UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO

ESCUELA ACADÉMICO PROFESIONAL DE DERECHO

TÍTULO

Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE ABOGADA

AUTOR

Leyla Keith Rivero Passuni

ASESOR

Dr. Erik Daniel Vildoso Cabrera

LÍNEA DE INVESTIGACIÓN

Derecho Penal

LIMA - PERU

2017

PÁGINA DEL JURADO

.....

Presidente

Mg. Urteaga Regal, Carlos Alberto

Magister

.....

Secretario

Dr.Roque Gutierrez, Nilda Yolanda

Doctor

.....

Vocal

Dr. Vildoso Cabrera, Erick Daniel

Doctor

DEDICATORIA

A mi progenitor, por el apoyo que me brindo, por la pasión que me heredo hacia la carrera.

AGRADECIMIENTO

A Dios, por ser mi Padre que siempre está conmigo, otorgándome fortaleza para seguir en la vida universitaria. A mi asesor Erik Vildoso Cabrera, quien me brindó orientación y guía en la elaboración de mi tesis.

DECLARACIÓN JURADA DE AUTENTICIDAD

Yo, Leyla Keith Rivero Passuni, con DNI Nº 44757254, a efecto de cumplir con las disposiciones vigentes consideradas en el Reglamento de Grados y Títulos de la Universidad César Vallejo, declaro bajo juramento que:

1. La tesis es de mi autoría.

2. He respetado las normas internacionales de cita y referencias para las fuentes consultadas, por lo tanto la tesis no ha sido plagiada ni total ni parcialmente.

3. La tesis no ha sido auto plagiada; es decir, no ha sido publicada ni presentada con anterioridad para obtener grado o título profesional alguno.

4. Los datos presentados en los resultados son reales; no han asidos falseados, duplicados ni copiados y por tanto los resultados que se presentan en la presente tesis se constituirán en aportes a la realidad investigada.

En tal sentido de identificarse fraude plagio, auto plagio, piratería o falsificación asumo la responsabilidad y la consecuencias que de mi accionar deviene, sometiéndome a las disposiciones contenidas en las normas académicas de la Universidad César Vallejo.

Lima, diciembre de 2017

Leyla Keith Rivero Passuni
DNI Nº 44757254

Presentación

Señores miembros del Jurado:

La presente investigación titulada **Delitos Informáticos y la Evidencia Digital en e Proceso Penal Peruano,** que se pone a Vuestra consideración tiene como finalida de conocer cuál es la situación actual de los Procesos Penales sobre Delito Informáticos y la incidencia que ha tenido la Evidencia Digital en los mismos, como l normativa a nivel nacional e internacional, sobre la recolección, obtención y l calificación y comprensión de la evidencia digital en la investigación e identificación d la autoría, procedentes del uso de las nuevas tecnologías, los cuales permiten accede impunemente y vulnerar varios bienes jurídicos, al ser delitos pluriofensivo. Es así, qu las nuevas tecnologías han incrementado enormemente las probabilidades d infracción contra la información, la indemnidad sexual, la intimidad personal y biene patrimoniales.

Así, cumpliendo con el reglamento de grados y títulos de la universidad César Vallejo la investigación se ha organizado de la siguiente manera: en la parte introductoria s consignan la aproximación temática, trabajos previos o antecedentes, teoría relacionadas o marco teórico y la formulación del problema; estableciendo en este, e problema de investigación, los objetivos y los supuestos jurídicos generales y específicos. En la segunda parte se abordara el marco metodológico en el que s sustenta el trabajo como una investigación desarrollada en el enfoque cualitativo, d tipo de estudio orientado a la comprensión a la luz del diseño de estudios de casos Acto seguido se detallaran los resultados que permitirá arribar a las conclusiones y sugerencias, todo ello con los respaldos bibliográficos y de las evidencias contenida en el anexo del presente trabajo de investigación.

La autora

Índice

Resumen

El presente trabajo de investigación se realizó en el ámbito del Derecho Penal con la finalidad de conocer cuál era la situación actual de los Procesos Penales sobre Delitos Informáticos y la incidencia que ha tenido la Evidencia Digital en los mismos, como la normativa a nivel nacional e internacional, sobre la recolección, obtención, la calificación y comprensión de la evidencia digital en la investigación e identificación de la autoría.

Debido a la existencia de una nueva Inseguridad Ciudadana por el incremento de los Delitos Informáticos, siendo la admisión de la evidencia digital fundamental para la existencia de Juicios Justos. Es así, que las nuevas tecnologías habían incrementado enormemente las probabilidades de infracción contra la información, la indemnidad sexual, la intimidad personal y bienes patrimoniales.

Asimismo, el desarrollo acelerado de las nuevas tecnologías había impactado de manera preponderante en las actividades que desarrollaban las personas a diario, creando una nueva dependencia al manejo de apps o aplicativos que facilitan la vida diaria, es decir en el Ciberespacio no solo estaríamos vulnerando la intimidad de la persona, sino también sus servicios, sus cosas, sus actividades. El mundo virtual es nuestro mundo real ahora y hay que dotarlo de seguridad. La necesidad que una evidencia digital sirva como prueba digital fehaciente donde el tema central sea la admisión de la misma dentro del proceso, con esto llegar a vincular al autor con el hecho delictivo y tenga un Proceso Penal correcto.

Palabra clave: Delitos Informáticos, Evidencia Digital, Derecho, Derecho Proceso Penal.

Abstract

The present research work was carried out in the area of Criminal Law in order to know the current situation of the Criminal Processes on Computer Crime and the impact that Digital Evidence has had on them, such as the national legislation and international, on the collection, obtaining, qualification and understanding of the digital evidence in the investigation and identification of the authorship.

Due to the existence of a new Citizen Insecurity for the increase of Computer Crime, being the admission of digital evidence fundamental for the existence of Fair Trials. Thus, new technologies had greatly increased the chances of infringement against information, sexual indemnity, personal privacy and assets.

Likewise, the accelerated development of new technologies had a preponderant impact on the daily activities of people, creating a new dependence on the management of applications or applications that facilitate daily life, that is, in Cyberspace not only would we be violating the intimacy of the person, but also their services, their things, their activities. The virtual world is our real world now and we have to provide it with security. The need for digital evidence serves as a reliable digital proof where the central theme is the admission of the same within the process, with this to link the author with the crime and have a correct Criminal Procedure.

Keyword: Computer Crime, Digital Evidence, Law, Criminal Procedure Law.

INTRODUCCIÓN

Aproximación Temática

El crimen en la actualidad ya supero todos los esquemas con la llegada de la tecnología. La aparición del internet ha permitido globalizar las oportunidades para llevar a cabo estos delitos, trasladándolo a puntos impensados del planeta tierra. Este comportamiento va en incremento muy rápidamente, siendo mayores los casos que se dan día con día, convirtiéndose en un desafío tanto como para la policía y las autoridades judiciales el combatirla.

Nuestro país no está exento de esta gran responsabilidad mundial. Por ende, la real importancia de esta problemática es estar a la vanguardia con las nuevas actualizaciones y los nuevos tipos de estrategias cometidas por los autores de los delitos informáticos. Visto que tecnología de la información ha planteado nuevos desafíos y la adaptación de las profesiones a la era digital. Es decir, a nivel mundial, en todas las áreas, en todas las profesiones, como un índice de conectividad va a estar ligados a la informática y en consecuencia usaran los accesos a internet como herramienta para estar acorde con las nuevas tecnologías.

Como acote principal se busca la especialización de índole policiaca, es por ello que tenemos en nuestro país a la DIVINDAT – División de Delitos de Alta Tecnología de la PNP, donde investigar crímenes sofisticados y la correcta recolección de evidencia es circunstancial para armar el caso y presentarlo ante los fiscales y jueces, esta es una tarea demasiado importante para los investigadores.

En esta posición una verdadera problemática de índole operática es el Volumen de datos a analizar, donde no se abastecen en lo absoluto el personal de la Divindat. Esto combinado con la problemática de la cooperación entre entidades de telecomunicaciones y la PNP, limitando el accionar al ser una gestión sumamente lenta. Con demasiadas barreras burocráticas.

Por otro lado, tenemos la cooperación internacional, que también no es lo suficientemente eficiente y necesita pulirse inmediatamente, para la obtención y cruce

real de información y así tener la situación real del caso en concreto. Esto en un caso puede retardar el análisis y tomar demasiado tiempo en la resolución de una investigación.

Aquí, el desenvolvimiento de la Informática Forense cobra un papel protagónico. Y es donde la problemática se anida. Visto que por más que se desarrolle un informe de primera por un perito informático autorizado, al ser este informe llevado al Fiscal y finalmente al Juez, por más traducción que tenga, no va ser comprendido correctamente, visto que tanto el Fiscal, como el Juez no tienen los conocimientos necesarios en informática y de esa manera hacer la correcta identificación del Autor del delito informático. Es decir, no toda la problemática está orientada a temas operativos o de naturaleza técnica, sino problemas relacionados a procedimientos, políticas, especialización, cooperación, entre otros que afectan la investigación, como el proceso judicial.

Para empezar, debemos entender que el sujeto que comete el delito no es un tipo común que sale a la calle y lo encuentran hurtando y puede ser señalado; este criminal está detrás de una cadena de números, está detrás de una red, un servidor, que maneja dispositivos que se convierten en prueba. Que estas pruebas pueden ser auto alterables, o auto destructibles, programadas anticipadamente, llegando a ser dispositivos volátiles. Es decir, el observador altera el objeto observado. Como la teoría de Newton toda Acción tiene una Reacción.

Por ello nunca se va a saber a ciencia cierta que ocurre en ese dispositivo si no tiene un trato especial. Es decir, la prueba digital es muy poderosa si es correctamente obtenida, te lo da todo, el cómo, el cuándo y porque se realizaron los hechos. Pero no basta con ser correctamente obtenida, sino correctamente manejada con la adecuada cadena de custodia e interpretada y es donde entran a tallar los Jueces y Fiscales.

Centrando la realidad problemática, estamos frente a un tipo de conducta indebida que usualmente queda impune, esto por la falta de preparación y conocimiento de nuestras

autoridades tanto judicial como policial, las cuales les falta las herramientas y procedimientos correctos para investigar este tipo de delitos.

Por ello instrumentalizar un procedimiento o un método adecuado para manejar investigaciones relacionadas con equipos informáticos, cumpliendo con la premisa de que estas prácticas deben ser aceptadas y puestas en acción de forma universal y respetando el debido proceso en el Proceso Penal Peruano es necesario y de aplicación inmediata en vista que este comportamiento social evoluciona muy rápidamente.

ANTECEDENTES

Como punto fundamental el tener referencias de estudios anteriores nutrirá la investigación por consecuente tener una base donde asentar la problemática y con esto establecimos las fuentes relacionadas con el tema.

Es decir, es de suma importancia tener antecedentes en un trabajo de investigación. En ese sentido **Salvador** (2009) nos menciona que "Son marcos de referencia que permiten ubicar el estudio en el área del conocimiento en que se inscribe el tema tratado" (p.197). Por otro lado, **Vara** (2010) indica "El inicio de todo estudio debe contar con una base de datos que sirvan de fuente de inspiración al investigador. Los datos que se recopilan tienen que estar relacionados el estudio" (p. 615).

Según lo antecedido, comprendemos su importancia al ser fuentes de información que enriquecieron el trabajo de investigación, los cuales pudieron ser tomados de referencia, por ello es relevante considerar a antecedentes de índole nacional o internacional para nutrir el Marco Teórico, esto ha sido un gran aporte base para su desarrollo.

Antecedentes nacionales

Gamarra (2017), en su Tesis "Implementación de la Política Publica de Fortalecimiento de la función Criminalística en la Policía: Problemas y Soluciones (2013-2106)" para obtener el grado de Magister en Ciencias Políticas y Gobierno con mención en Gestión

Pública y Políticas Publicas de la Pontificia Universidad Católica del Perú, el cual nos brinda un análisis profundo sobre las políticas públicas de seguridad Ciudadana a través del Decreto Legislativo N° 1219 sobre la Ley de fortalecimiento de la función criminalística, el cual se espera desarrollar en mejora de los peritos especialistas de la PNP y la Dirección Ejecutiva de Criminalística (DIREJCRI).
Por otro lado nos aporta la descripción del desarrollo de la modernización tecnológica de los equipos de Criminalística en la DIREJCRI – PNP en el periodo del 2013 al 2016. Como también saber en qué estado se encuentras sus infraestructuras de los laboratorios de criminalísticas de la PNP, como la comparación de cuál sería el ideal que debe alcanzar.

La tesis antes citada, corroboró los objetivos del Trabajo de Investigación y ayudó al desarrollo del Marco Teórico del mismo.

Nuñez (2016), en su Tesis "Derecho de identidad digital en internet" para obtener el Grado Académico de Doctor en Derecho y Ciencia Política de la Universidad Mayor de San Marcos, nos brinda un panoramas más completo sobre el Derecho informático en internet, como esta genera a su vez vulnerabilidad al no existir un Sistema que garantice la seguridad y confianza en los procesos electrónicos en internet. Nos establece que si bien tengo el derecho de usar y navegar internet, también tengo derecho a estar protegido y tener la seguridad que lo que desarrolle en el ciberespacio no este propenso a ataques informáticos. Por ende la tesis antes citada, corrobora los objetivos del Trabajo de Investigación y ayuda al desarrollo del Marco Teórico del mismo.

Suarez (2015), en su Tesis "La Ciberguerra y la aplicación de los Principios del Derecho Internacional Humanitario" para obtener el título profesional de Abogado de la Universidad San Martin de Porres, 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.

Nos permite según el resultado de la investigación de la tesis confirmar la necesidad de crear un Comité Especializado en Ciberguerra, como también sensibilizar a la población de esta realidad día con día. Por otro lado resalto la importancia de implementar de manera más exhaustiva el Derecho Internacional Humanitario.

La tesis antes citada, corroboró los objetivos del Trabajo de Investigación y ayudó al desarrollo del Marco Teórico del mismo.

Abanto (2012), en su Tesis "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" para obtener el Grado Académico de Maestro en Ciencias con mención en Ingeniería de Sistemas de la Universidad Nacional de Ingeniería, nos aporta un panorama total sobre la desprotección de datos personales, sus modalidades, como también como son aplicados los medios probatorios en el proceso penal y como la revolución de la evidencia digital merece un trato especial y debe ser regulado en alguna normativa. En estos puntos enfatiza en la necesidad que la evidencia digital para que llegue a ser valorada como prueba e insertada en el proceso penal debe ser no solo fehaciente, sino licita, por ello realiza una descripción detallada de cómo se debe realizar la búsqueda y recolección de aquella evidencia. Por otro lado nos plantea políticas y estrategias a nivel nacional sobre Ciberseguridad.

Por lo antecedido este antecedente, nos esclarece el desarrollo de la evidencia digital en el proceso penal, siendo fundamental para la investigación desarrollada.

Duarte (2012), en su Tesis "Valoración probatoria de los documentos audiovisuales" para obtener el Grado Académico de Magister en Derecho con mención en Derecho Procesal de la Universidad Nacional Mayor de San Marcos, nos aporta un enfoque importante sobre la prueba ilícita y su relación con los documentos audiovisuales, como también las garantías constitucionales que estarían involucradas con la obtención de documentos audiovisuales y su interrelación con la valoración probatoria que puedan llegar a tener y sean admitidos en el proceso penal.

Por ello este antecedente, nos esclarece el desarrollo de la evidencia digital en el proceso penal, siendo fundamental para la investigación desarrollada.

Antecedentes internacionales

Rincón (2015) en su Tesis Doctoral "El delito en la cibersociedad y la justicia penal internacional" para obtener el grado de Doctor en Derecho de la Universidad Complutense de Madrid, plantea que los límites fronterizos entre países no debiera ser un impedimento para la correcta investigación de los delitos informáticos, como su persecución, la determinación de su jurisdicción para que sean sancionados, ya que en el ciberespacio no existen fronteras y mientras el autor del delito está en un lugar, la victima afectada puede estar en otro lugar. Es por ello que este autor explica la necesidad de crear un sistema de justicia universal, centrando su investigación en el Derecho Comparado y la Cooperación Internacional.

La tesis citada sirvió de base para sustentar la justificación de la presente investigación, ya que en ella recogemos la problemática central de los Delitos informáticos y la Evidencia Digital en el Proceso Penal Peruano.

Giménez (2012), en su Tesis "Hacking y Ciberdelito" para obtener el grado de Ingeniero Técnico en Informática de Gestión de la Universidad Politécnica de Valencia, nos expone que desarrollar la investigación del delito informático es muy complejo, esta complejidad se incrementa peor aún si se trata de una Delincuencia Internacional que trabaja conjunto con el Crimen Organizado convirtiéndose en un tema muy engorroso tanto para el Ministerio Público como para los sectores Judiciales. Todo esto sumándose al fenómeno de la globalización ha venido creciendo notablemente y ha masificado el Delito Informático como tal.

Condensa también la comprensión del fenómeno llamado Ciberdelito y el nuevo Sujeto que aparece como es el Ciberdelincuente. Para complementar nos desarrolla la

comprensión del Hacker y sus variantes. Describe como tema fundamental el modo de actuación de un hacker. Como también el proceso por el cual ellos cometen el hecho delictivo.

Por último, nos brindó las primeras luces ante Ciberterrorismo, siendo la nueva forma de generar miedo o terror generalizado a una población, generando con ello una violencia directa contra las personas. Por ende la tesis antes citada, corrobora los objetivos del Trabajo de Investigación y ayuda al desarrollo del Marco Teórico del mismo.

Gercke (2014), en su Informe de la UIT "Ciberseguridad. Comprensión del Delitos informáticos: Fenómenos, Dificultades y Respuesta Jurídica" informe de la UIT (Unión Internacional de Telecomunicaciones), nos establece uno de los aportes más importes con respecto a estadísticas globalizadas para establecer el grado de afectación mundial sobre los Delitos informáticos. Comprendamos que la UIT es un organismo especializado de las Naciones Unidas para la Tecnología de la Información y la Comunicación que tiene 193 Estados Miembros y 700 Compañías Tecnológicas, por ende, estos informes nos permiten visualizar la situación real frente al desafío de combatir la Ciberdelincuencia, pues nos mantienen vulnerables mundialmente. Es decir, nos va plasmar los siete objetivos estratégicos que fueron establecidos en la Agenda sobre Ciberseguridad Global de la UIT, donde el objetivo principal es nutrir las legislaciones para que sean aplicadas mundialmente, todo acorde a los protocolos, estructuras y parámetros de cada Nación, también primando que las Ciberamenazas pueden provenir de cualquier parte del Mundo.

Este libro en el desarrollo de sus 6 capítulos corrobora uno a uno los objetivos de la investigación y por ende es un Antecedente vital para la sustentación de la misma.

Marco teórico

Para desarrollar la investigación necesitamos teorías establecidas. Por ello se procederá a identificar algunos conceptos enlazados al tema de estudio, los cuales serán fundamentales durante el proceso de la investigación, es por ello que es importante determinar el desarrollo del marco teórico dentro de una investigación. Para **Ñaupas** (2009) define el Marco Teórico como la base a la investigación del problema científico social. También se dice que es el fundamento teórico de la investigación porque en ese ítem del proyecto de investigación. (p.25), es decir el investigador expone su conocimiento de índole teórica y científica en base a las teorías antecedidas. Por ende se considera que nadie va poder investigar un problema donde no exista una base teórica o se desconozca

Delitos informáticos

El avance de las TIC´s ha traído importantes cambios a la sociedad, difiere terriblemente a la que conocíamos hace 15 años atrás. Estos cambios son sistemáticos y rápidos. Generando tener visiones renovadas del modo de vida constantemente. El hombre como ser que se adapta a los cambios, asume estas nuevas tecnologías y la aplica en su día a día, para su uso en beneficio de la sociedad, esto es válido mientras esta acción no vulnere los derechos de las otras personas, es una acción lícita, que puede ser desarrollada sin mayor implicancia.

Lamentablemente contrario a esto el internet y los medios electrónicos son usados como medio delictivo o es objeto de vulneración que puedan afectar y generar perjuicio en la sociedad, este fenómeno debe ser sancionado. A este tipo de comportamientos dañinos se les denomina Delitos informáticos, Cibercrimen o Ciberdelitos.

Según **Rayon & Gomez** (2014) "se entiende por "Ciberdelito" o "Cibercrimen" cualquier infracción punible, (...) en el que se involucra un equipo informático o Internet (...) pueda ser usado para la comisión del delito o puede ser objeto del mismo delito"

(p.211). El fenómeno informático ha dado pie a que las organizaciones criminales adquieran estas nuevas tecnologías y lo apliquen para la realización de sus crímenes. Aquí también observamos que el comportamiento del Sujeto Activo que realiza la acción es de una persona especializada en Tecnologías de la Información, son redes delictivas con alto grado de capacitación. Los cuales tienen constantemente vulnerada la Ciberseguridad.

Para **Gerke** (2014) "El Ciberdelito y la Ciberseguridad son aspectos que no pueden considerarse separados en un entorno interconectado. Esto queda demostrado en la Resolución de la Asamblea General de las Naciones Unidas de 2010 sobre la Ciberseguridad se aborda el Ciberdelito" (p.3). Esto debido a que los Delitos informáticos tiene una connotación mundial, visto que el Ciberespacio no tiene una jurisdicción establecida y el uso de estas Tecnologías se ha globalizado, es decir se utiliza la misma tecnología tanto en Perú como en China, el acceso y la transferencia de información es igual en todas las partes del planeta.

En la actualidad estamos frente a un desafío enorme para combatir al Delito Informatico, el problema de su persecución está centrada en llegar a obtener la identificación correcta de los autores eso incluyendo la ausencia de una cooperación eficaz. Por otro lado para muchos autores el Cibercrimen es más rentable que el tráfico de drogas, moviendo millones de dólares anuales. **Quinteros** manifiesta que la jurisdicción respecto a los Delitos informáticos en el ciberespacio es "planetario", por ende la ubicación territorial de los autores y de proveedores de servicios son muchos. Por ende enfoca que la problemática central de los Delitos informáticos no está en la ausencia de tipificación, ni jurisdicción sino en la determinación de un tribunal que pueda juzgar estos delitos (2014, p.186).

El Dr. Edwar Domínguez Fernández en su Conferencia "Cibernética y Delitos Informáticos" realizado el 23 de Mayo del presente año en el Poder Judicial del Perú, denomino a los Delitos Informáticos como "aquellas conductas que se dirigen a burlar los sistemas de dispositivos de seguridad, esto es invasiones a computadoras, correos

o sistemas de datas mediante una clave de acceso, conductas típicas que únicamente pueden ser cometidos a través de la tecnología", siendo esta denominación la más cercana a la realidad en nuestro país.

La clasificación de los Delitos informáticos, consideramos que puede ser utilizado como medio o como objeto material. **Zegarra** menciona que como medio se encuentran las conductas criminales que se valen de las computadores e internet, como método o medio de la comisión del ilícito (2015, p.111). Cabe explicar que la clasificación de uso como instrumento es para llegar a realizar los actos delictivos, siendo en muchos casos los delitos convencionales los que finalmente desean realizarse. También explica Zegarra que como objeto material se enmarcan las conductas criminales que van dirigidas contra las computadoras, (...), es decir, contra la informática (2015, p.111). Aquí debemos tener en claro que el objeto al que se refiere el autor es el objeto material, cuando de objeto jurídico se tratase, es sobre el efecto dañoso que tiene acerca del perjuicio de pérdidas de datos, por ejemplo.

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 como instrumento o medio categorizan a todas las conductas criminales que utilizan las Tics para la comisión del delito, como ejemplo en la falsificación de documentos vía computarizada (títulos, obras, tarjetas de crédito, cheques, etc.), o en la variación de los activos y pasivos en la situación contable de una empresa. Como también en el planteamiento y simulación de delitos convencionales (robo, homicidio, fraude, pedofilia, trata de personas, pornografía infantil, fraudes bancarios, etc.) o lectura, sustracción y copiado de información confidencial, modificación de datos tanto en la entrada como en la salida de información. También en el aprovechamiento indebido o violación de un código para

penetrar un sistema, introducción de instrucciones inapropiadas que puedan dañar al sistema, variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta apócrifa. Uso no autorizado e programas de cómputo. Alteración de funcionamiento de sistemas a través de virus informáticos. Introducción de instrucciones que provoquen interrupciones en la lógica interna de los programas. Obtención de información residual impresa en papel luego de la ejecución de trabajos. Acceso a áreas informatizadas en forma no autorizada. Intervención en líneas de comunicación de datos o teleproceso, etc.

Mientras que los Delitos Informáticos como fin u objeto enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física.

Es decir, en un ejemplo de programación de instrucciones que producen bloqueo total al sistema. Borrado e eliminación de base de datos de una empresa. Alteración en los servidores de una empresa. Destrucción de programas por cualquier método. Daño a la memoria. Atentado físico contra la maquina o sus accesorios. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados. Secuestros de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

Debemos tener en claro que el bien jurídico tutelado es la pureza técnica, el resguardo de los medios que integren el sistema informático. Gracias a la clasificación hemos ordenado y enmarcado algunas conductas que puedan ser consideradas como Delitos informáticos. Para la comprensión del mismo, establecer un listado que los contenga según su categorización.

Tipicidad de los Delitos informáticos

Para **López** (2013) la tipicidad es aquella cualidad atribuida a la conducta que se adecua al tipo penal. (p.53) Es decir esta conducta nos indica que el hecho está

inmerso en la ley penal, siendo la descripción que la contiene. Distinguiendo por un lado el tipo objetivo que está orientada a la acción, como el tipo subjetivo orientado al dolo o culpa. Con esto el legislador aparte de realizar una descripción objetiva del comportamiento punible, sino que argumenta y fundamenta el carácter ilícito que pueda tener.

La Tipicidad de los Delitos Informáticos busca establecer el tipo penal para delitos desarrollados con el fenómeno de las tecnologías informáticas, la cual ha generado una nueva forma de criminalidad.

Tipicidad Objetiva de los Delitos Informáticos

La Tipicidad Objetiva busca determinar con exactitud la lesión realizada a un bien jurídico debe ser considerada como la actividad de determinado sujeto y cuando esta afectación es solamente producto de la simple causalidad.
Realizamos un análisis de la norma y encontramos que la Tipicidad Objetiva de los Delitos Informáticos está determinados por ciertos puntos como es el Objeto del Delito, los Sujetos, la Acción Típica, la Relación de Causalidad o Nexo Causal, la Imputación Objetiva y finalmente los Elementos Descriptivos Normativos en relación a esta clase de Delitos.

El Objeto del Delito según **Hurtado** (2005) es la persona o cosa sobre la cual recae la acción delictuosa (p.413), es decir es todo lo que es el fin u objetivo de dañar. En lo referente a delitos informáticos tenemos delitos contra datos y sistemas informáticos, delitos informáticos contra la indemnidad y libertad sexual, delitos informáticos contra la intimidad y el secreto de las comunicaciones, delitos informáticos contra el patrimonio y delitos informáticos contra la fe publica.
La Acción Típica para **Hurtado** (2005) es el elemento esencial del aspecto objetivo del tipo legal consiste en un acto designado por el verbo principal de la descripción legal (p.413). Es decir, es la acción que es descrita con el verbo rector en la norma.

Con respecto a los delitos contra datos y sistemas informáticos sus acciones típicas serian el que deliberadamente e ilegítimamente accede ilícitamente, el que deliberadamente e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, el que deliberadamente e ilegítimamente inutiliza, total o parcialmente un sistema informatico, impida acceso, entorpece o imposibilite su funcionamiento.

En lo referente a delitos informáticos contra la indemnidad y libertada sexual, sus verbos rectores son el que a través de internet establece contacto o comunicación con una menor. Aquí sola la mera intención de contactarse ya es sancionado. Sobre los delitos informáticos contra la intimidad y el secreto de las comunicaciones la acción típica el que deliberadamente e ilegítimamente intercepta datos informáticos en trasmisiones no públicas. En los delitos informáticos contra el patrimonio el verbo rector seria el que deliberadamente e ilegítimamente diseña, introduce, altera, borra, suprime y clona datos informáticos en perjuicio de terceros. Por ultimo en lo referente a los delitos informáticos contra la fe pública la acción típica seria el mediante las tecnologías de la información suplante la identidad de una persona natural o jurídica.

Para **Hurtado** (2005) la Relación de Causalidad o Nexo Causal sea concebido como una categoría relacional de tipo social y jurídico (p.421). Donde se busca el nexo entre el hecho delictivo y el autor del delito. Por ello es necesario que exista una relación entre acción y resultado. En los delitos informáticos determinar el nexo causal está supeditada a la evidencia digital, el cual es el instrumento por el cual puedo situar al sujeto activo en el hecho delictivo. En este tipo de delitos especiales, este se torna más complejo.

Según **Hurtado** (2005) la Imputación Objetiva es la imputación del resultado al autor de la acción es determinada en el marco del tipo legal (p.421), y sea sancionado al sujeto activo por el hecho delictivo. En los delitos informáticos las penas oscilan entre uno a ocho años.

Para **Hurtado** los Elementos Descriptivos y Normativos son independientes uno del otro, siendo los elementos descriptivos los conceptos tomados del lenguaje común que se refieren a determinados hechos y que deben ser comprobados por el juez cognoscitivamente. Mientras que los elementos normativos se refieren a aquellos factores que solo pueden ser determinados mediante una apreciación de valor. (p.411) En lo referente a delitos informáticos se tiene que establecer correctamente el verbo rector para entender los elementos descriptivos de estos delitos especiales.

Sujetos de los Delitos informáticos

Tenemos que considerar como elemento a todo aquel que busca ser parte de un todo. En nuestro caso quienes están implicados en el hecho delictivo. Donde tenemos al Sujeto Activo y a Sujeto Pasivo.

Para Valdez y Lima citados por **Gil** (2007) consideran como Sujeto Activo a la persona que comete Ciberdelito con unas características específicas ya que no representa al delincuente común o clásico. Visto que estos tienen las habilidades para manejar los sistemas informáticos y usualmente por la posición de índole laboral en la que se pueda encontrar, se sitúan en zonas estratégicas para la facilidad en el acceso de información delicada, o bien son hábiles en el uso de sistemas informatizados. Por ende, no se trata del delincuente común, que puede ser fácilmente identificado, estos trabajan tras una cadena de números y su capacidad de comprensión es binaria. Tiene un alto grado de nivel de aptitudes que en la actualidad aun genera una seria de controversias en cuanto a la ética y al acceso a la educación sobre estos conocimientos proponiendo la limitación de los mismos.

Entre ellos tenemos a los denominados Hackers, que en muchos casos pueden ser los denominados Hacker éticos que son contratados por empresas para que vulneren e ingresen a sus sistemas y medir su grado de error para posteriori mejorar, en cambio los Crackers son generalmente personas que se introducen a sistemas informáticos remotos con la intención de destruir datos, alterar el sistema, etc.

Por otro lado, tenemos al Sujeto Pasivo que está constituido por la víctima del delito, siendo el que genera una conducta ya sea de acción u omisión en referencia al sujeto activo, y se incrementa en los casos de Delitos informáticos. De todas maneras gracias a este elemento podemos llegar a conocer los variados ilícitos que pueden cometer los delincuentes informáticos, siendo en muchas veces descubiertos casuísticamente debido al desconocimiento del modus operandi.

Delincuente Informático

Considerado como el Autor del Ciberdelito, en muchas ocasiones el Sujeto Activo en la realización del delito. **Gimenez** (2011) considera que los delincuentes informáticos, usualmente son personas de confianza, es decir suelen ser empleados que tienen acceso al sistema informático. Según las estadísticas, más del 90% de los delitos son cometidos por los usuarios del sistema y los otros por técnicos informáticos (p.104).

Dándonos a comprender que, según el fenómeno, el comportamiento de los delincuentes informáticos, son personas que acceden muy fácilmente a estos sistemas, saben sus deficiencias y debilidades. Conocen perfectamente como romper la Seguridad y bajar la información necesaria o destruirla.

Tipicidad Subjetiva de los Delitos Informáticos

La tipicidad subjetiva es aquella relacionada con el dolo y la culpa. Es decir para Hurtado (2005) constituía el mundo interno del autor utilizadas para describir el acto incriminado. (p.447). Por ello es determinante como factor para saber si es una acción típica o no. En los delitos informáticos es necesario determinar la intención o la manera en la que realizo este hecho delictivo para saber si encaja en el tipo penal, visto que existen delitos de mera actividad y delitos de resultado. Pero por ejemplo en lo referente al artículo 5 de la Ley de delitos informáticos tiene una denomina tendencia interna trascendente ya que representa un elemento subjetivo distinto al dolo, porque

describe una intención especial del agente lo cual denomina **Villavicencio** (2014) un delito de resultado cortado, porque el agente persigue un resultado posterior el cual es obtener material pornográfico o alguna actividad sexual. (p.49) Es decir la mera intención de acercamiento ya considerado delito al ser el sujeto pasivo uno que reúna una serie de condiciones, por ejemplo ser menor de edad.

Evidencia Digital

En la actualidad es considerada como una nueva fuente de evidencia. Ya que no es utilizada netamente para delitos informáticos, sino también para la comprensión en delitos convencionales, y servirá para sustentar el Caso Penal y relatar los hechos del acto delictivo.

Para **Gercke** (2014) la importancia de la evidencia digital es vital para los Delitos informáticos ya que incluye dos partes o dos fases, la primera aplicada a la denominada "técnica forense informática", el cual hace referencia al análisis de tipo sistemático sobre los equipos TI de esa manera llegar a encontrar la evidencia digital. Siendo la segunda fase la entrega y muestra de la evidencia analizada y estudiada en los tribunales, tomando en consideración que está vinculada a ciertos procedimientos que es necesario aplicar, visto que la información digital solo es visible cuando se imprime o visualiza recurriendo a TI (p. 253). Es decir que para que esta evidencia pueda ser observada para su comprensión debe ser exteriorizada tanto en papel impreso físico o en imágenes o videos. De esta manera pueda ser considerada en los juzgados.

Para **Ballesteros** (2014) la prueba electrónica es considerada como cualquier información obtenida solo que proviene de un medio digital, que es utilizado para validar la certeza de un hecho. (p.225), lamentablemente este instrumento es muy desconocido en el ámbito judicial en especial por jueces, magistrados, fiscales y en general por profesionales de Derecho. Por otro lado, no existe una regulación sobre el tema de manera precisa, contienen usualmente contradicciones de manera que

generan una disparidad de criterios para la admisibilidad de la misma como prueba en los juzgados.

Por lo mencionado comprender que una de las características de este tipo de pruebas es la volatilidad haciendo muy necesario que sea sustituida por unos protocolos seguros de actuación que garanticen su inalterabilidad o no manipulación por ningún movimiento, a veces tan fortuito, es decir como encender o apagar un ordenador, o mal intencionado por parte de los implicados en la comisión del delito.

Otro punto a rescatar es la urgente necesidad de crear profesionales del derecho en materia tanto de evidencia digital, como prueba electrónica para que garanticen su admisibilidad en el proceso al comprender y apreciar sus vulnerabilidades, como sus ventajas y garantías. De esta manera se reduzca la diferencia entre una prueba tradicional y la electrónica.

Metodología de recolección de evidencia digital

La metodología de recolección de evidencia digital compone un conjunto de pasos para la obtención dela evidencia digital a través de protocolos científicos que permitan darle la validez y confiabilidad a la evidencia, de esta manera sea fehaciente en el proceso penal. Debemos considerar que guiarnos por protocolo de recolección de evidencias digitales correcto, permite disminuir las probabilidades de que estas se alteren o destruyan, a pesar de esto, se debe considerar que se respeten las normas vigentes en el país sobre protocolos utilizados siendo considerada al evidencia en un proceso penal y declarada admisible.

Esta metodología debe tener tres ápices básicos que son las consideraciones previas antes de proceder a la recolección de evidencia digital, la cuáles serán desde los softwares especializados, los laboratorios, el recurso humano, entre otros. Por otro la manejar un proceso de recolección de evidencia digital y finalmente un proceso de almacenamiento y custodia de la evidencia digital.

En lo concerniente a las consideraciones para la Recolección de Evidencias Digitales, tenemos según **Salas** (2012) los siguientes:

Primero. Una relación de Principios Básicos:

-Incorporarse a los estándares y políticas referente a la seguridad que se debe tener en el lugar para la correcta manipulación del incidente.

-Realizar una captura de pantalla sobre el sistema con la mayor exactitud.

-Priorizar la toma de notas que contengan la mayor cantidad de detalles, como las fechas, horas, tipo de evidencia, etc. Estas deberán ser impresas firmadas y finalmente fechadas.

-Considerar si existiera una diferencia sobre el reloj del sistema y el Tiempo Universal Coordinado.

- Tener todo listo ante la probabilidad de volver a testificar (incluso años posteriores), donde necesitara la mayor cantidad de información sobre el peritaje. Por ende, las notas lo más detalladas son fundamentales.

- No tener demasiados cambios en el proceso de recolección de la evidencia. Es decir, limitarse únicamente a cambios externos, mas no internos como actualización de archivos digitales o cambios en los tiempos para accesar a los directorios.

- Sellar todas las vías de acceso externo, que tuviera la información, de esta manera limitar posibles copias o modificaciones no autorizadas.

-Nos vamos encontrar en disyuntivas entre recolectar o analizar la evidencia digital, se recomienda primero recolectar de manera correcta para su posterior análisis.

- Es necesario probar los procedimientos para asegurarnos su viabilidad y el manejo de los mismos en una crisis. Lo que se busca es automatizar los procedimientos, sin olvidar la instrumentalización, por un tema de celeridad. Siendo metódico.

- Cada dispositivo electrónico tiene un método de recolección de evidencia diferente, pero de seguir los lineamientos establecidos dentro del procedimiento de recolección. En muchos casos la velocidad será determinante cuando la carga de evidencia a analizar es considerable, por lo que será necesario distribuir el trabajo en diferentes equipos y poder reunir pruebas a la vez.

- Por otro lado, existen casos donde la colección de evidencia de un sistema en particular debe ser llevada paso a paso, para no perder ni alterar la información.
- Otro punto importante es ir avanzado con la recolección de evidencias digitales según la volatilidad que tenga el dispositivo entre uno y otro.
-Por todo lo antecedido, es necesario realizar una copia de prueba y obtener el Hass, que es copia a nivel de bits del sistema. Esto ayudara en el análisis forense, utilizando su copia de prueba a nivel bits, visto que si se aplica en el dispositivo principal este alteraría los tiempos de acceso del archivo.

Segundo. Orden de volatilidad

Esta busca priorizar el orden de las evidencias según las susceptibilidades de los dispositivos de ser volátiles, por ende, será más urgente iniciar con los equipos que tengan mayor volatilidad y terminar con los menos volátiles.

Tercero. Consideraciones de privacidad

El Código Penal Peruano específica en su Título IV "Delitos contra la Libertad", se debe considerar algunos puntos como es respetar la privacidad de las personas, como también si alguna información obtenida para la investigación va causar algún perjuicio no deberá ser publicada sin consentimiento de la persona interesada o por mandato judicial. También es importante la cooperación de las empresas nacionales y el gobierno para poder continuar con el procedimiento correspondiente sobre la recolección de evidencia digital sobre el incidente

Cuarto. Puntos Legales

Este ápice establece los requisitos que debe tener la evidencia para ser sujeta a una evaluación y posteriormente ser admitida como prueba en un proceso legal. La evidencia debe ser Admisible, es decir necesita tener y cumplir ciertos requisitos antes de ser llevado ante el proceso penal, también debe ser Auténtica, de esta manera poder demostrar el nexo causal con las pruebas materiales sobre el incidente. También de estar Completa, es decir la misma narra todo lo acontecido y no solo de manera parcial, por último, debe ser fiable y creíble, la primera no se debe tener duda alguna

de la forma en que la evidencia fue recolectada y luego la manera en que fue analizada, la segunda busca que esta llegue a ser comprensible y creíble para los jueces.

Quinto. Aspectos Logísticos

Después de todo lo antecedido se requerirá una serie de recursos para efectuar el estudio de las evidencias digitales.

a) Factor Humano: Constituida por un equipo de profesionales que son expertos en recolección y análisis de evidencias digitales.

b) Factor Material: Constituida por los instrumentos preparados para el fin del análisis forense, donde este debe ser una red aislada. También es importante contar con Anotaciones de Campo, Fichas o plantillas de recolección de información, cámara digital, guantes, fundas protectoras, equipos informáticos especializados y software apropiado.

En lo referente a proceso de recolección de evidencia digital tenemos primero la Transparencia, que son aquellos métodos que son utilizados en la recolección de evidencias visto que esta tiene que ser transparente y reproducible. Y por otro lado tener pasos determinados para cumplir con el procedimiento de recolección y de esta manera armar una lista de aquellos sistemas que estén vinculados con el incidente y de aquellos que se recogerán las pruebas. Aquí se considera los siguientes pasos:

-Determinar que es o no una evidencia, caso contrario no proceder con la recolección.

- Manejar el orden sobre la volatilidad que tenga cada sistema.

-Desaparecer las salidas externas.

-Anotar la hora del reloj del sistema.

-Consultar que objetos recolectados pueden ser finalmente probatorios, esto es a medida que avanza la investigación.

-Registrar cada paso realizado.

- Registrar a todas personas involucradas.

Finalmente, lo referido a los procedimientos sobre almacenamiento de las evidencias digitales tendremos a Registro y Codificación donde aquella evidencia que ha sido recolectada tendrá que ser registrada y posteriormente codificada, donde esta última guarda relación con el sitio donde suscitaron los hechos, registrada por fecha, lugar, caso al que pertenece.

Luego tendremos un Registro Fotográfico y Audiovisual donde se considerara lo siguiente:

- Fotografiar y/o filmar, el equipo sin desmontar (apagado con el cartel de número de serie).
- Fotografiar y/o filmar, el equipo desmontado (con el cartel visualizando números de serie de hardware).
- Fotografiar y/o filmar, la configuración del equipo por dentro.
- Fotografiar y/o filmar, el disco duro original y las copias (2) juntas (se debe ver la fecha, hora y las etiquetas), pasa corroborar la existencia de las copias y originales entregados al custodio.

Por último y transcendental tener una correcta Cadena de Custodia, siendo una serie de procedimientos que están orientados a la preservación de la evidencia digital. Siendo los siguientes:
- Primero la recolección e identificación de la evidencia digital.
- Realizar el análisis de la evidencia digital.
- Proceder al correcto almacenamiento de la evidencia digital.
- Tener la evidencia digital en perfecto estado. Proceder a la preservación.
- Cumplir los protocolos para realizar el transporte de la evidencia.
- Realizar la presentación en el juzgado.
- Proceder a regresarlo al propietario.

Es necesario en tener en cuenta los siguientes puntos en lo referente a la cadena de custodia:

- Que la manipulación de las evidencias sea mínima y el estudio de esta, sea por la menor cantidad de agentes.
- Tener en reserva la identidad de las personas que están implicadas desde la obtención hasta la presentación de la evidencia en el juzgado.
-Es de entera responsabilidad que la evidencia digital sea inmutable a pesar de los traspasos entre agentes.
-Llevar el registro de los tiempos, estos deben ser firmados por agentes, en cada uno de los intercambios entre estos sobre la evidencia en cada momento.

Todos los procedimientos descritos aunados al método científico tecnológico podrán lograr el objetivo de que la evidencia digital sea admitida, creíble y fehaciente dentro del proceso penal.

Metodología de análisis de evidencia digital

La metodología de análisis de evidencia digital busca a través de un método científico analizar la evidencia digital, como también producirla y presentarla en el proceso penal. Esta debe tener análisis exhaustivo, sea cual sea el tipo de evidencia digital. Aquí veremos análisis de los datos de la red, análisis de los datos de host, análisis de los medios de almacenamiento. Consideremos que lo que se va analizar son las denominadas "armas no convencionales - TIC", las cuales son invisibles y especiales, aquí la informática forense a la criminalística cibernética juega un papel muy importante.
Este análisis de los indicios binarios tiene el análisis lógico y tiene el análisis físico. En este punto se tienen varios conflictos visto que la tecnologías son cambiantes sin compatibilidad de equipos y accesorios, los sistema de archivos reside en memoria volatil-ram, los equipos 3g4g y 4.5g permiten clonación de equipo, es fácil de comprar-conseguir equipos de otros dueños, a pesar de que existe un avance en los operadores no hay plena identificación del usuario real, existe deficiencia en las diligencias para determinar la vinculación real del equipo celular móvil y delincuente, la ausencia en el servicio de telefonía celular móvil de registro de equipos y la Ingeniería social, como

las redes sociales y la base de datos a la mano del delincuente. Todo lo antecedido genera limitaciones y problemáticas para un correcto análisis forense.

En lo correspondiente a un correo se analiza de la siguiente manera una dirección del correo tiene dos partes: La parte de usuario (alumnoucv) y la parte de dominio (hotmail.com) donde la cuenta de alumnoucv@hotmail.com. Aquí tenemos que tener en claro que el usuario normalmente no está registrado y los Dominios sí. Por ende el correo electrónico ofrece la posibilidad de incluir attachments o apéndices que pueden ser archivos, bases de datos, audio, etc.

Finalmente procede realizar el informe donde se recopila y organiza los datos de las evidencias digitales para que sea presentada en el Juicio y finalmente admitida. Para ello debe cumplir una serie de requisitos que deben estar plasmados en el Informe. Primero de ser admisible, para ello se empleó una metodología adecuada tanto de recolección como de análisis. Segundo, demostrar su autenticidad, por ello es importante la copia espejo-bit a bit y firmas de seguridad. Tercero manejar una integral diligencia en contexto del escenario del delito. Cuarto, debe ser fiable donde la actuación de expertos, uso de técnicas y herramientas forenses legales. (no es admisible la prueba prohibida, ni la empleada con herramientas no permitidas). Quinto, esta debe ser clara, donde el proceso de extracción, aseguramiento, análisis y presentación debe ser entendible para el destinatario, debiendo usarse las técnicas demostrativas de evidencia física. Por ultimo debe ser creíble, donde este el título habilitante del perito, experiencia comprobada.

Ciberespacio

El Ciberespacio es considerado el ámbito de desarrollo para las redes y comunicaciones a través de internet, el espacio donde se almacenarán miles de millones de datos llenos de información en servidos de todas partes del planeta, que pueden ser compartidas, modificadas, alteradas, removidas, el cual esta

interconectado a nivel mundial. Ha ese fenómeno se le conoce como espacio de internet o Ciberespacio.

El Ciberespacio no tiene una real Jurisdicción porque escapa de los límites y protocolos físicos para establecerse como tal o cual país. Es más bien que maneja una jurisdicción internacional, del cual requiere una unificación de todas las naciones, para que la misma sea correctamente regulada.

Por otro lado, en esta área nos manejamos a través de protocolos de direccionamiento IP/TPCI, el cual permiten darle una identificación a su punto de acceso a internet. De esa manera tener un control del mismo. Como cuantos datos de internet estas consumiendo, el acceso a una velocidad determinada para acceder a los mismos, etc.

En este caso las operadoras juegan un papel importante en lo denominado "tráfico de datos". Este tipo de control es muy fácil ser vulnerado y engañado a través de simuladores y mecanismos tanto de hardware como software para que no pueda ser identificado el IP. Es decir, el puerto por donde se tiene acceso al Ciberespacio.

Ante todo, lo mencionado el Ciberespacio juega un papel fundamental porque es donde se sitúan los ciberdelincuentes para cometer los Delitos informáticos y al ser la Escena del delito, el cual es vulnerada una y otra vez, debe ser considerada como pieza fundamental de la investigación.

Peritos Informáticos

El Perito Informático es el encargado de realizar el análisis forense digital y de esa manera conseguir una serie de evidencias que demuestren los hechos que se investigan en un tipo de dispositivo. Este es un laborioso proceso, es decir, la necesidad de no vulnerar la Seguridad Jurídica nos exige que el Perito Informático sea Certificado y Calificado.

Para **Gercke** (2014) "la denominación de criminología informática es usada para describir la recopilación sistemática de datos y el análisis de TIC´s a fin de buscar pruebas digitales" (p.266). Esta prueba digital tiene un manejo especial. Es decir, se necesita la especialización de los peritos, estos requieren un conocimiento base orientado a Informática, porque ese conocimiento es cambiante y de esa manera saber cuáles son las últimas tendencias.

Por ende, no todo técnico es perito informático, ya que también se requieren conocimientos de investigación, para poder dar respuestas optimas referente al Caso y saber expresar el informe que realicen, saliéndose de los tecnicismos y de esta manera conseguir la comprensión necesaria en los entes jurisdiccionales.

Según **Gil** (2007) la informática forense abarca cuatro partes fundamentales 1) la identificación de evidencia digital, 2) preservación de la evidencia digital, 3) el análisis de la evidencia digital y 4) presentación de evidencia digital (p.512-513). Este proceso busca el informe técnico informático, donde el resultado final se derive de acápites legales. El análisis forense digital es la revisión de un medio informático. Se puede hacer un análisis forense digital incluso de una firma.

En conclusión, el peritaje informático es aquel en donde tiene que intervenir un instrumento informático. Y tiene que ser realizado por especialistas en la materia, para la obtención eficaz del informe sobre la prueba digital.

Informática Forense

Para algunos autores la Informática forense es el medio procedimental para la obtención de información de las actividades de los dispositivos digitales y el ciberespacio. En otras posturas lo consideran como la ciencia de investigación de la nueva era, totalmente necesario. Es decir, en la actualidad ya no hay delito en el que no se requiera un peritaje Informático Forense, donde la prueba digital está tomando más peso día con día.

Dentro de la postura investigativa consideramos lo que **Kindersley** (2003) entiende por Informática forense como la ciencia de investigación resumida a series de unos y ceros donde la información digital parece elusiva y fácil de ocultar. Cada vez que son almacenados, leídos, escritos, trasmitidos o impresos, los datos se multiplican sin parar (p.128). Esta denominación de ciencia, es avalada por el peso de índole investigativo, científico. Donde la necesidad de estar un paso más allá de la Ciberdelincuencia en cuanto a Hardware y Software es vital para enfrentarse a esta problemática y mostrar la verdad del hecho delictivo.

Cadena de Custodia

La cadena de custodia es considerada como el procedimiento que busca garantizar la originalidad de las evidencias y de esta manera establecer que cualquier muestra, rastros u objetos que hayan pasado por un análisis pericial y posteriormente ingresado en el proceso penal, cuando sea considerada, entonces, como prueba, sea la misma que se levantaron en la escena del delito.

Tener en cuenta que los que participan en la Cadena de Custodia son los servidores públicos y particulares que tengan nexo con las evidencias, incluyendo a terceros necesarios, como personal de salud en los hospitales cuando sea el caso. También se considera al personal que levante, examine, traslade, almacene, entregue, procese o estudie un elemento.

El objetivo central de la cadena de custodia es direccionar correctamente la futura prueba para que pueda ser utilizada en juicio, siendo esta una garantía procesal, en vista que garantiza que el elemento de prueba mostrada en el juicio, es el mismo de la escena del delito y que su integridad no ha sido cambiada o modificada a lo largo de la investigación.

En nuestro país el desarrollo legal de la Cadena de Custodia la veremos en el Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados (Aprobado por Resolución Nº 729-2006-MP-FN del 15.junio.2006), del Ministerio Público, dentro de los cuales nos desarrolla 5 principios fundamentales de los que podemos rescatar el Control (de todos los procedimientos), la Preservación (de las evidencias), la Seguridad (de las evidencias), la Mínima Intervención (de terceros ajenos), y lo más importante la Descripción Detallada (de las evidencias).

Con lo antecedido evidenciamos que en la actualidad existe una protocolización y estandarización para el recojo de las evidencias e indicios que se encuentren en la escena del Delito. Estos procedimientos son de suma importancia, ya que el olvido, la decidía, o intencionalidad negativa sobre el manejo de la prueba puede tumbar todo un proceso. Esto afectaría el objetivo y la finalidad de la Cadena de Custodia.

Instrumentalización de la Evidencia Digital

La instrumentalización de la Evidencia Digital consiste en la aplicación de las herramientas para el análisis cuidadoso de la evidencia digital, tanto en Hardware como Software. Estos instrumentos son especiales para esta clase de evidencia.
Estos instrumentos permiten el desarrollo del reconocimiento, recolección, custodia y análisis de la evidencia digital. En muchos casos permiten la reconstrucción de evidencias prácticamente perdidas. Recuperación de datos, interpretación de códigos binarios encriptados, sin alterar la evidencia, ni la forma de mostrar la información.

Una correcta instrumentalización nos permitirá tener a mano todo lo requerido para la manipulación de la evidencia asegurando su legalidad y futura admisibilidad en el Proceso Penal.

Investigación del Delito

La investigación es el paso inicial para la recopilación de información y de esta manera armar una hipótesis de la misma. Es la concepción clara de una interrogante y por ende se requiere la mayor cantidad de conocimiento sobre el tema para obtener la respuesta correcta.

Fierro Mendez (como se cita en Placencia, 2014) escribió:

> La etimología del término "investigación" nos sirve bastante bien como primera aproximación: la palabra proviene del latin in (en) y vestigare (hallar, inquirir, indagar, seguir, vestigios). De ahí el uso más elemental del término en el sentido de "averiguar o describir alguna cosa". También tenemos que "investigación" se considera un término derivado del latín investigatio, equivalente a acción y efecto de investigar y descubrir algo, la misma que en muchos casos delictivos es generada por alguna denuncia que informa de una circunstancia considerada como delito (p. 25).

Haciendo referencia a la notitia criminis, que puede llegar como una denuncia, siendo la primera noticia que se tiene del hecho delictivo, al ser solo meros receptores tenemos el trabajo de comprobar las supuestas hipótesis. Y es aquí donde inicia la investigación del delito.

El delito es entendido como la secuencia de acción o acciones que tienen una connotación ilícita, por ende es pasible de ser sancionado. La identificación de este tipo de conductas deviene de un dolo, es decir crea el fenómeno del perjuicio sobre un objeto jurídicamente protegido. Al hacerse evidente tal hecho no encontramos frente al delito.

Zaffaroni (como se cita en Hurtado, 2005), escribió:

> (...). Debe ser más bien comprendidos en el sentido de lo que el alemán se llama Garantietatbestand ("tipo legal de garantía"); que da entender es el conjunto de

> elementos que debe una acción para que el autor sea punible del hecho (adecuación a la descripción formal, el desvalor jurídico: antijuricidad; la reprochabilidad a su autor: culpabilidad), con excepción de las condiciones procesales necesarias. (p. 160)

Es decir que para se configure el delito debe tener una Acción Típica, ser antijurídica, culpable y punible. Para que este hecho delictivo sea una Acción Típica tiene que estar establecido en la norma, es decir tipificado conforme a ley. De no ser suficiente esta acción debe ser sancionable.

Con las teorías que nos anteceden determinamos que la Investigación del delito es la recolección de información, datos, huellas, indicios que nos den los conocimientos para aclarar las cuestiones referentes al hecho punible y de esa manera sean sancionados.

Identificación de la Autoría

Para la determinación de la Autoría es necesario conocer el requisito subjetivo del dolo o la culpa, en cualquiera de los supuestos la Autoría varia. En aquellos delitos de origen doloso el autor será aquel que busca o realiza la acción delictiva. Mientras que en delitos culposos la autoría se realiza de manera involuntaria, no ha existido una planificación previa y muchas veces es en legítima defensa.

Bockelman (como se cita en Hurtado, 2005), escribió:

> Según lo que sucedía con el Código derogado existe una diferencia, en el actual la noción de autor es parte del subsistema de la autoría que, junto con el de la participación en sentido estricto, forman el sistema general de la participación delictiva. La autoría, en verdad, no constituye una manera de ejecución colectiva del delito, pero es el punto de referencia de las demás formas de participación. (p.863)

Existiendo una diferencia entre el Sujeto Activo y el Autor del delito, ya que el Sujeto Activo solo se limita a realizar órdenes y proceder con el delito, mientras que el Autor, planifica, organiza, establece, y procura que existan todas las condiciones para la realización del delito. Es decir, puede ser una Autoría Mediata, como Autoría Inmediata. Aquí también se establecerá el grado de Participación, como la Coautoría.

Las principales características para la identificación de la autoría son el nexo causal, comprobados con los elementos de convicción, el dominio del hecho, o llamada también intención, ya sea con dolo o culpa, y finalmente el hecho delictivo en sí. Para Angulo "En todo caso, algo que sí queda puntualizado es que, si no pudiera ser individualizada e identificada a la persona, no podría decirse que se ha configurado el caso penal" (2014, p.143).

En síntesis, la identificación del autor del delito es necesaria para la aplicación de la sanción correspondiente, si no hay autor, que muchas veces es también el sujeto activo, no existiría el hecho delictivo y por ende no habría un caso penal. A falta de nexo causal, no habría vinculación con el autor. En consecuencia, caería la teoría del caso, por falta de comprobación.

Investigación de los Delitos informáticos

La vinculación de la Autoría con el hecho delictivo era suficiente para crear el denominado nexo causal. En delitos de alta especialización como los delitos informáticos, no es suficiente realizar la investigación del delito e identificación del autor. En la actualidad es necesario una investigación exhaustiva orientada solamente en la Autoría. La complejidad de estos delitos ha acaecido sobre los elementos de convicción convirtiéndolos en poco creíbles e incluso volátiles. El manejo de esto exige un tipo investigación centrada en la comprobación del delincuente real. Ya que el Autor de estos delitos no es un delincuente común, no es una acción netamente física, sino más digital, donde su lugar de aplicación de estos crímenes es el Ciberespacio.

Para Angulo el trabajo fiscal, siempre deberá estar dirigido a reunir elementos de convicción o una suma de indicios suficientes, para probar que se ha configurado una conducta ilícita, sancionando de modo claro por la norma penal, motivando a que el presunto autor sea castigado. (2014, p.48)

También considera Angulo que para consolidar el caso contra una persona resulta evidente que contra ella deben existir excelentes razones para atribuirle la responsabilidad de los hechos. Es decir, se consolida el caso con los elementos de convicción que tengan el nexo con el Autor. Por ello la vinculación como autor que contiene la acusación resulta ser una condición acabada. (p.150)

En conclusión, la importancia del nexo entre el hecho delictivo y el Autor, es tan relevante como su correcta identificación. Por ello la Investigación neta de los Delitos informáticos, se centra en una identificación ardua y especializada.

Eficacia del Enjuiciamiento

La palabra eficacia es de origen latín efficacĭa, siendo la eficacia aquella capacidad de alcanzar el efecto que espera o se desea tras la realización de una acción. Por ello no tiene por qué confundirse este concepto con el de eficiencia (del latín efficientĭa), visto que este es referente al uso racional de los medios para alcanzar un objetivo predeterminado (es decir, cumplir un objetivo con el mínimo de recursos disponibles y tiempo). La eficacia es llegar a la meta, mientras que la eficiencia es el uso adecuado y racional de los recursos para lograr este cometido.

Para Kelsen (1958):

> La eficacia del derecho quiere decir que los hombres se comportan en la forma en que, de acuerdo con las normas jurídicas deben comportarse, o sea, que las normas son realmente aplicadas y obedecidas. Decir que un orden jurídico es

> 'eficaz' significa simplemente que la conducta de la gente se ajusta a dicho orden. Con ello nada se afirma acerca de los motivos de tal conducta ni, en particular, sobre la 'compulsión psíquica' que pueda emanar del orden jurídico (p.46).

Estos son directrices que permiten que el proceso penal se lleve de acuerdo a ley y con las garantías necesarias para mantener el Debido Proceso, ante todo, si la normativa es imperativa positiva, esta va ser aplicada según lo establecido. Contrario censu puede crear un vacío y por ende no tendrías una Eficacia en su enjuiciamiento, ya que no cumpliría con los requisitos necesarios para armar el Caso penal.

Desde otra perspectiva Bobbio (2000), determina que "la eficacia es determinar si una norma es cumplida o no por las personas a quienes se dirigen o los destinatarios de la norma jurídica" (p.20). Dentro de este contexto la postura del autor determina que toda norma debe tener en cuenta tres criterios de valoración siendo apreciadas y encontradas dentro de un ordenamiento jurídico; estos criterios son: si es justa o injusta, si es válida o inválida, y si es eficaz o ineficaz, estos criterios son independientes entre sí, ya que no se necesitan para existir.

Para Ballesteros (2014), el entorno de la Ciberdelincuencia está creando cambios sumamente radicales en las estrategias que tienen que tener los abogados al momento de mostrar las pruebas informáticas o electrónicas en los procesos judiciales, esto debido a que la gestión y los criterios de admisibilidad se modifican considerablemente tomando en cuenta que tenemos un régimen jurídico tradicional sobre la prueba en cualquier tipo de proceso. En la actualidad en este tipo de procesos se hace necesario presentar documentos electrónicos y es preciso salvaguardar y adquirir las pruebas de una forma adecuada de esta forma su eficacia no podrá quedar desvirtuada en el proceso (p.225)

Lo antecedido describe la importancia de manejar las evidencias digitales lo más cuidadosamente posible en beneficio de llevar este tipo de investigaciones al proceso

de tal manera, que la prueba sea aceptada dentro del mismo y demuestre el nexo con el Autor del delito.

Por decir cuando hablamos de eficacia del enjuiciamiento, nos referimos a la potestad de llevar a buen recaudo el proceso judicial y pueda ser condenado correctamente el imputado. En otras palabras, que estos delitos no queden impunes y puedan ser juzgados conforme a ley.

Formulación del problema

Problema Genera

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

Problemas Específicos

Problema Especifico 1

¿Cómo la protección de la Evidencia digital influye en la clasificación de los Delitos Informáticos en el Proceso Penal peruano?

Problema Especifico 2

¿Cómo la determinación del Marco Legal de la Evidencia Digital repercute en la Tipicidad de los Delitos Informáticos en el Proceso Penal Peruano?

Justificación del estudio

En el aspecto personal resulto interesante realizar esta investigación, ya que, en el campo al recabar los datos de interés, las opiniones de los especialistas eran en algunos casos diferidas y complejas y en otros estandarizadas y simples, visto que el tema de Delitos informáticos no ha sido muy estudiado, es un tema relativamente nuevo, siendo sumamente importante dentro de la Carrera Profesional de Derecho.

En el aspecto Técnico esta investigación permitirá ver como un tema muchas veces dejado de lado por las autoridades influye mucho en la necesidad de combatir la Ciberdelincuencia y de esta manera se pueda incorporar acciones que estén dirigidas a estudiar, entender el tema y tratarlo. De esta comprender la importancia de la especialización sobre la influencia de Delitos que no son comunes.

En el aspecto práctico vemos como la sociedad necesita involucrarse en el tema de los Delitos informáticos, así como las entidades policiales, el ministerio público y entidades judiciales, y este es el fin principal de la investigación realizada visto que son ellos los actores dentro del proceso para llevar un caso de Delitos informáticos a enjuiciamiento y no quede impune. Por ende, establecer las herramientas necesarias para combatir la Ciberdelincuencia, donde una de ellas es el conocimiento y así tener una visión distinta de la problemática que acaece sobre la investigación.

En el aspecto metodológico vemos su importancia en cuanto a la preparación de la presente investigación, por ende, servirá como modelo para futuros estudios, y es que se ha basado en fuentes confiables y actualizadas lo que permiten evidenciar su utilidad.

El instrumento de medición será la Guía de entrevista, de esta manera poder recabar la información sobre esta problemática con los especialistas. Aquí determinar la población es un tanto complejo, visto que el Ciberespacio no tiene jurisdicción alguna, por ellos nos estamos orientado como población sobre aquellos sujetos que van a manejar todo el proceso una vez sucedido el hecho delictivo, es decir la realización del iter criminis, hasta la llegada de la noticia criminal, investigación, identificación de los autores, y enjuiciamiento o juicio oral en algunas partes del país. Los cuales son los policías de investigaciones DIVINDAT, los fiscales, jueces y abogados.

En el aspecto Institucional teniendo como casa de estudios a la Universidad Cesar Vallejo, este Proyecto de tesis se justifica por ser parte de los esfuerzos de la Universidad por forjar en sus estudiantes el deseo de investigación, y con ello mejorar

la visión de cada uno en su carrera. Esto será el mejor aporte para las siguientes promociones de Vallejianos.

Objetivos

Objetivo General

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

Objetivos Específicos

Objetivos Especifico 1

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

Objetivos Especifico 2

Constatar como la determinación del Marco Legal de la Evidencia Digital repercute en la Tipicidad de los Delitos Informáticos en el Proceso Penal Peruano.

Supuestos Jurídicos

Supuesto Jurídico General

S1: La admisión de la evidencia digital incide positivamente en los delitos informáticos en el proceso penal peruano.

Supuestos Jurídicos Específicos

Supuesto Jurídico 1

La protección de la Evidencia digital influye positivamente en la clasificación de los Delitos Informáticos en el Proceso Penal Peruano.

Supuestos Jurídicos 2

La determinación del Marco Legal de la Evidencia Digital repercute positivamente en la Tipicidad de los Delitos Informáticos en el Proceso Penal Peruano

II. MARCO METODOLÓGICO

2.1 Tipo de Investigación

Cualitativo - Aplicada

La tesis se desarrolló bajo el enfoque Cualitativo del tipo Aplicada, pues buscaba la comprensión de los fenómenos sociales que afectaban a la normativa en nuestro país y buscar una solución. Según Vara (2012) "Se llama investigación cualitativa a todo estudio que se concentra más en la profundidad y comprensión de un tema que en la descripción o medición. A la investigación cualitativa le interesa sintetizar un proceso, esquematizarlo, comprenderlo, más que sólo medirlo y precisarlo." (p.204). Por ende al determinar que el enfoque Cualitativo iba acorde a los objetivos de la investigación, se procedió a realizar el mismo sobre el mencionado Tipo de Investigación.

En lo referente al Tipo de Investigación Aplicada menciona Vara (2012) "El interés de la investigación aplicada es práctica, pues sus resultados son utilizados inmediatamente en la solución de problemas empresariales cotidianos. La investigación aplicada normalmente identifica la situación problema y busca, dentro de las posibles soluciones, aquella que pueda ser la más adecuada para el contexto específico."(p.202) Esto nos da pie a llegar a comprender el fenómeno y establecer soluciones a la problemática que lo aqueja.

2.2 Diseño de investigación

Teoría Fundamentada que está orientada a descubrir teorías, conceptos, hipótesis, y proposiciones partiendo directamente de los datos, y de supuestos partiendo de investigaciones y teorías previas.

En las investigaciones de enfoque cualitativo, se puede o no concebir un diseño, se sugiere que, si se haga, pero la implementación de los mismos se vuelve más flexible. Es decir, el investigador puede elegir y desarrollar uno o más diseños para iniciar previamente la recolección de datos.

La presente investigación se elaboró bajo un diseño de Teoría Fundamentada pues el investigador realiza un desarrollo conceptual de un área amplia de investigación. Es decir, propone concebir conceptos a partir de la información obtenida.

Todos los datos recabados son de carácter cualitativo es decir para identificar cual es la problemática sobre la investigación de la autoría de los Ciberdelitos y su enjuiciamiento, ya que es una perspectiva interpretativa que busca como centro la comprensión de determinada problemática.

2.3 Caracterización de Sujetos

Para la identificación de la problemática de la presente investigación sobre la situación actual de la investigación de la autoría y el enjuiciamiento de los Ciberdelitos, aplicaremos el instrumento de Guía de entrevista a un Juicio de Expertos, del cual tenemos a los siguientes Expertos:

Personal de la DIVINDAT – Perito Informático. - Especialistas del área policial del Perú PNP, en Delitos Informáticos y de Alta Tecnología.

Abogado Informático. - Abogado especialista en temas informáticos.

Fiscal. - Fiscal Penal, que ha tocado temas de Ciberdelitos.

Juez. - Juez Penal, que ha tenido casos de Ciberdelitos.

N°	Entrevistado	Cargo
1	Capitán Lenin Alemán Ticona	Departamento n°2 de Investigaciones de la DIVINDAT
2	Comandante Manuel Guerrero Zerpa	Jefe del Departamento n°1 de Investigaciones de la DIVINDAT-Abogado

3	Dr. Nilda Roque Gutierrez	Ex Jueza Penal – Doctora en Derecho – Magister en Derecho Penal y Procesal Penal - Directora de la Facultad de Derecho de la UCV Lima Norte.
4	Dr. Iván Alberto Osorio Solís	Fiscal Provincial Penal de Chanchamayo – Magister en Derecho Penal y Procesal Penal
5	Dra. Marjorie Alvarado Alvarado	Magister en Derecho Penal y Procesal Penal – Abogada Penalista Lima
6	Dr. Julio Cesar Ramírez Ramírez	Magister en Derecho Penal y Procesal Penal – Abogada Penalista Callao
7	Dr. Ernesto Barrionuevo Azaña	Doctor en Derecho – Magister Derecho Penal y Procesal Penal – Abogado Penalista Lima Norte
8	Dr. Jose Luis Pazzoni Veramendi	Master en Derecho Penal y Procesal Penal - Master en Derecho Corporativo – Abogado Penalista Lima Norte

9	Dr. Héctor Perca Copa	Master en Derecho Penal y Procesal Penal – Abogado Penalista Lima Norte
10	Dr. Marino Hernández Carrasco	Master en Derecho Penal y Procesal Penal - Master en Gestión Pública – Abogado Penalista Lima
11	Dra. Mery Vega Hinostroza	Master en Derecho Penal y Procesal Penal – Abogada Penalista Chanchamayo
12	Dr. Wilfredo Alberto Estares Cañarí	Master en Derecho Penal y Procesal Penal – Especialista en Derecho Municipal – Ejecutor Coactivo Municipalidad Distrital de San Ramón – Abogado Penalista Chanchamayo

Tabla 1. Listado de Especialistas Entrevistados – Fuente Propia.

Para esta investigación nos regiremos por un Juicio de Expertos, de los cuales tenemos a los de Informática Forense, es decir la DIVINDAT, Fiscales Penales, Jueces Penales, Abogados Penalistas e Ingenieros de Sistemas.

2.4 Población y muestra

En este estudio la población estaba conformada por Especialistas a Nivel Nacional sobre Ciberdelitos, entre ellos especialistas de la DIVINDAT, Peritos Informáticos,

Jueces, Fiscales y Abogados. Que influyen en el desarrollo del combate contra la Ciberdelincuencia en el país.

Población: A nivel nacional Especialistas sobre Ciberdelitos.

Según **Sampieri** (2014) si el Diseño de Estudio es Teoría Fundamentada, entrevistas o personas bajo observación, entonces la Muestra debe estar considerada entre 20 entrevistas. (p.385)

Muestra: Se considera como muestra a 20 Especialistas sobre Ciberdelitos.

Tipo de Muestreo:

No pro balístico, es decir serán solo 20 especialistas sobre Ciberdelitos, donde será necesario dividir a la población, y será libre de elegir a los sujetos de la muestro dentro de cada estrato.

Muestreo intencionado, es decir se determinarán y seleccionarán intencionalmente a los especialistas.

2.5 Técnicas e instrumentos de recolección de datos, validez y confiabilidad

Para la presente investigación utilizaremos las siguientes técnicas e instrumentos de recolección de datos:

Una de las técnicas utilizadas para esta investigación será la recolección de datos a través de la Entrevista y el instrumento es la Guía de Entrevista, siendo una de las técnicas más utilizadas para la investigación. Debido a que su objetivo es la especialidad determinada de un área donde se desarrolla el problema desarrollado en la tesis, se plantea realizar una entrevista dirigida y estructura, para lo cual hemos trabajado con un cuestionario donde se trascriben las respuestas tal y como las proporciona el entrevistado. También hemos determinado que es una entrevista focalizada ya que desarrollamos una serie de puntos específicos.

- Entrevista no estructurada. - Se desarrollarán como técnica para la recolección de datos, donde el entrevistador la efectúa tomando como base un guion, pero las preguntas son abiertas y no tienen estandarización. En el presente caso se aplicará un cuestionario de 10 preguntas dirigidas a especialistas en la materia sobre Delitos Informáticos y Evidencia Digital, es decir nos regiremos por un Juicio de Expertos, de los cuales tenemos a los de Informática Forense, es decir la DIVINDAT, Fiscales Penales, Jueces Penales, Abogados Penalistas e Ingenieros de Sistemas. Esta entrevista permitirá obtener información real y precisa de la población en estudio e identificar la problemática sobre Delitos Informáticos y Evidencia Digital en el Proceso Penal Peruano. Dicho instrumento se elaborará utilizando de base la Guía de Entrevista.

Para **Perez** (2012) "la entrevista debe ser concebida como una situación de dialogo intencionada entre dos o más individuos, direccionada a dar una respuesta a los objetivos empleados dentro de un proceso de investigación. (p.38)

Otra de las técnicas de recolección de datos utilizada será el Análisis Documental, Análisis Legislativos y Análisis Doctrinarios y su instrumento será la Guía de Análisis Documental. En la presente investigación se usará una seria de normas, doctrinas y documentación relevante para la investigación y estos serán recolectados con el instrumento Guía de Análisis Documental.

- Análisis Documental. - Se desarrolla como técnica de recolección de datos, donde el tesista, la efectúa tomando el fragmento más importante o relevante del todo el Documento a analizar, y posteriori realizar una crítica por parte del investigador del fragmento sustraído. El cual permitirá determinar si este documento apoya o no el Supuesto Jurídico establecido en el Proyecto de Investigación. Es necesario conocer los datos completos del documento para su valoración como la procedencia, fecha de promulgación o publicación, titulo completo, descripción del documento y autor.

2.6 Plan de análisis de datos o trayectoria metodológica

El análisis de datos en la precedente para la actividad de la interpretación. Los investigadores cualitativos hacen registros narrativos de los fenómenos que son estudiados mediante técnicas como la observación participante y las entrevistas no estructuradas. Luego de llevar a cabo la técnica para recolectar datos, se tabularán y organizarán los datos, en la tabla comparativa de los resultados.

Se aplicará el Método hermenéutico el cual Liliana, Arlines y Doris (citado por Valderrama, 2013) indica que la hermenéutica es aquella "ciencia y arte de la interpretación, sobre todo textos..." y el Método Inductivo y de esa manera llegar a la comprensión incluso de simbologías, siendo un tema trascendental de estudio para el hombre (p., 90). Siendo que el método hermenéutico e Inductivo busca la valoración de los datos y por ende realizar una real critica de su situación.

2.7 Aspectos éticos

En la presente investigación se respetó toda la normativa sobre Propiedad Intelectual, el Derecho de Autor, nos proporciona una fuente confiable para asentar las bases necesarias y así proceder con el desarrollo de la tesis. Cada antecedente, marco teórico, anexo, imagen, será correctamente citado y referenciado según las Normas APA. De esta manera la estructura del mismo trabajo van estar regidos por la Normas APA. Además, el Rigor Metodológico usado para la elaboración de esta investigación va de la mano con la Investigación Científica.

El trabajo de investigación tiene once fuentes académicas de los últimos 10 años y tiene diversos tipos de fuentes (artículo, libros, ponencias, tesis). De las cuales existen Nacionales y Extranjera. Estas fuentes han sido correctamente analizadas y aplicadas a la investigación del proyecto de tesis.

Por ende, también es necesario resaltar que estamos libres de cualquier tipo de plagio. Toda investigación anterior a la presente investigación paso el procedimiento de fichaje (resumen, textual, bibliográfico), y selección según el requerimiento de los Objetivos de la Tesis

III. RESULTADO

3.1. Descripción de Resultados: Técnica de Entrevista

ENTREVISTAS

Objetivo General: Analizar como 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?

Guerrero (2017)

Conforme a la primera pregunta formulada en la entrevista menciona que **no existe un buen nivel de legislación nacional, en vista que nuestra legislación se está adaptando recién a lo que especifica el Convenio de Budapest**. A pesar de que este ha sido suscrito el 2001 y han aparecido nuevas tecnologías que permiten a la delincuencia lograr su meta.

Roque (2017)

Conforme a la primera pregunta formulada en la entrevista menciona que **no existe un buen nivel de legislación nacional, en vista que es tomada de legislaciones de otros países** y al momento de copiarla y aplicarla es de manera errónea induciendo en muchos casos a cometer errores en la aplicación de la justicia.

Alemàn (2017)

Conforme a la primera pregunta formulada en la entrevista menciona que **no existe un buen nivel de legislación nacional, en vista que falta madurar mucho sobre estos ilícitos. En lo que respecta a la legislación internacional, conoce que existe buena legislación.**

Osorio (2017)

Conforme a la primera pregunta formulada en la entrevista menciona que **no existe un buen nivel de legislación nacional, en vista que a la tipificación de este delito**

en nuestra legislación se considera un delito con poca normativa por ende nos queda solo consultar otras legislaciones.

Alvarado (2017)

Conforme a la primera pregunta formulada en la entrevista menciona que **no existe un buen nivel de legislación nacional, porque falta nutrir la normativa sobre esos temas, configurar debidamente estos delitos. Sobre legislación internacional considero que ya tiene tiempo la normativa y es la correcta.**

Ramirez (2017)

Conforme a la primera pregunta formulada en la entrevista menciona que **no existe un buen nivel de legislación nacional, porque nuestra legislación son meras copias de otras legislaciones.** La legislación también está evolucionando.

Barrionuevo (2017)

Conforme a la primera pregunta formulada en la entrevista menciona que **si existe un buen nivel de legislación nacional, por lo menos ya tenemos una legislación independiente el cual regula estos delitos.** Aún falta cuajar muchos asuntos sobre este aspecto, pero considero estamos en buen camino.

Pazzoni (2017)

Conforme a la primera pregunta formulada en la entrevista menciona que **no existe un buen nivel de legislación nacional, en vista que estos delitos cambian muy rápidamente.** En lo internacional creo que también les falta una actualización legislativa sobre esta materia.

Perca (2017)

Conforme a la primera pregunta formulada en la entrevista menciona que **no existe un buen nivel de legislación nacional, en vista que estos delitos cambian muy rápidamente.** Aún existen muchas críticas sobre la legislación de delitos informáticos. En lo particular no he tocado casos de estos aún, pero de mi

conocimiento sé que falta mucho para acoger todas las formas de cometer estos delitos. En lo internacional estamos bien respaldados esto permitirá sustentar los casos para llegar a una buena resolución.

Hernández (2017)

Conforme a la primera pregunta formulada en la entrevista menciona que **no existe un buen nivel de legislación nacional, en vista hay una unidad especializada en la DIRINCRI de Delitos Informáticos, pero no hay una legislación actualizada.** Teniendo en cuenta que no existe una veracidad en los morosos, tomando en cuenta que en la práctica no hay mucha utilización por parte de la sociedad, falta especialistas.

Vega (2017)

Conforme a la primera pregunta formulada en la entrevista menciona que **no existe un buen nivel de legislación nacional, en vista que la esta regula comercial y penalmente las conductas relacionadas con la informática, pero que aún no contemplan en si los delitos informáticos.** Teniendo en cuenta la legislación internacional se basa en los tratados internacionales. El Perú es parte en tal razón puede recurrir a aquellos tratados.

Estares (2017)

Conforme a la primera pregunta formulada en la entrevista menciona que **no existe un buen nivel de legislación nacional, por cuanto todavía se presentan las siguientes vulneraciones: a- La falta de jerarquía en la red, que permita establecer sistemas de control lo que dificulta la verificación de la información que circule por este medio; b- El creciente número de usuarios y la facilidad de acceso al medio tecnológico; c- El anonimato de los cibernautas que dificulta su persecución tras la comisión de un delito a través de este medio; d- La facilidad de acceso a la información para alterar datos, destruir sistemas informáticos.**

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

Guerrero (2017)

Conforme a la segunda pregunta formulada en la entrevista menciona que **los operadores de derecho no están suficientemente capacitados para manejar temas de delitos informáticos.** Visto que nuestros procedimientos legales se inician con la asignación de competencias para fiscalías que se encuentran en turno cuando **debería existir una fiscalía especializada en delitos informáticos**.

Roque (2017)

Conforme a la segunda pregunta formulada en la entrevista alega que **los operadores de derecho no están suficientemente capacitados para manejar temas de delitos informáticos** porque es un tema relativamente nuevo y muchos de los operadores jurídicos no están debidamente capacitados.

Alemàn (2017)

Conforme a la segunda pregunta formulada en la entrevista alega que **los operadores de derecho no están suficientemente capacitados para manejar temas de delitos informáticos,** porque incluso la DIVINDAT teniendo una unidad especializada la cual busca estar a la vanguardia y no se puede, peor aún los operadores de derecho.

Osorio (2017)

Conforme a la segunda pregunta formulada en la entrevista alega que **los operadores de derecho no están suficientemente capacitados para manejar temas de delitos informáticos,** a nivel de instituciones.

Alvarado (2017)

Conforme a la segunda pregunta formulada en la entrevista alega que **los operadores de derecho no están suficientemente capacitados para manejar temas de delitos informáticos,** y no solo en materia penal, porque el tema de informática ha llegado a la parte administrativa judicial, al área civil y procesal. Por ello a la necesidad de que todos tengan conocimiento del mismo.

Ramirez (2017)

Conforme a la segunda pregunta formulada en la entrevista alega que **los operadores de derecho no están suficientemente capacitados para manejar temas de delitos informáticos,** y que existe una deficiencia para tener conocimiento sobre estos temas.

Barrionuevo (2017)

Conforme a la segunda pregunta formulada en la entrevista alega que **los operadores de derecho no están suficientemente capacitados para manejar temas de delitos informáticos,** porque solo se tienen nociones básicas, lo que se lee en los periódicos, noticias, pero falta un conocimiento profundo.

Pazzoni (2017)

Conforme a la segunda pregunta formulada en la entrevista alega que **los operadores de derecho no están suficientemente capacitados para manejar temas de delitos informáticos,** porque faltan más cursos, especializaciones, que se maneje la parte académica autónomamente.

Perca (2017)

Conforme a la segunda pregunta formulada en la entrevista alega que **los operadores de derecho no están suficientemente capacitados para manejar temas de delitos informáticos,** porque a pesar de mis años de litigante me falta capacitación sobre estos delitos de manera profunda y minuciosa. Por ende sé que muchos colegas con diferentes cargos carecen de estos conocimientos.

Hernández (2017)

Conforme a la segunda pregunta formulada en la entrevista alega que **los operadores de derecho no están suficientemente capacitados para manejar temas de delitos informáticos,** porque en los Delitos Informáticos los operadores judiciales utilizan planchas y no proyectos elaborados.

Vega (2017)

Conforme a la segunda pregunta formulada en la entrevista alega que **los operadores de derecho no están suficientemente capacitados para manejar temas de delitos informáticos,** en vista que el operador jurídico tiene que conocer todos los aspectos informáticos, telecomunicaciones, entre otros. Ya que para investigar un delito informático debe contar con personal calificado y conocedor del sistema informático y tener peritos forenses.

Estares (2017)

Conforme a la segunda pregunta formulada en la entrevista alega que **los operadores de derecho no están suficientemente capacitados para manejar temas de delitos informáticos,** por la falta de conocimiento científico, artístico y técnico o practico para valorar hechos y circunstancias relevantes en el asunto o adquirir certeza. Esto debido que el delito informático es relativamente reciente y están apareciendo en forma masiva con el uso de la tecnología.

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

Guerrero (2017)

Conforme a la tercera pregunta formulada en la entrevista menciona que **el perito se capacita constantemente, pero no se cuenta con las herramientas legales y técnicas para culminar con un debido proceso, esto los limita en algún caso.** Por otro lado, el número de efectivos policiales que trabaja en la DIVINDAT es

insuficiente para la cantidad de dispositivos de almacenamiento y telefonía móvil objeto de investigación.

Roque (2017)

Conforme a la tercera pregunta formulada en la entrevista menciona que **desconoce a peritos que se hayan especializado en este tipo de delitos.**

Alemàn (2017)

Conforme a la tercera pregunta formulada en la entrevista alega que **existe personal suficientemente capacitado, pero no existe la cantidad de recurso humano para ver el tema de las investigaciones.**

Osorio (2017)

Conforme a la tercera pregunta formulada en la entrevista alega que **no existe personal suficientemente capacitado por falta de presupuesto y no existe la cantidad de recurso humano para ver el tema de las investigaciones.**

Alvarado (2017)

Conforme a la tercera pregunta formulada en la entrevista alega que **no existe personal suficientemente capacitado, como tampoco existe la cantidad de recurso humano para ver el tema de las investigaciones.** Y la capacitación es fundamental en este tipo de peritos.

Ramirez (2017)

Conforme a la tercera pregunta formulada en la entrevista alega que **no existe personal suficientemente capacitado, como tampoco existe la cantidad de recurso humano para ver el tema de las investigaciones.** Lamentablemente hay demora en la evaluación de las evidencias digitales y eso es reflejo de ausencia de personal.

Barrionuevo (2017)

Conforme a la tercera pregunta formulada en la entrevista alega que **si existe personal suficientemente capacitado, pero no existe la cantidad de recurso humano para ver el tema de las investigaciones.** En vista que los fiscales demoran en realizar su acusación formal porque siguen a la espera del análisis de evidencia que han solicitado.

Pazzoni (2017)

Conforme a la tercera pregunta formulada en la entrevista alega que **si existe personal suficientemente capacitado, pero no existe la cantidad de recurso humano para ver el tema de las investigaciones.** Pero no tienen herramientas si las tienen están desfasadas.

Perca (2017)

Conforme a la tercera pregunta formulada en la entrevista alega que **si existe personal suficientemente capacitado, pero en esta área la tecnología avanza tan rápido que es complejo mantenernos a la vanguardia.** En lo de la carga de las investigaciones siempre falta personal, equipos más minuciosos, eso es lo usual.

Vega (2017)

Conforme a la tercera pregunta formulada en la entrevista alega que, **si existe personal suficientemente capacitado, pero los operadores judiciales no lo están.** En nuestro país existen peritos de todas las especialidades. El perito informático si es preparado y conoce su campo será de gran aporte, pero tiene que trabajar con abogados, ciber policías. Además, el juez también tiene que conocer todo lo referente al sistema informático para un debido proceso y una sentencia justa.

Estares (2017)

Conforme a la tercera pregunta formulada en la entrevista alega que, **no existe personal suficientemente capacitado, respecto a la capacitación de los peritos que solo existen en las capitales de las regiones, están capacitados en forma**

restringida debido a que no se cuenta con el instrumental para poder desarrollar o investigar con precisión el delito informático.

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

Guerrero (2017)

Conforme a la cuarta pregunta formulada en la entrevista menciona que **las herramientas utilizadas en la Informática Forense son óptimas para la investigación, pero únicamente para dispositivos de almacenamiento y equipos de telefonía, los cuales deben ser actualizados permanentemente, generando un costo que no es asumido oportunamente por el Estado**

Roque (2017)

Conforme a la cuarta pregunta formulada en la entrevista menciona que **desconoce sobre este tipo de herramientas.**

Alemàn (2017)

Conforme a la cuarta pregunta formulada en la entrevista alega que **se adolece de herramientas forenses, existen pocas.** Muchas no están licenciadas y ya no son utilizadas. En ese sentido hay deficiencia, deberíamos tener más herramientas.

Osorio (2017)

Conforme a la cuarta pregunta formulada en la entrevista alega que **no tienen herramientas forenses.** Que en la provincia de Chanchamayo no existe material logístico para tales investigaciones.

Alvarado (2017)

Conforme a la cuarta pregunta formulada en la entrevista alega que **desconoce sobre este tipo de herramientas.** Pero de ser optimas existirán más procesos sobre estos delitos.

Ramirez (2017)

Conforme a la cuarta pregunta formulada en la entrevista alega que **las herramientas utilizadas en la Informática Forense no son óptimas para la investigación.** La problemática radica en la existencia de mucha burocracia y papeleo para conseguir herramientas óptimas.

Barrionuevo (2017)

Conforme a la cuarta pregunta formulada en la entrevista alega que **desconoce sobre este tipo de herramientas.** Pero que no sería extraño que existan deficiencias.

Pazzoni (2017)

Conforme a la cuarta pregunta formulada en la entrevista alega que **las herramientas utilizadas en la Informática Forense no son óptimas para la investigación.** Porque eso se refleja en los índices de procesos llevados que manejan este tipo de evidencia.

Perca (2017)

Conforme a la cuarta pregunta formulada en la entrevista alega que **desconoce sobre este tipo de herramientas.** Pero se espera que sean las más óptimas. Aunque en la realidad se usa lo que se tiene y se hace lo que se puede sobre las investigaciones.

Hernández (2017)

Conforme a la cuarta pregunta formulada en la entrevista alega que **las herramientas utilizadas en la Informática Forense no son óptimas para la investigación.** Dependiendo que se va investigar, como por ejemplo la clonación de tarjetas, ya que

existe tecnología de punta para detectar, en vista que a nivel nacional e internacional deficiencia de información.

Vega (2017)

Conforme a la cuarta pregunta formulada en la entrevista alega que **las herramientas utilizadas en la Informática Forense no son óptimas para la investigación.** Estas sirven para lograr una investigación en el disco duro de las computadoras. Todo va evolucionando gracias al avance de la tecnología como, por ejemplo: EL SOFTWARE DE ANALISIS FORENSE, se usa cuando falla la computadora, recupera información perdida o borrada por completo y es la mejor en programas forenses. PLAING SLIGTH con esta podemos conocer la computadora, sistemas, discos duros, etc.

Estares (2017)

Conforme a la cuarta pregunta formulada en la entrevista alega que **las herramientas utilizadas en la Informática Forense no son óptimas para la investigación.** La Informática forense implica una serie de técnicas y métodos de investigación que permiten reconstruir lo más fielmente posible, la secuencia de eventos que tuvieran lugar, con la ayuda de equipos informáticos de última generación digital, que se cuenta parcialmente.

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

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?

Guerrero (2017)

Conforme a la quinta pregunta formulada en la entrevista menciona que **si abarcamos todos los delitos informáticos orientados a la vulneración de la información en cuanto a lo que podemos definir como delito informático puro,**

contamos con una legislación. Sin embargo para aquellos delitos en donde los medios informáticos son herramientas para cometer delitos su constante evolución impide su tipificación oportuna.

Roque (2017)

Conforme a la quinta pregunta formulada en la entrevista menciona que **no abarcamos todo los delitos informáticos que vulneran la información, en vista que hay muchos delitos que se cometen a través de redes sociales den donde por el desconocimiento de los usuarios no se llega a denunciar.**

Alemàn (2017)

Conforme a la quinta pregunta formulada en la entrevista alega que **no abarcamos todos los delitos informáticos que vulneran la información.** Existen muchas modalidades en la que los hechos no se adecuan a los únicos 3 artículos que nuestra legislación considera.

Osorio (2017)

Conforme a la quinta pregunta formulada en la entrevista alega que **no abarcamos todos los delitos informáticos que vulneran la información.** En la provincia de Chanchamayo se han reportado pocos casos de delitos informáticos.

Alvarado (2017)

Conforme a la quinta pregunta formulada en la entrevista alega que **no abarcamos todos los delitos informáticos que vulneran la información.** Porque los hechos no siempre se adecuan a los artículos establecidos en la ley de Delitos Informáticos.

Ramirez (2017)

Conforme a la quinta pregunta formulada en la entrevista alega que **si abarcamos todos los delitos informáticos que vulneran la información.** Porque ya procura lo más importante el combatir el acceso ilícito.

Barrionuevo (2017)

Conforme a la quinta pregunta formulada en la entrevista alega que **si abarcamos todos los delitos informáticos que vulneran la información.** Pero debemos pulir mejor las normas y la parte de colaboración ministerio público y policía nacional del Perú en la investigación.

Pazzoni (2017)

Conforme a la quinta pregunta formulada en la entrevista alega que **si abarcamos todos los delitos informáticos que vulneran la información.** Porque ya penamos el acceso ilícito y creo que eso engloba cualquier tipo de modalidad y puede ser adaptada.

Perca (2017)

Conforme a la quinta pregunta formulada en la entrevista alega que **si abarcamos todos los delitos informáticos que vulneran la información.** Pero falta pulir la legislación que se acerque más a nuestra realidad.

Hernández (2017)

Conforme a la quinta pregunta formulada en la entrevista alega que **no abarcamos *todos los delitos informáticos que vulneran la información.*** *Porque falta tipificar* en nuestra normativa y nuestra legislación del Código Penal.

Vega (2017)

Conforme a la quinta pregunta formulada en la entrevista alega que **no abarcamos todos los delitos informáticos que vulneran la información.** Porque cada país tiene su propia problemática y legislación. Las más conocidas son: Estafas, extorsión, robo de servicios, distribución de virus,

Estares (2017)

Conforme a la quinta pregunta formulada en la entrevista alega que **no abarcamos todos los delitos informáticos que vulneran la información.** Porque con la ley

30096 y su modificatoria, se está pretendiendo abarcar los delitos informáticos, pero se incide en forma genérica y analógica, por cuanto con el avance de la tecnología van dándose nuevas formas delictivas, lo que conlleva que tenemos que avanzar de igual con la tecnología.

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

Guerrero (2017)

Conforme a la sexta pregunta formulada en la entrevista menciona que **la problemática está en que día a día aparecen nuevas formas delictivas que involucran el uso de las TICS, lo que impide que sea considerado, aquellos comportamientos que vulneran bienes jurídicos que están protegidos en el Código Penal.**

Roque (2017)

Conforme a la sexta pregunta formulada en la entrevista menciona que **pese a que están regulados los delitos informáticos que utilizan las Tics como medio, en muchos casos son violentados por personas que conocen michos de informática y precisamente esa es la razón de la impunidad.**

Alemàn (2017)

Conforme a la sexta pregunta formulada en la entrevista alega que **no están bien regulado los delitos informáticos que utilizan las Tics como medio, considera que esto no es ni intencional ni por omisión, sino que hay una evolución en las modalidades que hacen que la legislación quede relegada.**

Osorio (2017)

Conforme a la sexta pregunta formulada en la entrevista alega que **no están bien regulado los delitos informáticos que utilizan las Tics como medio, porque no existe un mecanismo adecuado para el uso de investigaciones de estos delitos.**

Alvarado (2017)

Conforme a la sexta pregunta formulada en la entrevista alega que **no están bien regulado los delitos informáticos que utilizan las Tics como medio, porque estos cambian constantemente.** Todo esto provoca la informática visto que día con día llega a mas áreas y vincula la vida diaria de las personas por ende hay mayor cantidad de vulneración.

Ramirez (2017)

Conforme a la sexta pregunta formulada en la entrevista alega que **no están bien regulado los delitos informáticos que utilizan las Tics como medio, porque evoluciona muy rápido y cada día cambian de modalidades.**

Barrionuevo (2017)

Conforme a la sexta pregunta formulada en la entrevista alega que **no están bien regulado los delitos informáticos que utilizan las Tics como medio, porque falta establecer más modalidades, donde la tecnología avanza muy rápido, los delitos también.**

Pazzoni (2017)

Conforme a la sexta pregunta formulada en la entrevista alega que **no están bien regulado los delitos informáticos que utilizan las Tics como medio,** porque existe mayor vulnerabilidad en cuanto es usada la tecnología como medio y esto cambia constantemente.

Perca (2017)

Conforme a la sexta pregunta formulada en la entrevista alega que **no están bien regulado los delitos informáticos que utilizan las Tics como medio,** porque existe

mayor complejidad ya que es un delito pluriofensivo y perjudica mayor cantidad de objetos jurídicamente protegidos.

Hernández (2017)

Conforme a la sexta pregunta formulada en la entrevista alega que **no están bien regulado los delitos informáticos que utilizan las Tics como medio,** porque avanzan muy rápido, van abarcar más delitos convencionales

Vega (2017)

Conforme a la sexta pregunta formulada en la entrevista alega que **no están bien regulado los delitos informáticos que utilizan las Tics como medio,** porque es por el mal uso de las tecnologías de la información y el mal uso de las Tic´s que aplican sus conocimientos para fines destructivos o delictivos. El delincuente, el criminal se esconde, borra las pruebas. Los delitos convencionales son entre delincuentes y víctimas se lleva a cabo en todo tiempo y lugar.

Estares (2017)

Conforme a la sexta pregunta formulada en la entrevista alega que **no están bien regulado los delitos informáticos que utilizan las Tics como medio,** porque si bien las nuevas herramientas que ofrecen las Tic´s al servicio del hombre están relacionados con la trasmisión, procesamiento y almacenamiento digitalizada de información, así como un conjunto de procesos y productos que simplifican la comunicación y hacen más viables la infracción entre las personas. El desarrollo de la tecnología también ha traído consigo nuevas formas delictivas que tienen por medio y/o finalidad los sistemas informáticos e internet.

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

Guerrero (2017)

Conforme a la séptima pregunta formulada en la entrevista menciona que **sobre la tipicidad objetiva de los delitos informáticos a nivel policial se trata de adecuar el comportamiento delictivo al verbo rector y no siempre resulta entendible al fiscal debido a los constantes avances tecnológicos.**

Roque (2017)

Conforme a la séptima pregunta formulada en la entrevista alega que **parece que es muy escueto, muy pequeño para poder determinar este tipo de delito, se debería ampliar a más verbos rectores según la realidad y el contexto en el cual se presente.**

Alemàn (2017)

Conforme a la séptima pregunta formulada en la entrevista alega que **la tipicidad objetiva no esté bien estructurada, porque hay múltiples modalidades nuevas, que no se pueden adecuar a la legislación y cuesta hacerlo por la comprensión de las mismas.**

Osorio (2017)

Conforme a la séptima pregunta formulada en la entrevista alega que **la tipicidad objetiva si esté bien estructurada, pero que no existe un mecanismo de aplicación.**

Alvarado (2017)

Conforme a la séptima pregunta formulada en la entrevista alega que **la tipicidad objetiva está bien estructurada, solo que falta adecuar mejor los verbos rectores.**

Ramirez (2017)

Conforme a la séptima pregunta formulada en la entrevista alega que **la tipicidad objetiva no está bien estructurada en los delitos informáticos, porque no respeta la realidad nacional al ser copia de legislaciones internacionales.**

Barrionuevo (2017)

Conforme a la séptima pregunta formulada en la entrevista alega que **la tipicidad objetiva está bien estructurada en los delitos informáticos, pero falta distinguir la tentativa del delito consumado. Esto va traer complejidad.**

Pazzoni (2017)

Conforme a la séptima pregunta formulada en la entrevista alega que **la tipicidad objetiva no está bien estructurada en los delitos informáticos, porque falta adecuar el hecho delictivo peruano a la norma. La norma subsecuente con la realidad.**

Perca (2017)

Conforme a la séptima pregunta formulada en la entrevista alega que **la tipicidad objetiva está bien estructurada en los delitos informáticos, porque esta no varía es la misma para los diferentes delitos.**

Hernández (2017)

Conforme a la séptima pregunta formulada en la entrevista alega que **la tipicidad objetiva está bien estructurada en los delitos informáticos.**

Vega (2017)

Conforme a la séptima pregunta formulada en la entrevista alega que **la tipicidad objetiva está bien estructurada en los delitos informáticos.** La tipicidad objetiva ve el delito de intrusionismo informático. El Estado protege el patrimonio contenido en la base de datos (Bien Jurídico Protegido). Agravante del delito con el fin de obtener un beneficio económico. El sujeto pasivo (persona natural y/o jurídica tutelares de la base de datos).

Estares (2017)

Conforme a la séptima pregunta formulada en la entrevista alega que **la tipicidad objetiva no está bien estructurada en los delitos informáticos.** Debido al avance tecnológico ya que por medio de la tipicidad objetiva se busca proteger el bien jurídico. Por tanto, en este tipo de delitos no se puede establecer a la información como el único bien jurídico afectado, puede ser el principal y el más importante, sino a un conjunto de bienes que son afectados debido a la característica de la conducta típica en esta modalidad delictiva que consolida intereses colectivos.

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

Guerrero (2017)

Conforme a la octava pregunta formulada en la entrevista menciona que **definitivamente existe una evolución sobre lo conocido tradicionalmente como tipicidad subjetiva, porque los delincuentes informáticos tratan de buscar nuevos comportamientos.**

Roque (2017)

Conforme a la octava pregunta formulada en la entrevista alega que **ha existido una evolución sobre lo conocido tradicionalmente como tipicidad subjetiva, pues antes no constituía delito informático, pero dado a que la criminalidad organizada hace uso de internet se han ampliados los delitos con sus modalidades.**

Alemàn (2017)

Conforme a la octava pregunta formulada en la entrevista alega que **la tipicidad subjetiva ha sufrido una evolución, pero existe falta de interés por todos los operadores de justicia en conocer sobre ese aspecto.**

Osorio (2017)

Conforme a la octava pregunta formulada en la entrevista alega que **la tipicidad subjetiva ha sufrido una evolución, pero no existe muchos delitos informáticos en la Ciudad de Chanchamayo.**

Alvarado (2017)

Conforme a la octava pregunta formulada en la entrevista alega que **la tipicidad subjetiva ha sufrido una evolución. Tenemos un nuevo enfoque de lo denominado tentativa y delito consumado.**

Ramirez (2017)

Conforme a la octava pregunta formulada en la entrevista alega que **la tipicidad subjetiva ha sufrido una evolución. En cuanto a lo que en delitos convencionales entendemos como tentativa, en los delitos informáticos la tentativa ya es un delito consumado.**

Barrionuevo (2017)

Conforme a la octava pregunta formulada en la entrevista alega que **la tipicidad subjetiva ha sufrido una evolución. En cuanto son delitos especiales por ende el sujeto activo es alguien especializado en estos temas. No es el tipo común y corriente.**

Pazzoni (2017)

Conforme a la octava pregunta formulada en la entrevista alega que **la tipicidad subjetiva ha sufrido una evolución. En cuanto también ha evolucionado en lo jurisprudencial y doctrinal.**

Perca (2017)

Conforme a la octava pregunta formulada en la entrevista alega que **la tipicidad subjetiva ha sufrido una evolución**. Ahora existe un debate fuerte sobre el tema de dolo o culpa y lo que se considera como tentativa y delito consumado

Hernández (2017)

Conforme a la octava pregunta formulada en la entrevista alega que **la tipicidad subjetiva ha sufrido una evolución**. En vista que ha evolucionado en las proposiciones sexuales a menor de edad ya están tipificados, no lo estaban en nuestra normativa.

Vega (2017)

Conforme a la octava pregunta formulada en la entrevista alega que **la tipicidad subjetiva ha sufrido una evolución**. En vista que se requiere que el comportamiento sea realizado con dolo es decir conciencia y voluntad de cometer el delito. La tipicidad es expresamente para estos delitos reunidos en una Ley Especial.

Estares (2017)

Conforme a la octava pregunta formulada en la entrevista alega que **la tipicidad subjetiva ha sufrido una evolución**. En vista que ha el sujeto activo en esta modalidad delictiva viene evolucionando por que se requiere ciertas habilidades y conocimientos en el manejo del de sistemas informáticos que tienen como características: - Poseer importantes conocimientos informáticos. – Ocupar lugares estratégicos en el centro laboral, en los que se maneje información de carácter sensible. – No son delincuentes comunes y corrientes, sino que por el contrario son personas especializadas en la materia informática.

Objetivo Especifico 2: Constatar como la determinación del Marco Legal de la Evidencia Digital repercute en la Tipicidad de los Delitos Informáticos en el Proceso Penal Peruano.

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

Guerrero (2017)

Conforme a la novena pregunta formulada en la entrevista alega que **si existe el conocimiento adecuado en sobre el manejo de la evidencia digital en cuanto metodología y reconocimiento en vista que aun manejamos manuales de procedimientos internacionales. Aunque en la actualidad ya ha suscrito un documento sobre evidencia digital.**

Roque (2017)

Conforme a la novena pregunta formulada en la entrevista alega que **no existe el conocimiento adecuado en sobre el manejo de la evidencia digital en cuanto no se cumple con las directivas dadas por el Ministerio Publico, como es la cadena de custodia en este tipo de delitos.**

Alemàn (2017)

Conforme a la novena pregunta formulada en la entrevista menciona que **si existe el conocimiento adecuado en sobre el manejo de la evidencia digital en la DIVINDAT, en cierta forma suficiente. La carencia de conocimiento está en otras unidades a nivel nacional.**

Osorio (2017)

Conforme a la novena pregunta formulada en la entrevista menciona que **no existe el conocimiento adecuado en sobre el manejo de la evidencia, porque no existen los medios técnicos adecuados.**

Alvarado (2017)

Conforme a la novena pregunta formulada en la entrevista menciona que **si existe el conocimiento adecuado en sobre el manejo de la evidencia digital, pero aún no se ha legislado al respecto.**

Ramírez (2017)

Conforme a la novena pregunta formulada en la entrevista menciona que **no existe el conocimiento adecuado en sobre el manejo de la evidencia digital, ya que en**

varias áreas hay deficiencias. Los peritos deben estar correctamente y completamente capacitados.

Barrionuevo (2017)

Conforme a la novena pregunta formulada en la entrevista menciona que **no existe el conocimiento adecuado en sobre el manejo de la evidencia digital, ya que en varias áreas hay deficiencias. Pero se está empezando a mejorar los procedimientos por los menos en Lima, en provincia desconozco.**

Pazzoni (2017)

Conforme a la novena pregunta formulada en la entrevista menciona que **no existe el conocimiento adecuado en sobre el manejo de la evidencia digital, visto que falta un mayor reglamento para tener procedimientos adecuados.**

Perca (2017)

Conforme a la novena pregunta formulada en la entrevista menciona que **no existe el conocimiento adecuado en sobre el manejo de la evidencia digital.** Porque nosotros como abogados tradicionales no conocemos su manejo para exponerlo en un proceso. Esto será una ventaja para abogados que son nativos informáticos.

Hernández (2017)

Conforme a la novena pregunta formulada en la entrevista menciona que **no existe el conocimiento adecuado en sobre el manejo de la evidencia digital.** Porque considero que los operadores de justicia capacitan a los profesionales para poder dominar a estas pruebas digitales.

Vega (2017)

Conforme a la novena pregunta formulada en la entrevista menciona que **no existe el conocimiento adecuado en sobre el manejo de la evidencia digital.** Pero para el estudio se tiene diferencia elemento de un sistema informático (evidencia electrónica) y la información contenida en este (es la evidencia digital). La de

reconocimiento es el procesador de imágenes ordena y encamina el tipo de investigación.

Estares (2017)

Conforme a la novena pregunta formulada en la entrevista menciona que **si existe el conocimiento adecuado en sobre el manejo de la evidencia digital.** Pero en medida que avance la tecnología se requiere un conocimiento adecuado para la obtención de información (elementos de convicción) se constituye en una de las facetas útiles dentro del éxito, de una investigación criminal, aspecto que demanda de los investigadores encargados de la recolección, preservación, análisis y presentación de las evidencias digitales una eficaz labor que garantice la autenticidad o fin de ser utilizados posteriormente ante el proceso penal.

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?

Guerrero (2017)

Conforme a la décima pregunta formulada en la entrevista alega que **si es relevante la calidad de análisis del informe sobre evidencia digital, pero que el conocimiento deber ser para todos los operadores de justicia para su comprensión.**

Roque (2017)

Conforme a la décima pregunta formulada en la entrevista alega que **si es relevante la calidad de análisis del informe sobre evidencia digital porque de ello va depender que se considere como medio probatorio.**

Alemàn (2017)

Conforme a la décima pregunta formulada en la entrevista menciona que **si es relevante la calidad de análisis del informe sobre evidencia digital porque de ello va depender la decisión de admitir o no una prueba.**

Osorio (2017)

Conforme a la décima pregunta formulada en la entrevista menciona que **si es relevante la calidad de análisis del informe sobre evidencia digital, pero que nos falta más capacitación y logística.**

Alvarado (2017)

Conforme a la décima pregunta formulada en la entrevista menciona que **si es relevante la calidad de análisis del informe sobre evidencia digital, sin un buen análisis no podremos hablar de evidencia fehaciente y por ende no hay proceso.**

Ramirez (2017)

Conforme a la décima pregunta formulada en la entrevista menciona que **si es relevante la calidad de análisis del informe sobre evidencia digital, porque sin esto no tendríamos una prueba fehaciente para admitir en el proceso.**

Barrionuevo (2017)

Conforme a la décima pregunta formulada en la entrevista menciona que **si es relevante la calidad de análisis del informe sobre evidencia digital, porque esto determina el trascurso del proceso, no es solo recolectar la evidencia, sino su correcto análisis.**

Pazzoni (2017)

Conforme a la décima pregunta formulada en la entrevista menciona que, **si es relevante la calidad de análisis del informe sobre evidencia digital, porque sin un buen informe pericial como puedo aseverar la procedencia de la evidencia digital.**

Perca (2017)

Conforme a la décima pregunta formulada en la entrevista menciona que **si es relevante la calidad de análisis del informe sobre evidencia digital,** porque todo análisis pericial debe ser hecho cautelosamente siendo lo más claro y conciso posible. De no ser así no existiría proceso alguno valido.

Hernández (2017)

Conforme a la décima pregunta formulada en la entrevista menciona que, **si es relevante la calidad de análisis del informe sobre evidencia digital,** es de suma importancia ya que deberían existir peritos para los delitos de difamación.

Vega (2017)

Conforme a la décima pregunta formulada en la entrevista menciona que, **si es relevante la calidad de análisis del informe sobre evidencia digital,** ya que de ellos darán la prueba informática de aplicación en el aspecto penal, para que el juez decida la culpabilidad o la inocencia del Imputado o Sujeto Activo. Eje: Delitos de Pornografía infantil en internet, Propiedad Privada, Protección de Datos Personales y otros.

Estares (2017)

Conforme a la décima pregunta formulada en la entrevista menciona que, **si es relevante la calidad de análisis del informe sobre evidencia digital,** es importante en el proceso penal, porque de ello depende lo que se trata de identificar al delincuente informático.

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

Guerrero (2017)

Conforme a la décimo primera pregunta formulada en la entrevista alega que **no es suficiente el marco legal existe sobre la Cadena de Custodia porque está más dirigida al recojo de evidencias físicas y no digitales. Lo que ocasiona trastorno de carácter procedimental y administrativo.**

Roque (2017)

Conforme a la décimo primera pregunta formulada en la entrevista alega que **si es suficiente el marco legal existe sobre la Cadena de Custodia, pero en el uso a veces es distorsionada o manipulada la evidencia.**

Alemàn (2017)

Conforme a la décimo primera pregunta formulada en la entrevista alega que **no es suficiente el marco legal existe sobre la Cadena de Custodia porque en temas de delitos informáticos debe haber mayores precisiones y no es lo mismo tratar una evidencia digital que una evidencia común.**

Osorio (2017)

Conforme a la décimo primera pregunta formulada en la entrevista alega que **si es suficiente el marco legal existe sobre la Cadena de Custodia, pero que nos falta más capacitación al respecto.**

Alvarado (2017)

Conforme a la décimo primera pregunta formulada en la entrevista alega que **si es suficiente el marco legal existe sobre la Cadena de Custodia, pero sobre el manejo de la evidencia en general, sería importante agregar un capítulo especial sobre evidencia digital en el Reglamento.**

Ramirez (2017)

Conforme a la décimo primera pregunta formulada en la entrevista alega que **no es suficiente el marco legal existe sobre la Cadena de Custodia, porque en otras**

legislaciones como la Argentina esto no es un mero reglamento, sino una ley detallada. De esto carece la norma peruana.

Barrrionuevo (2017)

Conforme a la décimo primera pregunta formulada en la entrevista alega que **no es suficiente el marco legal existe sobre la Cadena de Custodia, porque debería estar normado como ley. Para tener mejor respaldo en cuanto al manejo de las evidencias y estas sean fehacientes.**

Pazzoni (2017)

Conforme a la décimo primera pregunta formulada en la entrevista alega que **si es suficiente el marco legal existe sobre la Cadena de Custodia, pero se debería ampliar un capitulo únicamente sobre evidencia digital.**

Perca (2017)

Conforme a la décimo primera pregunta formulada en la entrevista alega que **no es suficiente el marco legal existe sobre la Cadena de Custodia, porque solo es un mero reglamento. Debería estar en el código penal.**

Hernández (2017)

Conforme a la décimo primera pregunta formulada en la entrevista alega que **es suficiente el marco legal existe sobre la Cadena de Custodia, para sustentar los medios probatorios.**

Vega (2017)

Conforme a la décimo primera pregunta formulada en la entrevista alega que **es suficiente el marco legal existe sobre la Cadena de Custodia,** ya que esta es una evidencia única, cuando se compara con una documental. Es frágil, visto que una copia de un documento almacenado en un archivo es idéntica al original, no deja rastro que dejo la Primera copia.

Estares (2017)

Conforme a la décimo primera pregunta formulada en la entrevista alega que **no es suficiente el marco legal existe sobre la Cadena de Custodia,** para sustentar los medios probatorios. Porque en ello se establece los procedimientos y recalca si la tecnología avanza el marco legal también debe estar a la par.

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

Guerrero (2017)

Conforme a la décimo segunda pregunta formulada en la entrevista alega que **no hay una instrumentalización adecuada sobre la evidencia digital. Por ende considera que hace una capacitación a todos los operadores de justicia a fin de que se instrumentalicen los procesos de recojo de evidencia digital y su posterior análisis forense de manera correcta.**

Roque (2017)

Conforme a la décimo segunda pregunta formulada en la entrevista alega que **no se puede mencionar respecto al tema, porque desconoce en qué consiste o que se utiliza.**

Alemàn (2017)

Conforme a la décimo segunda pregunta formulada en la entrevista alega que **no hay una instrumentalización adecuada sobre la evidencia digital porque no hemos desarrollado los protocolos adecuados, ni estamos utilizando los medios suficientes para ello. Usamos lo que tenemos y esta al largo plazo podría acarrear problemas.**

Osorio (2017)

Conforme a la décimo segunda pregunta formulada en la entrevista alega que **el tema de la instrumentalización sobre evidencia digital no se da en la Ciudad de Chanchamayo.**

Alvarado (2017)

Conforme a la décimo segunda pregunta formulada en la entrevista alega que **no se puede mencionar respecto al tema, porque desconoce en qué consiste o que se utiliza.**

Ramirez (2017)

Conforme a la décimo segunda pregunta formulada en la entrevista alega que **no se podría mencionar al respecto detalladamente. Pero una buena instrumentalización es la necesaria para que cualquier evidencia sea considerada dentro del proceso.**

Barrionuevo (2017)

Conforme a la décimo segunda pregunta formulada en la entrevista alega que **desconozco sobre la instrumentalización usada Pero debe ser la adecuada sino invalidara la evidencia dentro del proceso.**

Pazzoni (2017)

Conforme a la décimo segunda pregunta formulada en la entrevista alega que **desconozco sobre la instrumentalización usada**

Perca (2017)

Conforme a la décimo segunda pregunta formulada en la entrevista alega que **desconozco sobre la instrumentalización usada. Pero es relevante en cuanto al manejo de la evidencia digital.**

Hernández (2017)

Conforme a la décimo segunda pregunta formulada en la entrevista alega que **desconozco sobre la instrumentalización usada. Por ejemplo, ya que un CD es una prueba instrumental para la admisión en el proceso penal peruano.**

Vega (2017)

Conforme a la décimo segunda pregunta formulada en la entrevista **alega no hay una instrumentalización adecuada sobre la evidencia digital, para ser utilizada como evidencia digital se requiere de conocimiento profundo en la materia, para saber cómo fue creado, se puede falsificar. Que información se puede perder. Que puede estar mal. Para ello el forense informático hará su informe con un buen análisis, la misma que será revisada con justicia.**

Estares (2017)

Conforme a la décimo segunda pregunta formulada en la entrevista alega que **no hay una instrumentalización adecuada sobre la evidencia digital, porque nos asegura a quienes deben de juzgar, sobre la base de los elementos probatorios, los cuales no hayan sufrido alteraciones o contaminación alguna desde su recolección, examen o custodia.**

3.2. Descripción de Resultados: Técnica de Análisis Documental

Descripción de la Fuente 1:

Luces y sombras en la lucha contra la delincuencia informática en el Perú. Esta publicación fue terminada en junio del 2014 bajo Licencia de Creative Commons.
Tipo de Documento: Articuló
Título del Documento: Luces y sombras en la lucha contra la delincuencia informática en el Perú.
Autor del Documento: Ricardo Elias Puelles
Fecha del Documento: Junio 2014
Procedencia del Documento: Perú

Consideración General:

El abogado Ricardo Elias Puelles realiza un artículo sobre la lucha contra la delincuencia informática en nuestro país. Como se iba desarrollando, datos estadístico de la DIVINDAT desde el año 2002 al 2012, en las diferentes regiones del país. Por otro lado nos describe detalladamente el desarrollo normativo que ha tenido la "Ley de Delitos Informáticos", desde que fue Proyecto de Ley y promulgada el 2013, como su comparación con la modificatoria que promulgaron en el 2014 y el Convenio de Budapest. Por ello ha sido un artículo fundamental para la investigación.

Conclusiones del Análisis Documental

En conclusión el estudio hecho por este investigador jurídico, en analizar la repuesta progresiva de los legisladores frente a este fenómeno de los delitos informáticos, como su evolución durante 10 años, con datos estadísticos de la Divindat podemos apreciar que en un incremento en el perjuicio económico que representa los delitos informáticos, siendo Lima la ciudad con mayor tasa de incidencias reportadas permitió observar que es un tema que se tiene que trabajar cuidadosamente, que en Perú aún no hay datos oficiales sobre pérdida económica. Que ha tenido una evolución en la norma que al comienzo era considerado delitos de peligro y no de resultado. Cuando su connotación real es que son delitos de mera actividad. Este experto analizo científicamente la evolución normativa, la evolución en la tipificación, la incidencia e impacto en el país, mostrando la necesidad de utilizar nuevas estrategias para combatir estos delitos. Sustentando en todos sus puntos mi Objetivo General y Objetivos específicos de la presente investigación.

Descripción de la Fuente 2:

Delitos Informáticos – Cybercrimes. Esta publicación fue terminada en diciembre del 2014 en la Revista IUS ET VERITAS de la Pontificia Universidad Católica del Perú.
Tipo de Documento: Articuló
Título del Documento: Delitos Informáticos – Cybercrimes
Autor del Documento: Felipe Villavicencio Terrenos

Fecha del Documento: Diciembre 2014
Procedencia del Documento: Perú

Consideración General:
El abogado Felipe Villavicencios Terrenos a través de su investigación determinó que la finalidad de la Ley de Delitos informáticos es prevenir y sancionar las conductas ilícitas que afecten los sistemas y datas informáticos concluyo que la Ley de Delitos Informáticos es prevenir y sancionar las conductas ilegales en contra de los mismos sistemas e información, como también el secreto de las comunicaciones, el patrimonio, la fe pública, así como la libertad sexual, siendo este un delito pluriofensivo mediante la utilización de las TIC

Conclusión del Análisis Documental
El estudio de todos los artículos de la Ley de Delitos Informáticos y el análisis de su tipicidad nos permitió dilucidar un nuevo fenómeno y el choque frente a lo conocido en la estructura de los delitos convencionales. A pareciendo lo que los juristas denominan delito de resultado cortado, también estamos frente a delitos de mera actividad, los que ha generado una discusión fuerte entre los operadores del derecho, en busca de la comprensión del mismo para poder ser correctamente juzgado sin vulnerar el Debido proceso. Permitiendo observar una tendencia interna trascendente porque representa un elemento subjetivo distinto al dolo, poniendo hincapié especial en la intención del agente, siendo considerada como un delito de resultado cortado. Demostrando la evolución en la tipicidad de estos delitos.

Descripción de la Fuente 3:
Anuario Estadístico policial del 2016. Esta publicación fue terminada en febrero del 2017 por la Dirección de Tecnología de la Información y Comunicaciones en la División de Estadística de la PNP.
Tipo de Documento: Anuario Estadístico
Título del Documento: Anuario Estadístico policial del 2016
Autor del Documento: División de Estadística de la PNP

Fecha del Documento: Febrero 2017

Procedencia del Documento: Perú

Consideración General:

La División de Estadística de la Dirección Tecnología de la Información y Comunicaciones, ente rector del Sistema Estadístico de la Policía Nacional del Perú, ha elaborado el Anuario Estadístico PNP 2016, el cual me complace en presentar, documento que es fruto de un trabajo constante y compartido entre los integrantes de los órganos componentes del Sistema Estadístico PNP. Tiene 26 Capítulos, donde uno es La Dirección de Investigación Criminal de la Policía Nacional de Perú (DIRINCRI PNP), durante el año 2016 ha registrado 22,881 denuncias por diferentes delitos; de los cuales 4,544 fueron resueltos equivalentes al 1.63%. Donde se encuentra la DIVINDAT – División de Investigación de Alta Tecnología.

Conclusión del Análisis Documental

En los datos estadísticos arrojados por la División de Estadística de la PNP, en un primer **Cuadro 3.2** sobre **Denuncias recibidas por Comisión de Delitos Registrados por la Dirincri PNP, según tipo de Delitos en el año 2016**, se aprecia que tuvimos **880 denuncias** recibidas sobre **Delitos Informáticos**, divididos en 4 trimestres. El primer trimestre (Enero a Marzo) con 196 denuncias. El segundo trimestre (Abril a Junio) con 193 denuncias. El tercer trimestre (Julio a Setiembre) con 206 denuncias y el ultimo y cuarto trimestre (Noviembre a Diciembre) con 285 denuncias.

En un segundo **Cuadro 3.4 sobre Detenidos según tipo de Delitos y Modalidades en la DIVINDAT – DIRINCRI PNP. Año 2016**, se aprecia que solo tuvimos **18 detenidos** sobre **Delitos Informáticos**, divididos en 4 cuatro trimestres. El primer trimestre (Enero a Marzo) con 5 detenidos. El segundo trimestre (Abril a Junio) con 1 detenido. El tercer trimestre (Julio a Setiembre) con 6 detenidos y el ultimo y cuarto trimestre (Noviembre a Diciembre) con 6 detenidos.

Nos que nos refleja una diferencia abismal entre las denuncias y los detenidos por este tipo de Delitos. Aquí resaltan una vez más las falencias de herramientas especializadas, instrumentalización, personal suficiente y capacitado, operadores jurídicos capacitados, entre otros. Lo cual requiere una especial atención porque este es el centro de la problemática de la investigación en curso.

3.3. Descripción de Resultados: Técnica de Análisis Jurisprudencial

Exp. N°3603-2015-85-1501-RP-PE-02

Delito: Delito Informático

Objeto Jurídicamente Protegido: Contra la Indemnidad y Libertad Sexual

Normativa: Art. 5 de la Ley de Delitos Informáticos. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.

Problemática Jurídica:

La victima de 13 años fue citada por medio del celular y Facebook con fotos obscenas con la intención de proceder a consumar el acto sexual, porque se descubrió en las conversaciones proposiones determinantes para comprobar su intención. La madre de la menor advierte de esto a la Fiscalía y lo cual se procede a detener al Sujeto activo.

Decisión:

Se resolvió con la Terminación anticipada de parte del demandado establecido en el Art. 468 del CPP, y se le dio una pena de 4 años y 6 meses.

Comentario:

En el mundo doctrinario se ha generado un debate referente al análisis de esta norma sobre el que a través de las tecnologías de la información contacta con un menor de 14 años para solicitar u obtener del material pornográfico o para consumar un acto sexual. También se considera a las que tienen entre 14 y 18 y medie el engaño. En este delito el verbo rector es el contactar, que sería establecer contacto o comunicación con alguien, pero considerando como elemento subjetivo determinar la intención del sujeto activo. Es decir, se busca la correcta interpretación de la misma. Es decir, si el análisis jurídico se agota únicamente en contactar, no se podría

configurar el delito pues lo que se busca es comprobar la tipicidad subjetiva final del sujeto activo, en cuanto se refiere al "para solicitar". Aquí se condena la intención. Por ende, el caso en mención ha establecido una jurisprudencia fundamental.

Exp. N°01719-2014-80-1601-JR-PE-06

Delito: Delito Informático

Objeto Jurídicamente Protegido: Contra la Indemnidad y Libertad Sexual

Normativa: Art. 5 de la Ley de Delitos Informáticos. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.

Problemática Jurídica:

El sujeto pasivo tiene 13 años fue contactada a través de Facebook donde se le solicitaron imágenes y se le realizaron proposiciones obscenas. La madre de la menor advierte de esto a la Fiscalía y lo cual se procede a detener al Sujeto activo.

Decisión:

La fiscalía solicito la Terminación Anticipada establecido en el Art. 468 del CPP, y se le dio una pena de 4 años y 6 meses.

Comentario:

De la jurisprudencia antecedida se ve un mismo patrón donde el contactar, pero con un fin que está en contra de la indemnidad sexual y libertad sexual es penado, todo esto se configura cuando son realizados a través de medios electrónicos (celular, Tablet, laptop, etc.) o el internet. Sobre este delito a comparación de los otros delitos informáticos establecidos en la ley tiene el 90% de incidencia de ser denunciado y sentenciado.

Exp. N°0514-2014 (13105-2014)

Delito: Delito Informático

Objeto Jurídicamente Protegido: Contra el Patrimonio

Normativa: Art. 8 de la Ley de Delitos Informáticos. Fraude Informático.

Problemática Jurídica:

Una persona mediante phishing, clona la página de un banco. El titular de la tarjeta ingresa a hacer nuevos movimientos, donde se aparece la página clonada.

Decisión:

La fiscalía solicito la Terminación Anticipada establecido en el Art. 468 del CPP, y se le dio una pena de 3 años, su pena finalmente no fue efectiva.

Comentario:

Sobre este delito, aquí estamos frente a un delito de criminalidad organizada. Pues no solo es una persona la involucrada, sino una red de criminalidad el cual busca realizar fraudes informáticos con herramientas y softwares de alta tecnología. El más conocido en este caso es el denominado phishing, aquí la página del banco es donde para que el titular de la tarjeta y cuenta procede a ingresar el número de tarjeta y su clave y posteriormente la página desaparece, con estos datos procede el sujeto activo a retirar 3,000 soles, haciendo una trasferencia a otra cuenta. La señora se percata del movimiento pues tiene conectada la aceptación a través de su correo electrónico, por lo cual sorprendida se acerca al banco, donde solicita el número de cuenta donde ha sido enviada la transacción, con el cual obtiene el nombre del sujeto activo. Este se defendió argumentando que saco una tarjeta por un favor a una señora y esta le daría 20 soles, por lo que accedió. Pero finalmente al realizar el peritaje correspondiente y el análisis de la evidencia digital se determinó que en su computador tenía varios programas con este fin, es decir tenía una actividad delictiva informática.

Exp. N°2587-2015

Delito: Delito Informático

Objeto Jurídicamente Protegido: Contra el Patrimonio

Normativa: Art. 8 de la Ley de Delitos Informáticos. Fraude Informático.

Problemática Jurídica:

En este caso el Sujeto Activo era conocida del Sujeto Pasivo, donde este por hacerle un favor presta su tarjeta y cede su número de cuenta y contraseña. Catorce meses después esta persona realiza una transacción a la cuenta del sujeto activo. Esta también es advertida mediante correo electrónico y se apersona al banco, procediendo a realizar la denuncia correspondiente.

Decisión:

La fiscalía solicito la Terminación Anticipada establecido en el Art. 468 del CPP, y se le dio una pena de 3 años.

Comentario:

En esta jurisprudencia se observa que el proceder a cometer delitos contra el patrimonio a través de medios electrónicos. Tenemos este tipo penal el cual sanciona diversas y variadas conductas sobre el indebido empleo de datos informáticos y la manipulación sobre el funcionamiento del sistema.

3.4. Descripción de Resultados: Técnica de Análisis Normativo

La ley de Delitos Informáticos nos presente un bagaje de artículos que han evolucionado el concepto no solamente legislativo sino de Teoría del Delito por la complejidad en su comprensión en cuanto a sus Tipicidad, tanto Objetiva como Subjetiva. Si bien es cierto nuestro legislador se preocupó por penalizar estas conductas, y la DIVINDAT está tratando de luchar contra este denominado Cibercrimen, se ve una deficiencia en cuanto apoyo interinstitucionales.

Interpretación de la Norma

Fragmento ubicado el Capítulo I de la Ley de Delitos Informáticos N° 30096

Artículo 1.

La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la delincuencia.

El presente fragmento nos establece que el objeto y la finalidad de esta ley es combatir los Delitos Informáticos o Delitos Informáticos, el cual nos refuerza la existencia de una normativa que nos avala esta persecución, ya que busca la correcta investigación y llegar al enjuiciamiento que garantice la sanción.

Fragmento ubicado en la Cuarta Disposición Complementaria de la Ley de Delitos Informáticos N° 30096

CUARTA. Cooperación operativa

Con el objeto de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de comunicaciones y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial, el Pe-CERT (Centro de respuesta temprana del gobierno para ataques cibernéticos), la ONGEI (Oficina Nacional de Gobierno Electrónico e Informática), Organismos Especializados de las Fuerzas Armadas y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa reformada en el plazo de treinta días desde la vigencia de la presente Ley."

El presente fragmento nos avala la tipificación de la cooperación entre instituciones para garantizar el intercambio de información para la correcta investigación del autor. Lo que en la actualidad se da en término medio, a pesar de haber sido tipificado. Esta disposición nos refuerza la necesidad de un apoyo consensuado entre instituciones, de esa manera realizar una buena investigación, más rápida, es decir, eficiente y eficaz.

Fragmento ubicado en la Quinta Disposición Complementaria de la Ley de Delitos Informáticos N° 30096

QUINTA. - Capacitación

Las instituciones públicas involucradas en la prevención y represión de los delitos informáticos deben impartir cursos de capacitación destinados a mejorar la formación profesional de su personal -especialmente de la Policía Nacional del Perú, el Ministerio Público y el Poder Judicial- en el tratamiento de los delitos previstos en la presente Ley.

En la presente Disposición Complementaria de la Norma establece la necesidad de impartir cursos de capacitación en 3 ámbitos, Policía Nacional del Perú, Ministerio Publico y Poder Judicial. Todo en miras de llevar a buen recaudo los enjuiciamientos de los Delitos Informáticos, con una correcta comprensión de la prueba. Es necesario reiterar la aplicación de esta disposición con mayor fuerza en el Ministerio Público y el Poder Judicial.

3.5. Descripción de Resultados: Técnica de Análisis Derecho Comparado

Objetivo General

Fragmento ubicado en el Capítulo III Cooperación Internacional del Convenio de Budapest.

Artículo 23 – Principios generales relativos a la cooperación internacional

Las partes cooperarán entre sí en la mayor medida posible de conformidad con las disposiciones del presente Capitulo, en aplicación de los instrumentos internacionales pertinentes sobre cooperación internacional en materia penal, de los acuerdos basados en legislación uniforme o recíproca y de su propio derecho interno, a efectos de las investigaciones o los procedimiento relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de delitos.

En el presente fragmento nos tipifica desde el 2001 la Cooperación Internacional que debe existir entre los Estados, para combatir los Delitos Informáticos a la par. Esto ratifica mi objetivo general en cuanto a la realidad del país. Por ende, la necesidad de validarse de una Cooperación Internacional fluida, que te permita tener la información en tiempo real. Esto ya era solicitado desde hace 16 años para ser aplicado progresivamente. Donde como principio general se estableció la cooperación internacional para una correcta investigación y una legislación uniforme para que pueda ser enjuiciado conforme a ley.

Fragmento ubicado en TÍTULO X DELITOS CONTRA LA INTIMIDAD, EL DERECHO A LA PROPIA IMAGEN Y LA INVIOLABILIDAD DEL DOMICILIO

CAPÍTULO I Del descubrimiento y revelación de secretos del Código Penal Español

Artículo 197

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

El presente fragmento primero no tiene una ley autónoma, es decir todos los delitos están establecidos en el Código Penal Español, a diferencia de nuestra legislación que es autónoma.

Al realizar la comparación en lo referente al Delito de Acceso e Interceptación Ilícita, el Derecho Español lo tiene en el Art. 197 al 201 – Descubrimiento y revelación de secreto, Art. 278 al 286 – Delitos relativos al mercado y consumidores (espionaje industrial) del Código Penal Español, a diferencia de nuestra normativa que lo tenemos en la Ley 30096 y su modificatoria la Ley 30171, establecido en el Articulo 2 – Delitos de Acceso Ilícito, Articulo 3 – Atentado contra la integridad de datos informáticos y Articulo 4 – Atentado a la Integridad de Sistemas Informáticos.

En este ejemplo clave vemos que nuestra legislación es incoherente pues no estaría incorporando el Art. 4 del Convenio de Budapest lo que está orientado al daño, borrado, deterioro, alteración, supresión, introducción o trasmisión de datos informáticos, esto da la gran posibilidad que cualquier acto material configure el delito de atentado a la integridad de sistemas informáticos, lo que está correctamente establecido en la Legislación Española.

Objetivo Especifico 1

Fragmento ubicado en el Capítulo III Cooperación Internacional del Convenio de Budapest.

Artículo 35 – Red 24/7

1.Cada Parte designará un punto de contacto localizable las 24 horas del día, siete días a la semana, con el fin de garantizar una asistencia inmediata para investigaciones relativas a delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito. Esta asistencia comprenderá toda acción que facilite las medidas que figuran a continuación, o su aplicación directa si lo permite el derecho y la práctica internos:

a. asesoramiento técnico;

b. conservación de datos, de conformidad con los artículos 29 y 30; y

c. obtención de pruebas, suministro de información de carácter jurídico y localización de sospechosos.

Este fragmento nos establece en el Convenio de Budapest la asistencia inmediata para el cruce de información de manera internacional y de esa manera perseguir y combatir la Ciberdelincuencia pues es un plus de apoyo que se le da a la investigación de la autoría. Esto debería ser un centro especializado en todos los países donde ofrezcan respuestas todos los días de la semana, las 24 horas del día y que se mantenga en constante comunicación.

Fragmento ubicado en TÍTULO VIII DELITOS CONTRA LA LIBERTAD E INDEMNIDAD SEXUALES.

Capítulo II bis165 De los abusos y agresiones sexuales a menores de trece años del Código Penal Español

Artículo 183 bis167

El que, a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de trece años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 y 189, siempre que tal propuesta se acompañe

de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos.
Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño.

El presente fragmente al realizar la comparación en lo referente al Delito Sexuales, el Derecho Español lo tiene en el Art.181, Art. 183.1, Art. 183 bis, Art.184 del Código Penal Español, a diferencia de nuestra normativa que lo tenemos en la Ley 30096 y su modificatoria la Ley 30171, establecido en el Articulo 5 – Delitos de Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.
En este ejemplo clave vemos que nuestra legislación establece igual que la española los delitos informáticos que buscan finalmente obtener material pornográfico o llegar al acto sexual con la menor. Aquí lo que se debe tener en cuenta es el "engaño" como elemento previsto para configurar el delito que es de mera actividad. Recordemos que el Tribunal Constitucional Peruano declaró que los mayores de 14 y menores de 18 años pueden tener relaciones sexuales ya que tienen el derecho a la libertad sexual, contrario a la indemnidad sexual que afecta a los menores de 14 años. Siendo delitos informáticos de medio es importante que medie la intencionalidad, el engaño y se compruebe la actividad.

Objetivo Especifico 2

Fragmento ubicado en el Capítulo II Medidas que deberán adoptarse a nivel nacional del Convenio de Budapest.

Artículo 22 – Jurisdicción

1. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto de conformidad con los artículos 2 a 11 del presente Convenio, cuando el delito se haya cometido:

a. en su territorio; o

b. a bordo de un buque que enarbole su pabellón; o

c. a bordo de una aeronave matriculada según sus leyes; o

d. por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.

Este fragmento del Convenio nos establece la necesidad de adoptar medidas legislativas para afirmar la jurisdicción en aplicación del enjuiciamiento de los Delitos Informáticos. Cosa en la actualidad no es del todo posible, visto que el Ciberespacio no tiene Jurisdicción donde se pueda establecer de tal o cual país, más bien tiene una jurisdicción internacional. Por ende, la situación actual, como los resultados y las perspectivas del enjuiciamiento de los Delitos Informáticos en Perú se encuentra en un punto inicial.

Fragmento ubicado en TÍTULO XIII DELITOS CONTRA EL PATRIMONIO Y CONTRA EL ORDEN SOCIOECONÓMICO.

CAPÍTULO VI De las defraudaciones SECCIÓN 1ª De las estafas

Artículo 248

1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2201. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

En el presente fragmento al realizar la comparación en lo referente al Delito de Fraude Informático, el Derecho Español lo tiene en el Art. 248 a 251 y Art. 623.4 del Código Penal Español, a diferencia de nuestra normativa que lo tenemos en la Ley 30096 y

su modificatoria la Ley 30171, establecido en el Articulo 8 – Delitos Fraude Informático.

En este ejemplo clave vemos que nuestra legislación establece igual que la española los delitos informáticos que buscan ir en contra del patrimonio. Aquí lo que se debe tener en cuenta que guarde relación y congruencia con los términos que se emplean en el Convenio de Budapest. De aquí una problemática que tiene España que esta investigación sea significativa, ya que dependiendo del planteamiento del delito da la posibilidad de iniciar la investigación y sancionar.

IV. DISCUSION

Horsford y Bayanne (2009) hace mención que la discusión es quien defina y analice los resultados obtenidos teniendo en cuenta la coherencia (...) (p.45)

4.1 Aproximación al objeto de estudio

Esta investigación de campo se ha hecho en tres puntos del país, entrevistando a operadores jurídicos para su amplia comprensión sobre su fenómeno en el país, donde sus expertos en llevar a cabo esta evaluación, nos manifiesta que existe una relación importante entre el establecimiento de la evidencia digital para el efectivo juicio de los delitos informáticos y que esto influye positivamente en su evolución constante sobre su tipificación. En el presente trabajo también tenemos a expertos de la DIVINDAT (División de Investigación de Delitos de Alta Tecnología). Es decir aquí tenemos experiencias y conocimientos de Peritos Informáticos, Policías, Jueces, Fiscales y Abogados.

Objetivo General

Entrevistas

En la presente investigación relacionada con los Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano cuyo objetivo general es Analizar como la admisión de la evidencia digital incide en los delitos informáticos en el proceso penal peruano, que durante el trabajo de campo se ha desarrollado entrevistas y el análisis de documentos de los cuales obtuvimos los siguientes resultados:

Se ha determinado que no existe un buen nivel de legislación nacional sobre los delitos informáticos, puesto que se ha basado a las respuestas correspondientes de los entrevistados se ha considerado la importancia de mejorar nuestra legislación sobre este tipo de delitos, donde 11 de 12 entrevistados coinciden en que es necesario una modificación o actualización de la misma. A si mismo señalan que los operadores jurídicos no están lo suficientemente capacitados sobre estos temas, los entrevistados indican que es necesario tomar medidas sobre el tema del desconocimiento, con cursos especializados, capacitaciones, seminarios, conferencias. De los cuales 11 de 12 coincidieron que, con una buena base

educativa, podrá haber mayor comprensión de las evidencias digitales y se siga el proceso judicial de los delitos informáticos.

Por otro lado, los expertos indicaron que se tiene personal capacitado, especializado como peritos informáticos, donde 8 de 12 coincidían que este personal se capacita constantemente, pero no se dan abasto por la cantidad de carga de investigaciones donde 12 de los 10 entrevistados coincidía que eso creaba demoras en el proceso de investigación y por ende mantenía en paro el futuro juicio. Todo lo antecedido considerando que los entrevistados 7 consideran que no se tienen herramientas óptimas para la investigación de los delitos informáticos, 1 considera que si y 4 desconocen específicamente sobre el tema. Esto refleja una vez más la falta de capacitación que necesitan los operadores jurídicos donde más del 30 % se omiten de responder por no estar preparados.

Análisis Documental

En los datos estadísticos arrojados por la División de Estadística de la PNP, en un primer Cuadro 3.2 sobre Denuncias recibidas por Comisión de Delitos Registrados por la Dirincri PNP, según tipo de Delitos en el año 2016, se aprecia que tuvimos 880 denuncias recibidas sobre Delitos Informáticos, divididos en 4 trimestres. El primer trimestre (Enero a Marzo) con 196 denuncias. El segundo trimestre (Abril a Junio) con 193 denuncias. El tercer trimestre (Julio a Setiembre) con 206 denuncias y el ultimo y cuarto trimestre (Noviembre a Diciembre) con 285 denuncias.

En un segundo Cuadro 3.4 sobre Detenidos según tipo de Delitos y Modalidades en la DIVINDAT – DIRINCRI PNP. Año 2016, se aprecia que solo tuvimos 18 detenidos sobre Delitos Informáticos, divididos en 4 cuatro trimestres. El primer trimestre (Enero a Marzo) con 5 detenidos. El segundo trimestre (Abril a Junio) con 1 detenido. El tercer trimestre (Julio a Setiembre) con 6 detenidos y el ultimo y cuarto trimestre (Noviembre a Diciembre) con 6 detenidos.

Nos que nos refleja una diferencia abismal entre las denuncias y los detenidos por este tipo de Delitos. Aquí resaltan una vez más las falencias de herramientas especializadas, instrumentalización, personal suficiente y capacitado, operadores jurídicos capacitados, entre otros. Lo cual requiere una especial atención porque este es el centro de la problemática de la investigación en curso.

Análisis Jurisprudencial

De acuerdo al análisis jurisprudencial se ha verificado 4 expedientes donde se visualizan los casos con mayor incidencia donde se encuentra 2 casos del Art. 5, contra la indemnidad y libertad sexual y 2 casos del Art. 8 contra el Patrimonio, sobre el Fraude Informático. De los que se denotan que como pena oscila entre los 3 años a 5 años. Al que se le aplica una reducción de la pena quedando muchas veces en penas menores a 3 años, que en todo caso ya no son penas efectivas, sino penas suspendidas. Por lo antecedido entendemos que no solo es la complejidad de la comprensión de los delitos informáticos, como la de la evidencia digital, que es fundamental para crear el nexo causal entre el demandado y el hecho delictivo. Sino también el grado de pena y que esta sea efectiva. Para que no queden impunes este tipo delitos.

Derecho Comparado

De acuerdo al análisis de derecho comparado, se verifico la Ley Española contra los delitos informáticos y el Convenio de Budapest. El primero no tiene una ley autónoma, es decir todos los delitos están establecidos en el Código Penal Español, a diferencia de nuestra legislación que es autónoma.

Al realizar la comparación en lo referente al Delito de Acceso e Interceptación Ilícita, el Derecho Español lo tiene en el Art. 197 al 201 – Descubrimiento y revelación de secreto, Art. 278 al 286 – Delitos relativos al mercado y consumidores (espionaje industrial) del Código Penal Español, a diferencia de nuestra normativa que lo tenemos en la Ley 30096 y su modificatoria la Ley 30171, establecido en el Articulo 2 – Delitos de Acceso Ilícito, Articulo 3 – Atentado contra la integridad de datos informáticos y Articulo 4 – Atentado a la Integridad de Sistemas Informáticos, mientras

que el Convenio de Budapest lo tiene establecido en el Art. 2 y Art. 4.1, donde reafirma que el bien jurídico protegido por estos tipos penales son la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.

En este ejemplo clave vemos que nuestra legislación es incoherente pues no estaría incorporando el Art. 4 del Convenio de Budapest lo que está orientado al daño, borrado, deterioro, alteración, supresión, introducción o trasmisión de datos informáticos, esto da la gran posibilidad que cualquier acto material configure el delito de atentado a la integridad de sistemas informáticos, lo que está correctamente establecido en la Legislación Española.

Por lo tanto luego del análisis e interpretación de los resultados en cuanto a los delitos informáticos y evidencia digital en el proceso penal en cuyo objetivo general es "Analizar como la admisión de la evidencia digital incide en los delitos informáticos en el proceso penal peruano", queda verificado que se cumple el Supuesto General planteado en el presente trabajo de investigación.

Objetivo Especifico 1

Entrevistas

En la presente investigación relacionada con los Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano cuyo objetivo específico 1 es "Distinguir como la protección de la Evidencia digital influye en la clasificación de los Delitos Informáticos en el Proceso Penal Peruano", que durante el trabajo de campo se ha desarrollado entrevistas y el análisis de documentos de los cuales obtuvimos los siguientes resultados:

Se ha determinado que hay una fuerte discusión entre si abarcamos todos los delitos informáticos puros, que tienen como objeto directo la vulneración de sistemas e información, puesto que se ha basado a las respuestas correspondientes de los entrevistados se ha mostrado la disparidad entre lo tipificado o no, donde el 7 de 12 entrevistados coinciden en que necesitamos abarcar mayor cantidad de actos delictivos porque estos evolucionan mientras que 5 de 12 restantes de los

especialistas considera que con los artículos tipificados podemos ajustar el hecho al delito y no hay necesidad de mayor legislación. A diferencia de los delitos informáticos de medio, donde no están lo suficientemente regulados, los entrevistados indican que es necesario tomar medidas sobre el tema normativo, y hacer severas modificaciones en esta clase de Delitos Informáticos. De los cuales 12 de 12 coincidieron que no están bien regulados los delitos informáticos como medio.

Por otro lado, los expertos están en una fuerte discusión, sobre el tema de la tipicidad objetiva, por ende, los resultados están divididos 50% y 50%, donde 6 de 12 coincidían que la tipicidad subjetiva está bien regulada, que la problemática únicamente radica en su interpretación, mientras 5 de los 10 entrevistados coincidía que eso la tipicidad subjetiva no está bien estructurada. Por otro lado, los 12 entrevistados coincidieron que la tipicidad subjetiva sufrió una evolución, en cuanto lo referente al dolo y el delito de mera actividad.

Análisis Documental

En conclusión el estudio hecho por este investigador jurídico, en analizar la repuesta progresiva de los legisladores frente a este fenómeno de los delitos informáticos, como su evolución durante 10 años, con datos estadísticos de la Divindat podemos apreciar que en un incremento en el perjuicio económico que representa los delitos informáticos, siendo Lima la ciudad con mayor tasa de incidencias reportadas permitió observar que es un tema que se tiene que trabajar cuidadosamente, que en Perú aún no hay datos oficiales sobre pérdida económica. Que ha tenido una evolución en la norma que al comienzo era considerado delitos de peligro y no de resultado. Cuando su connotación real es que son delitos de mera actividad. Este experto analizo científicamente la evolución normativa, la evolución en la tipificación, la incidencia e impacto en el país, mostrando la necesidad de utilizar nuevas estrategias para combatir estos delitos. Sustentando en todos sus puntos mi Objetivo General y Objetivos específicos de la presente investigación

Análisis Jurisprudencial

De acuerdo al análisis jurisprudencial se ha verificado 4 expedientes donde se visualizan los casos con mayor incidencia donde se encuentra 2 casos del Art. 5, contra la indemnidad y libertad sexual y 2 casos del Art. 8 contra el Patrimonio, sobre el Fraude Informático. De los que se denotan que como pena oscila entre los 3 años a 5 años. Donde visualizamos que la mayor cantidad de equipos informáticos son por medio del celular, y a través de redes sociales como el Facebook, en especial en delitos contra la indemnidad y libertad sexual. Por lo antecedido entendemos que no solo es la complejidad de la comprensión de los delitos informáticos, como la de la evidencia digital, que es fundamental para crear el nexo causal entre el demandado y el hecho delictivo. Sino también la protección que merecen los equipos informáticos que nos van a servir de evidencia para comprobar el hecho delictivo esta va a generar confianza y no vulnerara el debido proceso.

Derecho Comparado

De acuerdo al análisis de derecho comparado, se verifico la Ley Española contra los delitos informáticos y el Convenio de Budapest. El primero no tiene una ley autónoma, es decir todos los delitos están establecidos en el Código Penal Español, a diferencia de nuestra legislación que es autónoma.

Al realizar la comparación en lo referente al Delito Sexuales, el Derecho Español lo tiene en el Art.181, Art. 183.1, Art. 183 bis, Art.184 del Código Penal Español, a diferencia de nuestra normativa que lo tenemos en la Ley 30096 y su modificatoria la Ley 30171, establecido en el Articulo 5 – Delitos de Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, mientras que el Convenio de Budapest no está establecido, ni existe un consenso sobre la necesidad de tener este tipo penal regulado de manera penal.

En este ejemplo clave vemos que nuestra legislación establece igual que la española los delitos informáticos que buscan finalmente obtener material pornográfico o llegar al acto sexual con la menor. Aquí lo que se debe tener en cuenta es el "engaño" como elemento previsto para configurar el delito que es de mera actividad. Recordemos que el Tribunal Constitucional Peruano declaró que los mayores de 14 y menores de

18 años pueden tener relaciones sexuales ya que tienen el derecho a la libertad sexual, contrario a la indemnidad sexual que afecta a los menores de 14 años. Siendo delitos informáticos de medio es importante que medie la intencionalidad, el engaño y se compruebe la actividad.

Por lo tanto luego del análisis e interpretación de los resultados en cuanto a los delitos informáticos y evidencia digital en el proceso penal en cuyo objetivo específico 1 es "Distinguir como la protección de la Evidencia digital influye en la clasificación de los Delitos Informáticos en el Proceso Penal Peruano", queda verificado que se cumple el Supuesto Especifico planteado en el presente trabajo de investigación.

Objetivo Especifico 2

Entrevistas

En la presente investigación relacionada con los Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano cuyo objetivo específico 2 es "Constatar como la determinación del Marco Legal de la Evidencia Digital repercute en la Tipicidad de los Delitos Informáticos en el Proceso Penal Peruano.", que durante el trabajo de campo se ha desarrollado entrevistas y el análisis de documentos de los cuales obtuvimos los siguientes resultados:

Se ha determinado que existe un conocimiento adecuado del Manejo de la Evidencia digital, donde 8 de 10 entrevistados confirmaron, que está el conocimiento, pero faltan herramientas digitales para combatir las mismas. Además, los 12 expertos reiteraron la importancia de un buen informe del Perito Informático sobre la Evidencia Digital, la necesidad que tenga una buena calidad y la evidencia sea comprendida en todo aspecto y por ende admitida.

Por otro lado los expertos están en una fuerte discusión, sobre el tema del marco legal para la cadena de custodia, por ende los resultados están divididos 50% y 50%, donde 6 de 12 coincidían que es suficiente el Marco Legal que a la fecha tiene la Cadena de Custodia, cuando se refiere al Reglamento de la Cadena de Custodia, mientras 6 de los 12 entrevistados coincidía que hay ausencia de una mejor

normativa una ley especializada en Cadena de Custodia sobre Evidencia Digital, pues es otro el proceso de reconocimiento, recolección, custodia y análisis el que tiene este tipo de evidencias. Por otro lado 8 de los 12 entrevistados coincidieron no hay una correcta Instrumentalización de la Evidencia Digital, mientras que los 4 entrevistados restantes desconocían el tema de la Instrumentalización y se limitaron a no contestar.

Análisis Documental

El estudio de todos los artículos de la Ley de Delitos Informáticos y el análisis de su tipicidad nos permitió dilucidar un nuevo fenómeno y el choque frente a lo conocido en la estructura de los delitos convencionales. A pareciendo lo que los juristas denominan delito de resultado cortado, también estamos frente a delitos de mera actividad, los que ha generado una discusión fuerte entre los operadores del derecho, en busca de la comprensión del mismo para poder ser correctamente juzgado sin vulnerar el Debido proceso. Permitiendo observar una tendencia interna trascendente porque representa un elemento subjetivo distinto al dolo, poniendo hincapié especial en la intención del agente, siendo considerada como un delito de resultado cortado. Demostrando la evolución en la tipicidad de estos delitos.

Análisis Jurisprudencial

De acuerdo al análisis jurisprudencial se ha verificado 4 expedientes donde se visualizan los casos con mayor incidencia donde se encuentra 2 casos del Art. 5, contra la indemnidad y libertad sexual y 2 casos del Art. 8 contra el Patrimonio, sobre el Fraude Informático. De los que se denotan que como pena oscila entre los 3 años a 5 años. En los casos de Fraude Informático analizados encontramos que la instrumentalización requerida es muy necesaria para obtener la evidencia digital y sea correctamente analizada. Donde el uso de las herramientas tiene muchas falencias el cual produce que no se detecte el delito a tiempo. En los casos de Indemnidad Sexual este índice es muy alto y produce consecuencias fatales.

Derecho Comparado

De acuerdo al análisis de derecho comparado, se verifico la Ley Española contra los delitos informáticos y el Convenio de Budapest. El primero no tiene una ley autónoma, es decir todos los delitos están establecidos en el Código Penal Español, a diferencia de nuestra legislación que es autónoma.

Al realizar la comparación en lo referente al Delito de Fraude Informático, el Derecho Español lo tiene en el Art. 248 a 251 y Art. 623.4 del Código Penal Español, a diferencia de nuestra normativa que lo tenemos en la Ley 30096 y su modificatoria la Ley 30171, establecido en el Articulo 8 – Delitos Fraude Informático, mientras que el Convenio de Budapest está establecido en el Art. 8, donde se ve la necesidad de tener este tipo penal regulado de manera penal.

En este ejemplo clave vemos que nuestra legislación establece igual que la española los delitos informáticos que buscan ir en contra del patrimonio. Aquí lo que se debe tener en cuenta que guarde relación y congruencia con los términos que se emplean en el Convenio de Budapest. De aquí una problemática que tiene España que esta investigación sea significativa, ya que dependiendo del planteamiento del delito da la posibilidad de iniciar la investigación y sancionar.

Por lo tanto luego del análisis e interpretación de los resultados en cuanto a los delitos informáticos y evidencia digital en el proceso penal en cuyo objetivo específico 2 es "Constatar como la determinación del Marco Legal de la Evidencia Digital repercute en la Tipicidad de los Delitos Informáticos en el Proceso Penal Peruano", queda verificado que se cumple el Supuesto General planteado en el presente trabajo de investigación.

V. CONCLUSION

Primera

Se ha analizado como la admisión de la evidencia digital incide positivamente en los procesos penales sobre los delitos informáticos, porque se busca el esclarecimiento adecuado del hecho delictivo, la falencia es el grado de desconocimiento por parte de los operadores jurídicos que no consiguen tener comprensión ni del delito ni de las evidencias. Sumados a la existencia de una legislación que tiene carencias y no abarca todos los delitos con sus modalidades. Que a pesar de tener personal capacitado, peritos informáticos, especialistas de la DIVINDAT, estos no se dan abasto para la carga de investigaciones, tomando en cuenta que no ayudan las herramientas que tienen por no ser optimas o ha vencido su licencia para ser utilizadas. Por lo que genera demoras, por problemas burocráticos, hasta la obtención de una nueva licencia.

Segunda

Se ha distinguido como la protección de la evidencia digital en cuanto a cadena de custodia influye para que exista una correcta clasificación de los delitos informáticos, porque permite dilucidar y comprender el hecho delictivo informático y a pesar de ello no tenemos una buena legislación en temas de delitos informáticos como medio, se concluyó que tiene que ver con la estructura de la tipicidad objetiva y la evolución de la subjetiva, en vista que hay un fuerte debate en busca de la comprensión dogmática de los mismos.

Tercera

Se ha constatado como la determinación del Marco Legal sobre la Evidencia digital repercute en la tipicidad de los delitos informáticos, porque no existe un conocimiento adecuado de este tipo de evidencias, mucho menos en el manejo adecuado teniendo la instrumentalización pertinente, que permita una calidad de análisis pericial y un informe correcto para su comprensión, ya que esto es básico para la admisión de la evidencia digital dentro del proceso penal peruano. Se concluyó que es necesario un mejor marco legal en cuanto a la cadena de custodia y un manejo especial cuando se refiere a evidencia digital.

VI. RECOMENDACIONES

Primera

Se recomienda sobre la admisión de la evidencia digital en el proceso penal que exista una cooperación e intervención de todos los operadores del derecho. Si bien nuestro legislador se preocupó por penalizar este tipo de conductas y la DIVINDAT de luchar contra el Cibercrimen; especializando sus instituciones; el Ministerio Publico y el Poder Judicial han quedado exentos de esto. Considerando que las técnicas, análisis y comprensión de estos delitos no son los convencionales es necesario crear una Fiscalía Especializada en Delitos de Alta Tecnología, así como lo tiene España, Argentina y Paraguay.

Segunda

Se recomienda aplicar con suma urgencia una restructuración de las figuras jurídicas sobre los delitos informáticos que estén acorde a la realidad del país. Como también se mantengan a la vanguardia de los constantes cambios de modalidad que adquieren los delincuentes Informáticos. Por otro lado llegar a un consensó por parte de los juristas sobre la Tipicidad Subjetiva de estos delitos. También es necesario capacitaciones frecuentes a nuestros operadores de derecho, para que comprendan la estructura y puedan armar una buena Teoría del Caso, tanto por parte de fiscales y abogados.

Tercera

Se recomienda la creación de un marco legal que sustente o ampare la Cadena de Custodia, es básico para salvaguardar todas las metodologías sobre procedimientos de reconocimiento, recolección, análisis y protección de la evidencia digital. Se requiere también una mejor instrumentalización para la recolección de la evidencia digital y de esa manera obtener una calidad de análisis sobre los mismos, los cuales lo acrediten como prueba fehaciente dentro del proceso penal.

VII. REFERENCIAS BIBLIOGRAFICAS

REFERENCIAS BIBILOGRAFICAS

Abanto Garnique, J. L. (2012). La desproteccion de los datos personales de los cibernautas peruanos, expuestos a codigo malicioso y su incidencia en la vulneración al derecho a la intimidad. Repositorio Univesidad Nacional de Ingenieria.

Alonso, d. E., Cugat, M. M., Garcia, R. N., Lloria, G. P., Machado, P. F., Quinteros, O. G., . . . Riquet, A. M. (2014). *CIBERDELITOS* (1ra ed.). Buenos Aires, Argentina: Hammurabi.

Angulo Arana, P. (2014). *EL CASO PENAL - Base de la litigacion en el Juicio Oral.* Lima: Gaceta Juridica.

Benites Tangoa, J. (2010). Mecanismos de Celeridad Procesal principio de oportunidad y proceso de terminación anticipada en el codigo 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* (1ra ed.). (E. p. Santillán, Ed.) Mexico, Mexico: 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. Atribucion, Ed.) Obtenido de Hiperderecho: http://www.hiperderecho.org/2014/07/luces-y-sombras-de-la-delincuencia-informatica-en-peru/

Gamarra Chavarry, L. M. (2017). Implementacion de la Politica Publica de Fortalecimiento de la función criminalistica en la policia: 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: Union Internacional de Telecomunicaciones.

GIL ALBARRÁN, 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.

Hernández Sampieri, R. F. (2014). *Metodología de la investigación: Roberto Hernández Sampieri, Carlos Fernández Collado y Pilar Baptista Lucio* (6a. ed. ed.). México D.F: McGraw-Hill.

Hurtado Pozo, J. (2005). *Manual de Derecho Penal - Parte General I* (3RA EDICION ed.). Lima: Editora Juridica Grijley EIRL.

KELSEN, H. (2006). *¿Una nueva ciencia de la política?* (1ra ed.). Buenos Aires-Madrid: Katz editores S.A.

KINDERSLEY, D. (2003). *En la Escena del Crimen.* Madrid: Pearson Educación.

Kotler, & Armstrong. (2008). *Fundamentos de Marketing.* Mexico: Pearson Prentice Hall.

Luis, V. J. (5 de Noviembre de 2013). Delitos Informáticos. *Jurídica - Suplemento del Diario El Peruano*, págs. 6-7.

Monroy Galvez, J. F. (2009). *Teoria General del Proceso.* Lima: Libreria Communitas EIRL.

Montezuma Panez, O. (5 de Noviembre de 2013). Rumbo al Convenio de Budapest. *Juridica - Suplemento de El Peruano*, págs. 8-10.

Nuñez Ponce, J. C. (2016). Derecho de Identidad digital en internet. Repositorio Universidad San Marcos.

Placencia Rubiños, L. (2014). *El Habeas Corpus contra Actos de Investigación Preliminar.* Lima: Gaceta Juridica.

Rayon, B. M., & Gomez, H. J. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Juridico y Económico Escurialense, XLVII*, 209-234.

Rincon Rios, J. (2015). El delito en la cibersociedad y la justicia penal internacional. Madrid, Madrid, España: Universidad Complutense de Madrid.

Rioja Bermudez, A. (2008). *PROCESAL CIVIL : ALEXANDER RIOJA BERMUDEZ Información doctrinaria y jurisprudencial del derecho procesal civil.* Obtenido de PROCESAL CIVIL : ALEXANDER RIOJA BERMUDEZ Información doctrinaria y jurisprudencial del derecho procesal civil: http://blog.pucp.edu.pe/blog/seminariotallerdpc/2008/12/01/celeridad-procesal-y-actuacion-de-la-sentencia-impugnada-en-el-proceso-civil-peruano/

Salas Ordinola , E., Ramirez Garcia, A., & Nuñez Mori, O. (2012). Propuesta de Protocolo para la Recolección de Evidencias. *IUST VERITAS*, 1-8.

Suarez Vives, M. (2015). La Ciberguerra y la Aplicación de los principios del Derecho Internacional Humanitario. Lima: Repositorio Universidad San Martin de Porres.

TEMPERINI, M. (2015). El desafio de la lucha contra ek cibercrimen en Argentina. (F. d. UNL, Ed.) *Papeles del Centro de Investigacione*(16), 31-51.

VALDERRAMA MENDOZA, S. (2013). *Pasos para la elaborar Proyectos de Investigación Cientifica.* Lima: Editorial San Marcos EIRL.

Vara Horna, A. (2012). *Siete pasos para una tesis exitosa. Un método efectivo.* Lima: Facultad de Ciencias Administrativas y Recursos Humanos. USMP.

Villavicencios Terenos, F. (2014). Delitos Informaticos - Cybercrimes. *IUS ET VERITAS N° 49*, 284-304.

ZEGARRA, A. A. (Octubre de 2015). La Informatica como medio delictivo y como objeto material en la cibercriminalidad. Refutación de otras clasificaciones. *Actualidad Juridica, 263*, 107-113.

ANEXOS

TÍTULO DEL TRABAJO DE INVESTIGACIÓN	Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017.
PROBLEMA GENERAL	¿Cómo la admisión de la evidencia digital incide en los delitos informáticos en el proceso penal peruano?
PROBLEMAS ESPECIFICOS	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?
HIPÓTESIS (SUPUESTOS)	La admisión de la evidencia digital incide positivamente en los delitos informáticos en el proceso penal peruano.
HIPOTESIS ESPECIFICAS (SUPUESTOS ESPECIFICOS)	1.- La protección de la Evidencia digital influye positivamente en la clasificación de los Delitos Informáticos en el Proceso Penal Peruano. 2.- La determinación del Marco Legal de la Evidencia Digital repercute positivamente en la Tipicidad de los Delitos Informáticos en el Proceso Penal Peruano
OBJETIVO GENERAL	Analizar como la admisión de la evidencia digital incide en los delitos informáticos en el proceso penal peruano.
OBJETIVOS ESPECÍFICOS	1.-. Distinguir como la protección de la Evidencia digital influye en la clasificación de los Delitos Informáticos en el Proceso Penal Peruano. 2.- Constatar como la determinación del Marco Legal de la Evidencia Digital repercute en la Tipicidad de los Delitos Informáticos en el Proceso Penal Peruano.
DISEÑO DEL ESTUDIO	Nivel de Investigación Cualitativa - Aplicada. Diseño Teoría Fundamentada. Método Inductivo. Retrospectivo – Prospectivo
POBLACIÓN Y MUESTRA (SI CORRESPONDE)	En mi población es a nivel nacional tengo a especialistas entre ellos los integrantes de la Divindat, fiscales, abogados e jueces penales y ingenieros de sistemas que logran ver temas de Ciberdelitos.

ANEXO Nº 1: Matriz de consistencia

Categorización	Definición conceptual	Definición operacional	Sub categorías	Indicadores
Delitos Informáticos	Son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal, que hacen uso indebido de cualquier medio Informático y a través del mundo virtual de Internet.	X. Delitos Informáticos	X1.Clasificación. X2.Tipicidad.	X11 Objeto X12 Medio X21 Objetiva X22 Subjetiva
Evidencia Digital	Son las pruebas que sustentan los delitos informáticos y afines, son correos electrónicos, grabaciones generadas y conservadas en formato digital, fotografías digitales, mensajes de texto de celulares, llamadas reportadas en la base de datos de los operadores de telefonía móvil, entre otras.	Y. Evidencia Digital	Y1.Proteccion de Evidencias. Y2. Marco Legal.	Y11 Metodología de análisis. Y12 Metodología de Recolección. Y21 Cadena de Custodia. Y22 Instrumentalización Evidencia Digital

ANEXO Nº 2: Unidades Temáticas - Categorización

ANEXO Nº3: Validación de Instrumento

VALIDACION DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres:

1.2. Cargo e Institución donde labora:

1.3. Nombre del Instrumento motivo de evaluación:

1.4. Autor (A) de Instrumento:

II. ASPECTOS DE VALIDACION

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85
1. CLARIDAD	Esta formulado con lenguaje comprensible.										
2.OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.										
3.ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.										
4.ORGANIZACION	Existe una organización lógica.										
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales.										
6.INTENCIONALIDAD	Esta adecuado para valorar las variables de los Supuestos										
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.										
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos.										
9. METODOLOGIA	La estrategia responde una metodología y diseño aplicados para lograr probar los supuestos jurídicos.										
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.										

III. OPINION DE APLICABILIDAD

- El instrumento cumple con los Requisitos para su aplicación. [ ]
- El instrumento no cumple con los requisitos para su aplicación. [ ]

IV. PROMEDIO DE VALORACION: 95 %

Lima, 23 JUNIO del 20

FIRMA DEL EXPERTO INFORMANTE

DNI Nº [illegible] Telf: [illegible]

VALIDACION DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: Chávez Sánchez Jaime Eliber

1.2. Cargo e Institución donde labora: Docente UCV

1.3. Nombre del Instrumento motivo de evaluación: Ficha de entrevista

1.4. Autor (A) de Instrumento: [illegible]

II. ASPECTOS DE VALIDACION:

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.											X		
2.OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.											X		
3.ACTUALIDAD	Este adecuado a los objetivos y las necesidades reales de la investigación.											X		
4.ORGANIZACION	Existe una organización lógica.											X		
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales.												X	
6.INTENCIONALIDAD	Esta adecuado para valorar las variables de los Supuestos.												X	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.											X		
8. COHERENCIA	Existe coherencia entre lo problemas, objetivos, supuestos.											X		
9. METODOLOGIA	La estrategia responde una metodología y diseño aplicados para lograr probar los supuestos jurídicos.											X		
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.											X		

III. OPINION DE APLICABILIDAD

- El instrumento cumple con los Requisitos para su aplicación. — SI
- El instrumento no cumple con los requisitos para su aplicación. —

IV. PROMEDIO DE VALORACION: 91 %

Lima, 23 de Junio del 2017

FIRMA DEL EXPERTO INFORMANTE

DNI N° [illegible] Telf. 964266457

I. DATOS GENERALES

1.1. Apellidos y Nombres:

1.2. Cargo e Institución donde labora:

1.3. Nombre del instrumento motivo de evaluación:

1.4. Autor (A) de Instrumento:

II ASPECTOS DE VALIDACION

CRITERIOS	INDICADORES	INACEPTABLE				REGULAR				BUENA				MUY BUENA			
		40	45	50	55	60	65	70	75	80	85	90	95	100			
1.CLARIDAD	Está formulado con lenguaje comprensible													✓			
2.OBJETIVIDAD	Está adecuado a conductas observables													✓			
3.ACTUALIDAD	Está adecuado a los objetivos y las necesidades reales de la investigación													✓			
4.ORGANIZACION	Existe una organización lógica													✓			
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales													✓			
6.INTENCIONALIDAD	Está adecuado para valorar las categorías de los Supuestos													✓			
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos													✓			
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos.													✓			
9. METODOLOGIA	La estrategia responde una metodología y diseño aplicados para lograr verdad los supuestos													✓			
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.													✓			

III OPINION DE APLICABILIDAD

- El instrumento cumple con los Requisitos para su aplicación. ✓
- El instrumento no cumple con los requisitos para su aplicación. —

IV. PROMEDIO DE VALORACION 85 %

Lima, 23 de junio del 2017

FIRMA DEL EXPERTO INFORMANTE

DNI N° [illegible] Tel. [illegible]

VALIDACION DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: ...

1.2. Cargo e Institución donde labora: ...

1.3. Nombre del Instrumento motivo de evaluación: ...

1.4. Autor (A) de Instrumento: ...

II. ASPECTOS DE VALIDACION:

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE		
		40	45	50	55	60	65	70	75	80	85	90	95
1. CLARIDAD	Esta formulado con lenguaje comprensible.											X	
2.OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.											X	
3.ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.											X	
4.ORGANIZACION	Existe una organización lógica.											X	
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales.											X	
6.INTENCIONALIDAD	Esta adecuado para valorar las variables de los Supuestos.											X	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.											X	
8. COHERENCIA	Existe coherencia entre lo problemas, objetivos, supuestos.											X	
9. METODOLOGIA	La estrategia responde una metodología y diseño aplicados para lograr probar los supuestos jurídicos.											X	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.											X	

III. OPINION DE APLICABILIDAD

- El instrumento cumple con los Requisitos para su aplicación. — SI
- El instrumento no cumple con los requisitos para su aplicación. —

IV. PROMEDIO DE VALORACION: 90 %

Lima, 23 Junio del 2017

FIRMA DEL EXPERTO INFORMANTE

DNI N° ... Telf. ...

VALIDACION DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: Chávez Sánchez Jesus Alan

1.2. Cargo e Institución donde labora: Docente asesor

1.3. Nombre del Instrumento motivo de evaluación: Ficha de observación

1.4. Autor (A) de Instrumento: [illegible]

II. ASPECTOS DE VALIDACION:

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE		
		40	45	50	55	60	65	70	75	80	85	90	95
1. CLARIDAD	Esta formulado con lenguaje comprensible.												✓
2.OBJETIVIDAD	Esta adecuado a las leyes y principios científicos												✓
3.ACTUALIDAD	Este adecuado a los objetivos y las necesidades reales de la investigación.												✓
4.ORGANIZACION	Existe una organización lógica												✓
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales												✓
6.INTENCIONALIDAD	Esta adecuado para valorar las variables de los Supuestos												✓
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos												✓
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos.												✓
9. METODOLOGIA	La estrategia responde una metodología y diseño aplicados para lograr probar los supuestos jurídicos												✓
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												✓

III. OPINION DE APLICABILIDAD

- El instrumento cumple con los Requisitos para su aplicación. — Si
- El instrumento no cumple con los requisitos para su aplicación. —

IV. PROMEDIO DE VALORACION: 95 %

Lima, 23 de junio del 2017

FIRMA DEL EXPERTO INFORMANTE

DNI N° [illegible] Telf. 964746452

VALIDACION DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: Ortega Regal Carlos Alberto

1.2. Cargo e Institución donde labora: D.T.C. - U.C.V.

1.3. Nombre del Instrumento motivo de evaluación: Analisis Documental

1.4. Autor (A) de Instrumento: [illegible]

II. ASPECTOS DE VALIDACION:

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTA	
		40	45	50	55	60	65	70	75	80	85	90
1. CLARIDAD	Esta formulado con lenguaje comprensible										✓	
2 OBJETIVIDAD	Esta adecuado a las leyes y principios científicos										✓	
3. ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación										✓	
4 ORGANIZACION	Existe una organización lógica										✓	
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales										✓	
6.INTENCIONALIDAD	Esta adecuado para valorar las variables de los Supuestos										✓	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos										✓	
8. COHERENCIA	Existe coherencia entre lo problemas, objetivos, supuestos										✓	
9. METODOLOGIA	La estrategia responde una metodología y diseño aplicados para lograr probar los supuestos jurídicos										✓	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico										✓	

III. OPINION DE APLICABILIDAD

- El instrumento cumple con los Requisitos para su aplicación. ✓
- El instrumento no cumple con los requisitos para su aplicación. —

IV. PROMEDIO DE VALORACION: 85 %

Lima, 23 de junio del 2017

FIRMA DEL EXPERTO INFORMANTE

DNI N° [illegible] Telf. 994054775

ANEXO Nº 4: Instrumentos

FICHA DE ENTREVISTA

Título: "Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017"

Entrevistado:.....
Cargo/profesión/ grado académico: .....
.....
Institución: .....
.....
Lugar: .....
Fecha: .....

Objetivo general: Analizar como 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?

.....
.....
.....
.....

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

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 esta 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?

.....
.....
.....
.....

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

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.- De 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?

.....
.....
.....
.....

Que habiendo culminado de manera exitosa la entrevista, se agradece su importante colaboración.

Lima, 31 de Octubre del 2017

Leyla Keith Rivero Passuni DNI N° 44757254 ENTREVISTADOR	Nombre y Apellido: DNI N° ENTREVISTADO

GUIA DE ANALISIS DERECHO COMPARADO

I.- DATOS DEL DOCUMENTO:

Tipo de Documento*	Convenio
Título del Documento	Convenio sobre la Delincuencia Budapest
Autor del Documento	Los Estados Miembros del Consejo de Europa
Fecha del Documento	23/11/2001
Procedencia del Documento**	Internacional

II.- ANALIS DEL TESISTA

Objetivo	Fragmento	Análisis
Og: Analizar como la admisión de la evidencia digital incide en los delitos informáticos en el proceso penal peruano.	**Fragmento ubicado en el Capítulo III Cooperación Internacional del Convenio de Budapest.** **Artículo 23** – *Principios generales* relativos a la cooperación internacional Las partes cooperarán entre sí en la mayor medida posible de conformidad con las disposiciones del presente Capitulo, en aplicación de los instrumentos internacionales pertinentes sobre cooperación internacional en materia penal, de los acuerdos basados en legislación uniforme o recíproca y de su propio derecho interno, a efectos de las investigaciones o los procedimiento relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de delitos.	En el presente fragmento nos tipifica desde el 2001 la Cooperación Internacional que debe existir entre los Estados, para combatir los Delitos Informáticos a la par. Esto ratifica mi objetivo general en cuanto a la realidad del país. Por ende, la necesidad de validarse de una Cooperación Internacional fluida, que te permita tener la información en tiempo real. Esto ya era solicitado desde hace 16 años para ser aplicado progresivamente. Donde como principio general se estableció la cooperación internacional para una correcta investigación y una legislación uniforme para que pueda ser enjuiciado conforme a ley.
Oe1: Distinguir como la protección de la Evidencia digital influye en la clasificación	**Fragmento ubicado en el Capítulo III Cooperación Internacional del Convenio de Budapest.** **Artículo 35** – Red 24/7 1.Cada Parte designará un punto de contacto localizable las 24 horas del día, siete días a la semana, con el fin de garantizar una asistencia inmediata para investigaciones relativas a delitos	Este fragmento nos establece en el Convenio de Budapest la asistencia inmediata para el cruce de información de manera internacional y de esa manera perseguir y combatir la Ciberdelincuencia pues es un plus de apoyo que se le da a la investigación de la autoría. Esto debería ser un centro

de los Delitos Informáticos en el Proceso Penal Peruano	vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito. Esta asistencia comprenderá toda acción que facilite las medidas que figuran a continuación, o su aplicación directa si lo permite el derecho y la práctica internos: a. asesoramiento técnico; b. conservación de datos, de conformidad con los artículos 29 y 30; y c. obtención de pruebas, suministro de información de carácter jurídico y localización de sospechosos.	especializado en todos los países donde ofrezcan respuestas todos los días de la semana, las 24 horas del día y que se mantenga en constante comunicación.
Oe2: Constatar como la determinación del Marco Legal de la Evidencia Digital repercute en la Tipicidad de los Delitos Informáticos en el Proceso Penal Peruano	**Fragmento ubicado en el Capítulo II Medidas que deberán adoptarse a nivel nacional del Convenio de Budapest.** **Artículo 22** – Jurisdicción 1. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto de conformidad con los artículos 2 a 11 del presente Convenio, cuando el delito se haya cometido: a. en su territorio; o b. a bordo de un buque que enarbole su pabellón; o c. a bordo de una aeronave matriculada según sus leyes; o d. por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.	Este fragmento del Convenio nos establece la necesidad de adoptar medidas legislativas para afirmar la jurisdicción en aplicación del enjuiciamiento de los Delitos Informáticos. Cosa en la actualidad no es del todo posible, visto que el Ciberespacio no tiene Jurisdicción donde se pueda establecer de tal o cual país, más bien tiene una jurisdicción internacional. Por ende, la situación actual, como los resultados y las perspectivas del enjuiciamiento de los Delitos Informáticos en Perú se encuentra en un punto inicial.

ANEXO Nº 5: Cuadro de Denuncias y Detenidos de Delitos Informáticos del Año 2016

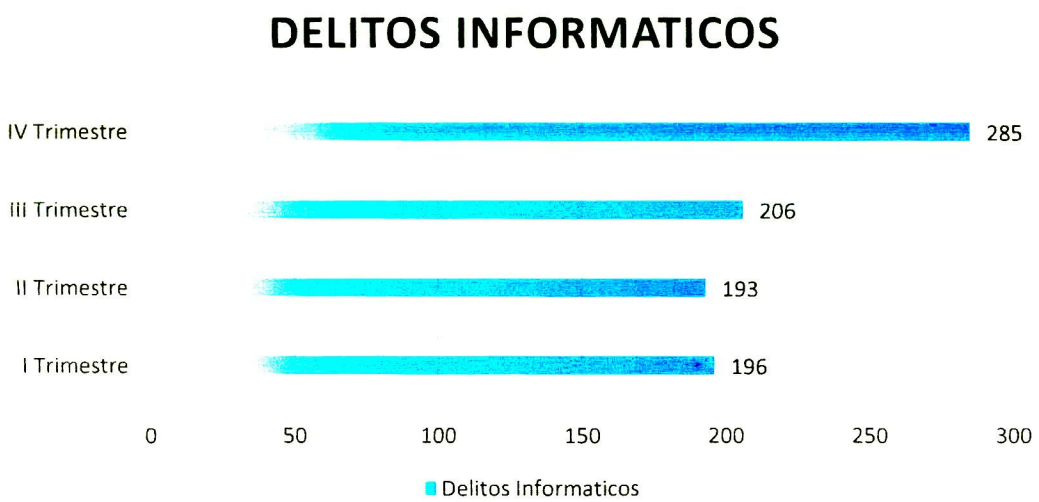


Figura. 1
Cantidad de denuncias recibidas por Comisión de Delitos Registrados por la DIRINCRI PNP según tipo de delito año 2016. ***Fuente:*** *Adecuación del Boletín Estadístico de la PNP.*

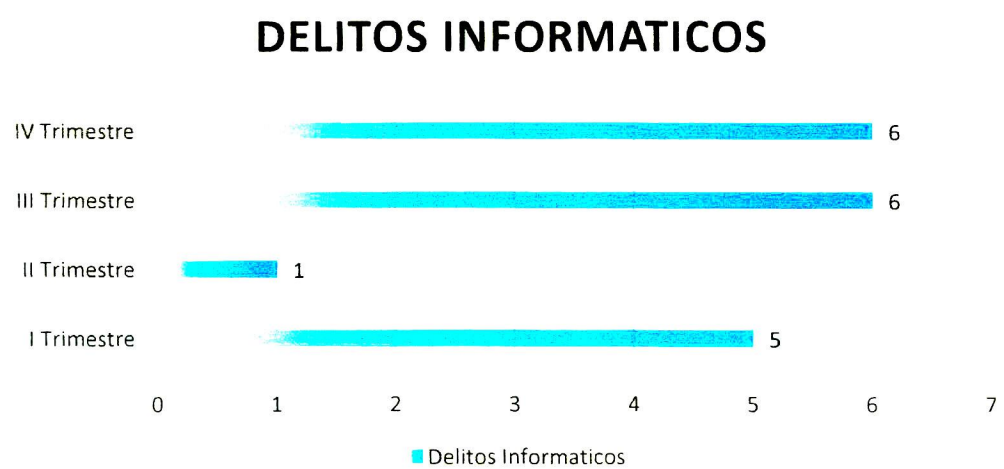
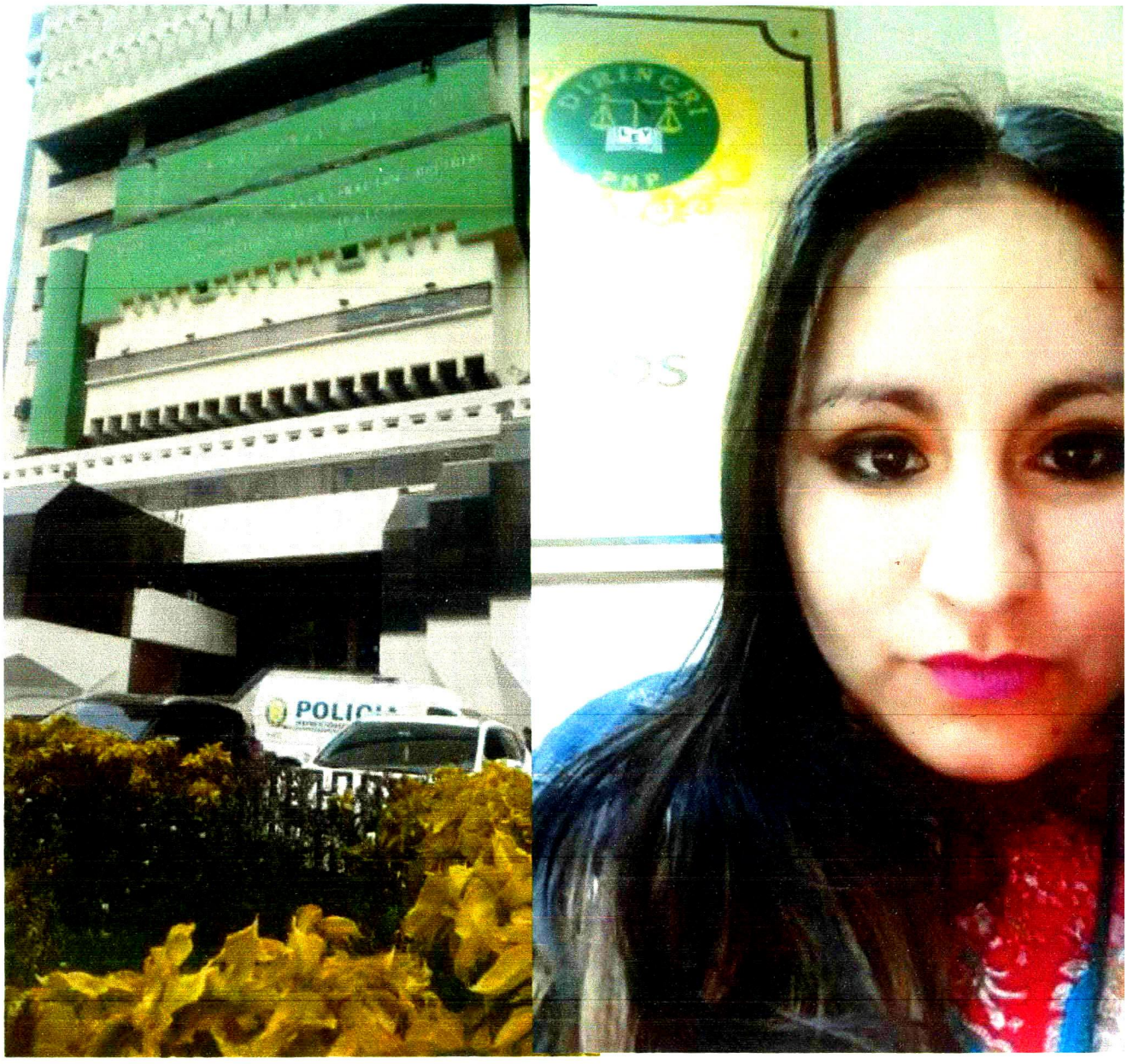


Figura. 2
Cantidad de detenidos según tipo de delito y modalidades en la DIVINDAT DIRINCRI PNP año 2016. ***Fuente:*** *Adecuación del Boletín Estadístico de la PNP*

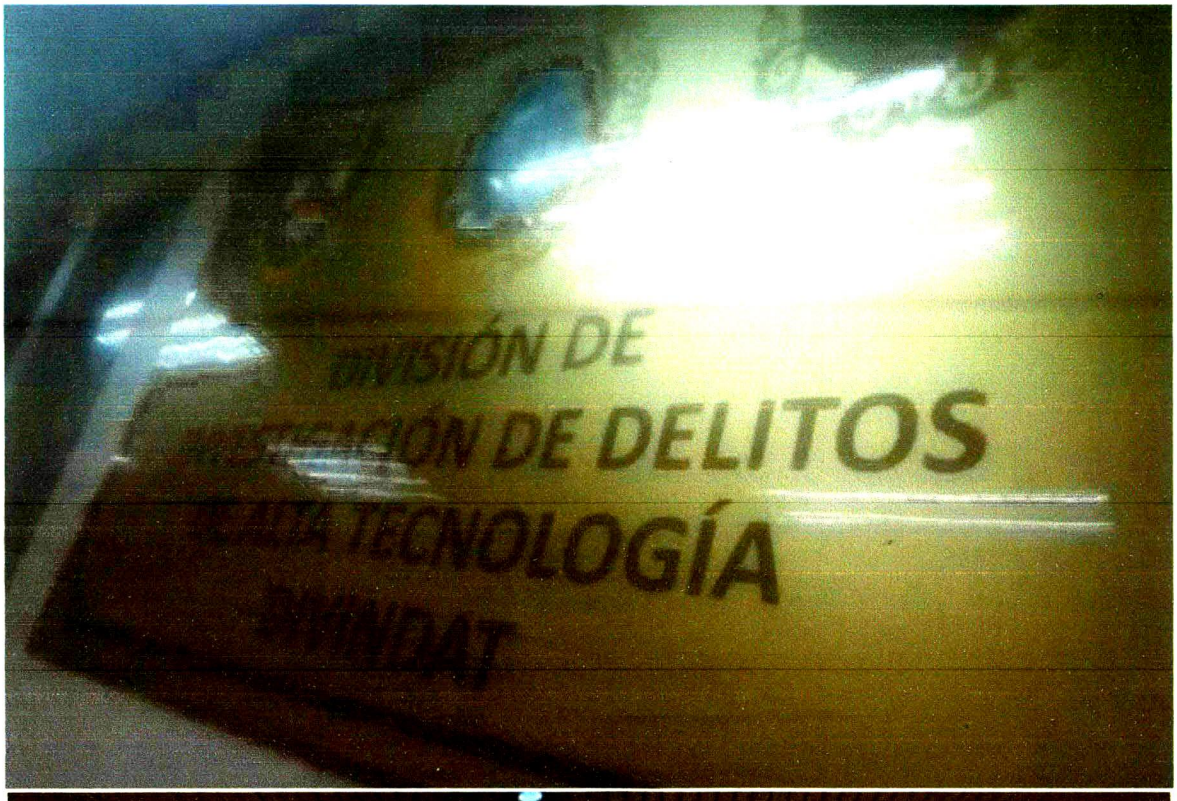
ANEXO Nº 6: Fotos de Entrevistas

Entrevista al Dr. Perca Copa, Hector

Visita a la DIRINCRI - DIVINDAT



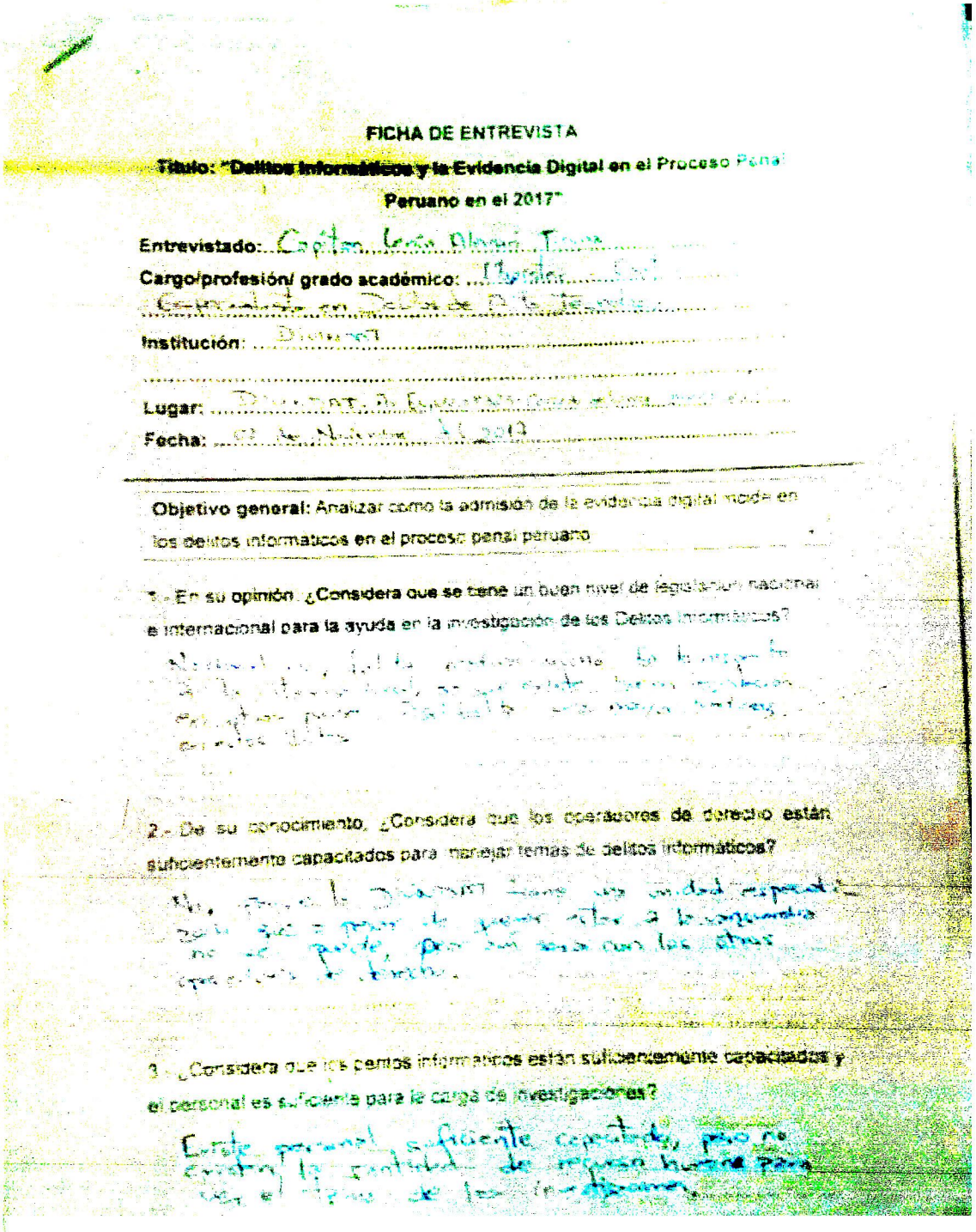
Entrevistas del Capitán Lenin Alemán Ticona y Comandante Manuel Guerrero Zerpa


DIVISIÓN DE
DELITOS
TECNOLOGÍA


DIRINCRI - PNP

ANEXO N° 7: Entrevistas

Entrevista Capitán Lenin Aleman Ticona



FICHA DE ENTREVISTA

Título: "Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017"

Entrevistado: Capitán Lenin Aleman Ticona

Cargo/profesión/ grado académico: Oficial Especialista en Delitos de Alta Tecnología

Institución: DIVINDAT

Lugar: Dirección de Investigación Criminal

Fecha: 02 de Noviembre del 2017

Objetivo general: Analizar como 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?

Si, actualmente existe la Convención de Budapest, que es un convenio internacional para la lucha contra los delitos informáticos.

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

No, porque la DIVINDAT tiene una unidad especializada que se encarga de capacitar a los operadores de derecho, pero no todos los operadores de derecho.

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

Existe personal suficiente capacitado, pero no existe la cantidad de recurso humano para cubrir el mapa de las investigaciones.

4 - ¿Considera que las herramientas utilizadas en la Informática Forense son optimas para la investigación?

Se adolece de herramientas [illegible]
Muchos no están [illegible]
En [illegible] hay deficiencias, [illegible]
mas herramientas.

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

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 [illegible] muchos vacíos [illegible]
En la [illegible] se [illegible] a los
delitos [illegible] de la [illegible]

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

No, esta [illegible] Considero que [illegible] no es
[illegible] por [illegible], sino que hay una evolución
en los [illegible] que hacen que la legislación
[illegible] relacionado.

7 -En su opinión ¿Cree usted que la estructura de la Tipicidad Objetiva en los Delito Informaticos es la adecuada?

No, [illegible] hay [illegible] modalidades nuevas que
no se [illegible] de [illegible] en la legislación
[illegible] por la [illegible] de las mismas.

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

Sí, por ...
todos los ...
Especial...

Objetivo específico 2: Constatar como la ... de Marco ... de la Evidencia Digital repercute en la Tipicidad de los De... en el Proceso Penal Peruano.

9 - ¿Considera que se tiene el conocimiento ... evidencia digital en cuanto a metodología de ...

En la ... sí, en ...
problema ... este ...
suficiente ... los ...

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?

Sí, es sumamente relevante. De ello va depender la decisión del juez o no una prueba.

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

No, porque en ... delitos informáticos ... mayores ... y no es lo mismo tener ... evidencia digital ... una ...

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

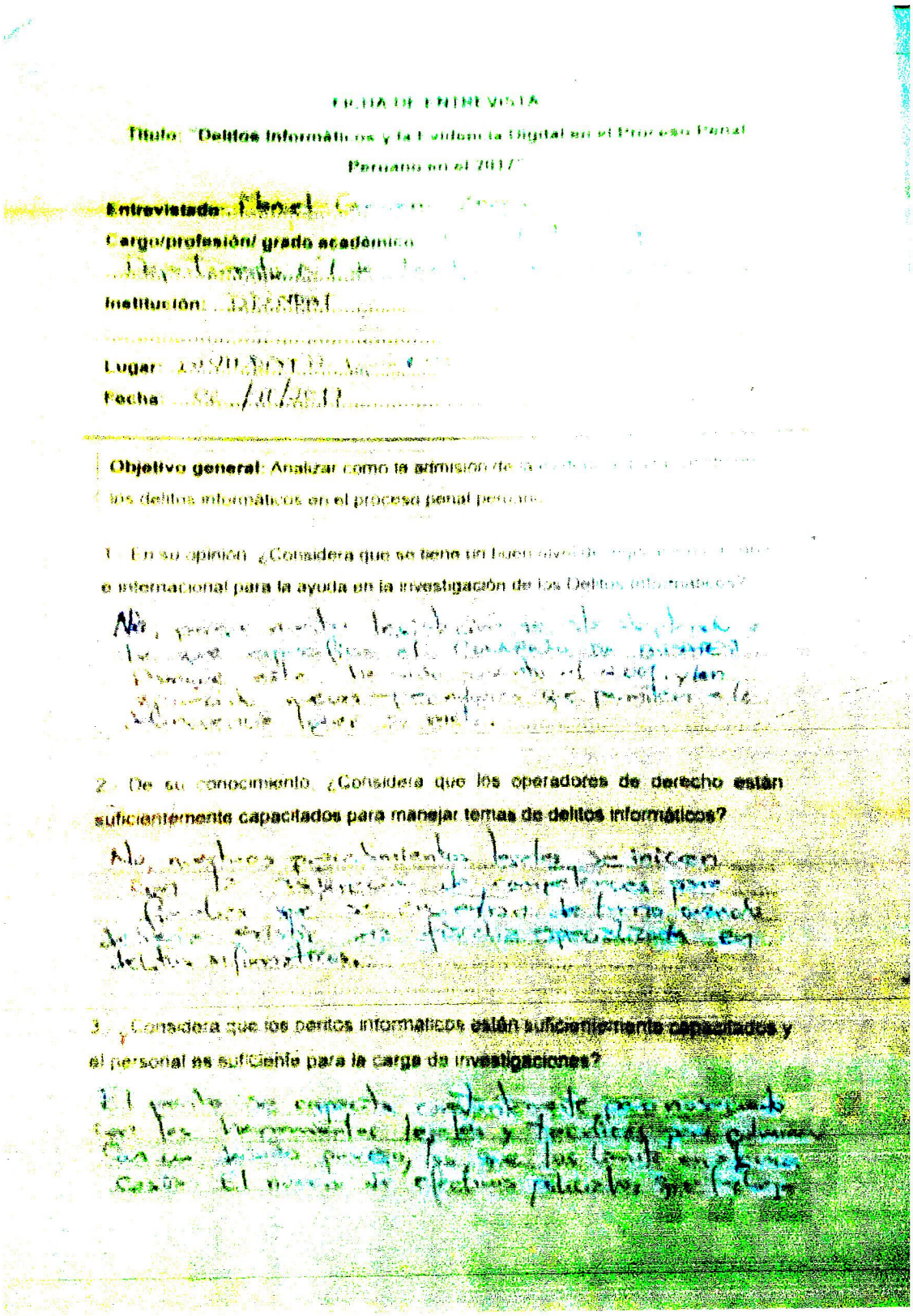
No del todo en realidad. Porque no tienen ... los ... adecuados ...

Que habiendo culminado de manera exitosa la entrevista, se agradece su importante colaboración.

Leyla Keith Rivero Passuni
DNI N° 44757254
ENTREVISTADOR

DNI N

Entrevista Comandante Manuel Guevara Zerpa



FICHA DE ENTREVISTA

Título: "Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017"

Entrevistado: [illegible]

Cargo/profesión/ grado académico

[illegible]

Institución: DIVINDAT

Lugar: [illegible]

Fecha: [illegible]

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

1. En su opinión ¿Considera que se tiene un buen nivel de [illegible] e informacional para la ayuda en la investigación de los Delitos Informáticos?

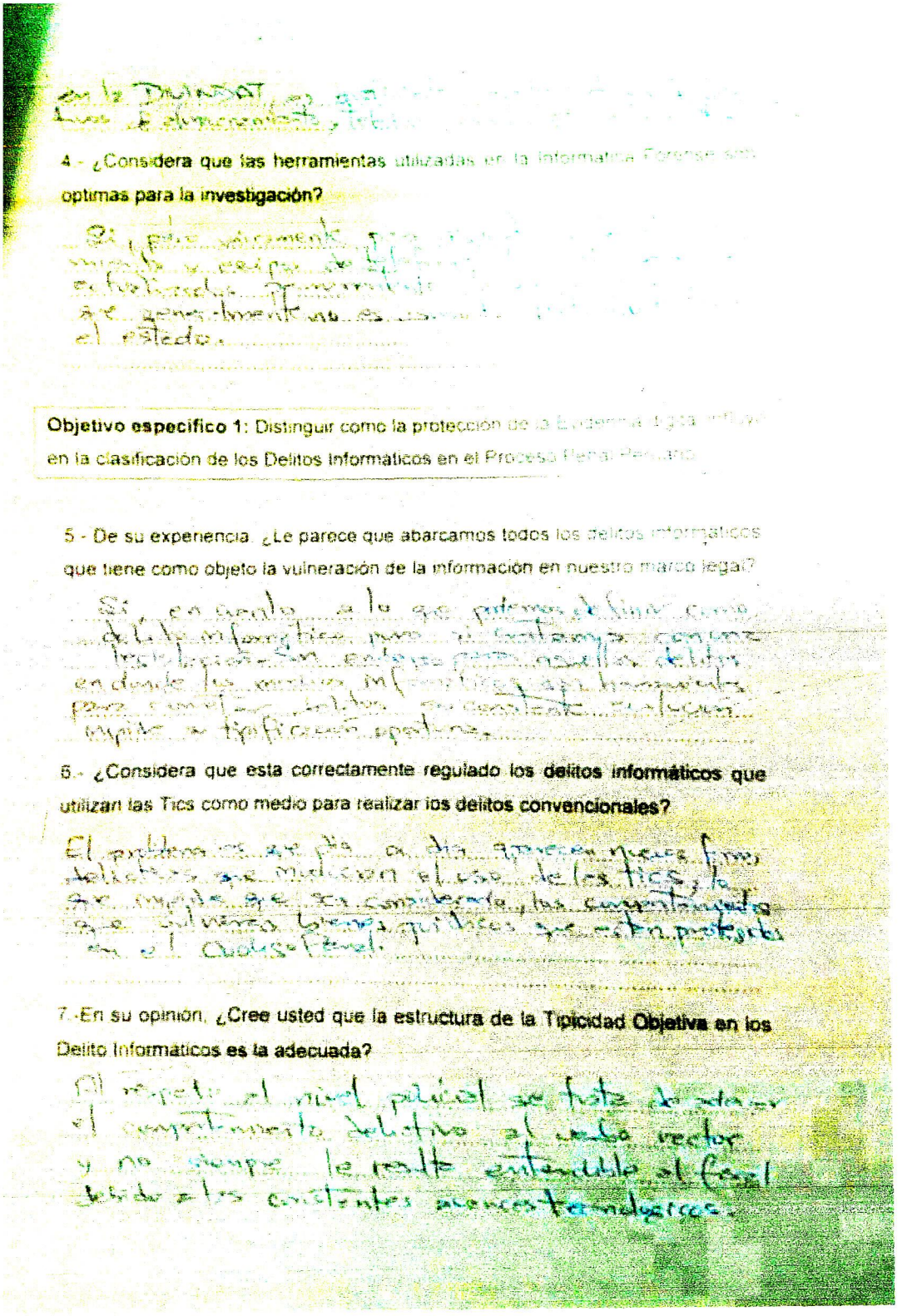
No, porque [illegible]

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

No, porque [illegible]

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

El [illegible]



4 - ¿Considera que las herramientas utilizadas en la Informática Forense son optimas para la investigación?

Si, pero mínimamente ... el estado.

Objetivo especifico 1: Distinguir como la protección de la Evidencia Digital influye en la clasificación de los Delitos Informaticos en el Proceso Penal Peruano

5 - De su experiencia ¿Le parece que abarcamos todos los delitos informaticos que tiene como objeto la vulneración de la información en nuestro marco legal?

Si, en cuanto a lo que podemos definir como ... tipificación apropiada.

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

El problema es que día a día aparecen nuevas formas ... en el Código Penal.

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

Al respecto el nivel policial se forta de saber ... frente a los constantes avances tecnologicos.

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

Objetivo específico 2: Constatar como la determinación de la Cadena de Evidencia Digital repercute en la Tipicidad de los Delitos Informáticos en el Código Penal Peruano.

9 - ¿Considera que se tiene el conocimiento adecuado sobre la cadena de evidencia digital en cuanto a metodología de reconocimiento y recojo?

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

11 - De 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 al proceso penal peruano?

Que habiendo culminado de manera exitosa la entrevista, se agradece su importante colaboración.

Lima 31 de Octubre del 2017

Leyla Keith Rivero Passuni
DNI N° 44757254
ENTREVISTADOR

Nombre y Apellido
DNI N°
ENTREVISTADO

Entrevista Doctora Nilda Roque Gutierrez

FICHA DE ENTREVISTA

Título: "Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017"

Entrevistado: ...

Cargo/profesión/ grado académico: ...

Institución: ...

Lugar: ...

Fecha: ...

Objetivo general: ...

los delitos informáticos ...

1.- En su opinión ¿Considera ... e internacional para la ayuda en la ...

...

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 [illegible] optimas para la investigación?

Objetivo especifico 1: Distinguir como la protección de la Evidencia Digital [illegible] en la clasificación de los Delitos Informáticos en el Ecuador Penal Ecuatoriano

5.- De su experiencia, ¿Le parece que abarcamos [illegible] que tiene como objeto la vulneración de la información en nuestro medio [illegible]

6.- ¿Considera que esta 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 los medios de evidencia sobre el contacto tradicionalmente en la tipicidad subjetiva de los Delitos [illegible]

Sí, se [illegible] contribuye a este [illegible] la criminalidad organizada [illegible] se han cometido los delitos [illegible]

Objetivo especifico 2: Constatar como la [illegible] Evidencia Digital repercute en la Tipicidad de los [illegible] Penal Peruano

9 - ¿Considera que se tiene el conocimiento [illegible] evidencia digital en cuanto a metodología de [illegible]

Considero que [illegible] cuenta con [illegible] Ministerio Público [illegible] Cadena en este tipo de delitos.

10 - De su conocimiento ¿Le parece que es relevante [illegible] informe realizado por los peritos informáticos para la admisión [illegible] digital en el proceso penal?

Es importante importante, para ello se depende que se considere como un medio probatorio.

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

Si, pero en el [illegible] es distorsionado o manipulado.

12 - En su opinion ¿Cree usted que la instrumentalización aplicada en la evidencia digital es la adecuada para su admisión el proceso penal peruano?

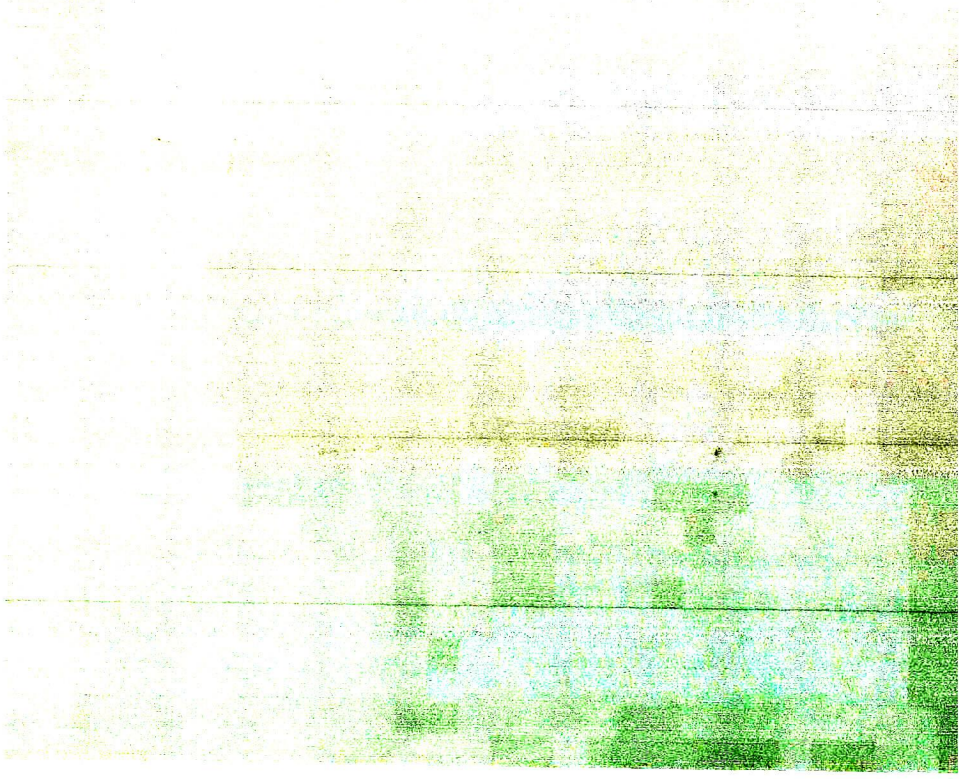
En [illegible] desconoce en que consiste, que utilizan.

Que habiendo culminado de manera exitosa la entrevista, se agradece su importante colaboración.

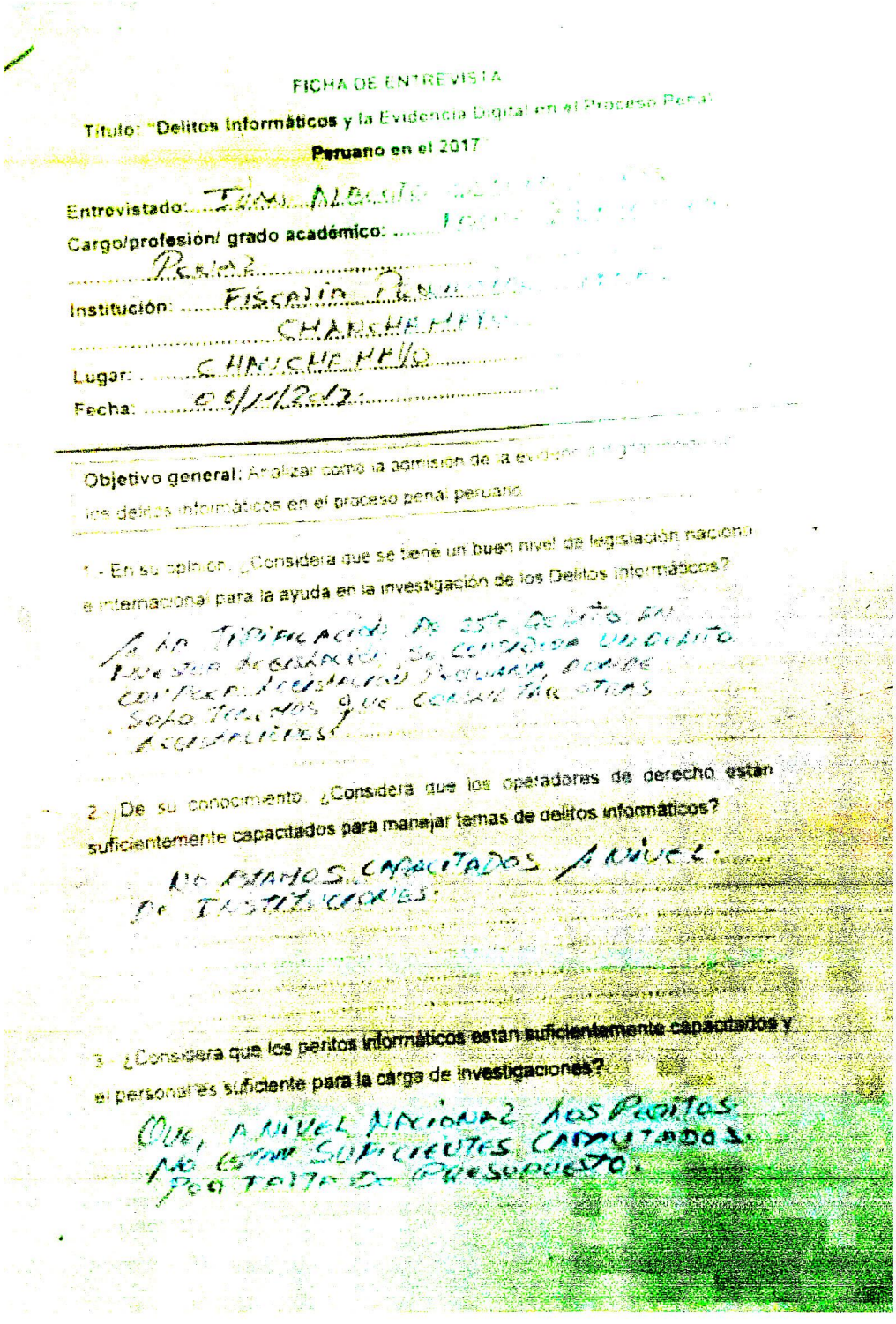
Lima 31 de Octubre de 2017

Leyla Keith Rivero Passuni
DNI N° 44757254
ENTREVISTADOR

Nombre y Apellido
DNI N°
ENTREVISTADO
ABOGADO
CALL N° 624



Entrevista Fiscal Provincial Chanchamayo Tomas Osorio



FICHA DE ENTREVISTA

Título: "Delitos informáticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017"

Entrevistado: TOMAS ALBERTO [illegible]

Cargo/profesión/ grado académico: [illegible] Penal

Institución: FISCALIA [illegible] CHANCHAMAYO

Lugar: CHINCHE PE/O

Fecha: 06/11/2017

Objetivo general: Analizar como la admisión de la evidencia digital [illegible] 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?

SI LA TIPIFICACIÓN DE ESTE DELITO EN PUESTO DE ESTADO SE CONSIDERA UN DELITO CONTRA [illegible] SOLO TENDRÍA QUE CONSULTAR CON ACUERDOS

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

NO ESTAMOS CAPACITADOS A NIVEL DE TIPIFICACIONES

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

QUE A NIVEL NACIONAL LOS PERITOS ESTAN SUFICIENTES CAPACITADOS. NO ESTAN SUFICIENTES POR TEMAS DE PRESUPUESTO.

4 - ¿Considera que las herramientas utilizadas en [illegible] son optimas para la investigación?

EN LA Provincia de [illegible]
Existe Material [illegible]
Tipo Investigación.

Objetivo especifico 1: Distinguir como la protección de la [illegible] en la clasificacion de los Delitos Informaticos en el Proceso Penal Peruano.

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

EN LA Provincia de CHACHAPOYAS
Se han Registrado Pocos casos
Informaticos.

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

NO Porque No Existe un Mecanismo
Adecuado para el uso de
Investigaciones de estos
Delitos.

En su opinion, ¿Cree usted que la estructura de la Tipicidad Objetiva en los lito Informáticos es la adecuada?

SI Es Asi Porque No Existen
un Mecanismo de Aplicación.

7.- De su experiencia, ¿Considera que [illegible] conocido tradicionalmente en la tipicidad [illegible]?

NO EXISTE [illegible]
EN LA CIUDAD [illegible]

Objetivo especifico 2: Constatar como la [illegible] Evidencia Digital repercute en la Tipicidad de los [illegible] Penal Peruano.

9.- ¿Considera que se tiene el conocimiento adecuado [illegible] evidencia digital en cuanto a metodología de reconocimiento [illegible]?

NO EXISTE LOS MEDIOS TECNICOS ADECUADOS.

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?

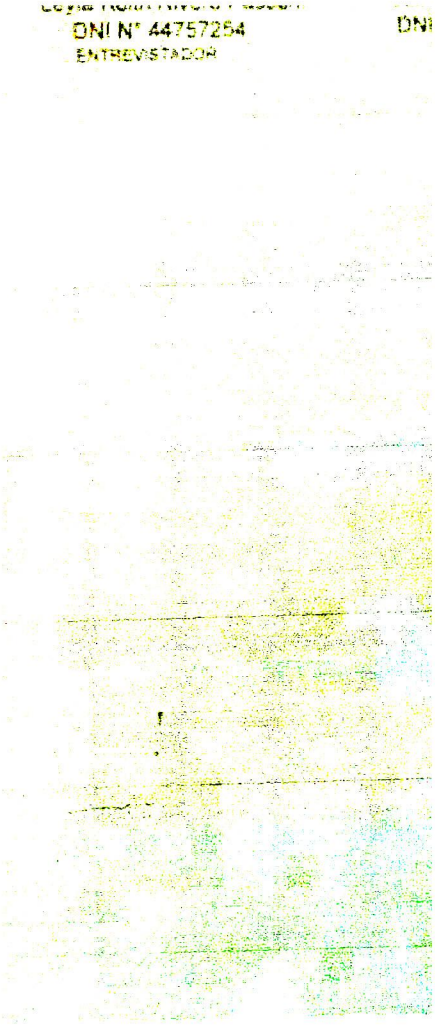
NOS FALTA MAS CAPACITACIÓN Y LOGISTICA.

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

SI PERO NOS FALTA CAPACITACION.

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

NO SE OPERA EN LA PROVINCIA DE CHANCHAMAYO.


DNI N° 44757254
ENTREVISTADOR

Entrevista Doctora Marjorie Alvarado Alvarado

FICHA DE ENTREVISTA

Título: "Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017"

trevistado:

rgo/profesión/ grado académico

itución:

gar:

cha:

bjetivo general: Analizar

s delitos informáticos en el

En su opinion, ¿Considera que se tiene un buen

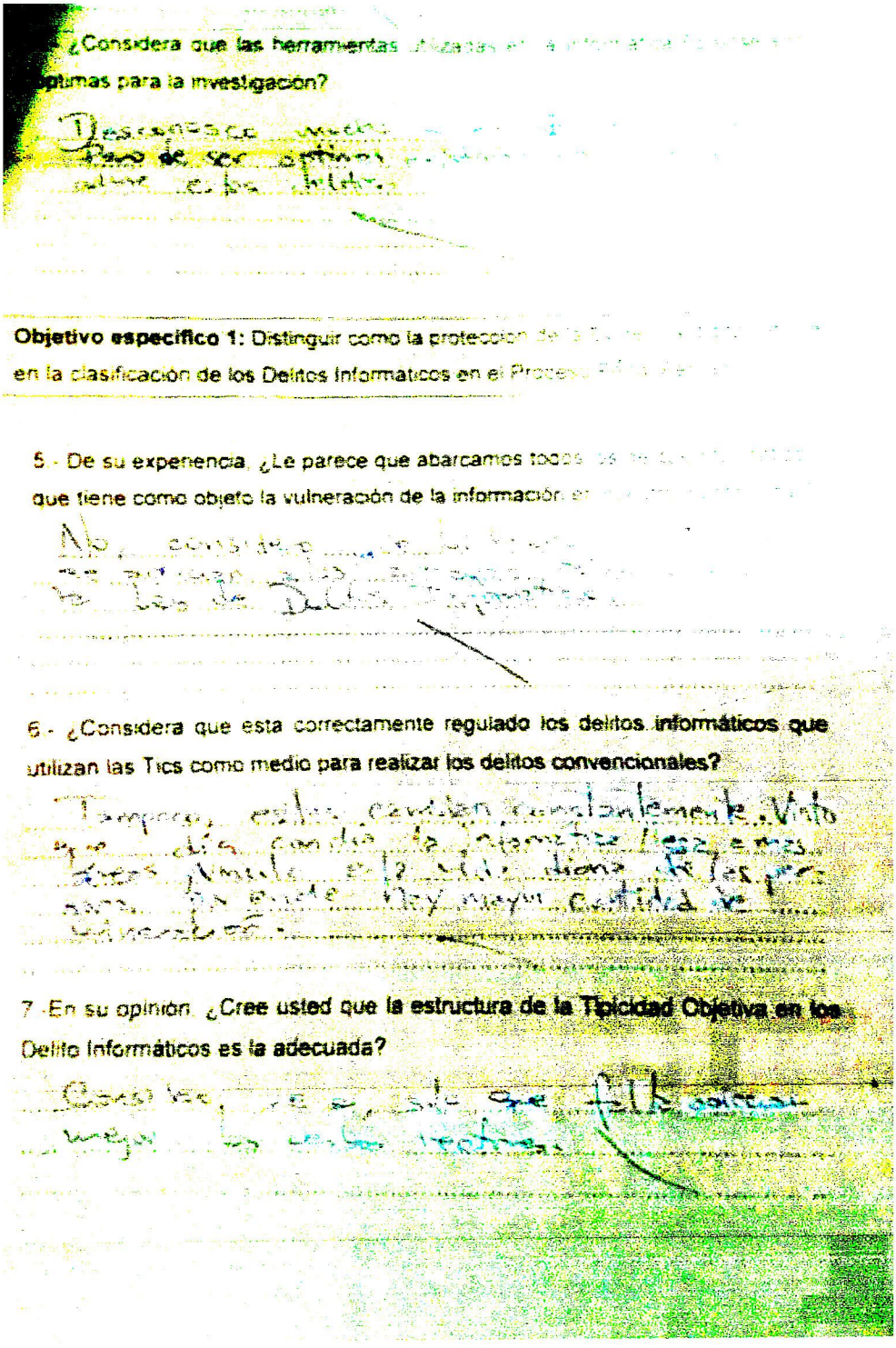
nternacional para la ayuda en la investigación de

De su conocimiento, ¿Considera que los operadores de derecho están

cientemente capacitados para manejar temas de delitos informáticos?

¿Considera que los peritos informáticos están suficientemente capacitados y

rsonal es suficiente para la carga de investigaciones?



¿Considera que las herramientas [illegible] óptimas para la investigación?

Objetivo específico 1: Distinguir como la protección [illegible] en la clasificación de los Delitos Informáticos en el Proce[illegible]

5.- De su experiencia, ¿Le parece que abarcamos todos [illegible] que tiene como objeto la vulneración de la información [illegible]

6.- ¿Considera que esta 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?

Se ha mejorado la ... en base ... teóricas y dele...

Objetivo específico 2: Constatar como la determinación del Marco Legal de la Evidencia Digital repercute en la Tipicidad de los Delitos Informáticos en el Código Penal Peruano.

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

Considero que ... no ... del tema

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?

Es fundamental ... sin ... no hay evidencia física ... no hay pruebas ... del ...

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

Si es el necesario ... el manejo de la ... no ... sobre ... digital

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

No tengo ... necesario ... tiene ... instrumentalización ...

Que habiendo culminado de manera exitosa la entrevista, se agradece su importante colaboración.

Lima, 31 de Octubre del 2017

Leyla Keith Rivero Passuni	Nombre y Apellido
DNI N° 44757254	DNI N°
ENTREVISTADOR	ENTREVISTADO

ABOGADA
Reg. C.A.L. N° 88586

Entrevista Doctor Julio Cesar Ramirez Ramirez

FICHA DE ENTREVISTA

Titulo: "Delitos Informaticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017"

Entrevistado: ....Dr. Julio ....

Cargo/profesión/ grado académico: ....Fiscal ....

Institución: ....Fiscalia....

Lugar: ....LIMA....

Fecha: ....09/6/2017....

Objetivo general: Analizar como la ... los delitos informáticos en el proceso ...

1.- En su opinión ¿Considera que se tiene ... e internacional para la ayuda en la investigación de los ...

No ... Sin ...

2.- De su conocimiento ¿Considera que los operadores de derecho están suficientemente capacitados para manejar temas de delitos informáticos?

Suficientemente ... Conocimiento sobre estos temas.

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

Lamentablemente hay demora en la elaboración de las Pericias ... y esto es reflejo de ... personal.

4.- ¿Considera que las herramientas utilizadas en la informática forense son óptimas para la investigación?

Considero que no son las optimas.

Objetivo especifico 1: Distinguir como la protección [illegible] en la clasificación de los Delitos Informáticos en el Proceso Penal [illegible]

5.- De su experiencia, ¿Le parece que abarcamos todo [illegible] que tiene como objeto la vulneración de la información [illegible]

Considero que no [illegible]

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

No, este tipo de [illegible] tiene cada vez mayor [illegible]

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

Considero que [illegible] la realidad [illegible] carga de legislarse [illegible]

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

Considero que [illegible] en lo que en los delitos [illegible] entendemos como tentativa [illegible] delito consumado [illegible]

Objetivo específico 2: Constatar como la determinación [illegible] Evidencia Digital repercute en la Tipicidad de los Delitos Informáticos [illegible] Penal Peruano.

9.- ¿Considera que se tiene el conocimiento adecuado sobre [illegible] evidencia digital en cuanto a metodología de reconocimiento y [illegible]

Considero [illegible] [illegible] y completamente [illegible]

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

Es fundamental. Sin un buen análisis no [illegible] tener una evidencia [illegible] para [illegible] considerado como prueba.

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

[illegible] [illegible] detallado en la [illegible] por ejemplo [illegible]

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

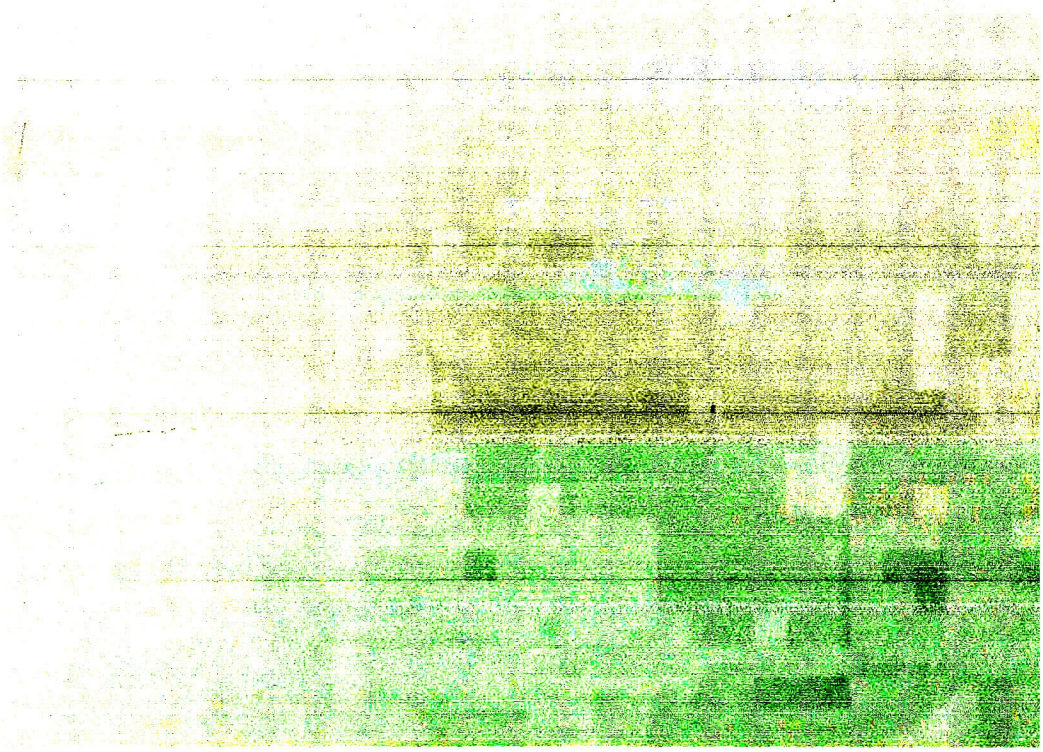
No [illegible] detalladamente [illegible] instrumentalización [illegible] para [illegible]

Que habiendo culminado de manera exitosa la entrevista [illegible]
importante colaboración.

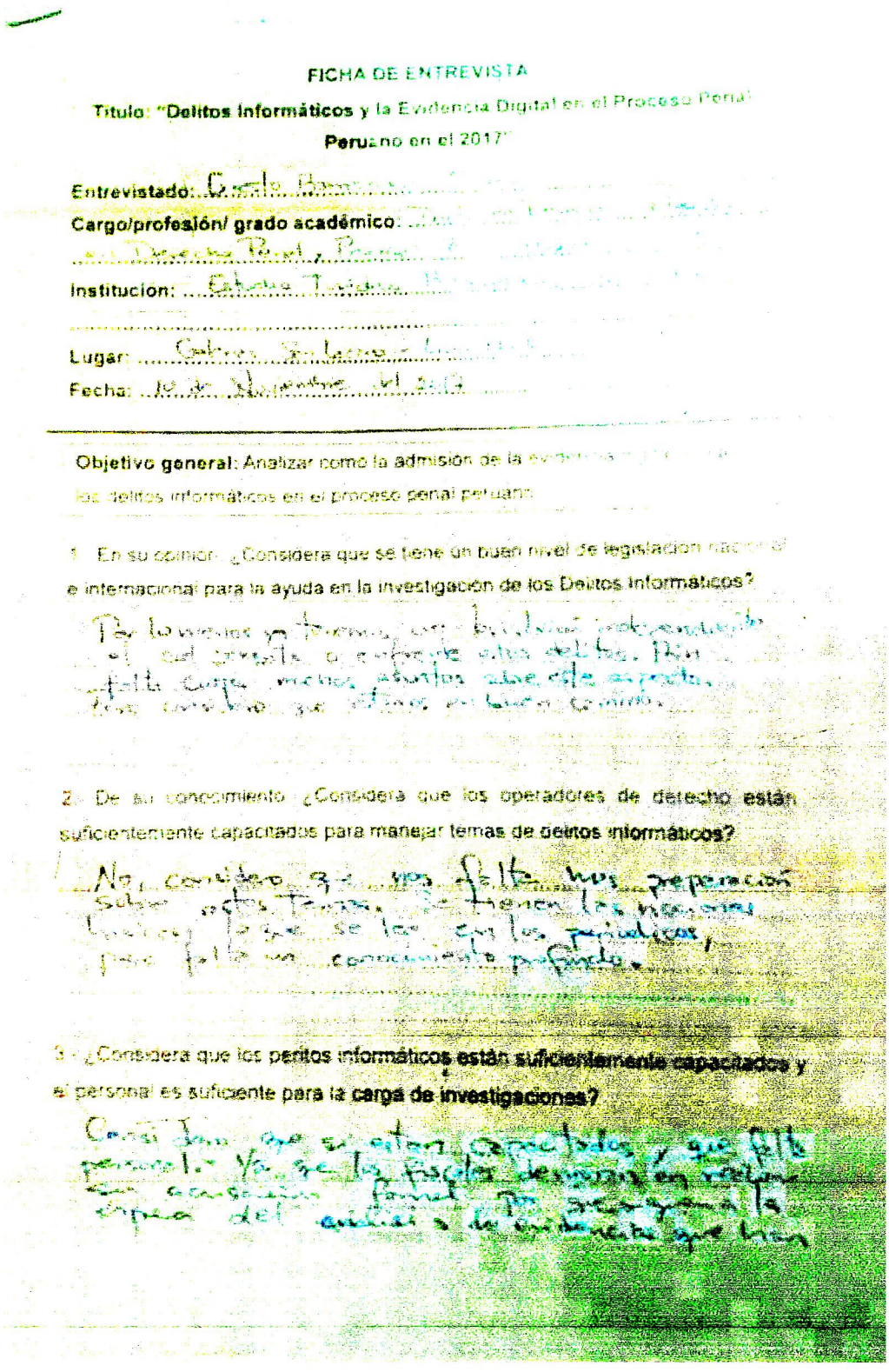
Lima, 31 de Octubre del 2017

Leyla Keith Rivero Passuni
DNI N° 44757254
ENTREVISTADORA

Nombre y Apellido
DNI N°
ENTREVISTADO



Entrevista Doctor Ernesto Barrionuevo Azaña



FICHA DE ENTREVISTA

Titulo: "Delitos informáticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017"

Entrevistado: Ernesto Barrionuevo

Cargo/profesión/ grado académico: Abogado Derecho Penal y Procesal Penal

Institucion: Estudio Jurídico

Lugar: Cabrera, Barranco - Lima

Fecha: 10 de Noviembre del 2017

Objetivo general: Analizar como la admisión de la evidencia digital 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?

Por lo menos en Perú, creo que la ley está cumpliendo el rol correcto a enfrentar estos delitos. Pero falta cubrir muchos asuntos sobre este aspecto, pero creo que vamos en buen camino.

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

No, considero que nos falta mas preparación sobre estos temas, se tienen los mismos cursos pero solo en los periodicos, pero falta un conocimiento profundo.

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

Creo que no están capacitados y que falta personal. Ya que la fiscalía recurre en varias ocasiones a peritos de empresas privadas para que apoyen a la investigación que llevan

¿Considera que las herramientas utilizadas en la Informática Forense son óptimas para la investigación?

Objetivo especifico 1: Distinguir como la protección [illegible] en la clasificación de los Delitos Informáticos en el Proceso Penal

5.- De su experiencia ¿Le parece que abarcamos todos los [illegible] que tiene como objeto la vulneración de la información en [illegible]

6.- ¿Considera que esta 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?

Si, definitivamente ... [illegible] el Aspecto ... [illegible] en estos temas ... [illegible]

Objetivo específico 2: Constatar como la determinación ... [illegible] Evidencia Digital repercute en la Tipicidad de los Delitos ... [illegible] Penal Peruano.

9.- ¿Considera que se tiene el conocimiento adecuado ... [illegible] evidencia digital en cuanto a metodología de reconocimiento ... [illegible]

Considero que se está ... [illegible] los procedimientos por los ... [illegible] ... [illegible]

10.- De su conocimiento, ¿Le parece que es relevante la ca[illegible] informe realizado por los peritos informáticos para la admisión de la evidencia digital en el proceso penal?

Es fundamental el análisis de los peritos ... determinar el tracurso de un proceso, no es solo recolectar la evidencia, sino su correcto análisis.

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

Considero que debe estar normado como ley o dentro de un código ... tener mayor manejo de las evidencias y su [illegible]

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

Desconozco sobre la instrumentalización ... Pero debe ser la adecuada sino se [illegible]

Que habiendo culminado de manera exitosa la entrevista, se agradece su importante colaboración.

Lima, 31 de Octubre del 2017

ERNESTO BARRIONUEVO CACHAY
ABOGADO
C.A.L. 65588

Leyla Keith Rivero Passuni
DNI N° 44757254
ENTREVISTADOR

Nombre y Apellido
DNI N°
ENTREVISTADO

Entrevista Master Jose Luis Pazzoni Veramendi

FICHA DE ENTREVISTA

Titulo: "Delitos informáticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017"

Entrevistado: Jose Luis Pazzoni Veramendi

Cargo/profesión/ grado académico: Abogado Penalista

Institución: Estudio Jurídico

Lugar: Cabo San Lucas

Fecha: 10 de Noviembre del

Objetivo general: Analizar como la admisión de la evidencia digital en los delitos informaticos en el proceso penal peruano

1.- En su opinion ¿Considera que se tiene un buen convenio internacional para la ayuda en la investigación de los delitos informáticos?

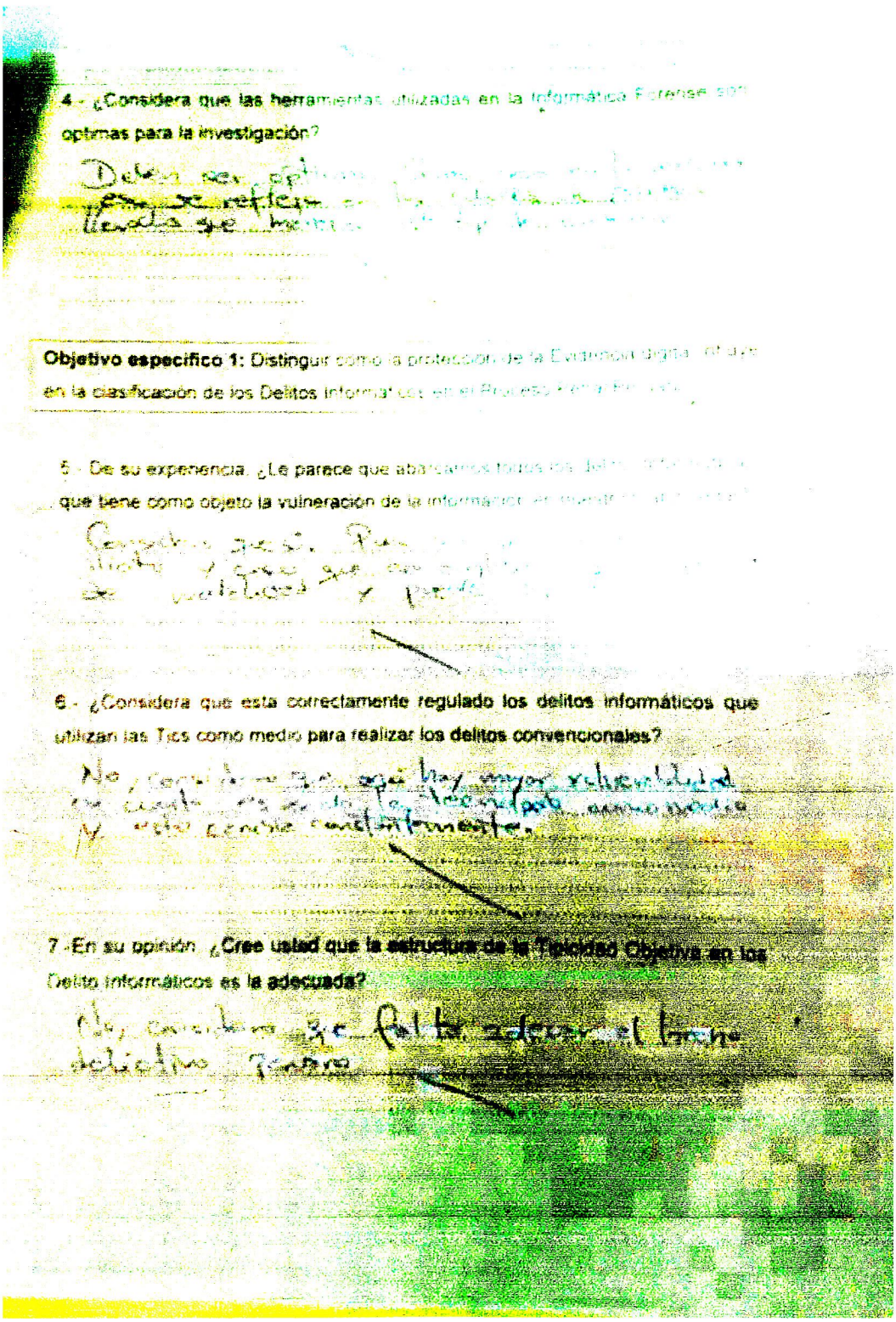
Considero que no, en esta era muy rapidamente. En la actualidad en nuestra legislación sobre este tema.

2.- De su conocimiento ¿Considera que los operadores de derecho están suficientemente capacitados para manejar temas de delitos informáticos?

No, falta mayor conocimiento sobre este tema. Capacitaciones, cursos, especializaciones. En la parte academica desarrollarlo extensamente.

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

No hay personal suficiente. Considero que los peritos si estan capacitados, pero no tienen herramientas y si las tienen estan obsoletas.



4 - ¿Considera que las herramientas utilizadas en la Informática Forense son optimas para la investigación?

Objetivo especifico 1: Distinguir como la protección de la Evidencia Digital influye en la clasificación de los Delitos Informáticos en el Proceso Penal Peruano

5 - De su experiencia, ¿Le parece que abarcamos todos los delitos que bene como objeto la vulneración de la información

6 - ¿Considera que esta 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?

Sí, existe una evolución normativa y en

Objetivo especifico 2: Constatar como la determinación del Marco ... de la Evidencia Digital repercute en la Tipicidad ... Penal Peruano.

9.- ¿Considera que se tiene el conocimiento ... evidencia digital en cuanto a metodología de ...

No lo creo. Falta una ... para procedimiento ...

10.- De su conocimiento ¿Le parece que es relevante la ... informe realizado por los peritos informáticos para la admisión de la evidencia digital en el proceso penal?

Sí, es relevante en todo aspecto. Un buen informe pericial como puede ser la evidencia digital.

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

Considero que es relevante es más que suficiente. Hay se debería cumplir un capítulo únicamente sobre evidencia digital.

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

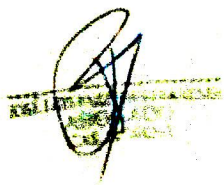
No sabría decirte sobre este aspecto. Desconozco.

Que habiendo culminado de manera exitosa la entrevista, se agradece su importante colaboración.

Lima, 31 de Octubre del 2017

Leyla Keith Rivero Passuni
DNI N° 44757254
ENTREVISTADOR

Nombre y Apellidos
DNI N°



Entrevista Magister Hector Perca Copa

FICHA DE ENTREVISTA

Título: "Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017"

Entrevistado: ...Hector...

Cargo/profesión/ grado académico: ...Fiscal Penal - Je...

Institución: ...Cabana...

Lugar: ...Cabana Sanchez...

Fecha: ...10 de Noviembre...

Objetivo general: Analizar como la admisión de la ... los delitos informáticos en el proceso penal peruano

1.- En su opinión, ¿Considera que se tiene un buen ... e internacional para la ayuda en la investigación de los ...

...No existen muchos cursos sobre los delitos informáticos. Es importante ... para capacitar todos los años de capacitación hacia ... Ministerio Público existe, pero esta no ... para la investigación de ...

2.- De su conocimiento ¿Considera que los operadores de derecho están suficientemente capacitados para manejar temas de delitos informáticos?

...No, considero que a pesar de ... de Litigante ... falta capacitación sobre estos delitos ... Pocos ... pero ... y ... a nivel ...

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

...Considero que no, pero en ... los ... cuentan ... rápido que ... para ... de ... siempre ... personal, ...

es es la usual.

4.- ¿Considera que las **herramientas** utilizadas en la informatica Forense son optimas para la investigación?

No conozco sobre las

Objetivo especifico 1: Distinguir como la protección de la [illegible] en la clasificación de los Delitos Informáticos en el Proceso Penal Peruano

5.- De su experiencia, ¿Le parece que abarcamos todos los [illegible] que tiene como objeto la vulneración de la información en nuestro [illegible]

Considero que si, pero falta [illegible]

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

No, sobre este aspecto no se conoce mayor complejidad ya que es [illegible] y siempre la misma cantidad de delitos [illegible]

7.-En su opinión ¿Cree usted que la estructura de la Tipicidad Objetiva en los Delito informaticos es la adecuada?

Considero que si, esto no varia es la misma para los diferentes delitos.

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

En este aspecto
texto sobre el
se especializa
Contaremos. Si he

Objetivo específico 2: Constatar como la determinación del Marco Legal de la Evidencia Digital repercute en la Tipicidad de los Delitos Informáticos en el Proceso Penal Peruano

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

Sobre evidencia física sí, sobre
digital no. Porque muchos
manejarla no capacita en
una ventaja para los llamados

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

Todo análisis pericial debe ser hecho cautelosa-
mente y lo más claro y conciso posible, sino
de que estamos hablando. No existe proceso sólido. Es fundamental

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

No solo es un mero reglamento. Eso si debería
estar en el código penal y

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

Desconozco sobre ese aspecto pero lo
es relevante contar al momento de la

Que habiendo culminado de manera exitosa la entrevista, se agradece su importante colaboración.

Lima 31 de Octubre del 2017

HECTOR J. PERCA COPA
ABOGADO
REG. CAL. N° [illegible]

Leyla Keith Rivero Passuni
DNI N° 44757254
ENTREVISTADOR

Nombre y Apellido
DNI N°
ENTREVISTADO

Entrevista Magister Marino Hernández Carrasco

FICHA DE ENTREVISTA

Título: "Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017"

Entrevistado: Dr. Mauro Hernández Carrasco

Cargo/profesión/ grado académico: Egresado de Doctorado en Gestión Pública

Institución: Universidad Cesar Vallejo

Lugar: Los Olivos

Fecha: 28/4/2015

Objetivo general: Analizar como la admisión de la evidencia digital influye 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, actualmente hay una unidad especializada en la Dirincri de Delitos Informáticos, no hay una legislación actualizada, teniendo en cuenta que no existe una veracidad en los procesos. Teniendo en cuenta que en la práctica no hay mucha capacitación por parte de la sociedad, falta especialistas.

2 - De su conocimiento ¿Considera que los operadores de derecho están suficientemente capacitados para manejar temas de delitos informáticos?

No, Porque en los Delitos Informáticos los operadores Jurídicos utilizan plantillas y no proyectos elaborados.

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

Los Peritos Informáticos están suficientemente capacitados pero los operadores Judiciales no lo están.

¿Considera que las herramientas [illegible] óptimas para la investigación?

Dependiendo que se va investigar, como se genera la generación de tecnología de punta para delitos a nivel nacional e internacional de información.

Objetivo específico 1: Distinguir como la protección de la [illegible] en la clasificación de los Delitos Informáticos en el Proceso Penal [illegible]

5. De su experiencia, ¿Le parece que abarcamos todos los delitos [illegible] que tiene como objeto la vulneración de la información en nuestra [illegible]

No de los delitos informáticos actualmente existen tipificados en nuestra novatina en nuestra legislación del Código Penal.

6.- ¿Considera que esta 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?

Los Delitos Informáticos que existen están actualmente tipificados.

8.- De su experiencia, ¿Considera que ha existido una evolución en el concepto tradicionalmente en la tipicidad subjetiva de un delito

Sí, ya que ha adquirido como [illegible] Sexuales a menor de edad ya [illegible] antes no lo estaban en nuestro [illegible]

Objetivo específico 2: Constatar como la determinación de la Evidencia Digital repercute en la Tipicidad de los Delitos Informá[illegible] Penal Peruano

9.- ¿Considera que se tiene el conocimiento adecuado sobre e[illegible] evidencia digital en cuanto a metodología de reconocimiento y reco[illegible]

Considero que los operadores de justicia [illegible] a los profesionales para poder [illegible] estas pruebas digitales

10.- De su conocimiento, ¿Le parece que es relevante la calidad de anális[illegible] informe realizado por los peritos informáticos para la admisión de la evide[illegible] digital en el proceso penal?

Es sumamente importante ya que dilucida existen penas para los delitos informáticos

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

Es importante que es necesario el marco legal para sustentar los medios probatorios

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

Claro ya que es una prueba instrumental para la admisión el proceso penal peruano.

Que habiendo culminado de manera exitosa la entrevista, se agradece su importante colaboración.

Lima, 31 de Octubre del 201

ABOGADO
Reg. CAL 27880

Leyla Keith Rivero Passuni
DNI N° 44757254
ENTREVISTADOR

Nombre y Apellido
DNI N°
ENTREVISTADO

Entrevista Abogado Mery Vega Hinostroza

FICHA DE ENTREVISTA

Título: "Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017"

Entrevistado: Mery Vega Hinostroza

Cargo/profesión/ grado académico: Abogada

Institución: Estudio Jurídico "Mery Vega H"

Lugar: JR. ARICA #184 LA MERCED - CHYO

Fecha: 2017.

064-532291 998072665

Objetivo general: Analizar como 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?

La legislación nacional Regula comercial y penalmente las conductas ilicitas relacionados con la informatica. pero aun no contemplan en sus delitos informaticos. La legislacion internacional se basa en los tratados internacionales. El Perú es parte en tal razon puede recurrir a aquellos tratados. Todo evidencia mara de acuerdo al problema.

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

El operador juridico tiene que conocer todos los aspectos informaticos, telecomunicaciones, entre otros, ya que para investigar un delito informatico debe contar con personal calificado y conocedor del sistema informatico y tener peritos Forenses.

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

En nuestro país, existen peritos de todas las especialidades. El perito Informático si los preparados y conoce su campo será de gran aporte, pero tiene q' trabajar con abogados, ceber policial. Ademas

El Juez también tiene q' conocer todo lo referente al sistema Informática para un debido Proceso y una sentencia justa.

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

Sirven para lograr una Investigación en el uso de las Computadoras. Todo va evolucionando Gracias al avance de la tecnología como por ejemplo: El SOFTWARE DE ANALISIS FORENSE, se usa cuando falla la computadora, recupera información perdida o borrada por completo y la mejor en Programas Forenses. Plaing Sleuth con esta podemos conocer la computadora, sistema, Discos Duros etc.

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

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 ya q' cada región Tiene su propia problemática y legislación. Los más conocidos son: Estafas Extorsión, Robo de servicios, distribución de Virus, Robo de propiedad intelectual, Fraude, pornografía infantil, acceso no autorizado; en el Perú en el nivel medio, ahora se ha incrementado el % delincuencial en la informática.

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

Los delitos informáticos es por el mal uso de las tecnologías de la información y el mal uso de las TICS que usan para conocimientos para fines destructivos o delictivos. El Delincuente, el criminal se esconde, borra las pruebas. Los delitos convencionales la entre delincuentes y victimas se lleva a cabo en todo tiempo y lugar.

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

La tipicidad objetiva ve el delito de intrusismo informático. El Estado protege el patrimonio contenida en la base de datos (Bien Jurídico protegido) Agravante del delito con el fin de obtener un beneficio económico El sujeto pasivo (persona natural y/o jurídica Titulares de la Base de datos).

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

Se requiere que el comportamiento sea realizado con dolo (de dar consciencia y voluntad de cometer el delito. La tipicidad la expresamente para estos delitos. Penal Ley Especial.

Objetivo específico 2: Constatar como la determinación del Marco Legal de la Evidencia Digital repercute en la Tipicidad de los Delitos Informáticos en el Proceso Penal Peruano

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

Por supuesto que no, pero para el estudio se tiene diferencia el elemento de un sistema informático (es la evidencia electrónica) y la información contenida en este (es la evidencia) digital. La de reconocimiento es el procesador de ensayos ordena y encamina

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? El tipo de investigación

Es importante, ya q' ellos darán la prueba informática de aplicación en el aspecto penal, para q' el juez decida la culpabilidad o la inocencia del Imputado o sujeto activo. Ejm: Delitos de Pornografía infantil en internet, prop. privada, protección de datos personales y otros

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

Si, ya que está es una evidencia física, cuando se confiara con una documental. Es frágil ya q' una copia de un dcto. almacenado en un archivo es idéntica al original, no deja rastro que deje la copia.

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

Para ser utilizada como evidencia digital se requiere de conocimiento profundo en la materia, para saber como fue creado, se puede falsificar. Que información se

perder. Qué puede ocurrir mal. Para el Perito Informático para su información. Con un buen asesor, la misma que será usada con justicia.

Que habiendo culminado de manera exitosa la entrevista, se agradece su importante colaboración.

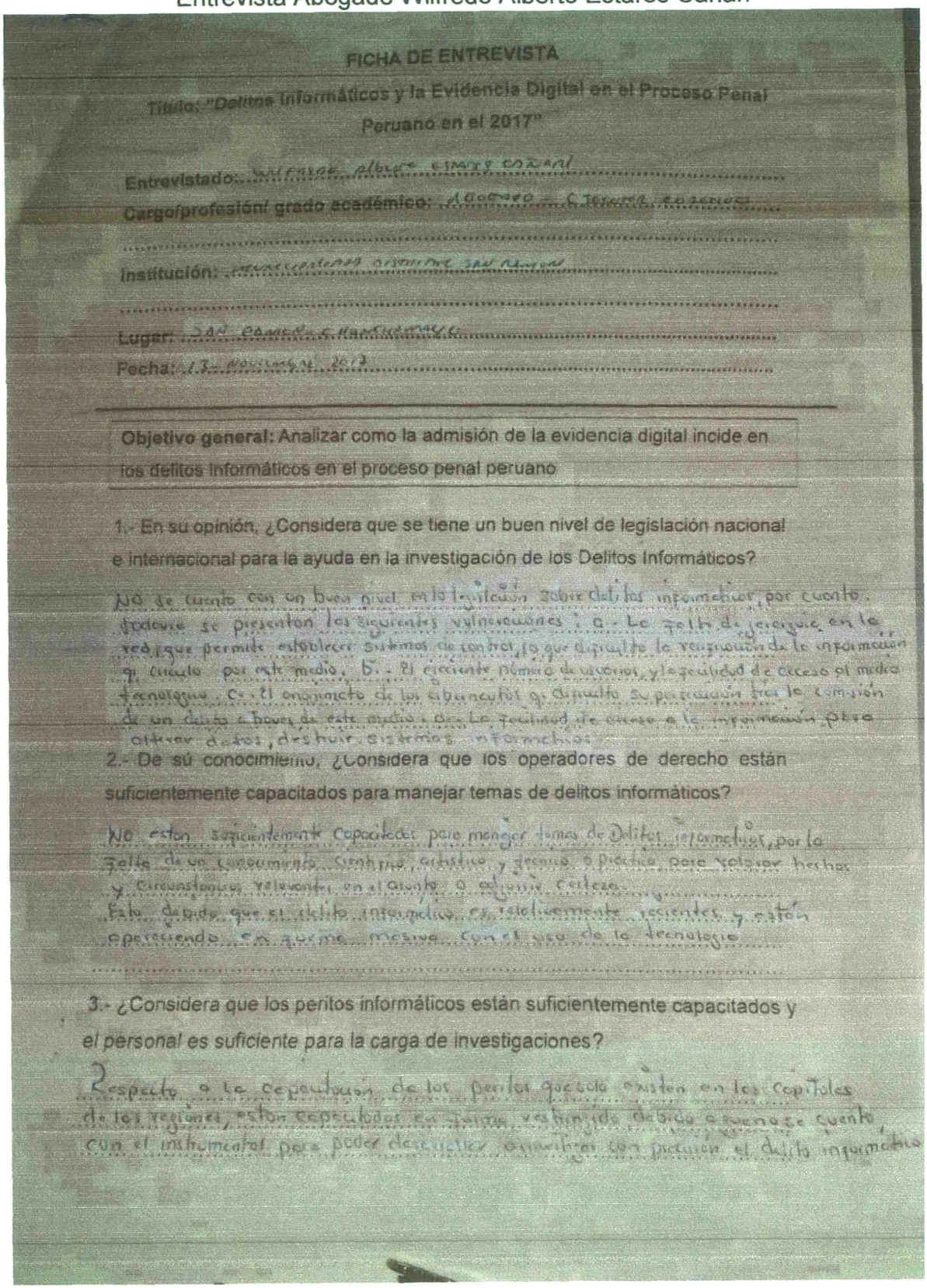
Lima, 31 de Octubre del 2017

Mery Vega Hinostroza
ABOGADO
Reg. C.A.J. 3508

Leyla Keith Rivero Passuni
DNI N° 44757254
ENTREVISTADOR

Nombre y Apellido:
DNI N° 20549653
ENTREVISTADO

Entrevista Abogado Wilfredo Alberto Estares Cañari



FICHA DE ENTREVISTA

Título: "Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017"

Entrevistado: wilfredo alberto estares cañari

Cargo/profesión/ grado académico: abogado - ciencias sociales

Institución: universidad privada san pedro

Lugar: san pedro - chimbote

Fecha: 13 - noviembre - 2017

Objetivo general: Analizar como 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 se cuenta con un buen nivel en la legislación sobre delitos informáticos, por cuanto todavía se presentan las siguientes vulneraciones: a.- La falta de cerrojos en la red, que permite establecer sistemas de control, lo que dificulta la recuperación de la información q. circula por este medio. b.- El creciente número de usuarios y la facilidad de acceso al medio tecnológico. c.- El anonimato de los delincuentes q. dificulta su persecución tras la comisión de un delito a través de este medio. d.- La facilidad de acceso a la información para obtener datos, destruir sistemas informáticos.

2.- De sú conocimiento, ¿Considera que los operadores de derecho están suficientemente capacitados para manejar temas de delitos informáticos?

No estan suficientemente capacitados para manejar temas de delitos informáticos, por la falta de un conocimiento científico, técnico y jurídico o práctico para valorar hechos y circunstancias relevantes en el cuanto a obtener certeza.

Esto debido que el delito informático es relativamente recientes y están operando en forma masiva con el uso de la tecnología

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

Respecto a la capacitación de los peritos que solo existen en los capitales de las regiones, estan capacitados en forma vertical debido a que no se cuenta con el instrumental para poder descubrir criminales con picardia el delito informatico

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

La informática forense implica un conjunto de técnicas y métodos de investigación, que permite reconstruir, lo más fielmente posible, la secuencia de eventos que tuvieron lugar, con la ayuda de equipos informáticos de última generación digital, que se cuenta parcialmente.

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

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?

Con la de la ley N° 30096 y su modificatoria, se esta pretendiendo abarcar los delitos informáticos, pero se inicio en forma genérica y cronológica, por cuanto con el avance de la tecnología van dando se nuevas formas delictivas, lo que conlleva que tenemos que avanzar de igual con la tecnología.

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

No estan correctamente regulados los Delitos Informaticos, si bien los nuevos herramientas que ofrecen las Tic al servicio del hombre estan relacionadas con la transmision, procesamiento y almacenamiento digitalizado de informacion, asi como un conjunto de procesos y productos que simplifican la comunicacion y hacen mas viables la interaccion entre las personas. El desarrollo de la tecnologia tambien ha dado consigo nuevas formas delictuales q tienen por medio y/o finalidad los sistemas informaticos e internet.

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

No esta adecuado, debido al avance tecnologico, ya que por medio de la tipicidad objetiva se busca proteger el bien juridico.

Por tanto, en este tipo de delitos nose puede establecer ala informacion como el unico bien juridico afectado, por ser el principal y el más importante, sino un conjunto de bienes que son afectados, debido a la caracteristica de la conducta tipica en esta modalidad delictiva que colisiona con diversos intereses colectivos

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

Que el sujeto activo en esta modalidad delictual viene evolucionado porque se requiere ciertos habilidades y conocimientos en el manejo del sistema informatico que tienen como caracteristicas: - Poseer importantes conocimientos informaticos. - Ocupar lugares estrategicos en su centro laboral, en los que se maneja información de caracter sensible. No son delincuentes comunes y corrientes sino q. por el contrario son personas especializadas en la materia informatica

Objetivo específico 2: Constatar como la determinación del Marco Legal de la Evidencia Digital repercute en la Tipicidad de los Delitos Informáticos en el Proceso Penal Peruano.

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

Se tiene el conocimiento adecuado, pero a medida que avance la tecnologia se requiere un conocimiento adecuado para la obtencion de información (elementos de conviccion) se constituye en uno de los factores utiles dentro del exito de una investigacion criminal, aspecto que demanda de los investigadores encargados de la recolección preservación, analisis y presentación de las evidencias digitales una mayor labor q. garantice la autenticidad e integridad de dichas evidencias, a fin de ser utilizados posteriormente ante el proceso penal.

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?

Es importante en el proceso penal, porque de ello depende lo que se trata de identificar al delincuente informatico.

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

Es necesario porque en ello se establece los procedimientos y recaudos si la tecnologia avanza el marco legal tambien debe estar a la par.

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

Es lo adecuado porque ello nos ayuda a quienes deben de hacer, sobre la base de los elementos probatorios, los cuales no hayan sufrido alteración o contaminación alguna desde su recolección, examen y custodia

Que habiendo culminado de manera exitosa la entrevista, se agradece su importante colaboración.

MUNICIPALIDAD DISTRITAL SAN RAMON
EJECUTORIA COACTIVA
Wilfredo A. Alvarez Cuadros
ABOGADO
Reg. A.J. 0236
EJECUTOR COACTIVO

Leyla Keith Rivero Passuni
DNI N° 44757254
ENTREVISTADOR

Nombre y Apellido:
DNI N°
ENTREVISTADO