UNIVERSIDAD PRIVADA SAN CARLOS

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE DERECHO

TESIS

DELITOS INFORMÁTICOS Y LA EVIDENCIA DIGITAL EN EL PROCESO PENAL PERUANO 2023

PRESENTADA POR:

JERRY KENT PORTUGAL ROMAN

PARA OPTAR EL TÍTULO PROFESIONAL DE:

ABOGADO

PUNO – PERÚ

2024

PLAGIARISM CHECK.ORG

6.97%

SIMILARITY OVERALL

SCANNED ON: 29 DEC 2023, 10:35 PM

Similarity report

Your text is highlighted according to the matched content in the results above.

IDENTICAL 3.61%

CHANGED TEXT 3.36%

Report #19236613

JERRYKENT PORTUGAL ROMAN DELITOS INFORMÁTICOS Y LA EVIDENCIA DIGITAL EN EL PROCESO PENAL PERUANO 2023 RESUMEN En la presente investigación como eje principal son los delitos informáticos y la evidencia digital de los mismos, por la que se tuvo objetivo general: Analizar cómo la admisión de la evidencia digital incide en los delitos informáticos en el proceso penal peruano. 1 2 ElMétodo usado en la presente investigación se da a través de un diseño no experimental de corte transversal con enfoque cualitativo por su naturaleza jurídica, en el modelo jurídico descriptivo. Elinstrumento utilizado fue la entrevista lo que nos permitió recoger toda la información necesaria. Se ha obtenido como conclusión general: Se ha establecido que la prueba digital, independientemente de su clasificación jurídica como documento electrónico, mensaje de datos u otras formas, se acepta generalmente como medio de prueba válido en las legislaciones penales. Por lo tanto, está permitido utilizar pruebas digitales ante un tribunal para establecer la veracidad o falsedad de las circunstancias de hecho controvertidas o la responsabilidad penal del acusado. Palabras Clave: Evidencia digital, cibercrimen, delitos informáticos. ABSTRACT The main focus of this research is computer crimes and the digital evidence of the same, for which the general objective was: To analyse how the admission of digital evidence affects computer crimes in the Peruvian criminal process. 1 4 Themethod used in this research was a

Yudy Roxana ALANIA LAQUI
Oficina de Repositorio Institucional

UNIVERSIDAD PRIVADA SAN CARLOS

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE DERECHO

TESIS

DELITOS INFORMÁTICOS Y LA EVIDENCIA DIGITAL EN EL PROCESO PENAL PERUANO 2023

PRESENTADA POR:

JERRY KENT PORTUGAL ROMAN

PARA OPTAR EL TÍTULO PROFESIONAL DE:

ABOGADO

APROBADA POR EL SIGUIENTE JURADO:

PRESIDENTE : _____
Dr. BENITO PEPE CALSINA CALSINA

PRIMER MIEMBRO : _____
M.Sc. YANINA MILAGROS HUANCA EXCELMES

SEGUNDO MIEMBRO : _____
Mtro. JOEL JAEN PUMA COILA

ASESOR DE TESIS : _____
Mg. MARTIN WILLIAM HUISA HUAHUASONCCO

Área: Ciencias Sociales.

Sub Área: Derecho

Línea de Investigación: Derecho.

Puno, 23 de febrero del 2024.

DEDICATORIA

Este informe de tesis lo Dedico, con mucho cariño a mis hijos Carmen del Rosario y Gadiel Jamil Kent y a mi compañera y esposa Edith, personas muy importantes y valiosas en mi vida, ellos me impulsan a lograr mis metas y objetivos con mucha fuerza.

También dedico este trabajo a mis padres y hermanos, quienes siempre están en todo momento motivándome a seguir adelante con mi vida.

AGRADECIMIENTO

Agradezco a Dios, por bendecirme en el desarrollo de esta tesis, a mi familia por incentivarme día a día a lograr mis objetivos trazados. A la Universidad Privada “San Carlos”, a mis docentes por compartir sus enseñanzas idóneas y a mi Asesor M. Sc. Martin William HUISA HUAHUASONCO, quien con paciencia y mucho entusiasmo me guio en la elaboración del presente informe.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE ANEXOS

RESUMEN

En la presente investigación como eje principal son los delitos informáticos y la evidencia digital de los mismos, por la que se tuvo objetivo general: Analizar cómo la admisión de la evidencia digital incide en los delitos informáticos en el proceso penal peruano. El Método usado en la presente investigación se da a través de un diseño no experimental de corte transversal con enfoque cualitativo por su naturaleza jurídica, en el modelo jurídico descriptivo. El instrumento utilizado fue la entrevista lo que nos permitió recoger toda la información necesaria. Se ha obtenido como conclusión general: Se ha establecido que la prueba digital, independientemente de su clasificación jurídica como documento electrónico, mensaje de datos u otras formas, se acepta generalmente como medio de prueba válido en las legislaciones penales. Por lo tanto, está permitido utilizar pruebas digitales ante un tribunal para establecer la veracidad o falsedad de las circunstancias de hecho controvertidas o la responsabilidad penal del acusado.

Palabras Clave: Evidencia digital, Cibercrimen, Delitos informáticos.

ABSTRACT

The main focus of this research is computer crimes and the digital evidence of the same, for which the general objective was: To analyse how the admission of digital evidence affects computer crimes in the Peruvian criminal process. The method used in this research was a non-experimental cross-sectional design with a qualitative approach due to its legal nature, in the descriptive legal model. The instrument used was the interview, which allowed us to collect all the necessary information. As a general conclusion: It has been established that digital evidence, regardless of its legal classification as an electronic document, data message or other forms, is generally accepted as a valid means of evidence in criminal legislations. Therefore, it is permissible to use digital evidence in court to establish the truth or falsity of disputed factual circumstances or the criminal liability of the accused.

Keywords: Digital evidence, Cybercrime, Computer crime.

INTRODUCCIÓN

En la presente tesis nace a partir de la problemática de la evidencia digital y los cibercrímenes, por lo que se trató de dar un panorama desde la perspectiva de uno de los actore importantes dentro de la investigación de este delito, la PNP, por lo que se analizó de manera descriptiva jurídica. El Método de la presente investigación presenta un diseño no experimental de corte transversal con enfoque cualitativo y por su naturaleza jurídica descriptiva.

Es importante mencionar la estructura por la que se desarrolló la presente investigación, siendo esta dividida en cuatro capítulos, los cuales se componen desde el Planteamiento del Problema, Marco teórico, marco metodológico y los resultados de la Investigación.

En el Capítulo I, se formula el problema, destacando los antecedentes y los objetivos. En el Capítulo II, se desarrolla el marco teórico, con énfasis en la base teórica y la definición conceptual, en este apartado es importante mencionar que por cuanto el enfoque de estudio es cualitativo se omitió contar con hipótesis. En el Capítulo III, se desarrolló la metodología, precisando el tipo, diseño de investigación y los instrumentos que se usaron para la investigación, asimismo las técnicas de recolección de datos. En el Capítulo IV, se realizó la exposición de los resultados analizando e interpretando los mismos. Finalizando con las conclusiones, recomendaciones, y en los anexos se incluyen los instrumentos de investigación, la matriz de consistencia y los documentos necesarios para un mayor ahondamiento del tema de investigación.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA, ANTECEDENTES Y OBJETIVOS DE LA INVESTIGACIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA.

Las dinámicas sociales en el Perú están sujetas a continuas transformaciones, y en este caso nos centraremos en el dominio de la tecnología. Específicamente, examinaremos la prevalencia de comportamientos digitales ilícitos, que plantean desafíos a la eficacia de los marcos legales para regularlos debido a su naturaleza generalizada. La duración de un día está sujeta a variaciones según el estilo de vida adoptado por un individuo. Por tanto, el objetivo de este estudio es determinar el proceso regulatorio adecuado para adquirir y posteriormente preservar las "huellas digitales" asociadas a estos comportamientos, comúnmente denominadas "evidencias digitales" en el ámbito del cibercrimen. Esta investigación tiene como objetivo explorar la legislación probatoria pertinente para establecer la responsabilidad penal.

Por lo tanto, la adquisición y preservación de evidencia digital requiere una comprensión integral de los requisitos legales, lo que a su vez facilita la identificación del tratamiento, las fuentes y las características apropiadas de dicha evidencia. Este conocimiento es crucial para garantizar la adquisición y preservación consistente y efectiva de evidencia digital a largo plazo.

Como resultado de las circunstancias antes mencionadas, existe una necesidad reconocida de abordar los desafíos que plantean las actividades delictivas digitales y las

complejidades procesales asociadas. En consecuencia, el establecimiento de Fiscalías Especializadas en Delitos Cibernéticos ha surgido como una solución viable, en la que a un organismo gubernamental competente (como el Ministerio Público) se le confía la responsabilidad de manejar diversas formas de delitos cibernéticos.

Además, el desafío persistente en el campo de la logística se relaciona con la escasez de análisis de expertos. Este problema se atribuye principalmente a la limitada disponibilidad de recursos humanos con conocimientos especializados en el tema, así como a la ausencia de herramientas informáticas de análisis adecuadas. Esta observación ha sido destacada por los expertos en la materia antes mencionados.

1.1.1 Problema General

1. ¿Cómo la admisión de la evidencia digital incide en los delitos informáticos en el Proceso penal peruano?

1.1.2 Problemas Específicos.

1. ¿Cómo la protección de la evidencia digital influye en la clasificación de los Delitos Informáticos en el Proceso Penal Peruano?
2. ¿Cómo la determinación del Marco Legal de la Evidencia Digital repercute en la tipicidad de los delitos informáticos en el Proceso Penal Peruano?

1.2 ANTECEDENTES

Los trabajos previos o antecedentes son el conjunto de toda conclusión obtenidas por investigaciones pasadas relacionadas al tema que se investiga. En ese sentido citaremos algunas investigaciones relacionadas al tema planteado:

1.2.1 A NIVEL INTERNACIONAL

(SICHACA, 2019) En su publicación académica titulada "Requisitos legales previos para la admisibilidad legal de las pruebas digitales", el autor llega a la siguiente conclusión: "La

regulación existente relativa a las pruebas digitales es inadecuada, por lo que se requiere una comprensión exhaustiva de los principios y normas legales que rigen las pruebas y el derecho procesal, así como la familiaridad con las metodologías y procedimientos que garanticen la presentación adecuada de las pruebas digitales de una manera jurídicamente sólida." En pocas palabras, es crucial que los operadores jurídicos posean conocimientos suficientes y actualizados de los avances tecnológicos relacionados con las actividades delictivas digitales. Este requisito se refleja en la normativa legal, que incluye las disposiciones necesarias para combatir eficazmente dichas actividades. Por lo tanto, es imperativo que los operadores jurídicos se mantengan constantemente informados y actualizados sobre la evolución de las conductas delictivas digitales.

Rincon (2015) En su Tesis Doctoral titulada "El delito en la cibersociedad y la justicia penal internacional", con la que obtuvo el Doctorado en Derecho por la Universidad Complutense de Madrid, el autor defiende que las fronteras geográficas de los países no deben obstaculizar la investigación y persecución eficaz de los delitos informáticos. Subraya que en el ciberespacio, donde no existen fronteras físicas, la localización del autor puede diferir de la de la víctima, lo que hace crucial determinar la jurisdicción para el castigo. El autor insiste en la necesidad de establecer un sistema de justicia universal, con especial atención al Derecho Comparado y a la Cooperación Internacional.

Duarte (2017), El libro "Valoración probatoria de los documentos audiovisuales" explora la conexión entre las pruebas ilícitas y los documentos audiovisuales, así como las garantías constitucionales asociadas a la adquisición de tales documentos. También examina el valor probatorio de los documentos audiovisuales y su admisibilidad en el proceso penal. Esta investigación fue realizada como parte de los requisitos para obtener el grado de Magíster en Derecho con especialidad en Derecho Procesal por la Universidad Nacional Mayor de San Marcos.

Contar con antecedentes en el trabajo de investigación es crucial. Según Salvador (2009), los marcos de referencia se utilizan para situar un estudio dentro de un determinado dominio de conocimiento que abarca el tema en cuestión (p. 197). Por el contrario, según Vara (2010), un estudio debe partir de una base de datos que actúe como catalizador de las ideas del investigador. Los datos adquiridos deben ser directamente relevantes para la investigación" (p. 615).

Gercke (2014), El informe titulado "Ciberseguridad" de la UIT. "Comprender la ciberdelincuencia: Fenómenos, Desafíos y Respuesta Legal" ofrece una visión significativa de las estadísticas mundiales que ayudan a evaluar la magnitud de las repercusiones globales derivadas de la ciberdelincuencia. La Unión Internacional de Telecomunicaciones (UIT), organización especializada de las Naciones Unidas para las Tecnologías de la Información y la Comunicación (TIC), está formada por 193 Estados miembros y 700 empresas tecnológicas. Los estudios publicados por la UIT ofrecen una visión útil de la situación actual de la ciberdelincuencia y ponen de relieve las debilidades que encontramos en todo el mundo para contrarrestar. En esencia, se ajustarán a los siete objetivos estratégicos especificados en la Agenda de Ciberseguridad Global de la UIT. El objetivo principal es fomentar la creación de una legislación que pueda aplicarse a escala mundial, respetando al mismo tiempo los procedimientos, instituciones y parámetros de cada nación. Además, reconoce que los ciber peligros pueden surgir en cualquier lugar del planeta.

1.2.2 A NIVEL NACIONAL

(Escobedo, 2018) En su publicación titulada "La Admisibilidad y Valor Probatorio de las Pruebas Digitales en el Sistema Jurídico Peruano 2018", el autor concluye que los delitos informáticos que ocurren en el ciberespacio están estrechamente vinculados al internet, dando lugar a delitos transnacionales que sobrepasan los límites de las leyes y jurisdicciones individuales. Este tipo de delitos involucran a múltiples países en un solo

hecho. Teniendo en cuenta el concepto adquirido, resulta evidente que estos delitos necesitan herramientas tecnológicas para su comisión dentro del ámbito digital. En concreto, la utilización de "Internet" sirve como medio de transmisión de los datos necesarios para la ejecución de dichas conductas delictivas digitales. Esto permite que la vulneración de bienes jurídicos se produzca con independencia de las fronteras geográficas, abarcando distancias que van desde meros metros a extensos kilómetros, o incluso atravesando continentes. En consecuencia, se plantea el reto de establecer la demarcación territorial y determinar el marco jurídico responsable de abordar y sancionar tales delitos.

Gamarra (2017), En su tesis "Implementación de la Política Pública de Fortalecimiento de la Función Criminalística en la Policía: Problemas y Soluciones (2013-2106)", el autor realiza un profundo análisis de las políticas públicas de seguridad a través del Decreto Legislativo Nº 1219 de la Ley de Fortalecimiento de la Función Criminalística. El objetivo de esta política es mejorar los conocimientos de los peritos especializados de la PNP y de la Dirección Ejecutiva de Criminalística (DIREJCRI).

A la inversa, ofrece una representación del avance de la modernización tecnológica de los equipos forenses en el DIREJCRI - PNP entre 2013 y 2016. Además de conocer el estado actual de la infraestructura del laboratorio de criminalística de la PNP, también es importante evaluar su rendimiento en relación con los estándares deseados.

Nuñez (2016), Por otro lado, presenta un retrato de los avances en la actualización tecnológica de los equipos forenses en el DIREJCRI - PNP de 2013 a 2016. Es fundamental evaluar el desempeño de la infraestructura del laboratorio de criminalística de la PNP en relación a los estándares previstos, además de conocer su estado actual.

Suarez (2015), en su Tesis "La Ciberguerra y la aplicaciÓn de los Principios del Derecho Internacional Humanitario", el cual nos brinda las primeras luces para una Propuesta de

"Plan Estratégico de Ciberseguridad en el Perú", como la necesidad que tendría el Estado de difundir el Derecho Internacional Humanitario.

Abanto (2016), En su tesis titulada "La desprotección de los datos personales de los internautas peruanos, expuestos a códigos maliciosos y su incidencia en la vulneración del derecho a la intimidad", el autor presenta un análisis exhaustivo de la inadecuada salvaguarda de los datos personales, sus diversas modalidades y la aplicación de métodos probatorios en el proceso penal. El autor también hace hincapié en la necesidad de una normativa especial para hacer frente a la naturaleza evolutiva de las pruebas digitales. Subraya la necesidad de que las pruebas digitales sean fiables y legales para que puedan considerarse pruebas valiosas y utilizarse en los procedimientos penales. En consecuencia, ofrece una relación exhaustiva de los métodos adecuados para buscar y recopilar dichas pruebas. A la inversa, establece políticas e iniciativas nacionales globales en materia de ciberseguridad.

1.2.3 A NIVEL LOCAL

Hecha la búsqueda bibliográfica respectiva no se han encontrado trabajos relacionados con el presente tema de investigación en el ámbito local.

1.3 OBJETIVOS DE LA INVESTIGACIÓN

1.3.1 Objetivo general

1. Analizar cómo la admisión de la evidencia digital incide en los delitos informáticos en el proceso penal peruano.

1.3.2 Objetivo específico

1. Distinguir como la protección de la Evidencia digital influye en la clasificación de los Delitos Informáticos en el Proceso Penal Peruano.

2. Determinar cómo el Marco Legal de la Evidencia Digital repercute en la Tipicidad de los Delitos Informáticos en el Proceso Penal Peruano

CAPÍTULO II

MARCO TEÓRICO, CONCEPTUAL E HIPÓTESIS DE LA INVESTIGACIÓN

2.1 MARCO TEÓRICO

Delitos informaticos

El rápido desarrollo y la adopción generalizada de las Tecnologías de la Información y la Comunicación (TIC) han dado lugar a importantes transformaciones en la sociedad, que presentan un marcado contraste con el panorama social de hace 15 años. Dichas alteraciones exhiben un carácter sistemático y expeditivo. Generan continuamente nuevas perspectivas sobre el estilo de vida. Los seres humanos, como individuos adaptables, adoptan e incorporan la tecnología emergente a su vida cotidiana, utilizándose para mejorar la sociedad. Sin embargo, es crucial asegurarse de que estas acciones no infringen los derechos de los demás. Mientras estos esfuerzos se mantengan dentro de los límites de la legalidad, pueden llevarse a cabo sin más complicaciones. Lamentablemente, por el contrario, la utilización de Internet y de los medios electrónicos como herramientas para actividades delictivas o como plataformas para cometer infracciones supone una amenaza significativa para la sociedad, que requiere medidas punitivas adecuadas. Este tipo de conducta perjudicial se denomina comúnmente delito informático, ciberdelito o ciberdelincuencia.

Según Rayon & Gomez (2014) El término "ciberdelito" se refiere a cualquier acto delictivo que esté sujeto a consecuencias jurídicas, como afirma el autor (p.211). Este tipo de delito implica la utilización de equipos informáticos o Internet, ya sea para la ejecución del

delito o como objetivo del delito en sí. La llegada de la tecnología informática ha facilitado la adquisición y utilización de estas novedosas herramientas por parte de las organizaciones criminales, permitiéndoles perpetrar actividades ilícitas. En este contexto, cabe destacar que el Sujeto Activo responsable de ejecutar la acción tiene un patrón de comportamiento acorde con un individuo que posee conocimientos especializados en el campo de las Tecnologías de la Información. Estos individuos están afiliados a redes criminales y exhiben un notable nivel de experiencia y capacitación. Su ciberseguridad se ve frecuentemente comprometida.

El problema contemporáneo del delito cibernético plantea un obstáculo importante en términos de su persecución, principalmente debido a la dificultad para identificar con precisión a los individuos responsables de tales actividades delictivas. Este desafío se ve exacerbado aún más por la falta de cooperación eficiente entre las partes interesadas relevantes. Sin embargo, vale la pena señalar que el ciberdelito a menudo resulta ser una actividad más lucrativa para numerosos delincuentes, superando las ganancias generadas por el tráfico de drogas y resultando en el movimiento de millones de dólares anualmente. Según Quinteros, la jurisdicción relativa al cibercrimen en el ciberespacio es de naturaleza global, lo que resulta en una multitud de ubicaciones territoriales tanto para los perpetradores como para los proveedores de servicios. Por lo tanto, el autor enfatiza que la cuestión principal relacionada con el delito cibernético no surge de la falta de criminalización o jurisdicción, sino más bien del establecimiento de un tribunal competente capaz de juzgar estos delitos (2014, p.186).

En el contexto de la clasificación de la ciberdelincuencia, se reconoce que puede manifestarse como medio o como elemento material. Según Zegarra (2015, p.111), el comportamiento delictivo que incluye la utilización de ordenadores e internet como modus operandi se observa dentro del ámbito de los medios de comunicación. Es importante señalar que la categorización del uso como herramienta se refiere a su utilización en la comisión de actividades delictivas, siendo los delitos tradicionales a menudo los objetivos

finales en muchos casos. Zegarra (2015, p. 111) aclara además que las actividades delictivas dirigidas a los ordenadores, es decir, las dirigidas a la tecnología de la información, se clasifican como delitos contra objetos materiales.

Clasificación de los Delitos informáticos

Diversos autores han dejado varias posturas sobre la clasificación de los delitos informáticos. Pero Tellez citado por Gil (2007) tiene la clasificación más acorde a nuestra investigación.

Los delitos informáticos, también conocidos como delitos informáticos, engloban todas las actividades ilícitas que utilizan las tecnologías de la información y las comunicaciones (TIC) como herramienta o método. Esto incluye actividades como la alteración fraudulenta de documentos digitales (como valores, propiedad intelectual, tarjetas de crédito, cheques, etc.) y la manipulación de registros financieros dentro del sistema contable de una empresa. Además del desarrollo estratégico y modelamiento de actividades criminales tradicionales como robo, homicidio, fraude, explotación infantil, trata de personas, pornografía infantil y fraude financiero, entre otras.

Los delitos informáticos se refieren a actividades delictivas que apuntan específicamente a computadoras, sus periféricos o programas como entidades tangibles. En el contexto de las instrucciones de programación, se puede observar que existe un caso en el que el sistema experimenta un cese total de funcionalidad. El acto de eliminar y erradicar la base de datos de una empresa. Participar en manipulación no autorizada de la infraestructura de servidores de una corporación. El acto de hacer que los programas sean inoperables por diversos medios. Deterioro cognitivo. El acto de agredir físicamente a la máquina o sus componentes asociados. El acto de sabotaje político o terrorismo implica la destrucción o incautación deliberada de centros nerviosos computarizados. El acto de apoderarse de medios magnéticos, que contienen información valiosa, con la

intención de extorsionar a personas u organizaciones mediante chantaje, que generalmente implica la exigencia de pagos de rescate, entre otros métodos.

Tipicidad de los Delitos informáticos

Para Lopez (2013) La tipicidad se refiere a la característica atribuida al comportamiento que se ajusta al arquetipo delictivo (p. 53). En otras palabras, este comportamiento significa que el acto entra dentro del ámbito del Derecho penal, ya que encarna los elementos definitorios de dicho Derecho. Cabe distinguir entre el tipo objetivo, caracterizado por su naturaleza centrada en la acción, y el tipo subjetivo, que se orienta hacia el dolo o la culpa. El legislador no sólo ofrece una descripción objetiva de la conducta que puede ser sancionada, sino que también presenta argumentos y pruebas para respaldar su naturaleza ilícita.

El objetivo de este estudio es determinar los rasgos característicos de los delitos informáticos, que han surgido como consecuencia de los avances en las tecnologías informáticas, dando lugar así a una forma distinta de conducta delictiva.

Tipicidad Objetiva de los Delitos Informáticos

El objetivo del concepto de tipicidad es determinar los criterios precisos para calificar la lesión de un bien jurídico como resultado directo de la actuación de un determinado individuo, en contraposición a ser sólo un resultado de la simple causalidad.

Se realizó un análisis de la norma para determinar la tipicidad objetiva de los delitos informáticos. Este análisis consideró varios factores, incluyendo el objeto del delito, los sujetos involucrados, la acción típica realizada, la relación causal o nexo causal, la imputación objetiva y los elementos descriptivos normativos asociados a esta categoría de delitos.

Según Hurtado (2005), el objetivo del delito se refiere al individuo o entidad a la que se dirige la actividad ilegal (p.413). En otras palabras, abarca todas las entidades que sirven

como foco u objetivo del acto delictivo. En el ámbito de la delincuencia informática, pueden distinguirse varias clasificaciones, que abarcan delitos relacionados con datos y sistemas informáticos, violaciones contra la autonomía sexual y la libertad personal, violaciones de la intimidad y la confidencialidad de las comunicaciones, delitos contra la propiedad y transgresiones contra la confianza pública.

La Accion Tipica para Hurtado (2005) El componente básico del aspecto objetivo de la categoría jurídica está formado por una acción especificada por el verbo principal de la definición jurídica (p.413). En otras palabras, el verbo principal de la norma describe la acción.

Sujetos de los Delitos informáticos

Es imperativo reconocer a cualquier individuo que aspire a convertirse en constituyente de una entidad colectiva. En el escenario actual, quienes se dedican a perpetrar actividades delictivas son el centro de nuestro análisis. Se observa la presencia tanto de un sujeto activo como de un sujeto pasivo.

Para Valdez y Lima citados por Gil (2007) El Sujeto Activo en la ciberdelincuencia se refiere a un individuo que posee rasgos distintivos y no se ajusta al perfil típico de un delincuente. Poseen los conocimientos necesarios para gestionar sistemas informáticos y suelen estar situados en lugares estratégicos para facilitar el acceso a información sensible. Por otra parte, muestran destreza en el manejo de sistemas informáticos. Por lo tanto, no se ajustan al perfil de un delincuente típico, que puede ser fácilmente reconocido; en cambio, operan de forma encubierta a través de una serie de códigos numéricos, y su comprensión se basa en la lógica binaria. Su excepcional destreza sigue provocando numerosos debates éticos y educativos, con sugerencias de restringir el acceso a estos conocimientos.

(EnfoqueDerecho, 2021) El ámbito de la ciberdelincuencia contra la propiedad intelectual abarca varias formas de comportamiento ilícito. Sin embargo, establecer la comisión de estos delitos presenta importantes retos en términos de prueba probatoria

Los ataques cibernéticos puros se refieren a instancias en las que se utilizan tecnologías novedosas como medio empleado y como objetivo, mientras que las réplicas de ataques cibernéticos implican la utilización de nuevas tecnologías para perpetrar actividades delictivas convencionales.

Sugiero que la correlación entre el delito cibernético y los delitos relacionados con la propiedad intelectual, también denominados "delitos contra los derechos intelectuales" de acuerdo con el Código Penal, cae dentro del ámbito del segundo dominio. La utilización de nuevas tecnologías, como Internet y el diseño de software, así como la creación de herramientas de comunicación masiva, facilitan la perpetración de delitos que antes prevalecían antes de su difusión generalizada.

¿Cuál es el problema relacionado con la presentación y evaluación de la evidencia? El tema que nos ocupa se refiere a la investigación realizada en entornos digitales. El proceso de investigación y adquisición de evidencia digital es intrínsecamente complejo, particularmente cuando no se ejecuta con precisión. Esta complejidad surge de la volatilidad inherente asociada con la evidencia digital. Actualmente, el objeto en cuestión está en nuestro poder; pero posee el potencial de desaparecer en un pequeño lapso de segundos o minutos. Como ilustración, considere el escenario hipotético de transmitir un mensaje por un medio telegráfico, en el que el mensaje se vuelve efímero y está sujeto a destrucción en un período de tiempo específico de 3, 5 o 10 segundos posteriores a su lectura. En el caso de que la información autodestructiva no se retenga en los dispositivos electrónicos, ¿qué métodos podría emplear la fiscalía para recuperar ese material?

Delincuente Informático

El individuo comúnmente considerado como el autor del ciberdelito es frecuentemente el agente activo responsable de ejecutar la actividad ilícita. Según Giménez (2011), los individuos que participan en actividades delictivas informáticas suelen ser personas que ocupan puestos de confianza, como empleados con acceso autorizado a sistemas informáticos. Basándose en datos estadísticos, se ha observado que más del 90% de las actividades delictivas son perpetradas por individuos que poseen conocimientos y familiaridad con el sistema, mientras que en el resto de los casos intervienen técnicos informáticos (p.104).

Esto sugiere que, basándose en el fenómeno, la conducta de los individuos implicados en actividades delictivas informáticas se caracteriza por su cómodo acceso a estos sistemas y su familiaridad con sus vulnerabilidades y deficiencias. Los individuos poseen un conocimiento exhaustivo de cómo eludir las medidas de seguridad, lo que les permite recuperar o erradicar la información requerida.

¿El Perú tiene un marco regulatorio sobre estos delitos contra la Propiedad Intelectual?

El Título VII del Código Penal de 1991 se refiere a los "Delitos contra los derechos intelectuales" y comprende dos capítulos que se examinarán en este análisis.

La categoría inicial se denomina "Delitos contra los derechos de autor y derechos afines", mientras que la categoría posterior se denota como "Delitos contra la propiedad industrial". El primer caso se prevé en el marco de los artículos 216 a 221, mientras que el segundo capítulo se prevé en el marco de los artículos 222 a 225.

Desde el punto de vista normativo, existe una estructura completa destinada a salvaguardar y abordar este fenómeno delictivo en particular.

Por el contrario, en el contexto de la discusión de la ciberdelincuencia, es imperativo reconocer la existencia de normas diferenciadas. La Ley N° 30096, conocida como Ley de Delitos Informáticos, fue promulgada oficialmente en octubre de 2013.

2.2 MARCO CONCEPTUAL

Ciberdelito: Un ciberdelito se refiere a cualquier actividad ilegal que se lleva a cabo en el ámbito digital o utilizando tecnologías de la información y la comunicación. Estas actividades pueden incluir fraudes en línea, ataques informáticos, robo de datos, difusión de malware y otros actos maliciosos realizados con fines ilícitos.

Legislación Cibernética: La legislación cibernética es el conjunto de leyes y regulaciones que rigen las actividades en línea y los comportamientos en el mundo digital. Incluye disposiciones específicas para abordar ciberdelitos, establecer penalidades por violaciones y proporcionar un marco legal para la investigación y el enjuiciamiento de delitos informáticos.

Evidencia Digital: La evidencia digital se refiere a cualquier información o datos electrónicos que pueden ser presentados en un proceso legal para respaldar afirmaciones o acusaciones. Esto puede incluir registros de actividad en línea, correos electrónicos, chats, archivos y otros elementos digitales que se utilizan para demostrar la comisión de un ciberdelito o identificar a los perpetradores.

Ingeniería Social: La ingeniería social implica manipular a las personas para que realicen ciertas acciones o divulguen información confidencial. En el contexto de los ciberdelitos, esto podría incluir engañar a individuos para que revelen contraseñas, información financiera u otros datos personales, con el objetivo de perpetrar fraudes en línea u otros tipos de ataques.

Delincuente Cibernético: Un delincuente cibernético es un individuo o grupo que participa en actividades ilegales en línea. Estas personas utilizan habilidades técnicas

para llevar a cabo ciberdelitos, como ataques de phishing, robo de identidad, distribución de malware o pirateo de sistemas, con el propósito de obtener beneficios financieros o causar daño.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1 METODOLOGÍA.

El trabajo de investigación será de tipo básico, porque todos los aspectos fueron teorizados, de enfoque cuantitativo y de tipo descriptivo jurídico.

3.2 ZONA DE ESTUDIO

3.2.1 Población:

La población es una fuente de información compuesta por personas u objetos, que tienen una o más características en común necesarios para la investigación, según (Arias, 2012), la población es aquel grupo de elementos que se encuentran delimitados por el problema y objetivo del trabajo de investigación, dichos elementos tienen características similares.

La población fue compuesta por los efectivos policiales del Área de Investigación Criminal AREINCRI PNP de la jurisdicción de la provincia de Puno.

3.3 TAMAÑO DE MUESTRA

3.3.1 Muestra

La muestra sera tomada utilizando procedimientos aleatorios y técnicas estadísticas. La muestra del estudio estuvo conformada por un grupo representativo de procesos de alimentos, como no se conoce el número exacto en el distrito judicial de la provincia de

Puno, la muestra se obtuvo mediante la siguiente página web de extracción de muestra estadística (Hernández R.; Fernández C. 2010).

La muestra estuvo conformada por 23 efectivos policiales de la AREINCRI PNP - Puno.

3.3.2 Enfoque

Nuestro estudio se basó en el enfoque cualitativo, que corresponde al tipo de investigación jurídico descriptivo

3.4 MÉTODOS Y TÉCNICAS

3.4.1 Instrumentos

La técnica de recolección de datos será la guía de entrevista y el instrumento a utilizar será la entrevista

La entrevista

Se desarrolló una entrevista y se aplicó a los 23 efectivos policiales de la AREINCRI PNP - Puno.

3.5 IDENTIFICACIÓN DE VARIABLES

3.5.1 Variables

Tabla 01: Categorías

VARIABLE	INDEPENDIENTE	DEPENDIENTE
DELITOS INFORMATICOS	**X**	
EVIDENCIA DIGITAL		**X**

Nota: Fuente de Elaboración Propia

3.5 MÉTODO O DISEÑO ESTADÍSTICO

Marco Metodológico

La investigación se enmarca dentro del enfoque cualitativo, de tipo básico, con el diseño descriptivo jurídico.

Procesos y Análisis

Luego de la aplicación de la entrevista a los efectivos policiales, se procedió a sistematizar las respuestas y filtrarlas por palabras clave de tal forma que sea más sencillo la exposición de los resultados, de esta manera se pretende mostrar la realidad de los hechos en las variables materia de estudio.

3.6 MATERIALES Y EQUIPO

- Internet, bibliografía, artículos y libros tanto físicos como digitales.

CAPÍTULO IV

EXPOSICIÓN Y ANÁLISIS DE RESULTADOS

En este capítulo se presentan los resultados obtenidos a partir del instrumento de recogida de datos, lo que nos permitirá extraer conclusiones definitivas y ofrecer recomendaciones.

4.1 ANÁLISIS Y DESCRIPCIÓN DE LOS RESULTADOS

Se procede a presentar cada una de las interrogantes planteadas en el instrumento de recolección de forma ordenada, en función de la misma, y cada una de las respuestas obtenidas se sintetizaron para una mejor comprensión mediantes las palabras claves.

PREGUNTA 1: En su opinión, considera que se tiene un buen nivel de legislación nacional e internacional para la ayuda en la investigación de los delitos informáticos?

La mayoría de los entrevistados respondieron: Que no, porque falta la implementación de medios logísticos, así también mencionan que no se tiene buena regulación, razón por la cual no se logra tener resultados favorables en las investigaciones, actualmente no se cuenta con peritos especializados en la PNP, para que coadyuven en la investigación en este tipo de delitos.

La minoria de los entrevistados refirieron: Que si, se tiene una buena regulación nacional, sin embargo falta capacitar y especializar al personal policial y a los operadores de justicia.

PREGUNTA 2: De su conocimiento, considera que los operadores de derecho están suficientemente capacitados para manejar temas de delitos informáticos?

La mayoría de los entrevistados refirieron: No pueden precisar, o simplemente mencionaron que no.

La minoria de los entrevistados respondieron: No, considero que les falta mucha capacitación, es debida a la falta de logística y capacitadores.

PREGUNTA 3: ¿Considera que los peritos informáticos están suficientemente capacitados y el personal es suficiente para la carga de investigaciones?

La mayoría de los entrevistados refirieron: No pueden precisar, o simplemente mencionaron que no.

Algunos entrevistados respondieron: Insuficiencia en capacitaciones, asimismo de los pocos peritos informáticos que hay en Puno se desconoce si capacitación,

PREGUNTA 4: ¿Considera que las herramientas utilizadas en la Informática Forense son Óptimas para la investigación?

La mayoría de los entrevistados respondieron: No, el estado debería tener mejores sistemas informáticos en vista que las que se tienen en su mayoría están desactualizadas o no se tiene las licencias correspondientes y mucho menos actualizadas, por ende podemos decir que están obsoletas. Además de la falta de mucha logística.

En la jurisdicción de Puno no se cuenta con herramientas tecnológicas, toda vez que no se cuenta con un departamento criminalístico o de evidencia digital e informática forense.

Algunos mencionaron: Si, por supuesto

PREGUNTA 5: De su experiencia, Le parece que abarcamos todos los delitos informáticos que tiene como objeto la vulneración de la información en nuestro marco legal?

La mayoría de los entrevistados respondieron: Que no, toda vez que el personal policial o investigador policial no se encuentra capacitado para resolver todos los delitos informáticos y mucho menos aún poder manejar evidencia digital. Esto también porque lamentablemente las oficinas no están abastecidas ni implementadas para este tipo de delitos.

Asimismo no se abarcan todos los tipos de delitos informáticos, ya que la mayoría de denuncias registradas se dan más por acceso ilícito de sistemas y fraude informático. Y esto seguirá siendo un problema y un gra reto porque con el pasar de los años existen nuevas modalidades y formas de cometer delitos en el ámbito digital.

Por ende se necesitan peritos en esta materia para que no se centralice en Lima.

La minoria de los entrevistados refirieron: Si, pero igual falta especialistas.

PREGUNTA 6: ¿Considera que los peritos informáticos están suficientemente capacitados y el personal es suficiente para la carga de investigaciones?

La mayoría de los entrevistados respondieron: Que no, porque los delitos informáticos son dinámicos, cada vez se producen de distinta forma y no son fáciles de detectar para cualquier usuario. Asimismo no está correctamente regulado porque el personal policial no maneja las TICS. Los delitos informáticos están mis ramente aplicados y regulados.

La minoria de los entrevistados refirieron: Solamente indicaron si.

PREGUNTA 7: En su opinión Cree usted que la estructura de la Tipicidad Objetiva en los Delitos Informáticos es la adecuada?

La mayoría de los entrevistados respondieron: No, asimismo refieren algunos que no podrían decirlo por no estar capacitados.

No porque falta investigación en el tema y capacitaciones de los mismos.

No es la adecuada puesto que la institución no cuenta con presupuesto para implementar la última tecnología, además que el tipo debería ser más específico y riguroso.

La minoria de los entrevistados refirieron: Si, pero solo de algunos delitos informáticos comunes.

PREGUNTA 8: De su experiencia, Considera que ha existido una evolución sobre lo conocido tradicionalmente en la tipicidad subjetiva de los Delitos Informáticos?

La mayoría de los entrevistados respondieron:Si, porque aprovechan el uso de la tecnología para vulnerar accesos tecnológicos, asimismo que haya habido evolución no quita que esta sea suficiente .

Algunos también comentaron que falta capacitación respecto el tema de la tipicidad dentro de la Institución Policial.

La minoria de los entrevistados refirieron: No, ya que no puede haber mucha evolución en algo que es nuevo como en el caso de delitos informáticos.

PREGUNTA 9: ¿Considera que se tiene el conocimiento adecuado sobre el manejo de la evidencia digital en cuanto a metodología de reconocimiento y recolección?}

La mayoría de los entrevistados respondieron: No, ya que para eso debe existir personal especializado, y que no cuenta con capacitación suficiente, y mucho menos con material tecnológico para su recolección.

Algunos de los entrevistados refirieron: Si, existe el manual de evidencia digital.

PREGUNTA 10: De su conocimiento, le parece que es relevante la calidad de análisis del informe realizado por los peritos informáticos para la admisión de la evidencia digital en el proceso penal?

La mayoría de los entrevistados respondieron: Si, porque son pruebas contundentes.

Algunos comentaron que hasta la actualidad no han podido visualizar un informe de perito informático, porque no saben si es relevante la calidad de los mismos. También mencionaron que en la mayoría de casos estos informes se van directamente a la fiscalía y ellos no tienen acceso.

PREGUNTA 11: Desde su perspectiva ¿Cree usted que el marco legal que tiene la cadena de custodia sobre evidencia digital es el necesario?

La mayoría de los entrevistados respondieron: Que sí, para poder evitar la adulteración, pérdida u otro del bien que se encuentra incautado.

La mayoría de los entrevistados refirieron: No, porque aún se tiene que implementar normativas y directivas que apoyan la evidencia digital.

PREGUNTA 12: En su opinión, ¿cree usted que la instrumentalización aplicada en la evidencia digital es la adecuada para su admisión el proceso penal peruano?

La mayoría de los entrevistados respondieron: Que no, porque nos falta conocer el avance de nuevas tecnologías,

La mayoría de los entrevistados refirieron: Si es adecuado pero aún falta mucho por conocer, o simplemente si.

CONCLUSIONES

Primera: Se ha establecido que la prueba digital, independientemente de su clasificación jurídica como documento electrónico, mensaje de datos u otras formas, se acepta generalmente como medio de prueba válido en las legislaciones penales. Por lo tanto, está permitido utilizar pruebas digitales ante un tribunal para establecer la veracidad o falsedad de las circunstancias de hecho controvertidas o la responsabilidad penal del acusado.

Segunda: La evidencia digital posee un doble carácter, sirviendo tanto como documento y como elemento material de prueba que puede ser utilizado para establecer indicios. La admisibilidad del mensaje de datos o prueba digital como elemento material de prueba en un proceso penal vendrá determinada por las condiciones en las que se obtenga dicho elemento. Si alguna de estas condiciones coincide con las especificadas en la legislación penal, la prueba se considerará admisible y podrá introducirse en el juicio. La importancia de lo anterior radica principalmente en la autenticación de las pruebas digitales. Sin embargo, si se presenta como elemento material probatorio o evidencia física, debe ser autenticada de manera diferente.

Tercera: Para que una prueba digital sea considerada como tal, debe cumplir ciertos criterios. Debe ser relevante, significativa y beneficiosa para el proceso judicial. Además, debe presentarse en un juicio formal y público, en el que todas las partes tengan la oportunidad de exponer sus argumentos, y en presencia del juez. Una vez cumplidas

todas las condiciones mencionadas, las pruebas pueden considerarse admisibles en el proceso penal y someterse a la valoración del juez.

RECOMENDACIONES

Primera: Se recomienda la creación y cumplimiento de normas legales efectivas aplicables a la realidad peruana y de la necesidad de crear un cuerpo normativo específico o bien crear un apartado especial en el código penal que incluya el mayor número de delitos informáticos, con términos adecuados a la actualidad que vive los peruanos.

Segunda: Se recomienda al Organismo Legislativo, un proyecto de ley y que tome conciencia de la necesidad del mismo, por el cual se pueda disminuir los delitos informáticos que surgen de las redes sociales, así como el control y la prevención de los mismos en Perú y de esta forma erradicarla con el tiempo, ya que dichas acciones, se ven reflejadas en la opinión que posee la sociedad internacional en nuestro país.

Tercera: Se recomienda la regulación de términos informáticos como internet, redes sociales, sitios de web ilegales, etc, toda vez que Perú es uno de los muchos países que se encuentra atrasado en lo que a la regulación de la tecnología respecta. Pues vivimos en un mundo tecnológico y por ello Perú debe de apegarse a este nuevo mundo, para combatir de forma eficiente el ciber-crimen, que surge de las redes sociales.

BIBLIOGRAFÍA

Abanto Garnique, J. L. (2012). La desprotección de los datos personales de los cibernautas peruanos, expuestos a código malicioso y su incidencia en la vulneración al derecho a la intimidad. Repositorio Universidad Nacional de Ingeniería.

Alonso, d. E., Cugat, M. M., Garcia, R. N., Lloria, G. P., Machado, P. F., Quinteros, 0. G., . . . Riquet, A. M. (2014). CIBERDELITOS (Ira ed.). Buenos Aires, Argentina: Hammurabi.

Angulo Arana, P. (2014). EL CAS° PENAL - Base de la litigación en el Juicio Oral. Lima: Gaceta Jurídica.

Benites Tangoa, J. (2010). Mecanismos de Celeridad Procesal principio de oportunidad y proceso de terminación anticipada en el código procesal penal 2004 y su aplicación en el distrito judicial de Huaura. Lima, Lima, Peru: Universidad San Marcos.

Bobbio, N. (2000). El filósofo y la política. Antología (Ira ed.). (E. p. Santillan, Ed.) México, México: Editorial Fondo de Cultura Económica.

Calderón Sumarriva, A. C. (2013). El ABC del Derecho Penal. Lima: San Marcos - EGACAL.

Chamorro Bernal, F. (2008). La Tutela Jurisdiccional Efectiva. La Tutela Jurisdiccional Efectiva. Barcelona, España: BOSH.

Duarte Silva, L. M. (2012). Valoración probatoria de los documentos audiovisuales. Repositorio Universidad San Marcos.

Elias, P. R. (Junio de 2014). LUCES Y SOMBRAS. (L. C. Atribución, Ed.) Obtenido de Hiperderecho:

http://www.hiperderecho.org/2014/07/luces-y-sombras-de-la-delincuencia-informatica-en-peru/

EnfoqueDerecho.com. (2021, septiembre 22). Ricardo Elías Puelles | Piratería y ciberdelitos contra la Propiedad Intelectual. *Enfoque Derecho | El Portal de Actualidad Jurídica de THĒMIS*. https://www.enfoquederecho.com/2021/09/22/ricardo-elias-puelles-pirateria-y-ciberdelitos-contra-la-propiedad-intelectual/

Gamarra Chavarry, L. M. (2017). Implementación de la Política Pública de Fortalecimiento de la función criminalística en la policía: Problemas y soluciones (2013-2016). Repositorio Pontificia Universidad Catolica del Peru.

Gercke, M. (2014). CIBERSEGURIDAD. Comprensión del Ciberdelito: Fenómenos, Dificultades y Respuesta Jurídica. Ginebra, Suiza: Unión Internacional de Telecomunicaciones.

GIL ALBARRAN, G. E. (2007). DERECHO INFORMÁTICO. Lima: Megabyte S.A.C. Gimenez Solano, V. M. (03 de Octubre de 2011). Hacking y ciberdelito. (U. P. Valencia, Ed.) Obtenido de RiuNet - Repositorio Institucional UPV: http://hdl.handle.net/10251/11856

Gonzales Perez, J. (2010). El Derecho a la Tutela Jurisdiccional. El Derecho a la Tutela Jurisdiccional. Madrid, España: CIVITAS.

Hernandez Sampieri, R. F. (2014). Metodología de la investigación: Roberto Hernandez Sampieri, Carlos Fernandez Collado y Pilar Baptista Lucio (6a. ed. ed.). Mexico D.F: McGraw-Hill.

ANEXOS

Anexo 01: Matriz de consistencia

TÍTULO	PROBLEMA	OBJETIVO	VARIABLE	METODOLOGÍA
DELITOS INFORMÁTICOS Y LA EVIDENCIA DIGITAL EN EL PROCESO PENAL PERUANO 2023	**GENERAL** ¿Cómo la admisión de la evidencia digital incide en los delitos informáticos en el proceso penal peruano?	**GENERAL** Analizar cómo la admisión de la evidencia digital incide en los delitos informáticos en el proceso penal peruano.	**INDEPENDIENTE** DELITOS INFORMATICOS	**TIPO O MODELO DE INVESTIGACIÓN** Jurídico descriptivo
	ESPECÍFICO ¿Cómo la protección de la evidencia digital influye en la clasificación de los Delitos Informáticos en el Proceso Penal peruano? ¿Cómo la determinación del Marco Legal de la Evidencia Digital repercute en la tipicidad de los delitos informáticos en el Proceso Penal Peruano?	**ESPECÍFICO** Distinguir como la protección de la Evidencia digital influye en la clasificación de los Delitos Informáticos en el Proceso Penal Peruano. Determinar cómo el Marco Legal de la Evidencia Digital repercute en la Tipicidad de los Delitos Informáticos en el Proceso Penal Peruano	**DEPENDIENTE** EVIDENCIA DIGITAL	**METODOLOGÍA O ENFOQUE DE INVESTIGACIÓN** Cuantitativo

Anexo 02: Entrevista

Entrevista

Entrevistado:

Cargo/profesional/ grado académico:

Institución:

Lugar: **Fecha:**

Objetivo general: Analizar cómo la admisión de la evidencia digital incide en los delitos informáticos en el proceso penal peruano

1. En su opinión, considera que se tiene un buen nivel de legislación nacional e internacional para la ayuda en la investigación de los delitos informáticos?

2. De su conocimiento, considera que los operadores de derecho están suficientemente capacitados para manejar temas de delitos informáticos?

3. ¿Considera que los peritos informáticos están suficientemente capacitados y el personal es suficiente para la carga de investigaciones?

4. ¿Considera que las herramientas utilizadas en la Informática Forense son Óptimas para la investigación?

5. De su experiencia, Le parece que abarcamos todos los delitos informáticos que tiene como objeto la vulneración de la información en nuestro marco legal?

6. ¿Considera que está correctamente regulado los delitos informáticos que utilizan las Tics como medio para realizar los delitos convencionales?

7. En su opinión, ,Cree usted que la estructura de la Tipicidad Objetiva en los Delito Informáticos es la adecuada?

8. De su experiencia, Considera que ha existido una evolución sobre lo conocido tradicionalmente en la tipicidad subjetiva de los Delitos Informáticos?

9. ¿Considera que se tiene el conocimiento adecuado sobre el manejo de la evidencia digital en cuanto a metodología de reconocimiento y recolección?

10. De su conocimiento, le parece que es relevante la calidad de análisis del informe realizado por los peritos informáticos para la admisión de la evidencia digital en el proceso penal?

11. Desde su perspectiva ¿Cree usted que el marco legal que tiene la cadena de custodia sobre evidencia digital es el necesario?

12. En su opinión, ¿cree usted que la instrumentalización aplicada en la evidencia digital es la adecuada para su admisión el proceso penal peruano?

Gracias!

Anexo 03: Entrevistas realizadas

Anexo 02: Entrevista

Entrevista

Entrevistado: Jonny Karol CONDORI PEÑALOZA

Cargo/profesional/ grado académico: S2 PNP - Pesquisa.

Institución: PNP

Lugar: Puno **Fecha:** 18 de Setiembre del 2023.

Objetivo general: Analizar cómo la admisión de la evidencia digital incide en los delitos informáticos en el proceso penal peruano

1. En su opinión, considera que se tiene un buen nivel de legislación nacional e internacional para la ayuda en la investigación de los delitos informáticos?
   No, en vista que no se logra tener resultados favorables en la investigación, actualmente no se cuenta en la PNP peritos informáticos para realizar la coordinacion en este tipo de delitos.
2. De su conocimiento, considera que los operadores de derecho están suficientemente capacitados para manejar temas de delitos informáticos?
   No, ya que las delegenias no son acorde a la investigacion de estos delitos.
3. ¿Considera que los peritos informáticos están suficientemente capacitados y el personal es suficiente para la carga de investigaciones?
   Actualmente no se cuenta con peritos informaticos en la ciudad de Puno, y si en la ciudad de Lima pero no se realiza la coordinacion por su misma carga laboral.
4. ¿Considera que las herramientas utilizadas en la Informática Forense son Óptimas para la investigación?
   No, el estado deberia invertir en nuevas herramas informaticas en vista que estas son obsoletas o no tienen licencia actualizado.
5. De su experiencia, Le parece que abarcamos todos los delitos informáticos que tiene como objeto la vulneración de la información en nuestro marco legal?
   No se abarca el total de los delitos informaticos, las denuncias registradas se dan, más por acceso ilicito de hermas y fraude informatico.

25

6. ¿Considera que está correctamente regulado los delitos informáticos que utilizan las Tics como medio para realizar los delitos convencionales?

No, porque los delitos informaticos son dinamicos cada vez se producen de distinta forma y no son fáciles de detedar para cualquier usuario.

7. En su opinión, ,Cree usted que la estructura de la Tipicidad Objetiva en los Delito Informáticos es la adecuada?

Deberia ser más especifico y más riguroso.

8. De su experiencia, Considera que ha existido una evolución sobre lo conocido tradicionalmente en la tipicidad subjetiva de los Delitos Informáticos?

Si, hubo una evolución sin embargo no es reciente.

9. ¿Considera que se tiene el conocimiento adecuado sobre el manejo de la evidencia digital en cuanto a metodología de reconocimiento y recolección?

Si, existe a la actualidad un Manual de Evidencia Digital.

10. De su conocimiento, le parece que es relevante la calidad de análisis del informe realizado por los peritos informáticos para la admisión de la evidencia digital en el proceso penal?

Hasta la actualidad no he podido revisar un informe de perito informatico.

11. Desde su perspectiva ¿Cree usted que el marco legal que tiene la cadena de custodia sobre evidencia digital es el necesario?

Si, para evitar la adulteracion, pérdida u otro del bien que se encuentra incautado.

12. En su opinión, ¿cree usted que la instrumentalización aplicada en la evidencia digital es la adecuada para su admisión el proceso penal peruano?

Si es adecuado pero falta muchos vacios que se deberia controlar.

26