UNIVERSIDAD DE HUANUCO

FACULTAD DE DERECHO Y CIENCIAS POLITICAS

UDH

UNIVERSIDAD DE HUANUCO

DELITOS INFORMÁTICOS COMETIDOS A TRAVÉS DE REDES SOCIALES Y SU TRATAMIENTO EN EL MINISTERIO PUBLICO EN LA CIUDAD DE HUÁNUCO, 2016.

TESIS PARA OBTAR EL TITULO PROFESIONAL DE ABOGADO

TESISTA:

Bach. ROMERO OCAMPO, Meylin Del Pilar

ASESOR:

Dr. Aguirre Soto, Luis Feliciano

HUÁNUCO- PERÚ

ABRIL- 2017

DEDICATORIA

La presente tesis se la dedico a Dios y a mi mamá

Que siempre estuvo a mi lado y nunca

Perdió la fe

AGRADECIMIENTO

Agradezco a Dios y a mi mama, a mi esposo Aris

Que siempre han estado a mi lado luchando

Para poder sacar mi titulo

INDICE

RESUMEN

Objetivo: Determinar los delitos informáticos cometidos a través de las redes sociales y el tratamiento que le brinda el Ministerio Publico en la ciudad de Huánuco, 2016.

Metodología: observacional, prospectivo, transversal, descriptivo.

Conclusion: Los delitos informáticos más frecuentes fueron la Alteración, daño o destrucción de base de datos; el Tráfico ilegal de datos; el Atentado a la integridad de datos informáticos; el Atentado a la integridad de sistemas informáticos; las 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. El Tratamiento de los delitos informáticos presentados en el Ministerio Publico en la ciudad de Huánuco, fue de la siguiente manera: un 57,9% fueron archivados y un 42,1% terminaron en un proceso normal y con la sentencia dictada.

INTRODUCCION

Cuando se plantea el tema del estado general de la justicia en Perú, se suele decir que el problema no radica en la falta de leyes, sino en el incumplimiento de las leyes ya vigentes. Esta declaración es verdadera tanto para la seguridad ciudadana como para otros aspectos de la ley. Sin embargo, los avances y el uso de la tecnología han presionado al legislador para que promulgue más leyes o al menos para actualizar las vigentes.

En este sentido, durante el año pasado se han desarrollado discusiones sobre los diferentes comités y organizaciones auxiliares del Congreso Nacional para elaborar un proyecto de ley sobre delitos informáticos. Se dio un primer paso con la propuesta Ley de Delitos Informáticos [pdf] elaborada por el congresista Juan Carlos Eguren.

A finales de 2011, el abogado Luis Miguel Reyna Alfaro pronunció un discurso sobre la ley propuesta en un evento académico en el que discutió el estatus legal de los delitos informáticos en Perú. El blog ICJ: Instituto de Capacitación Jurídica, publicó el discurso, cuyas conclusiones críticas afirman: Si bien la intención de actualizar nuestras leyes penales a la luz de las nuevas tecnologías de la información es plausible, la identificación incorrecta del derecho legal y las inconsistencias en la clasificación de la conducta pueden demostrar una intervención criminal "simbólica" en este asunto. Por lo tanto, es necesario sugerir cambios al texto jurídico actual que no sólo son teóricamente coherentes, sino que son los más eficaces en la protección de la información. Esta es la única manera de

justificar el uso del derecho penal, que, como bien sabemos, es la rama del derecho que incurre en las consecuencias más drásticas.

Posteriormente, el presidente de la Comisión de Justicia y Derechos Humanos del Congreso hizo algunas aclaraciones a las dudas planteadas por el puesto anterior, pero sus explicaciones no fueron del todo satisfactorias e incluso tomaron otro enfoque, como explica Morachimo en otro post, en el que Añade: Consultado sobre los hechos por el Diario 16, el Presidente de la Comisión de Justicia y Derechos Humanos amplió sus descargas refiriéndose a este blog. Aparentemente, los blogs no tienen derecho a opinar sobre este tema salvo que directamente interesados. "Quisiera hacer otra aclaración. Me parece muy sospechoso que un blogue se tome el trabajo y el tiempo de revisar este predictamen. Esta es la preocupación más importante que las personas que cometen delitos informáticos, puede ser aquí donde comienza el 'vestíbulo' de las personas a las que perjudica que esta ley se promulgue ", finalizó el congresista.

La presente tesis pretende describir los comportamientos que se pueden reconocer como delitos informáticos en dichas redes y como se está adecuando la normatividad en el Perú a este crecimiento constante de las tecnologías de información y comunicación para prevenir, proteger y establecer un adecuado manejo. Para concluir que las nuevas prácticas delictivas en nuestro país están a la mano de la aplicación de los avances tecnológicos, pero a pesar de esto en el Perú existen las bases legales a partir de las cuales se puede empezar a combatir las diferentes modalidades de delitos informáticos, analizando e interpretando la norma existente para identificar su alcance, obteniendo así elementos de juicio para desarrollar políticas y estrategias en este tema. En base a la anterior descripción

nuestro propósito de la presente investigación fue determinar los delitos informáticos cometidos a través de las redes sociales y saber qué tipo de tratamiento le brinda el Ministerio Publico en la ciudad de Huánuco.

CAPÍTULO I

PROBLEMA DE INVESTIGACIÓN

1.1. Descripción del Problema

Las actividades informáticas delictivas están en crecimiento a nivel global, incluyendo a América Latina. El delito cibernético es el mal uso de Internet. Los delitos cibernéticos son "Delitos que se llevan a cabo contra personas o encuentros de persona con un proceso de pensamiento criminal para dañar deliberadamente la integridad de la persona explotada o razón física o daño mental a la persona victimizada directamente o de una manera indirecta, utilizando tecnologías de vanguardia de telecomunicaciones de Sistemas, por ejemplo, Internet (salas de chat, mensajes, Hojas de aviso y reuniones). Dichos actos ilícitos pueden socavar una la seguridad del país y el bienestar presupuestario. Cuestiones que abarcan este tipo de actos criminales han terminado prominentes, especialmente aquellos que abarcan la ruptura, invasión de los derechos de autor, Hay problemas adicionales de protección cuando los datos privados se pierden o se bloquean, legal o en general. (Palazzi, 2000).

El incremento de tecnología disponible, tanto para el delincuente como las víctimas, combinado con el escaso conocimiento o información sobre cómo protegerse de los posibles delitos que se pueden sufrir a través de las nuevas tecnologías, otorga a los delincuentes las llaves a las puertas de un inmenso campo fértil de potenciales víctimas de ataques. Por otro lado, el crecimiento sostenido del mercado negro de la información, funciona como motor que impulsa una importante

masa de ataques informáticos, principalmente destinados a obtener bases de datos con información personal. De acuerdo a uno de los estudios de mayor relevancia mundial en delitos informáticos, en el cuál se han entrevistado más de 13.000 adultos en 24 países, para el año 2012, se calculó que los costos directos asociados con los delitos informáticos que afectan a los consumidores en el mundo ascendieron a US$ 110.000 billones en doce meses. El mismo estudio revela que por cada segundo 18 adultos son víctimas de un delito informático, lo que da como resultado más de un millón y medio de víctimas de delitos informáticos cada día, a nivel mundial (Temperini, 2013).

En un contexto de incremento de la ciberdelincuencia organizada a nivel mundial, los llamados “paraísos legales informáticos”, son los considerados al momento de ejecución de estas actividades. En palabras del Dr. Marcelo Riquert , habida cuenta de las posibilidades que brindan las nuevas tecnologías de la comunicación y la aparición en escena de un nuevo espacio, el virtual o ciberespacio, en materia de delincuencia, facilitando la afectación de bienes jurídicos a una distancia y con una velocidad impensadas, resulta un lugar común la afirmación de estar en presencia de una problemática frente a la que el proceso de homogeneización legislativa y de cooperación en los ámbitos sustantivos y adjetivos, es una necesidad ineludible si se quiere evitar la existencia de "paraísos" de impunidad (RIQUERT, 2011).

La variedad, amplitud y complejidad de los sistemas de información que adquieren, requieren o encuentran disponibles las organizaciones actuales, junto a la dinámica del permanente cambio observado en las tecnologías de la información y las comunicaciones, han impulsado de múltiples formas y, al mismo tiempo,

condicionado las grandes transformaciones de las organizaciones, los mercados y el mundo de la modernidad y de la posmodernidad. Son cambios que, además de sus innegables ventajas, han traído simultáneamente para las personas y las organizaciones, amenazas, riesgos y espectros de incertidumbre en los escenarios de internet, intranet, desarrollo tecnológico, gestión de la información, la comunicación y los sistemas (Álvarez Marañón & Pérez García, 2004).

Con cada vez mayor frecuencia y mayor impacto, los dispositivos de almacenamiento y procesamiento de información –llámense servidores, estaciones de trabajo o simplemente PC– son vulnerados en sus elementos más sensibles, dejando expuestos no sólo múltiples y significativos datos de distinto valor (financiero, crediticio, estratégico, productivo…), sino los mismos patrimonios reales de personas y organizaciones y, aún más, su dignidad, su honra y su vida. Con el avance de la tecnología informática y su influencia en casi todas las áreas de la vida social y empresarial, han surgido comportamientos ilícitos llamados de manera genérica delitos informáticos, que han abierto un amplio campo de riesgos y también de estudio e investigación, en disciplinas jurídicas y técnicas, pero especialmente en aquellas asociadas con auditoría de sistemas o auditoría informática. En este documento se describen los antecedentes y el origen del fenómeno en su dimensión delictiva, junto con el concepto de diversos autores y autoridades nacionales e internacionales que han estudiado y enfrentado el tema y que hoy sirven de apoyo para contextualizar su impacto en el ámbito informático y jurídico y, por supuesto, en el social y económico (Ojeda Pérez J. E., 2010).

A partir del acelerado incremento en las posibilidades de interrelación global por el uso de la comunicación satelital (la internet, el correo electrónico, los teléfonos

celulares, las redes sociales…), las personas y las organizaciones privadas y públicas han quedado expuestas, por las vulnerabilidades de los sistemas de intercomunicación y manejo de la información y por la falta de preparación y de cuidado en su uso, al progresivo y peligroso impacto de la ciberdelincuencia (Ojeda Pérez J. E., 2010).

1.2. Formulación del Problema.

1.2.1. Problema Principal

¿Cuáles son los delitos informáticos cometidos a través de las redes sociales y que tratamiento le brinda el Ministerio Publico en la ciudad de Huánuco, 2016?

1.2.2. Problemas Específicos

- ✓ ¿Cuáles son los delitos informáticos cometidos a través de las redes sociales en el Ministerio Publico en la ciudad de Huánuco, 2016?
- ✓ ¿Cuál es el tratamiento de los delitos informáticos presentados en el Ministerio Publico en la ciudad de Huánuco, 2016?

1.3. Objetivo General

Determinar los delitos informáticos cometidos a través de las redes sociales y el tratamiento que le brinda el Ministerio Publico en la ciudad de Huánuco, 2016.

1.4. Objetivos Específicos

- ✓ Identificar los delitos informáticos cometidos a través de las redes sociales en el Ministerio Publico en la ciudad de Huánuco, 2016.
- ✓ Identificar el tratamiento que se le brinda a los delitos informáticos presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.

1.5. Justificación de la investigación

El espacio cibernético es el dominio generado a partir de la interconexión entre ordenadores y redes de telecomunicaciones para almacenar, modificar e intercambiar datos a través de sistemas en red e infraestructuras físicas asociadas sin tener en cuenta la geografía física. Por lo tanto, su seguridad depende en gran medida de los datos y la seguridad de las TIC.

En realidad, debido a la gran dependencia del ciberespacio de la informática y las telecomunicaciones para casi todas las actividades y servicios, es extremadamente peligroso ignorar el creciente fenómeno de los delitos cibernéticos y el creciente número de amenazas a la vida ciudadana, las actividades ciudadanas y los sistemas gubernamentales.

Las fuentes de amenazas cibernéticas pueden ser accidentes no intencionales, o debido a vulnerabilidades y negligencia. Sin embargo, también pueden ser intencionales, como ataques directos a sistemas. Los objetivos de los atacantes de sistemas pueden ser cerrarlos, acceder a estos sistemas y robar datos cruciales, hacer transferencias financieras ilegales, interrumpir registros o manipular datos y código para introducir instrucciones dañinas. Los atacantes pueden ser hackers recreativos, crackers o terroristas. Esto puede suceder para las entidades e intereses empresariales, así como para el sector público y el gobierno.

Las instituciones bancarias, la energía, las agencias estatales, los hospitales, los negocios, la educación e incluso los asuntos sociales dependen en gran medida de su presencia en línea.

Con la información fluyendo a través de los límites de los diferentes sistemas legales conectados a diferentes redes alrededor del mundo, existe una creciente necesidad de proteger la información personal, fondos y activos, así como la seguridad nacional.

Por lo tanto, las cuestiones de seguridad cibernética están ganando interés tanto por el sector público como por el privado.

En base a la anterior descripción nuestro propósito de la presente investigación es poder determinar los delitos informáticos cometidos a través de las redes sociales y saber qué tipo de tratamiento le brinda el Ministerio Publico en la ciudad de Huánuco.

1.6. Limitaciones de la investigación

- ✓ La limitación de los recursos económicos, pues el presupuesto que sea aprobado puede modificar las características del tiempo de estudio, la recolección de los instrumentos por parte de los encuestadores dependerá del presupuesto.
- ✓ La limitación del recurso humano, pues solo se cuenta con el investigador para recolectar los datos.
- ✓ El diseño a aplicarse, que no es experimental, solo se limitara a describir una realidad.

1.7. Viabilidad

1.7.1. Viabilidad académica.

El estudio es factible académicamente pues se sustenta en bases teóricas y conceptuales, seleccionadas de fuentes primarias y secundarias.

1.7.2. Viabilidad institucional.

El estudio es factible institucionalmente por contar con la autorización del ministerio público para la recolección de datos el cual servirá para realizar el informe final de tesis.

1.7.3. Viabilidad económica.

El estudio es factible económicamente pues los recursos económicos necesarios para realizar dicho estudio estarán a cargo del investigador.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes

2.1.1. Antecedentes internacionales

En el Ecuador el año 2016 Alcívar Trejo, Carlos investigo **"Los medios de comunicación y la estafa electrónica. Nueva forma de delito".** La estafa electrónica es un fenómeno delictivo que en los últimos años gracias al desarrollo global se ha implicado dentro de las leyes ecuatorianas. Tomando relevancia en el ámbito de la criminalidad informática, catalogado como una nueva forma de delito informático sobre el que gira la ciberdelincuencia. A pesar de que esta definición es muy difícil de especificar, ya que se basa en varios aspectos cibernéticos, se estipula según el grupo de abogados de Portaley Madrid como: "la producción de un daño patrimonial cuantificable mediante un comportamiento externo, impropio de un proceso automatizado informático, que altera los datos gestionados por éste, con ánimo lucro y en perjuicio de tercero" (Portaley). Este fraude se da en el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación. Estos tienen como objetivo causar daños o provocar pérdidas o impedir el uso de información de terceros. Es por esto que ante este crimen que se esconde en el anonimato, se debe investigar para establecer una sanción y, por ende, justicia. Siendo esta la importancia del tema establecido, pues muchos ecuatorianos son víctimas de esta estafa, pero lamentablemente no conocen sus derechos ni el peligro que esto conlleva. El

objetivo general es revisar las normas legales existentes en Ecuador, viendo los códigos acerca de las normas y penas legales sobre estos delitos en nuestro país. Además de conceptualizar la definición de delitos informáticos y realizar la respectiva encuesta y determinar una conclusión basado en los resultados de esta (Alcívar Trejo, 2016).

En el año 2014, se realizó el estudio titulado **"Un análisis de la naturaleza de los grupos involucrados en delitos cibernéticos".** Este documento explora la naturaleza de los grupos involucrados en el delito cibernético. Describe brevemente la definición y el alcance del delito cibernético, los retos teóricos y empíricos para abordar lo que se sabe acerca de los delincuentes cibernéticos y el papel probable de los grupos del crimen organizado. El documento da ejemplos de casos conocidos que ilustran el comportamiento individual y grupal y las motivaciones de los delincuentes típicos, incluyendo los actores estatales. Se describen diferentes tipos de ciberdelincuencia y diferentes formas de organización delictiva, basándose en la tipología sugerida por McGuire (2012). Es evidente que una gran variedad de estructuras organizativas está involucrada en el delito cibernético. Las actividades empresariales o con fines de lucro, y especialmente la ciberdelincuencia cometida por actores estatales, parecen requerir liderazgo, estructura y especialización. Por el contrario, la actividad de protesta tiende a ser menos organizada, con una cadena de mando débil (si es que la hay). (Broadhurst, 2014)

En el año 2015, Gurpreet Dhillon y Steve Moores investigaron **"Delitos informáticos: teorizar sobre el enemigo dentro".** La mayoría de los delitos

informáticos ocurren porque un empleado actual de una organización ha subvertido los controles existentes. Al considerar dos estudios de caso, este trabajo analiza los crímenes informáticos resultantes de violaciones de las salvaguardias por parte de los empleados. El documento sugiere que se deben poner en marcha varios controles técnicos, de procedimiento y normativos para prevenir actos ilegales y maliciosos. En última instancia, un buen equilibrio entre varios tipos de controles ayudaría a instituir un medio rentable para hacer que la conducta accidental e intencional fuera difícil. Esto también garantizaría, siempre que fuera posible, la rendición de cuentas individual de todas las acciones negativas potencialmente sensibles. (Gurpreet & Steve, 2005)

En el año 2014, Kumar Vinit realizo la investigación titulada **“Paradigmas actuales y futuros del delito cibernético y de la seguridad - Tendencias de crecimiento y aumento”.** El crimen cibernético es todo aquello que se acerca a los crímenes involucrados con el medio ambiente donde siempre está involucrada una red y los pasos implementados para controlar o superar esta ciber seguridad. La cultura de trabajo de todos los sectores está avanzando hacia la digitalización y los sistemas basados en la nube con el fin de aumentar la eficiencia del trabajo con mayor precisión. Además de esto, la mayoría de las personas les gusta usar sitios de redes sociales y servidores de correo electrónico de muchas maneras directa o indirectamente. El delito cibernético es un tipo de delito en el que se requiere de conocimientos técnicos no sólo para romperlo, sino para hacer un usuario seguro o para aplicar cualquier especialidad preventiva. En este artículo

hemos descrito acerca de los fundamentos de este terrible crimen, la reciente investigación y desarrollo en el ámbito de la seguridad cibernética, los tipos de crímenes y una pequeña encuesta con una empresa de TI. Nuestro objetivo con esta investigación es comprobar el nivel de conciencia de los delincuentes cibernéticos y de seguridad y sugerir pasos necesarios que realmente pueden ser útiles para hacer que el entorno cibernético sea seguro, robusto y digno de confianza. (Kumar, 2014)

En el año 2000 Carter D., investigo **"Cómo funcionan los criminales tecnológicos"**. Si bien hay cuatro tipos principales de delitos informáticos, múltiples delitos pueden ocurrir durante cualquier transacción penal. Los crímenes en los que el equipo es el objetivo incluyen el robo de la propiedad intelectual o la información de marketing, el chantaje o el sabotaje de los sistemas operativos y programas. En todos estos crímenes, el delincuente usa la computadora para obtener información o para dañar los programas operativos. En el segundo tipo de delito, los procesos de la computadora, es decir, su instrumentalidad, más que el contenido de los archivos reales, se utiliza para cometer el crimen. Los delitos en esta categoría incluyen el uso fraudulento de cajeros automáticos, fraude de tarjetas de crédito y fraude de telecomunicaciones. En otro tipo de delito informático, la computadora no es esencial para que ocurra el delito, sino que está relacionada con el acto criminal. Por ejemplo, los infractores de drogas pueden usar computadoras para registrar información sobre su lavado de dinero, tráfico y otras actividades ilegales. La cuarta categoría incluye los delitos recientemente inventados relacionados con la proliferación de computadoras, como la

piratería de software, el mercadeo negro y el robo de equipos informáticos. Algunos problemas únicos relacionados con la delincuencia informática se refieren a cuestiones de propiedad intelectual, el concepto de malversación por computadora, y las cuestiones internacionales. (Carter, 2000)

2.1.2. Antecedentes nacionales

A nivel nacional tenemos los datos Temperini, Marcelo Gabriel en su estudio titulado **“Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte”.** De acuerdo a diferentes estudios actuales, los delitos informáticos son los de mayor crecimiento en los últimos años, con una proyección cada vez mayor. La posibilidad de su comisión a través de Internet permite que, sin mayores complicaciones, el delincuente pueda estar en un determinado país, utilizar servicios de otro, para finalmente atacar a una o más víctimas de un tercer país interviniente. A modo de conclusión se lograron obtener estadísticas actualizadas con un ranking de países de acuerdo al estado de situación en la regulación penal de los delitos informáticos más importantes, así como la lista de delitos informáticos menos sancionados (Temperini, 2013).

En 1991 se describieron los virus peruanos. Al igual que la corriente búlgara, en 1991 apareció en el Perú el primer virus local, autodenominado „Mensaje y que no era otra cosa que una simple mutación del virus "Jerusalem-B" y al que su autor le agregó una ventana con su nombre y número telefónico. Los virus con apellidos como Espejo, Martínez y Aguilar fueron variantes del Jerusalem-B y prácticamente se difundieron a nivel nacional.

Continuando con la lógica del tedio, en 1993 empezaron a crearse y diseminarse especies nacionales desarrolladas con creatividad propia, siendo alguno de ellos sumamente originales, como los virus Katia, Rogue o F03241 y los polimórficos Rogue II y Please Wait (que formateaba el disco duro). La creación de los virus locales ocurre en cualquier país y el Perú no podía ser la excepción.

2.2. Bases teóricas

En 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inicio un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales (Estrada Garavilla, 2011).

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad" (Estrada Garavilla, 2011).

Se entiende Delito como: "acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas". Finalmente, la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define Delito Informático como "cualquier comportamiento antijurídico, no ético o no

autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos."

"Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma". Adicionalmente, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran erigir un marco de seguridad para los sistemas informáticos (Campos, 2015).

2.3. Definiciones conceptuales

2.3.1. Red social en internet

Las rede sociales son sitios web que ofrecen servicios y funcionalidades de comunicación diversos para mantener en contacto a los usuarios de la red. Se basan en un software especial que integra numerosas funciones individuales: blogs, wikis, foros, chat, mensajería, entre otros, en una misma interfaz y que proporciona la conectividad entre los diversos usuarios de la red. Son redes de relaciones personales, también llamadas comunidades, que proporcionan sociabilidad, apoyo, información y un sentido de pertenencia e identidad social. Estas están conformadas por grupos de personas con algunos intereses similares, que se comunican a través de proyectos. Existe un cierto sentido de pertenencia a un grupo con una cultura común: se comparten unos valores, unas normas y un lenguaje en un clima de confianza (Rodríguez Arbeláez, 2011)

Los tipos de las redes sociales se dividen en tres grandes categorías (Alcívar Trejo, 2016) :

Redes personales: Se componen de cientos de miles de usuarios en los que cada uno tiene su pequeño “espacio” con su información, sus fotos, su música, etc. Y cada uno se puede relacionar con los demás de múltiples maneras, aunque todas ellas involucran el uso de Internet de una u otra forma. Ejemplo: Facebook es una red personal.

Redes temáticas: Son similares a las anteriores, aunque se diferencian por el hecho de que suelen centrarse en un tema en concreto y proporcionan las funcionalidades necesarias para el mismo. Por ejemplo, una red de cine, una de informática, de algún tipo de deporte, etc.

Redes profesionales: Son una variedad especial de las anteriores, dedicadas exclusivamente al ámbito laboral, en todas sus vertientes. Pueden poner en contacto a aquellos que ofrecen trabajo con los que lo buscan, crear grupos de investigación, entre otros.

2.3.2. Delito informático

Es importante buscar una aproximación que permita relacionar la normatividad jurídica con la realidad y con las tendencias de la tecnología y los delitos informáticos por esto para definir el delito informático se han venido incorporando diferentes conceptos de distintos autores:

Julio Tellez Valdez (2007) en su libro derecho informático, enfoca el delito informático desde el punto de vista típico y atípico y lo define como “actitud contraria a los intereses de las personas en que se tiene a los computadores como instrumento o fin (concepto atípico) o las conductas típicas, antijurídica o culpables

en las que se tienen los computadores como instrumento o fin (Ojeda Pérez, Rincón Rodríguez, Arias Flórez, & Daza Martínez, 2010).

Alberto Suarez Sánchez (2009), por su parte señala: “en conclusión, el delito informático está vinculado no solo a la realización y una conducta delictiva a través de miembros o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto, sino también a la afectación de la información pese cómo bien jurídico tutelado, diferente de los intereses jurídicos tradicionales.

Davara Rodríguez (2007) el delito informático es la realización de una acción que, reuniendo las características que delimitan el concepto delito sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnere los derechos del titular de un elemento informático. (Ojeda Pérez, Rincón Rodríguez, Arias Flórez, & Daza Martínez, 2010)

2.3.3. Clasificación Según la Actividad Informática.

2.3.3.1. Sabotaje informático.

El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema. (Lopez Hernandez, 2011).

2.3.3.2. Fraude a través de computadoras.

Estas conductas consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas.

2.3.3.3. Delitos informáticos contra la privacidad.

Grupo de conductas que de alguna manera pueden afectar la esfera de privacidad del ciudadano mediante la acumulación, archivo y divulgación indebida de datos contenidos en sistemas informáticos.

Existen circunstancias agravantes de la divulgación de ficheros, los cuales se dan en función de:

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

También se comprende la interceptación de las comunicaciones, la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación, se piensa que entre lo anterior se encuentra el pinchado de redes informáticas.

Interceptación de e-mail: En este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

2.3.3.4. Pornografía infantil.

La distribución de pornografía infantil por todo el mundo a través de la Internet está en aumento. Durante los pasados cinco años, el número de condenas por transmisión o posesión de pornografía infantil ha aumentado de 100 a 400 al año en un país norteamericano. El problema se agrava al aparecer nuevas tecnologías, como la criptografía, que sirve para esconder pornografía y demás material "ofensivo" que se transmita o archive.

2.3.3.5. Seguridad cibernética

La seguridad cibernética alude a las innovaciones y procedimientos para asegurar las máquinas, los sistemas y la información Vulnerabilidades y agresiones no aprobadas a través de Internet por delincuentes digitales. ISO 27001 es el estándar universal de seguridad cibernética que da un modelo para crear, actualizar, trabajar, comprobar, auditoría, mantenimiento y mejora de la seguridad de la información Sistema de gestión.

2.3.3.6. Herramientas Preventivas para delitos informáticos

1) Cortafuegos

En términos de computación, firewall es todo acerca de un sistema Marco de seguridad que supervisa el acercamiento y el Movimiento del sistema amigable centrado alrededor conectado al principio establecido. El firewall constituye un límite entre un Seguro, un sistema interno seguro y un sistema alternativo que a aceptado para no ser seguro y confiado. Los firewalls existen tanto una disposición de producto y como un aparato de equipo.

Numerosos accesorios de firewalls basados ofrecen además otros Utilidad al sistema interior aseguran, por ejemplo, Pasando como un servidor DHCP para ese sistema. Numerosos switches que pasan información entre sistemas Segmentos de cortafuegos y, nuevamente, numerosos Los firewalls pueden realizar capacidades de dirección fundamentales. La ingeniería de cortafuegos se desarrolló a finales de los Internet era una innovación razonablemente nueva en cuanto a su Utilización mundial y la red.

2) Antivirus

El software antivirus o anti-virus es una máquina de Programación utilizada para evitar, localizar y desarraigar perniciosos de programación. La programación antivirus fue creada inicialmente Para descubrir y evacuar las infecciones de la máquina, Sin embargo, con la expansión de Tipos de malware, la programación antivirus empezó a dar Seguridad de otros peligros de la máquina. Específicamente, La programación antivirus puede protegerse de: Browser vengativo Objetos auxiliares (BHOS), ladrones del programa, ransomware, llave Madereros, pasajes secundarios, rootkits, caballos de Troya, gusanos, LSPS maligno, dialers, herramientas de fraude, adware y spyware.

Algunos artículos incorporan adicionalmente seguridad de otros Peligros de las máquinas, URLS viciadas y contaminadas, spam, Truco y ataques de phishing, personalidad en línea (protección), Web de mantenimiento de asaltos de dinero, estrategias de construcción social, Amenaza persistente avanzada (APT), botnets, ataques DDOS.

3) Honeypots

En la fraseología de máquina, un honeypots es una trampa situada a Reconocer, evitar o, de alguna manera, neutralizar los esfuerzos Utilización no aprobada de marcos de datos. Para la mayoría Parte, un honeypots comprende una máquina, información o un Sitio del sistema que parece, por todas las cuentas, ser Un sistema, sin embargo, está realmente desenganchado y observado, y Que parece contener datos o un bien de calidad para Asaltantes Esto es como la policía que burla a un criminal y Después de dirigir la observación encubierta.

2.3.3.7. Seguridad contra los delitos informáticos

La seguridad cibernética consiste en fomentar la confianza y la seguridad en el uso de las TIC para garantizar la confianza en la sociedad de la información. En consecuencia, podemos definirlo como todas las actividades y operaciones encaminadas a reducir y prevenir amenazas y vulnerabilidades, y tener políticas de protección; respuesta al incidente; Recuperación, aseguramiento de datos, aplicación de la ley y operaciones militares y de inteligencia relacionadas con la seguridad del espacio cibernético. (Mona Al-achkar Jabbour, 2016)

Por lo tanto, la seguridad cibernética toca prácticamente todas las actividades y todos los ciudadanos de todo el mundo; Ofrece enormes oportunidades para mejorar el desarrollo humano y lograr una mejor integración en la sociedad de la información. También apoya un mayor acceso al conocimiento ya la educación, así como al desarrollo de políticas y estrategias.

Por otra parte, impone nuevos tipos de paradigmas comerciales, profesionales y sociales, dando lugar a una serie de problemas jurídicos y técnicos que deben abordarse sobre la base del respeto de su naturaleza y necesidades especiales. Por lo tanto, se necesita un enfoque diferente y metodologías diferentes a las adoptadas antes de la era de la tecnología de la información y la comunicación. (Mona Al-achkar Jabbour, 2016)

Sin embargo, muchos gobiernos y sociedades temen el impacto negativo que las TIC pueden tener sobre sus propios ciudadanos debido a los peligros potenciales que conlleva y por los desafíos económicos, sociales y de seguridad que plantea.

En consecuencia, la falta de seguridad en el ciberespacio socava la confianza en la sociedad de la información. Esto es especialmente el caso con muchas intrusiones

en todo el mundo, lo que resulta en el robo de dinero, activos y sensibles información militar, comercial y económica.

En las instituciones legales y reguladoras que carecen de ciberespacio, la seguridad socava la realización de todo el potencial de la revolución de la tecnología de la información.

En consecuencia, se necesita una atención especial para evitar que el ciberespacio se convierta en una fuente de peligro para los estados y ciudadanos y para prevenir la aparición de un paraíso cibernético.

Las autoridades encargadas tratan de encontrar una forma de prevenir y castigar nuevas formas de actividad delictiva, como los delitos relacionados con las TIC que implican asaltos informáticos. Muchos gobiernos ya han adoptado reglamentos y legislaciones particulares como respuesta a la necesidad de asegurar la adopción de medidas de seguridad. (Mona Al-achkar Jabbour, 2016)

2.3.4. Hipótesis

Hipótesis del investigador

Si los delitos informáticos cometidos a través de redes sociales las mismas que no se identifican a los autores por falta de peritos especialistas, entonces su tratamiento en el ministerio publico conduce al Archivamiento de las denuncias.

2.3.5. Variables

Variable independiente: Redes sociales

Variable Dependiente: Delitos informáticos

Operacionalización de variables (Dimensiones e Indicadores)

VARIABLES	DIMENSIONES	INDICADORES
Variable independiente: Redes sociales	a) Acceso abusivo a un sistema informático b) Obstaculización ilegítima de sistema informático o red de telecomunicación c) Daño informático d) Uso de software malicioso e) Hurto por medios informáticos y semejantes f) Transferencia no consentida de activos g) Suplantación de sitios web para capturar datos personales. h) Transferencia no consentida de activos	a) Presente b) No presente
Variable dependiente: Delitos informáticos	a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.) b) Variación de los activos y pasivos en la situación contable de las empresas. c) Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.) d) Lectura, sustracción o copiado de información confidencial. e) Modificación de datos tanto en la entrada como en la salida. f) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas. g) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa. h) Uso no autorizado de programas de cómputo. i) Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas. j) Alteración en el funcionamiento de los sistemas, a través de los virus informáticos. k) Obtención de información residual impresa en papel luego de la ejecución de trabajos. l) Acceso a áreas informatizadas en forma no autorizada. m) Intervención en las líneas de comunicación de datos o teleproceso.	a) Presente b) No presente

CAPITULO III

MATERIALES Y METODOS

3.1. Método y diseño

Según el número de variables estudiadas es **descriptivo**.

3.1.1. Método de la investigación

Método inductivo

3.1.2. Diseño de la investigación

El estudio tiene un diseño transversal descriptivo.

3.2. Tipo y nivel de investigación (Referencial)

3.2.1. Tipo

Según la intervención del investigador el estudio es **observacional,** solo se observa y se describe en forma precisa los fenómenos

Según la planificación de la medición de la variable de estudio es **prospectivo,** porque el estudio pertenece al tiempo futuro y la recolección de datos lo realiza el investigador a partir de la fuente secundaria.

Según el número de mediciones de la variable de estudio es **transversal,** porque los instrumentos se aplicarán en un solo momento y las variables se medirán una sola vez.

3.2.2. Nivel de investigación

Nivel descriptivo. Describe fenómenos sociales o clínicos en una circunstancia temporal y geográfica determinada. Su finalidad es describir y/o estimar parámetros. Se describen frecuencias y/o promedios; y se estiman parámetros con intervalos de confianza (Supo, 2014)

3.3. Población y muestra

A. Población

La población está determinada por todas las denuncias en el Ministerio Público de Huánuco en el periodo de enero a diciembre del 2016, haciendo un total 620 procesos.

B. Muestra

El tamaño de la muestra será calculado con un coeficiente de confianza al 95%, y con un error del 5%. Para ello se utilizará la siguiente formula:

$$n = \frac{\mathrm{N}.Z_{\sigma}^{2}.P.Q}{e^{2}(N-1)+.Z_{\sigma}^{2}.P.Q}$$

Dónde:

n = El tamaño de la muestra que queremos calcular

N = Tamaño del universo que es igual 35

Z = Nivel de confianza 95% -> Z=1,96

e = Es el margen de error máximo que admito (5%)

p = Probabilidad de éxito (0.5)

Q = Probabilidad de fracaso (0.5)

$$n = \frac{620\text{x } 1.96^2 x\ 0.5\ x\ 0.5}{0.05^2(620-1)+.1.96^2 x\ 0.5\ x\ 0.5}$$

$$\boldsymbol{n = 440}$$

Por tanto, se trabajará con una muestra de 38 casos.

C. Delimitación geográfica, temporal y temática

El presente trabajo de investigación se encuentra delimitado bajo las siguientes dimensiones:

- **Dimensión Geográfica**

  La presente investigación se realizó en el Ministerio Público de Huánuco.

- **Dimensión Temporal**

  La presente investigación abarcara el periodo comprendido entre enero a agosto del 2016, con la finalidad de poder caracterizar, describir y explicar las características de las variables del presente estudio.

- **Dimensión Temática**

  La presente investigación se enmarcará dentro de los fundamentos teóricos, doctrinales y tecnológicos sobre los delitos informáticos, como también en la metodología y procedimiento de la investigación desarrollada.

3.4. Técnicas e instrumentos de investigación

2.4.1. Para la recolección de datos

Para la presente investigación se utilizó las siguientes técnicas:

- ✓ **Entrevistas y Encuestas:** aplicadas a los especialistas y expertos con respecto a los aspectos legales delitos informáticos teniendo en cuenta las variables e indicadores del presente trabajo

- ✓ **Análisis Documental**: los que se utilizaran de la información bibliográfica relacionada con los delitos informáticos.

- ✓ **Análisis** Estadístico: los que se utilizaran de los datos relacionados a las variables durante el periodo de enero a diciembre del 2016

2.4.2. para la presentación de datos (cuadros y gráficos)

Los datos serán presentados en tablas, cuadros, figuras y gráficos analizados con la aplicación de la estadística descriptiva. Los resultados serán presentados en cuadros, teniendo en cuenta las variables de la investigación, para ello se utilizó la estadística descriptiva en sus siguientes técnicas:

- Ordenamiento y Clasificación.
- Graficas Estadísticas.
- Procesamiento Computarizado con Excel.
- Procesamiento Computarizado con SPSS.

CAPITULO IV

RESULTADOS

4.1. Procesamiento de datos (Cuadros Estadísticos con su respectivo análisis e interpretación)

Tabla n° 01

Delitos informáticos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.

Procedimientos judiciales por Delitos informáticos	Frecuencia	Porcentaje
Alteración, daño o destrucción de base de datos	115	26,1
Tráfico ilegal de datos	85	19,3
Atentado a la integridad de datos informáticos	60	13,6
Atentado a la integridad de sistemas informáticos	55	12,5
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	45	10,2
Interceptación de datos informáticos	40	9,0
Fraude informático	20	4,5
Suplantación de identidad	10	2,2
Abuso de mecanismos y dispositivos informáticos	10	2,2
	440	100

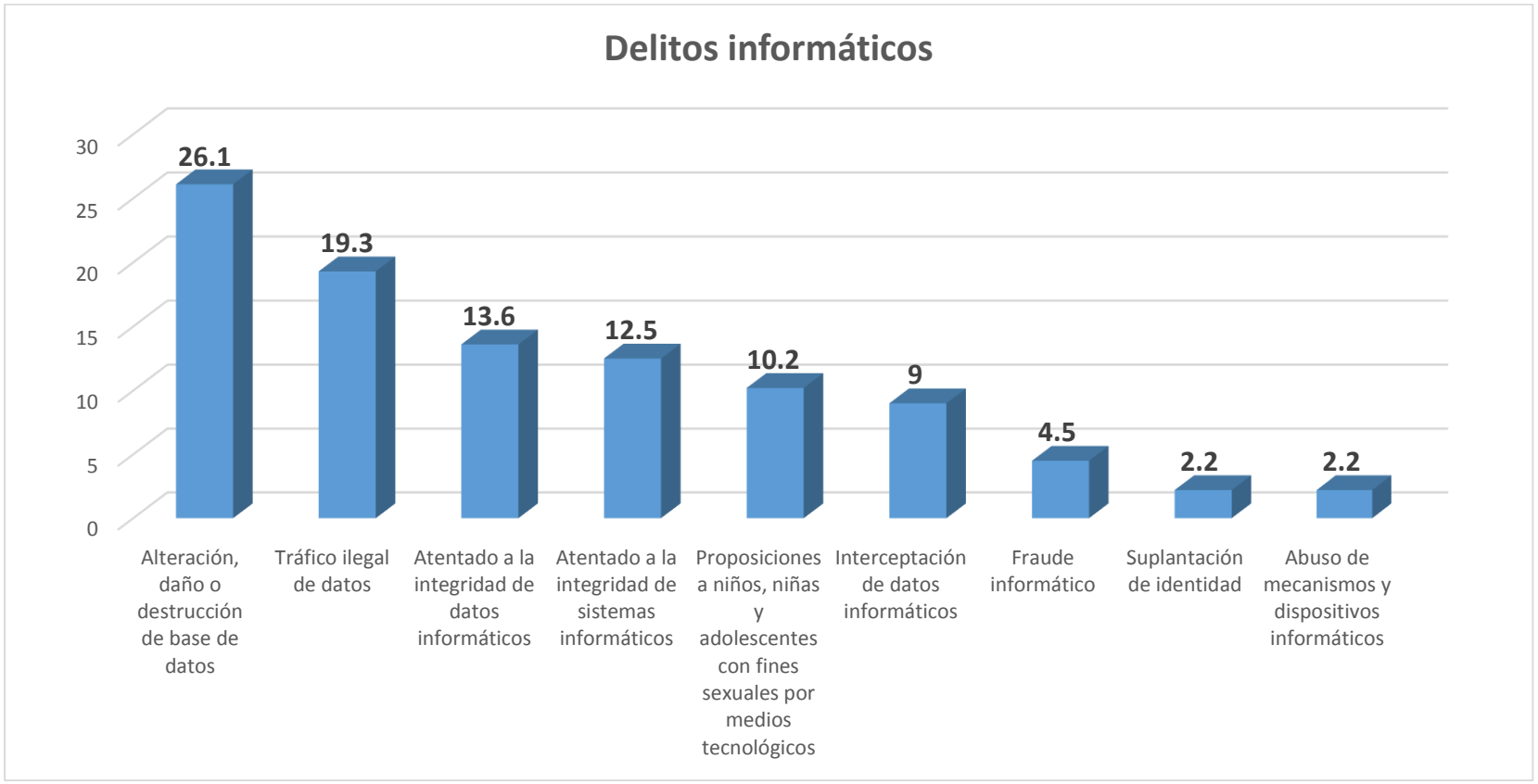
Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Interpretación y análisis:

Al analizar los delitos informáticos más frecuentes podemos apreciar que la Alteración, daño o destrucción de base de datos representa el 26,1%; el Tráfico ilegal de datos 19,3%; el Atentado a la integridad de datos informáticos el 13,6%; el Atentado a la integridad de sistemas informáticos un 12,5%; las Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos 10,2%; la Interceptación de datos informáticos el 9,0%; el Fraude informático 4,5%; la Suplantación de identidad el 2,2% y el Abuso de mecanismos y dispositivos informáticos el 2,2%.

Grafico n° 01

Representación gráfica de los Delitos informáticos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.



Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Tabla n° 02

Alteración, daño o destrucción de base de datos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.

Alteración, daño o destrucción de base	Frecuencia	Porcentaje
Total, de casos que fueron archivados	75	65,2
Total, de casos que terminaron en sentencia	40	37,8
Total	115	100

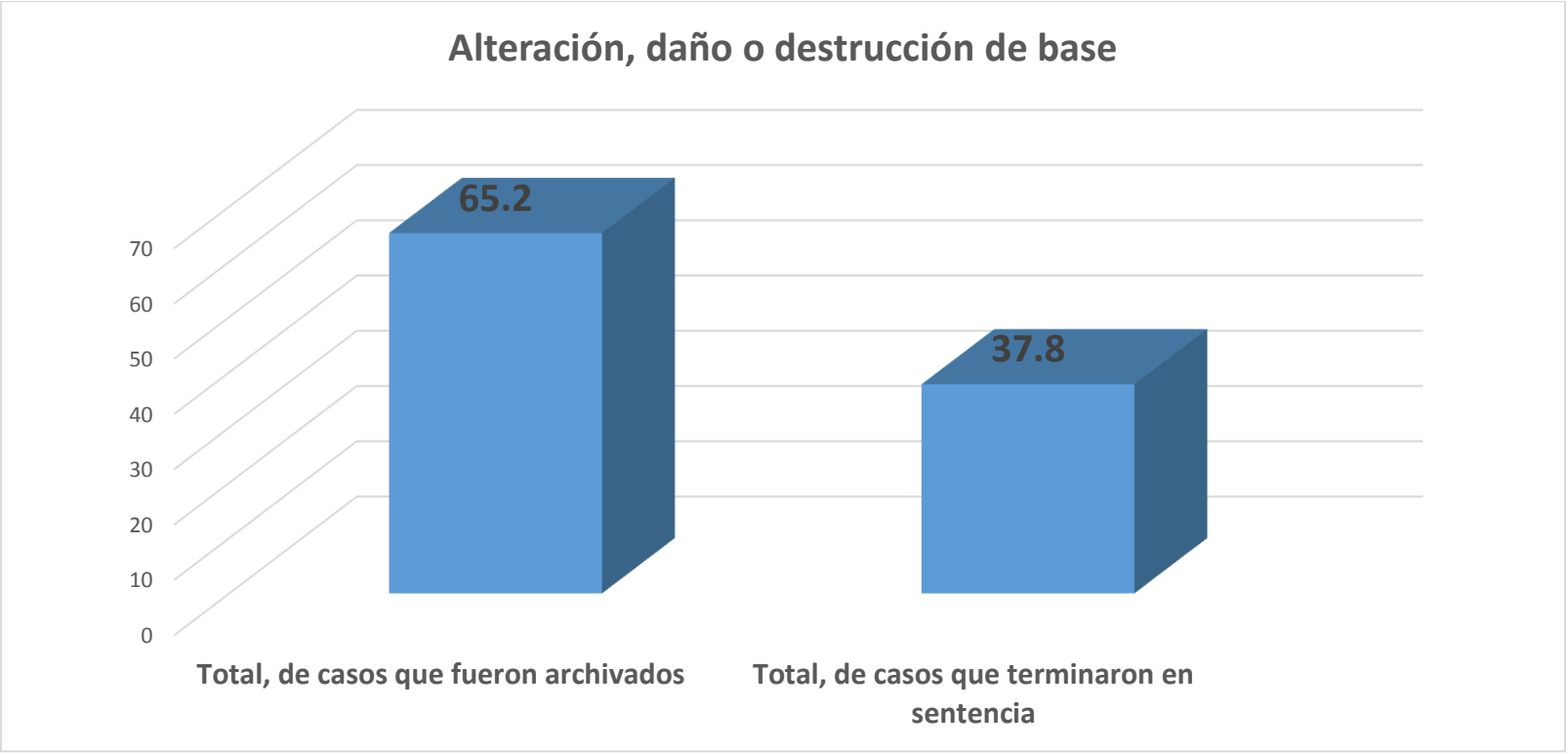
Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Interpretación y análisis:

De los delitos informáticos tipificados como Alteración, daño o destrucción de base de datos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, podemos apreciar que un 65,2% fueron archivados y un 37,8% pudieron recibir una sentencia.

Grafico n° 02

Representación gráfica de la Alteración, daño o destrucción de base de datos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.



Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Tabla n° 03

Tráfico ilegal de datos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.

Tráfico ilegal de datos	Frecuencia	Porcentaje
Total, de casos que fueron archivados	50	58,8
Total, de casos que terminaron en sentencia	35	41,2
Total	85	100

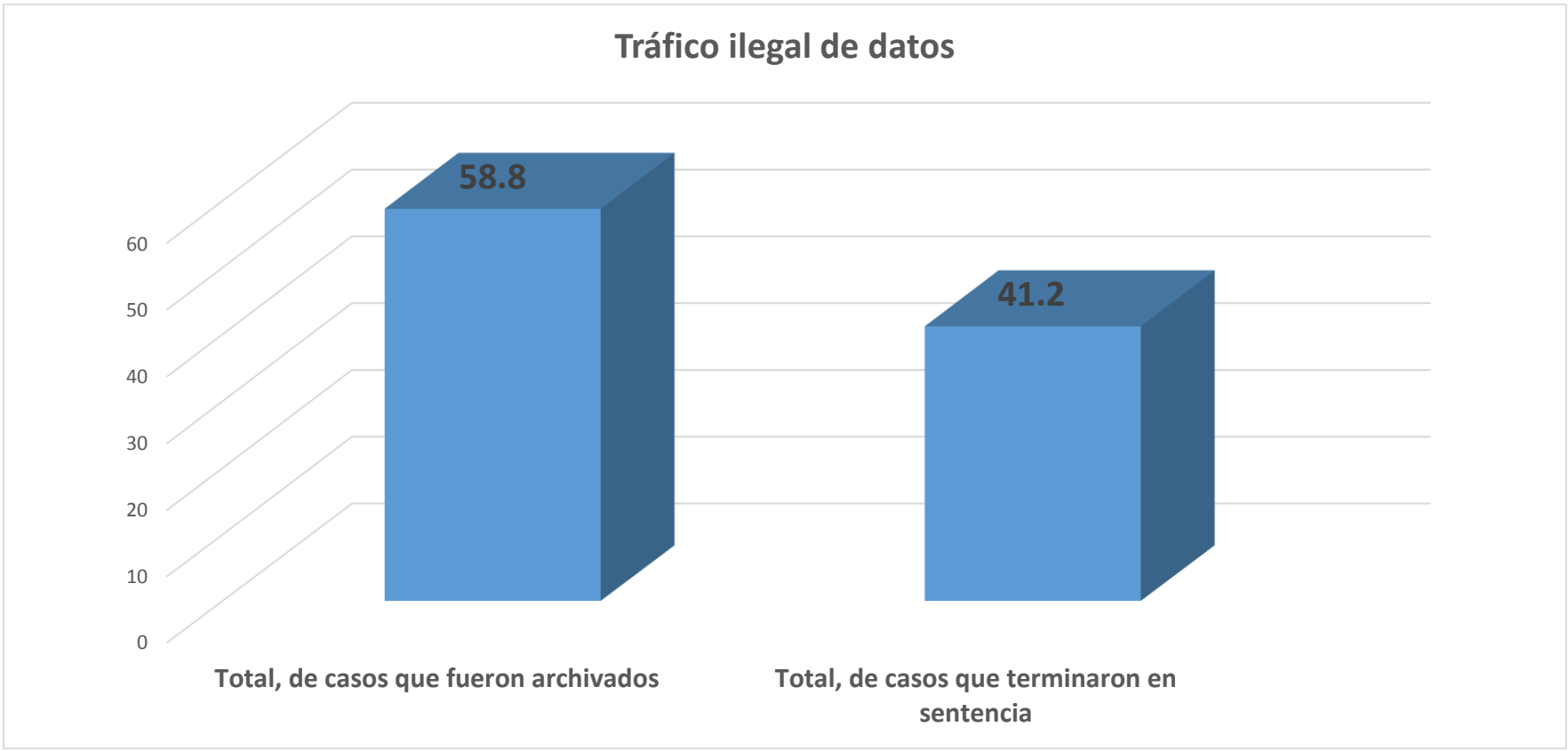
Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Interpretación y análisis:

De los delitos informáticos tipificados como **Tráfico ilegal de datos cometidos** a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, podemos apreciar que un 58,8% fueron archivados y un 41,2% pudieron recibir una sentencia.

Grafico n° 03

Tráfico ilegal de datos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.



Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Tabla n° 04

Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.

Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	Frecuencia	Porcentaje
Total, de casos que fueron archivados	30	50
Total, de casos que terminaron en sentencia	30	50
Total	60	100

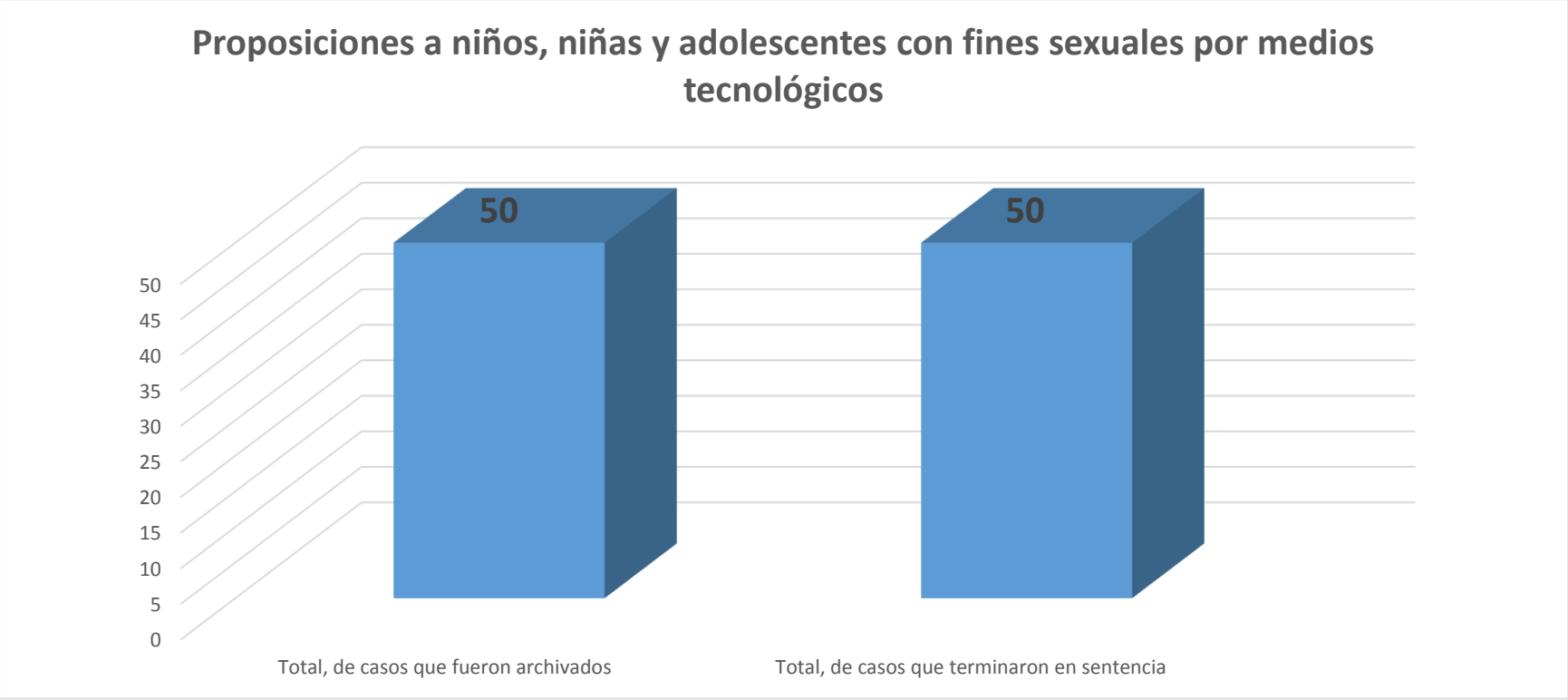
Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Interpretación y análisis:

De los delitos informáticos tipificados como **Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco**, podemos apreciar que un 50% fueron archivados y un 50% pudieron recibir una sentencia.

Grafico n° 04

Representación gráfica sobre las Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.



Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Tabla n° 05

Atentado a la integridad de datos informáticos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.

Atentado a la integridad de datos informáticos	Frecuencia	Porcentaje
Total, de casos que fueron archivados	30	54,5
Total, de casos que terminaron en sentencia	25	45,5
Total	55	100

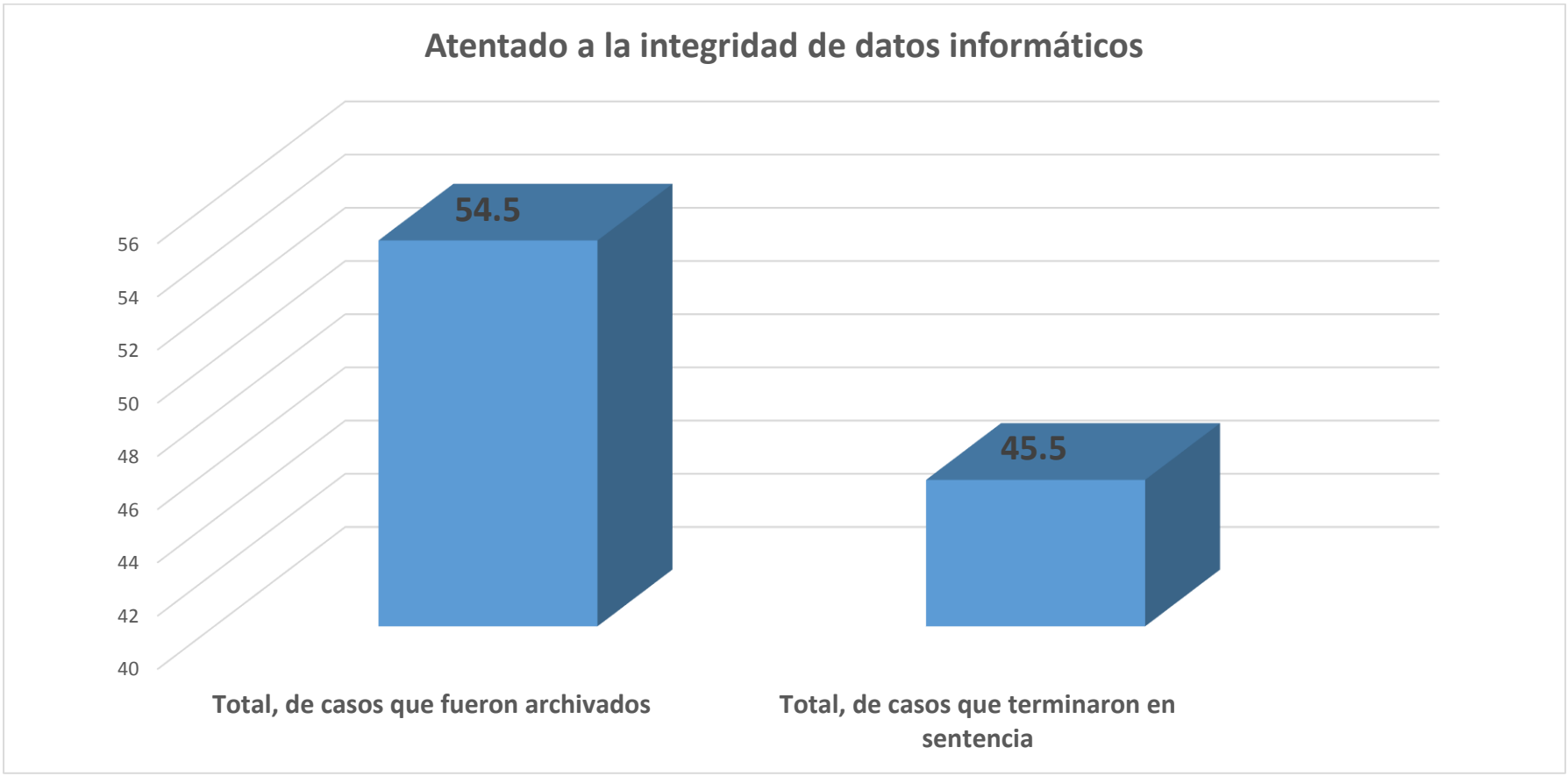
Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Interpretación y análisis:

De los delitos informáticos tipificados como **Delitos informáticos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco**, podemos apreciar que un 54,5% fueron archivados y un 45,5% pudieron recibir una sentencia.

Grafico n° 05

Representación gráfica sobre los Delitos informáticos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.



Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Tabla n° 06

Atentado a la integridad de sistemas informáticos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.

Atentado a la integridad de sistemas informáticos	Frecuencia	Porcentaje
Total, de casos que fueron archivados	25	55,5
Total, de casos que terminaron en sentencia	20	44,5
Total	45	100

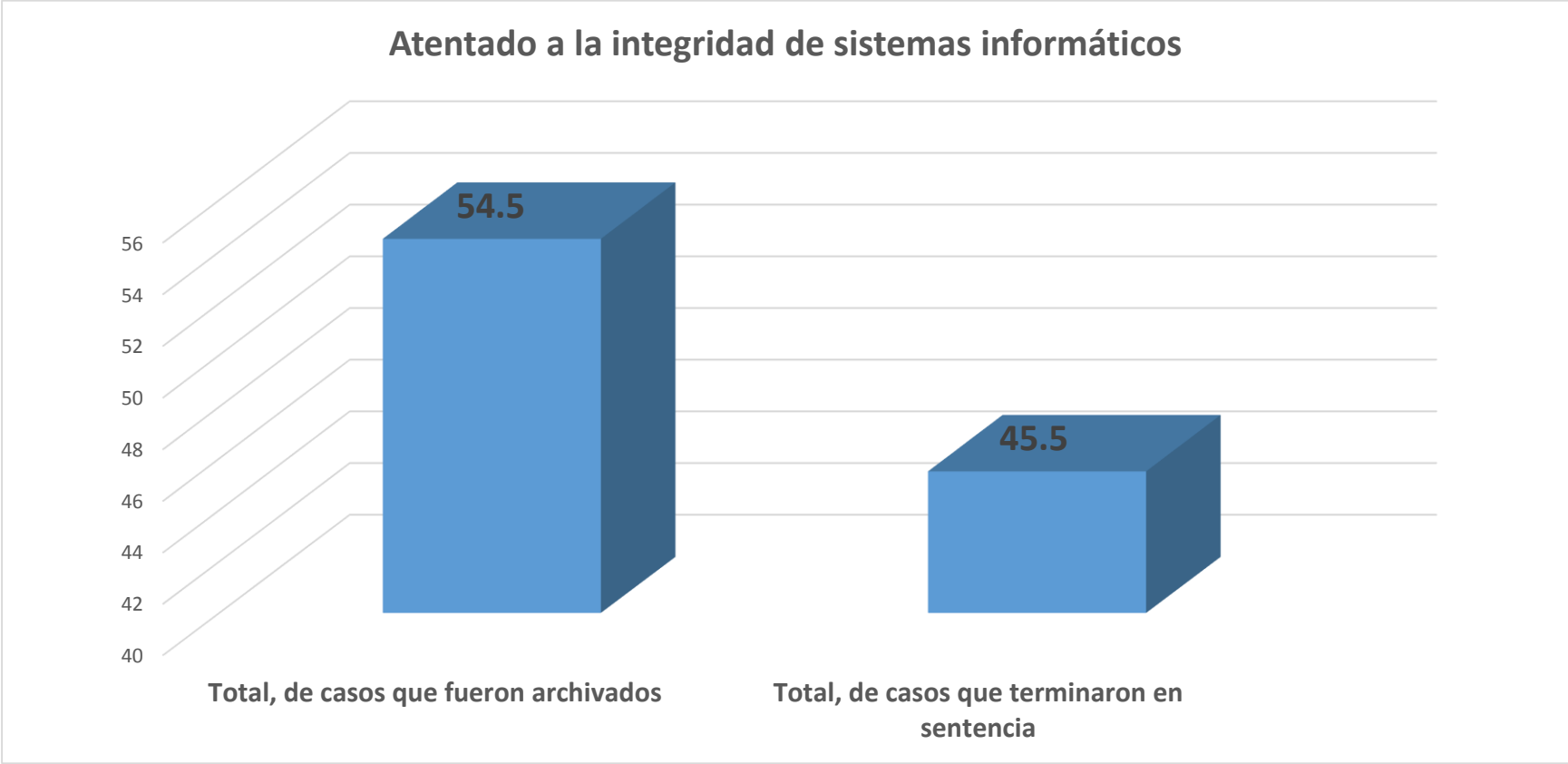
Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Interpretación y análisis:

De los delitos informáticos tipificados como **Atentado a la integridad de sistemas informáticos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco**, podemos apreciar que un 55,5% fueron archivados y un 44,5% pudieron recibir una sentencia.

Grafico n° 06

Representación gráfica sobre los Atentado a la integridad de sistemas informáticos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.



Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Tabla n° 07

Interceptación de datos informáticos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.

Interceptación de datos informáticos	Frecuencia	Porcentaje
Total, de casos que fueron archivados	25	62,5
Total, de casos que terminaron en sentencia	15	37,5
Total	40	100

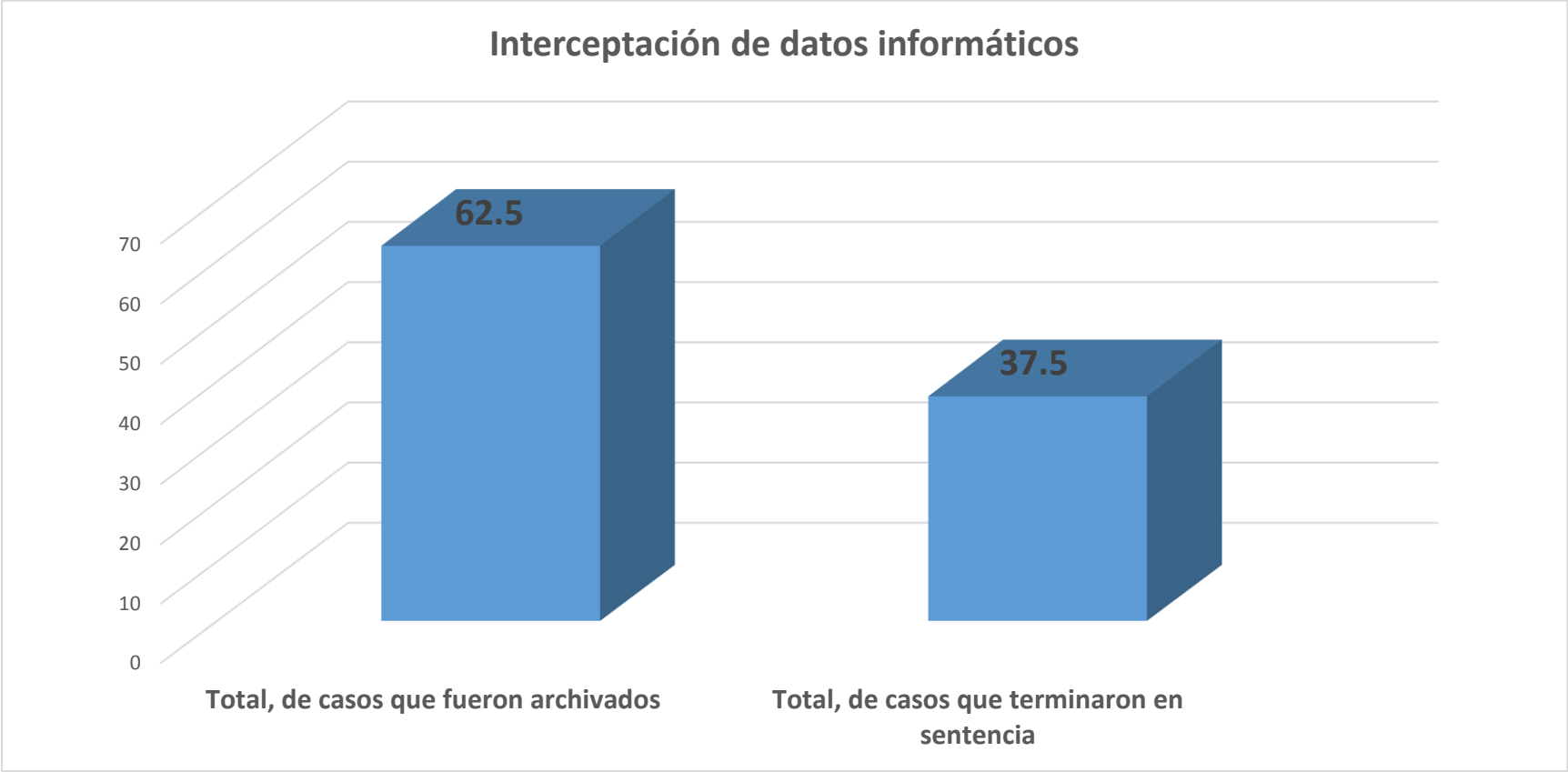
Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Interpretación y análisis:

De los delitos informáticos tipificados como **Interceptación de datos informáticos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco**, podemos apreciar que un 62,5% fueron archivados y un 37,5% pudieron recibir una sentencia.

Grafico n° 07

Representación gráfica sobre la Interceptación de datos informáticos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.



Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Tabla n° 08

Fraude informático cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.

Fraude informático	Frecuencia	Porcentaje
Total, de casos que fueron archivados	10	50
Total, de casos que terminaron en sentencia	10	50
Total	20	100

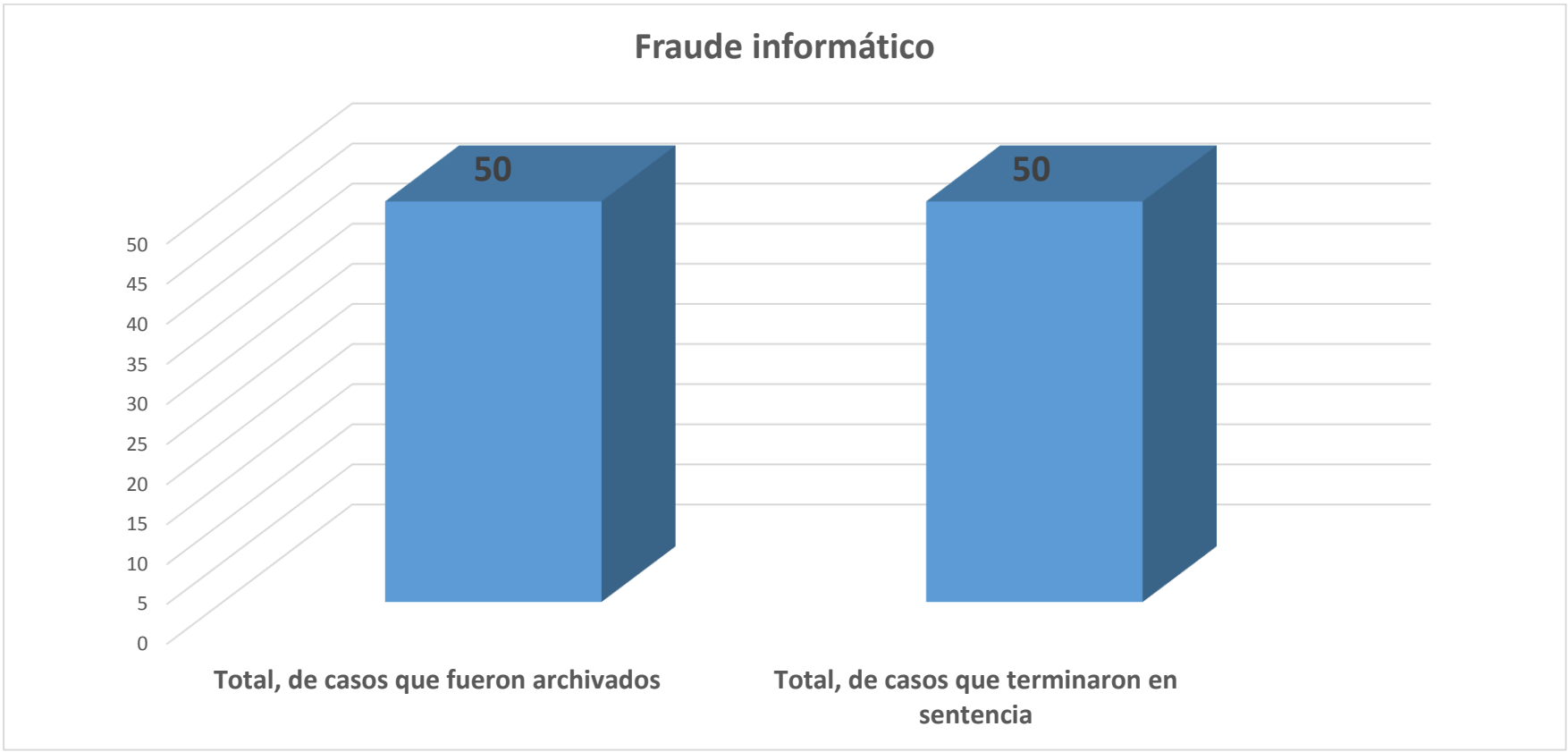
Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Interpretación y análisis:

De los delitos informáticos tipificados como **Fraude informático cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco**, podemos apreciar que un 50% fueron archivados y un 50% pudieron recibir una sentencia.

Grafico n° 08

Representación gráfica sobre el Fraude informático cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.



Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Tabla n° 09

Suplantación de identidad cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.

Suplantación de identidad	Frecuencia	Porcentaje
Total, de casos que fueron archivados	5	50
Total, de casos que terminaron en sentencia	5	50
Total	10	100

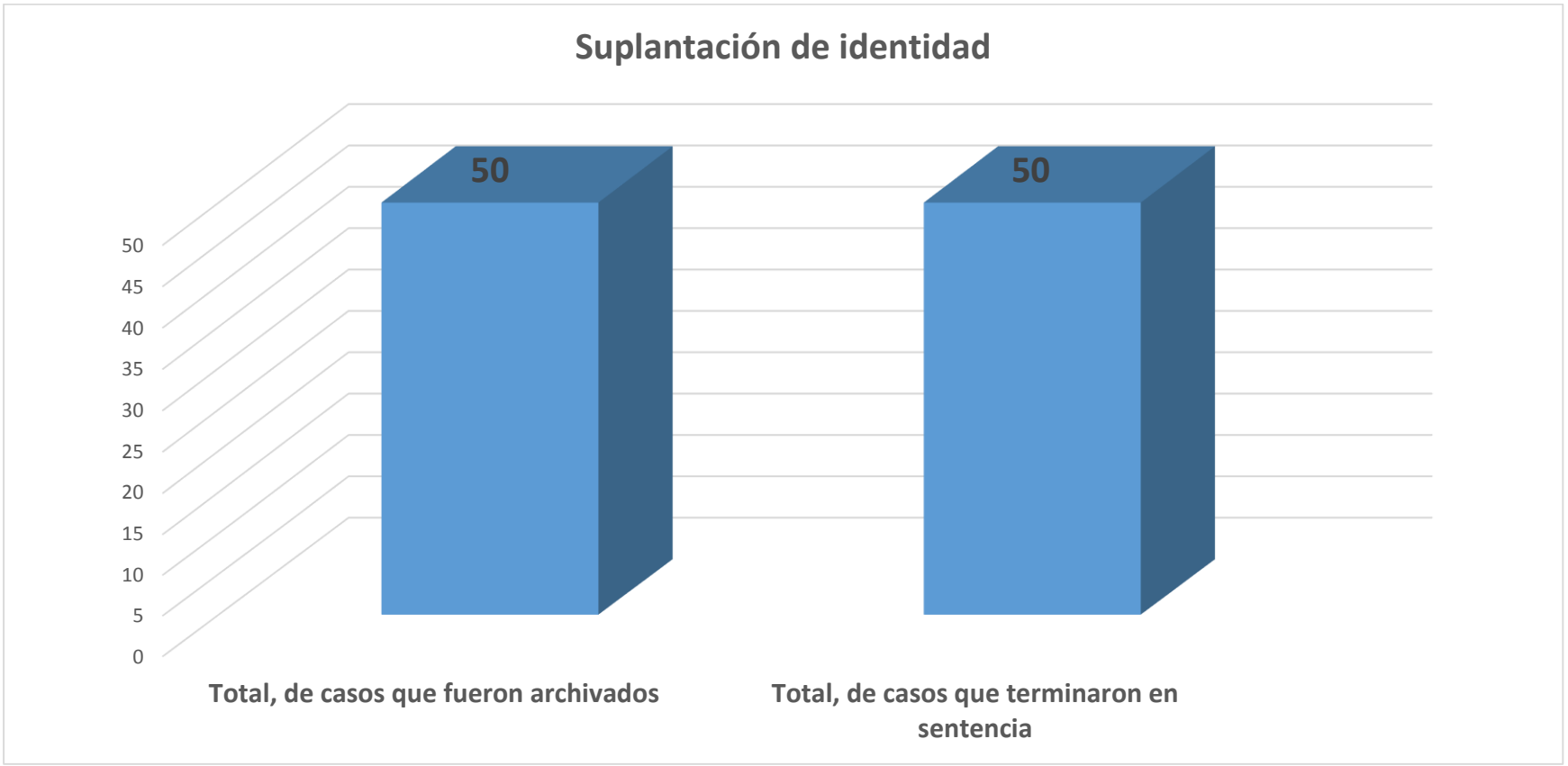
Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Interpretación y análisis:

De los delitos informáticos tipificados como **Suplantación de identidad cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco**, podemos apreciar que un 50% fueron archivados y un 50% pudieron recibir una sentencia.

Grafico n° 09

Representación gráfica sobre la Suplantación de identidad cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.



Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Tabla n° 10

Abuso de mecanismos y dispositivos informáticos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.

Abuso de mecanismos y dispositivos informáticos	Frecuencia	Porcentaje
Total, de casos que fueron archivados	5	50
Total, de casos que terminaron en sentencia	5	50
Total	10	100

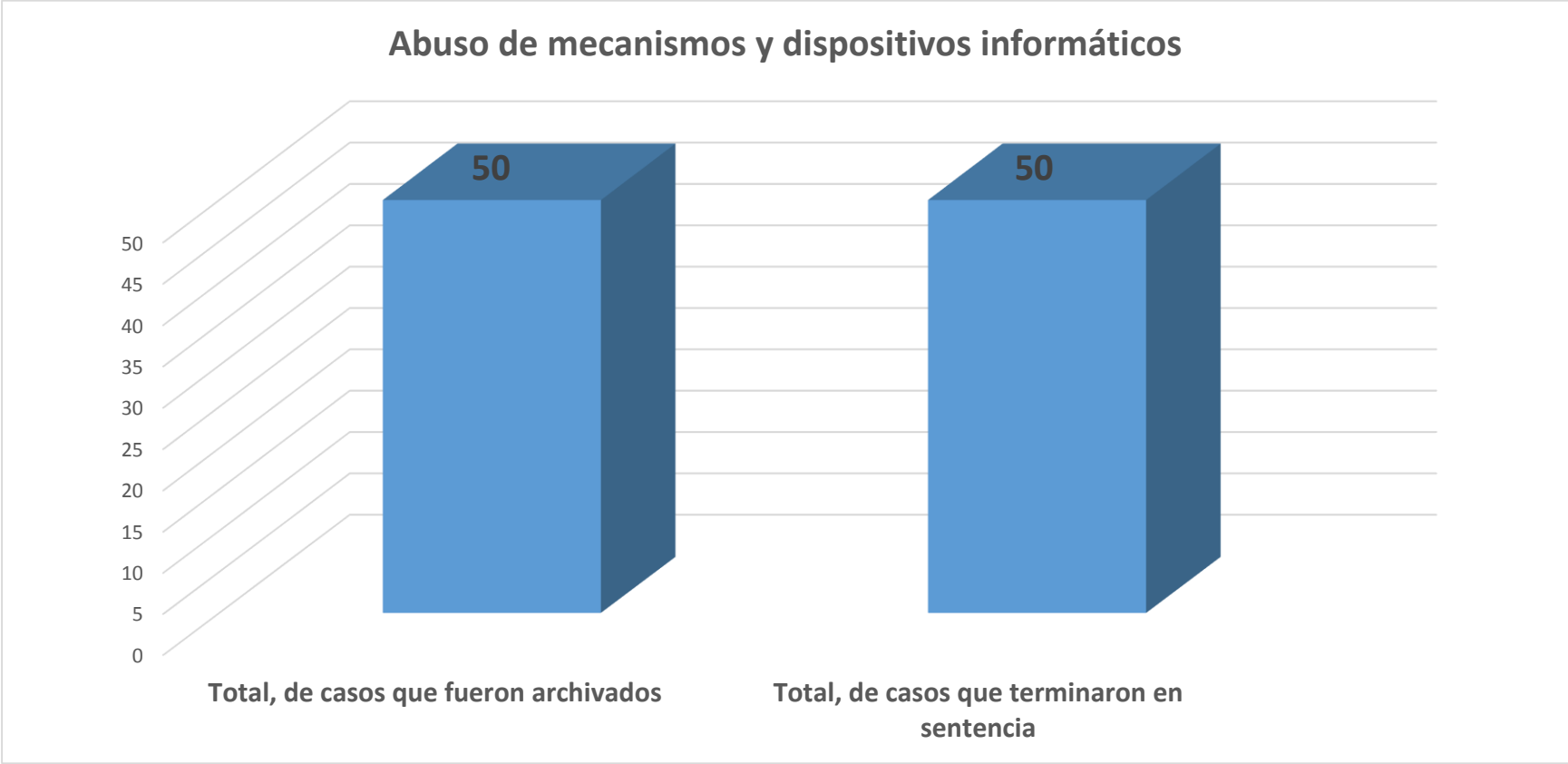
Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Interpretación y análisis:

De los delitos informáticos tipificados como **Abuso de mecanismos y dispositivos informáticos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco,** podemos apreciar que un 50% fueron archivados y un 50% pudieron recibir una sentencia.

Grafico n° 10

Representación gráfica sobre el Abuso de mecanismos y dispositivos informáticos cometidos a través de las redes sociales presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.



Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Tabla n° 11

Tratamiento de los delitos informáticos presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.

Procedimientos judiciales por Delitos informáticos	Frecuencia	Porcentaje
Total, de casos que fueron archivados	255	57,9
Total, de casos que terminaron en sentencia	185	42,1
Total	440	100

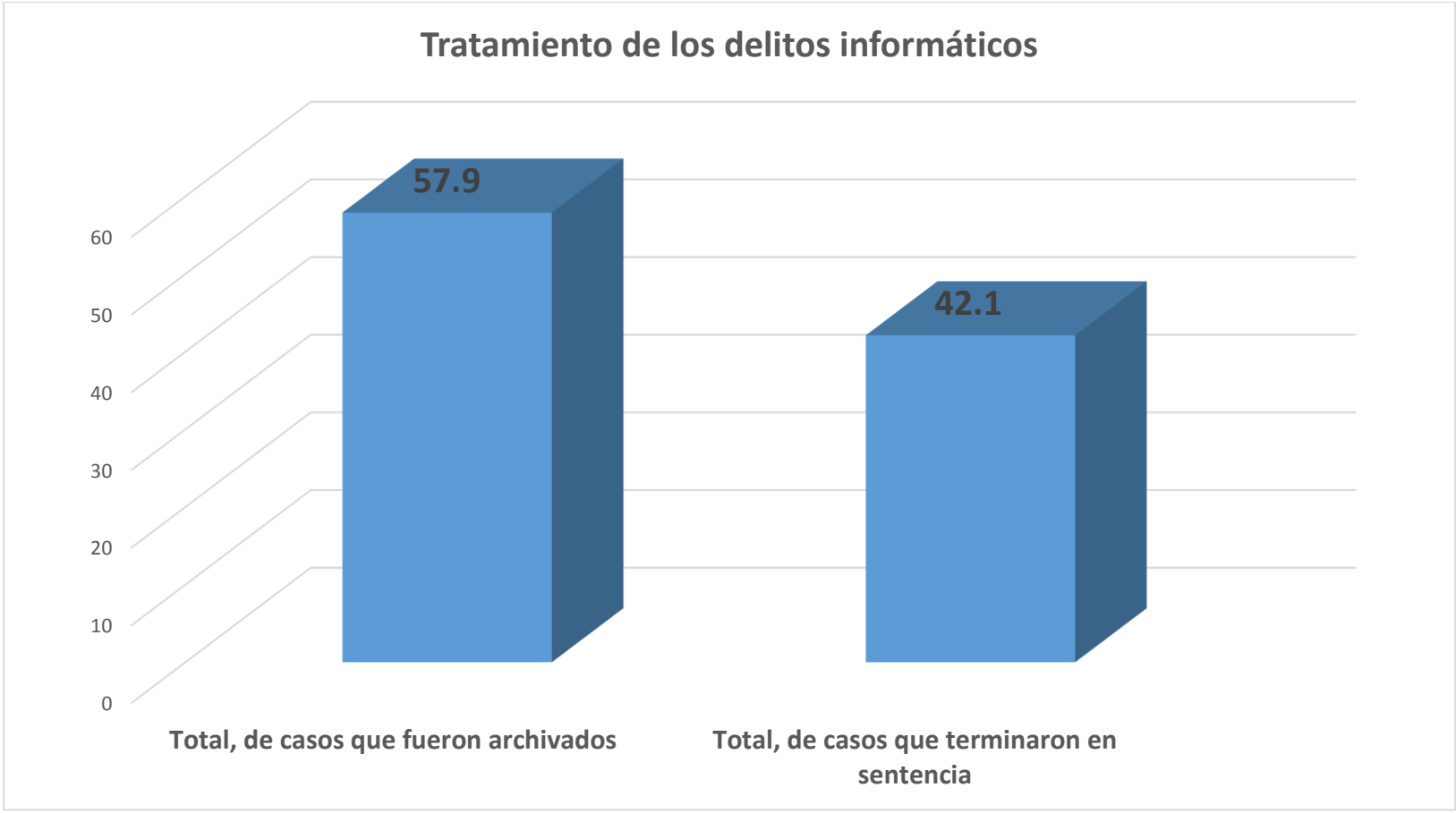
Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

Interpretación y análisis:

El Tratamiento de los delitos informáticos presentados en el Ministerio Publico en la ciudad de Huánuco, fue de la siguiente manera: un 57,9% fueron archivados y un 42,1% terminaron en un proceso normal y con la sentencia dictada.

Grafico n° 11

Tratamiento de los delitos informáticos presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.



Fuente: instrumento de recolección
Investigadora: Meylin del Pilar Romero Ocampo.

CAPITULO V

DISCUSIÓN DE RESULTADOS

5.1. Presentar la contratación de los resultados del trabajo de campo con los referentes bibliográficos de las bases teóricas

Al transcurrir la investigación y los temas examinados, en este capítulo el objetivo es llegar a una discusión de los resultados obtenidos durante la realización del presente trabajo. Esto con el objeto de determinar si la pregunta inicial de dicha investigación fue respondida y si los objetivos fueron alcanzados.

Para ello es necesario realizar nuevamente la pregunta que inicio todo ¿Cuáles son los delitos informáticos cometidos a través de las redes sociales y que tratamiento le brinda el Ministerio Publico en la ciudad de Huánuco, 2016?

Esta interrogante es las que se han procurado resolver durante la realización de la presente tesis, analizando nuestra legislación, la situación actual y las conductas atípicas que afectan a nuestra sociedad.

Los delitos informáticos se presentan en todo tipo de sociedades del mundo y en el Perú no es un país ajeno a dichas situaciones, pero lastimosamente se encuentra a la deriva en lo que respecta a la adaptación de sus leyes a la nueva era tecnológica, permaneciendo de esta forma ajeno a lo todo aquello que es necesario para la regulación y aplicación eficaz del mismo, si bien el país peruano posee normas que buscan proteger a la

sociedad, estas dejan de lado la tecnología y se olvidan del hecho de que el mundo es de cambio constante y el ordenamiento jurídico de los países debe adaptarse a ello.

La base de la adecuada conducta en el mundo cibernético es adquirida desde el hogar, la escuela o colegio, hasta las amistades e influencias en la persona; pero aun tomando en cuenta algunas medidas de precaución, nadie está extinto de los expertos en delitos en la red, por lo que es necesario que la víctima denuncie y reporte el hecho criminal y que los investigadores estén plenamente capacitados en materia digital, electrónica y cibernética para la investigación y correcta resolución del caso.

Al analizar los delitos informáticos más frecuentes en el Ministerio público de Huánuco pudimos apreciar que la destrucción de base de datos representa el 26,1%; el Tráfico ilegal de datos 19,3%; el Atentado a la integridad de datos informáticos el 13,6%; el Atentado a la integridad de sistemas informáticos un 12,5%; las Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos 10,2%; la Interceptación de datos informáticos el 9,0%; el Fraude informático 4,5%; la Suplantación de identidad el 2,2% y el Abuso de mecanismos y dispositivos informáticos el 2,2% tales resultados concuerdan con los datos elaborados a nivel nacional por Temperini, Marcelo Gabriel en su estudio titulado **“Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte”.** De acuerdo a diferentes estudios actuales, los delitos informáticos son los de mayor crecimiento en los últimos años, con una proyección cada vez mayor. En este marco, la presente investigación

tiene por objeto analizar la situación de los delitos informáticos en la región, en su aspecto material sustantivo, a través de un desarrollo de derecho comparado sobre los diferentes países de Latinoamérica (Temperini, 2013).

5.2. Presentar la contrastación de la hipótesis general en base a la prueba de hipótesis (en caso de haberla formulado)

Nuestra prueba de hipótesis planteada manifestaba lo siguiente **"Si los delitos informáticos cometidos a través de redes sociales las mismas que no se identifican a los autores por falta de peritos especialistas, entonces su tratamiento en el ministerio publico conduce al Archivamiento de las denuncias",** dicha prueba de hipótesis se evidencio en nuestros resultados, pues como se evidencio el Tratamiento de los delitos informáticos presentados en el Ministerio Publico en la ciudad de Huánuco, fue que el 57,9% fueron archivados a falta de la identificación de los autores por falta de peritos especialistas. Para contrastar nuestra prueba de hipótesis con otros estudios y teorías pudimos evidenciar que en el Ecuador el año 2016 Alcívar Trejo, Carlos investigo **"Los medios de comunicación y la estafa electrónica. Nueva forma de delito",** cuyo objetivo fue el objetivo general es revisar las normas legales existentes en Ecuador, viendo los códigos acerca de las normas y penas legales sobre estos delitos en nuestro país. Además de conceptualizar la definición de delitos informáticos y realizar la respectiva encuesta y determinar una conclusión basado en los resultados de esta (Alcívar Trejo, 2016). Así mismo en Chile el año 2013 Oxman, Nicolás investigo las "**Estafas**

informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming". Este trabajo aborda la imputación penal de los fraudes informáticos de apoderamiento patrimonial más comunes en Chile. Teniendo en cuenta las posibilidades que ofrece el derecho comparado, se tratan el "phishing" y el "pharming" como tipos de estafa informática (Oxman, 2013). En Colombia el año 2012 Rodríguez Arbeláez, Juan David investigo el **“Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación”.** Para concluir que las nuevas prácticas delictivas en Colombia están a la mano de la aplicación de los avances tecnológicos, pero a pesar de esto en Colombia existen las bases legales a partir de las cuales se puede empezar a combatir las diferentes modalidades de delitos informáticos, analizando e interpretando la norma existente para identificar su alcance, obteniendo así elementos de juicio para desarrollar políticas y estrategias en este tema (Rodríguez Arbeláez, 2011).

CONCLUSIONES

Al analizar los delitos informáticos más frecuentes podemos apreciar que la Alteración, daño o destrucción de base de datos representa el 26,1%; el Tráfico ilegal de datos 19,3%; el Atentado a la integridad de datos informáticos el 13,6%; el Atentado a la integridad de sistemas informáticos un 12,5%; las Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos 10,2%; la Interceptación de datos informáticos el 9,0%; el Fraude informático 4,5%; la Suplantación de identidad el 2,2% y el Abuso de mecanismos y dispositivos informáticos el 2,2%.

El Tratamiento de los delitos informáticos presentados en el Ministerio Publico en la ciudad de Huánuco, fue de la siguiente manera: un 57,9% fueron archivados y un 42,1% terminaron en un proceso normal y con la sentencia dictada.

RECOMENDACIONES

1. Se debe realizar un análisis de la legislación penal vigente por parte del Organismo Legislativo en lo relativo a los delitos informáticos, a efecto de determinar si los tipos delictivos vigentes, alcanzan a cubrir todas las acciones que en la práctica atentan contra los sistemas informáticos y el uso adecuado de los mismos.

2. El Ministerio Publico debe establecer un protocolo con procedimientos mínimos, para la recuperación de la evidencia informática y su evaluación pericial, el cual debe contener el perfil del perito informático, los procedimientos de recuperación de la evidencia informática, de su peritación y requisitos del informe pericial, que permitan la confiabilidad de esta evidencia como rnedio de prueba.

3. A través de una instrucción del Fiscal General del Ministerio Publico debe de ser autorizado, un protocolo de procedimientos en la investigación informática, el cual debe ser implementado por medio de un Manual Para la investigación de delitos informáticos.

4. Se debe crear en el Ministerio Público, en la Dirección de Criminologías, una Unidad de Investigación Informática, con competencia en la recuperación de la evidencia digital en las escenas del crimen de los delitos informáticos y su análisis pericial, debiendo estar dotada de personal adecuado y equipos y programas informáticos apropiados.

REFERENCIAS BIBLIOGRÁFICAS

Alcívar Trejo, C. (2016). Los medios de comunicación y la estafa electrónica. Nueva forma de delito. In Crescendo. Derecho., 3(1), 61-77.

Álvarez Marañón, G., & Pérez García, P. P. (2004). Seguridad informática para la empresa y particulares. Madrid: McGraw-Hill.

Broadhurst, R. (2014). An Analysis of the Nature of Groups engaged in Cyber Crime. International Journal of Cyber Criminology, 1-20.

Campos, M. A. (07 de abril de 2015). Historia del delito informatico. Recuperado el 01 de setiembre de 2016, de http://delitosinformaticospe.blogspot.pe/2015/04/historia-del-delito-informatico.html

Carter, D. (2000). Cómo funcionan los criminales tecnológicos. FBI Law Enforcement Bulletin, 21-27.

Estrada Garavilla, M. (12 de junin de 2011). DELITOS INFORMÁTICOS. Recuperado el 01 de setiembre de 2016, de: https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf

Gurpreet, D., & Steve, M. (2005). Delitos informáticos: teorizar sobre el enemigo dentro. Computers & Security, 22.

Kumar, V. (2014). Paradigmas actuales y futuros del delito cibernético y de la seguridad - Tendencias de crecimiento y aumento. International Conference on Artificial Intelligence with Applications in Engineering and Technology, 22.

Lopez Hernandez, M. A. (12 de junio de 2011). SEGURIDAD INFORMATICA. Recuperado el 01 de setiembre de 2016, de: http://alejandr00022.blogspot.pe/p/seguridad-informatica.html

Mona Al-achkar Jabbour. (1 de febrero de 2016). Seguridad Cibernetica contra delitos informaticos. Obtenido de: http://worldjusticeproject.org/blog/importance-cyber-security

Ojeda Pérez, J. E. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. cuad. contab, 11(28), 41-66.

Ojeda Pérez, J. E., Rincón Rodríguez, F., Arias Flórez, M. E., & Daza Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuaderno de contabilidad, 49.

Oxman, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming". Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, 41(1), 211 - 262.

Palazzi, P. A. (2000). Delitos Informáticos Ad-Hoc. Buenos Aires.

RIQUERT, M. A. (2011). ESTADO DE LA LEGISLACIÓN CONTRA LA DELINCUENCIA INFORMÁTICA EN EL MERCOSUR. Recuperado el 01 de agosto de 2016, de: https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_88.pdf

Rodríguez Arbeláez, J. D. (12 de junio de 2011). Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación. Recuperado el 31 de agosto de 2016, de: http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1334/2/Delitos%20en%20las%20Redes%20Sociales.pdf

Supo, J. (2014). Recuperado el 24 de mayo de 2016, de Niveles de Investigación: http://seminariosdeinvestigacion.com/niveles-de-investigacion/

Temperini, M. G. (12 de junio de 2013). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. Recuperado el 01 de setiembre de 2016: de http://conaiisi.unsl.edu.ar/ingles/2013/82-553-1-DR.pdf

ANEXO

Ficha de recolección de datos

DELITOS INFORMÁTICOS COMETIDOS A TRAVÉS DE REDES SOCIALES Y SU TRATAMIENTO EN EL MINISTERIO PUBLICO EN LA CIUDAD DE HUÁNUCO, 2016.

1. **Interferencia, acceso o copia ilícita contenida en base de datos**
   a) Total, de casos presentados
   b) Total, de casos que fueron archivados
   c) Total, de casos que terminaron en sentencia
2. **Alteración, daño o destrucción de base de datos.**
   a) Total, de casos presentados:
   b) Total, de casos que fueron archivados:
   c) Total, de casos que terminaron en sentencia:
3. **Tráfico ilegal de datos**
   a) Total, de casos presentados:
   b) Total, de casos que fueron archivados:
   c) Total, de casos que terminaron en sentencia:
4. **Atentado a la integridad de datos informáticos**
   a) Total, de casos presentados:
   b) Total, de casos que fueron archivados:
   c) Total, de casos que terminaron en sentencia:
5. **Atentado a la integridad de sistemas informáticos**
   a) Total, de casos presentados:

b) Total, de casos que fueron archivados:

c) Total, de casos que terminaron en sentencia:

6. **Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos**

a) Total, de casos presentados:

b) Total, de casos que fueron archivados:

c) Total, de casos que terminaron en sentencia:

7. **Interceptación de datos informáticos**

a) Total, de casos presentados:

b) Total, de casos que fueron archivados:

c) Total, de casos que terminaron en sentencia:

8. **Fraude informático**

a) Total, de casos presentados:

b) Total, de casos que fueron archivados:

c) Total, de casos que terminaron en sentencia:

9. **Suplantación de identidad**

a) Total, de casos presentados:

b) Total, de casos que fueron archivados:

c) Total, de casos que terminaron en sentencia:

10. **Abuso de mecanismos y dispositivos informáticos**

a) Total, de casos presentados:

b) Total, de casos que fueron archivados:

c) Total, de casos que terminaron en sentencia:

- Resolución de Aprobación del proyecto de trabajo de investigación
- Resolución de Nombramiento de Asesor
- Matriz de Consistencia

MATRIZ DE CONSISTENCIA

TITULO: DELITOS INFORMÁTICOS COMETIDOS A TRAVÉS DE REDES SOCIALES Y SU TRATAMIENTO EN EL MINISTERIO PUBLICO EN LA CIUDAD DE HUÁNUCO, 2016.

TESISTA: MEYLIN DEL PILAR ROMERO OCAMPO

FORMULACION DEL PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES	TECNICAS
PROBLEMA GENERAL: ¿Cuáles son los delitos informáticos cometidos a través de las redes sociales y que tratamiento le brinda el Ministerio Publico en la ciudad de Huánuco, 2016? **PROBLEMA ESPECIFICOS:** ✓ ¿Cuáles son los delitos informáticos cometidos a través de las redes sociales en el Ministerio Publico en la ciudad de Huánuco, 2016? ✓ ¿Cuál es el tratamiento de los delitos informáticos presentados en el Ministerio Publico en la ciudad de Huánuco, 2016?	**Objetivo General:** Determinar los delitos informáticos cometidos a través de las redes sociales y el tratamiento que le brinda el Ministerio Publico en la ciudad de Huánuco, 2016. **Objetivos Específicos** -Identificar los delitos informáticos cometidos a través de las redes sociales en el Ministerio Publico en la ciudad de Huánuco, 2016. -Identificar el tratamiento que se le brinda a los delitos informáticos presentados en el Ministerio Publico en la ciudad de Huánuco, 2016.	**Hipótesis del investigador** Si los delitos informáticos cometidos a través de redes sociales las mismas que no se identifican a los autores por falta de peritos especialistas, entonces su tratamiento en el ministerio publico conduce al Archivamiento de las denuncias.	**Variables** **Variable independiente** Redes sociales **Variable Dependiente** Delitos informáticos	Entrevistas Encuestas Análisis Documental Análisis Estadístico **METODOLOGIA** Observacional Prospectivo Transversal descriptivo