitos Informáticos y delitos comunes cometidos a través de la informática”, Valencia, Tirant Lo Blanch.
- VILLAVICENCIO, F. (2013), “Derecho Penal – Parte General”, 4 reemp, Lima, Grijley.

WEBGRAFÍA

- https://issuu.com/universidaddel/docs/tesis_lic_derecho_ever_sanchez_u_la
- https://es.wikipedia.org/wiki/Delito_inform%C3%A1tico
- <http://www.monografias.com/trabajos6/delin/delin.shtml>
- <http://derecho-informado.blogspot.pe/2013/09/tesis-delitos-informaticos.html>
- <https://es.scribd.com/doc/63118627/Plan-de-Tesis-DELITOS-INFORMATICOS>
- http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
- <http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1334/2/Delitos%20en%20las%20Redes%20Sociales.pdf>
- <http://mjv.viegasociados.com/wpcontent/uploads/2011/05/DelitosInformaticos.pdf>

ANEXOS

MATRIZ DE CONSISTENCIA

Eficacia de la ley de los delitos informáticos en el Distrito Judicial de Huánuco 2017

PROBLEMA GENERAL Y ESPECÍFICOS	OBJETIVO GENERAL Y ESPECÍFICOS	HIPÓTESIS GENERAL Y ESPECÍFICOS	VARIABLES	DIMENSIONES	INDICADORES	METODOLOGÍA	TÉCNICAS	INSTRUMENTOS
Problema general: ¿Cuál es el nivel de eficacia de la ley de los delitos informáticos en el Distrito Judicial de Huánuco 2017? Problemas específicos ¿-Existen vacíos legales en la ley de los delitos informáticos que se administra en el Distrito Judicial de Huánuco 2017? ¿-Cuál es el porcentaje de denuncias de delitos informáticos que obran en las fiscalías penales del Distrito Judicial de Huánuco 2017? --Cuál es la diferencia entre la ley de los delitos informáticos que se administra en	Objetivo General Demostrar el nivel de eficacia de la ley de los delitos informáticos en el Distrito Judicial de Huánuco 2017. Objetivos específicos -Identificar los vacíos legales en la ley de los delitos informáticos que se administra en el Distrito Judicial de Huánuco 2017. -Determinar el porcentaje de denuncias de delitos informáticos que obran en las fiscalías penales del Distrito Judicial de Huánuco 2017. -Analizar las diferencias de la ley de los delitos informáticos que se administra en el Distrito Judicial de Huánuco 2017 con otras legislaciones internacionales.	Hipótesis general El nivel de eficacia de la ley de delitos informáticos en el Distrito Judicial de Huánuco, es muy baja, porque siguen incrementándose su infracción por las penas benignas. Hipótesis específicos -Existen vacíos legales que dificultan la sanción de estos delitos en la ley de delitos informáticos que administra el Distrito Judicial de Huánuco, porque su regulación no es precisa y existen ambigüedades. -El porcentaje de denuncias que obran en las fiscalías penales del Distrito Judicial de Huánuco es un 10% porque las denuncias en su mayoría son archivadas por falta de elementos de convicción.	Delitos informáticos	-Regulación legislativa. -Eficacia en el cumplimiento. -Reincidencia	- Existencia de normas legales para tratar los delitos informáticos - Regulación de sanciones para los infractores - Atención a las víctimas de delitos informáticos - Celeridad en los procesos - Sanción a los infractores - Denuncias archivadas - Infractores reincidentes	Tipo -Básico Enfoque -Mixto Nivel -Descriptiva Diseño -Descriptiva simple M O	Encuestas	Cuestionarios Preguntas cerradas

el Distrito Judicial de Huánuco 2017 con otras legislaciones internacionales?		-La diferencia entre la Ley de Delitos Informáticos que se administra en el Distrito Judicial de Huánuco con otras leyes internacionales que sancionan el mismo ilícito penal es que estas son precisas y no existen ambigüedades.			• Causales de reincidencia • Acciones tomadas contra los reincidentes			
---	--	--	--	--	---	--	--	--

ENCUESTA A JUECES Y FISCALES DEL DISTRITO JUDICIAL DE HUÁNUCO, SOBRE DELITOS INFORMÁTICOS

Señores Jueces / fiscales, les solicitamos responder las preguntas que se formulan a continuación que tiene el propósito de conocer de qué manera se atiende los delitos informáticos en este distrito judicial, respuestas que serán utilizadas con fines de investigación académica. Le pedimos responder a todas las preguntas en forma anónima. No hay respuestas buenas ni malas, sino diferentes.

1. DATOS GENERALES

1.1 Cargo que ocupa en el Poder Judicial y/o ministerio Público

- a) Juez () b) Fiscal ()

1.2 PREGUNTAS

1. ¿Cuántas son las normas que regulan estos delitos informáticos?

- a. 1-2 () b. 2 a mas ()

2. ¿Cuáles son estas normas que regulan los delitos informáticos?

3. ¿Cree usted que las penas son muy benignas para estos tipos de delitos?

- a. Si () b. No ()

4. ¿Existe una atención eficaz a las víctimas de estos delitos?

- a. Si () b. No ()

5. ¿En los procesos seguidos contra los delitos informáticos se da la celeridad?

- a. Si () b. No ()

6. ¿Al final de cada proceso seguido por estos delitos se sancionó a los imputados de esos casos?

- a. Si () b. No ()

7. ¿Se archivan muchas denuncias sobre estos casos de delitos informáticos?
- a. Si () b. No ()
8. ¿Cuál es la causal en su mayoría para el archivamiento de estas denuncias?
9. ¿De los casos tomados acerca de estos delitos cuantos fueron infractores reincidentes?
- a. 1 a 10 () b. 10 a 20 ()
10. ¿Qué acciones se toman en su despacho para tratar a los reincidentes de estos delitos?