ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

La admisibilidad y el valor probatorio de la evidencia digital en el Sistema Jurídico Peruano 2018

TESIS PARA OPTAR EL GRADO ACADÉMICO DE:

Maestro en Derecho Penal y Procesal Penal

AUTOR:

Br. Miguel Ángel Osco Escobedo

ASESOR:

Dr. Edwin Alberto Martínez López

SECCIÓN:

Derecho

LÍNEA DE INVESTIGACIÓN:

Procesal Penal

LIMA - PERÚ

2019

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

DICTAMEN DE LA SUSTENTACIÓN DE TESIS

EL / LA BACHILLER (ES): **OSCO ESCOBEDO, MIGUEL ANGEL**

Para obtener el Grado Académico de ***Maestro en Derecho Penal y Procesal Penal,*** ha sustentado la tesis titulada:

LA ADMISIBILIDAD Y EL VALOR PROBATORIO DE LA EVIDENCIA DIGITAL EN EL SISTEMA JURÍDICO PERUANO, 2018

Fecha: 23 de enero de 2019 Hora: 11:00 a.m.

JURADOS:

PRESIDENTE: Dr. José Antonio Galindo Heredia **Firma:** .....

SECRETARIO: Dr. Willian Flores Sotelo **Firma:** .....

VOCAL: Dr. Edwin Alberto Martinez López **Firma:** .....

El Jurado evaluador emitió el dictamen de:

APROBAR POR UNANIMIDAD

Habiendo encontrado las siguientes observaciones en la defensa de la tesis:

.....

.....

.....

.....

Recomendaciones sobre el documento de la tesis:

APA

.....

.....

.....

.....

Nota: El tesista tiene un plazo máximo de seis meses, contabilizados desde el día siguiente a la sustentación, para presentar la tesis habiendo incorporado las recomendaciones formuladas por el jurado evaluador.

Dedicatoria

La presente tesis la dedico a mi familia y personas en especial, principalmente a mi madre por brindarme en todo momento su confianza y apoyo, a mi Padre por sus concejos y a mis hijos fuente de inspiración y fuerza para seguir adelante en la senda de superación para mi realización profesional

Agradecimiento

En primera instancia agradezco a mi Policía Nacional del Perú quien me formo en disciplina y responsabilidad y me dio la oportunidad de conocer el fascinante mundo de la tecnología, en las diferentes unidades donde preste servicio. Sencillo no ha sido, pero gracias a las exigencias y compromisos que me requería, he logrado grandes objetivos como culminar de mi tesis con éxito y obtener una afable titulación profesional.

Declaración de Autoría

Yo, Miguel Ángel Osco Escobedo, estudiante de la Escuela de Posgrado, Maestría en Derecho Penal y Procesal Penal, de la Universidad César Vallejo, Sede Lima Norte; declaro el trabajo académico titulado “La admisibilidad y el valor probatorio de la evidencia digital en el Sistema Jurídico Peruano, 2018” presentada, en 320 folios para la obtención del grado académico de Maestro en Derecho Penal y Procesal Penal, es de mi autoría.

Por tanto, declaro lo siguiente:

He mencionado todas las fuentes empleadas en el presente trabajo de investigación, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes, de acuerdo con lo establecido por las normas de elaboración de trabajos académicos. No he utilizado ninguna otra fuente distinta de aquellas expresamente señaladas en este trabajo.

Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro grado académico o título profesional. Soy consciente de que mi trabajo puede ser revisado electrónicamente en búsqueda de plagios.

De encontrar uso de material intelectual ajeno sin el debido reconocimiento de su fuente o autor, me someto a las sanciones que determinen el procedimiento disciplinario.

Lima, 19 de Enero del 2019

_____

Miguel Angel Osco Escobedo
DNI: 43555690

Presentación

Señores miembros del jurado calificador

Presento a ustedes mi tesis titulada “La admisibilidad y el valor probatorio de la evidencia digital en el Sistema Jurídico Peruano, 2018”, cuyo objetivo fue: establecer los procedimientos en el manejo de la evidencia digital dentro de la actividad probatoria como elementos de prueba, con especial énfasis en la recolección, preservación, análisis y presentación, garantizándose la autenticidad e integridad a fin de ser presentada en el proceso de juicio oral, en cumplimiento del Reglamento de grados y Títulos de la Universidad César Vallejo, para obtener el Grado Académico de Maestro.

En el presente trabajo, se estudia ante la necesidad de enfrentar las nuevas formas de cibercriminalidad denominada delitos informáticos, en ellas la evidencia digital como medio de prueba para incriminar el ciberdelito dentro de un marco jurídico confiable empleando herramientas tecnológicas para su admisibilidad y valor probatorio, El estudio comprende los siguientes capítulos: el capítulo I se refiere a la introducción; el capítulo II se refiere al Marco metodológico; el capítulo IV se refiere a la discusión; el capítulo V a las conclusiones; el capítulo VI a las recomendaciones. Por último, el capítulo VII menciona las referencias bibliográficas y los anexos respectivos.

El resultado obtenido en la presente investigación es que “la evidencia digital no tiene un tratamiento especial en el Nuevo Código Procesal Penal, siendo tratado como una prueba documental, por lo que su admisibilidad y valor probatorio en un proceso judicial no cuenta con la normatividad necesaria, siendo muy urgente incorporarlo en el sistema jurídico del Perú”

Señores miembros del jurado esperamos que esta investigación sea evaluada y merezca su aprobación.

Los Olivos, 19 Enero del 2018

Br Miguel Ángel Osco Escobedo

Índice de contenido

Índice de tablas

Página

.

Índice de figuras

Resumen

La presente investigación titulada: La admisibilidad y el valor probatorio de la evidencia digital en el Sistema Jurídico Peruano, 2018; tuvo como objetivo general conocer y establecer los procedimientos en la investigación, manejo y traslado de la evidencia digital, dentro de la actividad probatoria que se fundamente por un lado, teniendo en cuenta lo establecido por la ley, y por otro los procedimientos técnicos mediante el empleo de herramientas tecnológicas.

El método empleado fue deductivo, el tipo de investigación fue básica, de nivel descriptivo, de enfoque cualitativo, de diseño no experimental. La población estuvo formada por fiscal representante del Ministerio Publico, personal PNP especialista en delitos de alta tecnología representante de la Policía Nacional del Perú, y un experto de tecnologías en delitos financieros del sistema bancario. La técnica empleada para recolectar información fue la observación, entrevista, análisis documental y los instrumentos de recolección de datos fueron, cuestionarios, guía de observación, guía de entrevista.

Se llegaron a las siguientes conclusiones: La prueba digital no solo es insuficiente, sino, no cuenta con un tratamiento especial en el Nuevo Código Procesal Penal del 2004, así como los operadores de justicia jueces, fiscales, abogados litigantes y el personal de la Policía Nacional no están capacitados en el manejo de procedimientos de hallazgo, recojo, tratamiento y traslado de las evidencias digitales.

Palabas claves: Tecnologías de Información y Comunicación (TIC), Ciberespacio, Cibercriminalidad, evidencia digital.

Abstract

The present investigation entitled: The admissibility and probative value of digital evidence in the Peruvian Legal System, 2018; Its general objective was to know and establish the procedures in the investigation, handling and transfer of digital evidence, within the evidentiary activity that is based on one side, taking into account what is established by law, and on the other the technical procedures through the use of technological tools.

The method used was deductive; the type of research was basic, descriptive level, qualitative approach, non-experimental design. The population consisted of a representative of the Public Prosecutor's Office; PNP personnel specialized in high-tech crimes, representative of the National Police of Peru, and a technology expert in financial crimes of the banking system. The technique used to collect information was observation, interview, documentary analysis and data collection instruments were observation guide, interview guide.

The following conclusions were reached: The digital proof is not only insufficient, but does not have special treatment in the New Code of Criminal Procedure of 2004, as well as the justice operators judges, prosecutors, trial lawyers and police personnel National are not trained in the handling of discovery procedures, collection, treatment and transfer of digital evidence.

Key words: Information and Communication Technologies (ICT), Cyberspace, Cybercrime, digital evidence.

I. Introducción

1.1 Trabajos previos

Trabajos previos internacionales.

Ramírez y Castro (2018) realizaron un Informe final de proyecto aplicado para optar el título de Especialista en Seguridad Informática que trato del *"Análisis de la Evidencia Digital en Colombia como soporte judicial de Delitos Informáticos mediante cadena de custodia*", correspondiente a la Universidad Nacional abierta y a distancia unad Escuela de Ciencias Básicas e Ingeniería especialización en Seguridad Informática Villavicencio, Colombia. Al respecto el informe define la finalidad de la cadena de custodia indicando que en esencia es mantener y preservar la integridad física así como lógica de una posible prueba o evidencia. Esta preservación debe realizarse desde el mismo instante de la recopilación o registro, su almacenamiento, transporte y análisis hasta finalizar con su entrega a la autoridad judicial. Es menester indicar que para que la cadena de custodia sea calificada como válida, necesariamente un perito o entidad judicial o del estado debe certificar y validar que el proceso de custodia se haya llevado de manera correcta, esta intervención evitara la contaminación de la evidencia. Al respecto los autores opinan que la participación de personal calificado es una decisión vital ya que por ejemplo si se decide dejar el equipo encendido se corre el riesgo de ser detectado e identificado y que se activen métodos o acciones que generen el borrado o destrucción de la información contenida en el equipo y que esta sea irrecuperable, es decir, entre más tiempo se deje encendido, mayor será el daño que este generado. Por el contrario, si se decide apagar el equipo, puede haber métodos o acciones que eliminen la información contenida no solo en los equipos de cómputo local sino en el dispositivo de almacenamiento externo de la misma red.

Jiménez (2018) en su tesis titulada "*Desarrollo de una aplicación de uso didáctico para comunicación segura de datos a través de la red",* sustentada en la Escuela Politécnica Nacional de Quito; refiere en los servicios de integridad la función que cumple el algoritmo "Un algoritmo Hash es una función que toma una cadena o mensaje de longitud variable y

produce un valor hash de longitud fija, también llamado resumen de mensaje, que se emplea para verificar la integridad de los datos y mensaje, que se emplea para verificar la integridad de los datos y mensajes, se representa como una cadena corta de letras aleatorias y números, es como una huella digital de un mensajes, es un proceso unidireccional, pues no es posible crear el texto original utilizando cualquier función del hash inverso, si los datos originales cambian incluso por un carácter, la función hash producirá un valor hash diferente, por lo tanto, el receptor sabrá que la información original ha cambiado" (p.33).

Justo (2017) Policía Federal Argentina Área Digital Asociación por los Derechos Civiles elaboraron el trabajo *"Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal"*, correspondiente al proyecto financiado por Ford Foundation. Dicha investigación enfatiza la importancia y facultades en el ámbito procesal penal que deben de tener los investigadores en las diferentes modalidades del Cibercrimen tales como procesos, servicios, actividades o manejo de información que se realizan en línea, considerándose que un mismo ilícito se puede realizar en diferentes jurisdicciones (países), por la naturaleza del internet. Los operadores de justicia para tener éxito en sus investigaciones y decisiones, deben validar la información; móvil del ilícito, pero al involucrar diferentes países se presenta el problema de la jurisdiccionalidad o en su defecto la rogatoria internacional que se realiza para tener respuesta del pedido de información, conllevado a la demora de la investigación judicial incumpliéndose los plazos de investigación.

Di lorio, Castellone, Constanzo, Curti, et al. (2017) Libro de la Universidad fasta Ediciones, Mar del Plata, Argentina titulado *"El rastro digital del delito, aspecto técnico, legales y estratégicos de la Informática Forense*", al respecto el indicado libro refiere que durante una investigación penal pueden presentarse escenarios donde la información se encuentre ubicada fuera de la República Argentina, planteándose en ese momento dificultades que representan desafíos para los investigadores. Existen convenios bilaterales y tratados de asistencia recíproca entre algunos países en lo que respecta a medidas de investigación y de prueba. La normatividad

internacional que se avoca a esta dificultad es la Convención de Cibercriminalidad de la Unión Europea (Budapest, 2001), a la que Argentina ha mostrado su intención de adherir pero aún no la ha ratificado formalmente en el Congreso Nacional. Ante ello se ha ido adaptando su legislación de acuerdo al texto de ese Convenio, quedando aún pendiente la adecuación de las normas procesales. No obstante ello, la Convención de Budapest puede ser tomada como punto de referencia para adoptar criterio en diversas problemáticas procesales y para optimizar lo relativo a la gestión de diligencias investigativas y/o probatorias. Hay asimismo normas de cooperación entre autoridades policiales, con determinadas empresas globales (como Facebook, Twitter, Microsoft Corporation, Google y Apple) quienes exigen a los investigadores seguir al pie de la letra procedimientos en miras a lograr el objetivo de conseguir la información de un usuario determinado. Una de las grandes dificultades se da en el sentido que estas entidades tienen representación en el país no convirtiéndolas en multinacionales a las que se les pueda hacer cumplir una orden judicial argentina siendo, por tanto, el Estado quien debe ajustarse a los cánones establecidas por ellas. Incluso ciertas compañías, aun teniendo una oficina en la República Argentina, se amparan en que su existencia sólo es empleada a los efectos comerciales, por lo cual al encontrarse la información requerida judicialmente en servidores extranjeros las peticiones que se cursen deben ajustarse a las exigencias legales del País en donde éstos se encuentren.

Lasso (2017) presento una Monografía para optar al título de Especialista en Seguridad Informática de la Universidad Nacional abierta y a distancia, unad Escuela de Ciencias Básicas Tecnología e Ingeniería Especialización en Seguridad Informática Palmira, titulada *“Estado del peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia”,* al respecto precisa que el estudio del fenómeno, denominado comúnmente delincuencia o criminalidad informática, y la motivación de contar con una capacidad de respuesta legal adecuada, ha permitido que se dé solución jurídica a muchos de los aspectos concernientes al cibercrimen tanto desde el Derecho Penal como desde el Derecho Procesal Penal, vinculándose el manejo ilícito de la informática con la protección de lo

que se ha denominado bien jurídico tutelado de la información y de los datos mediante la expedición de la ley 1273 de 2009. La creciente incidencia de la Ciberdelincuencia a determinado la inminente necesidad de contar con un ordenamiento jurídico que sancione de forma adecuada a la cibercriminalidad, no solo desde la identificación de los delitos cometidos y el establecimiento de penas sino también desde el procedimiento penal admitido para dar solución a las investigaciones en las que se vea involucrada evidencia digital. En Colombia existen soportes constitucionales, el Derecho al Debido Proceso consagrado en el artículo 29 de la Constitución mediante la Sentencia C-980/10, Ley 527 de 1999 y la Ley 906 de 2004 en donde se expide el Código de Procedimiento Penal, que brinda herramientas para la presentación de la evidencia digital durante un proceso judicial, aunque también dan a conocer la urgencia de la mejoría del Estatuto Procesal Penal de modo que sea suficiente y su interpretación y aplicación no sea incongruente.

Trabajos previos nacionales.

Claros y Castañeda (2017) presentaron el libro de la editora y distribuidora Ediciones Legales e.i.r.l Perú titulado *"Nuevo Código Procesal Penal comentado Tomo I",* al respecto precisa que el Nuevo Código Procesal Penal en su Capítulo VI de la Exhibición forzosa y la Incautación, Articulo 220 Diligencia de secuestro o exhibición, numeral 5 que la Fiscalía de la Nación, a fin de garantizar la autenticidad de lo incautado, dictara el Reglamento correspondiente a fin de normar el diseño y control de la cadena de custodia, así como el procedimiento de seguridad y conservación de los bienes incautados. Se formuló el Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados, el cual establece que los fiscales observarán que se cumplan lineamientos mínimos, debiéndose Iniciar la colección de elementos materiales y evidencias con los objetos grandes y movibles, posteriormente se recolecta aquellos que requieren de un tratamiento o técnica especial, seleccionándolos y clasificándolos, debiéndose utilizar embalajes apropiados de acuerdo a su naturaleza, etiquetándolos o rotulándolos para una rápida ubicación e identificación o precintándolos según el caso, llenándose el formato de

cadena de custodia el cual no podrá tener modificaciones o alteraciones y que al ser transportados, debe preservarse su integridad, manteniéndolos libres de todo riesgo o peligro de alteración, deterioro o destrucción.

Jiménez (2017) presento un libro de ediciones Jurista editores E.I.R.L Perú titulado *"Manual de Derecho Penal Informático*", al respecto hace referencia sobre los lineamientos generales de la criminalidad informática y sugiere el modelo europeo como mejor alternativa a seguir para una actuación globalizada contra la ciberdelincuencia transnacional, por las nuevas formas de colaboración entre estados europeos, quienes con una visión integradora, parten del deseo común de llegar a conclusiones semejantes, sobre cuál debe ser el tratamiento adecuado de determinados fenómenos en aras de una mayor eficacia, siendo el Tratado de Ámsterdam uno de ellos entre otros, y el Convenio Europeo de Asistencia Judicial en Materia Penal el de mayor importancia en relación a los ciberdelitos. Dichas asistencias prevén soluciones concretas como son el intercambio de información, equipos de investigación conjuntos, transmisión de documentos, interceptación de comunicaciones, etc. Su incidencia en la persecución del ciberdelito queda bien acreditada.

Nessi (2017) presento el Proyecto de apoyo al sector Justicia American Bar Association Rule of law Initiative aba roli Perú, Ministerio Publico y Policía Nacional del Perú, titulada *"Manual de Evidencia Digital",* al respecto precisa que debe tenerse en cuenta que quienes participen en los diferentes actos, ya sean estos, estrictamente de aseguramiento o análisis de la evidencia o de conducción de la investigación penal, lo harán bajo las prescripciones del Nuevo Código Procesal Penal Decreto Legislativo N° 957 el mismo que prescribe en su artículo 67, el aseguramiento de la escena del delito será llevado a cabo por funcionarios de la Policía Judicial que cuenten con un conocimiento técnico avanzado en cuanto al manejo de la evidencia digital, debiendo dar inmediata noticia de ello al Fiscal. Es importante precisar que es de vital importancia que quienes intervengan en la escena del delito sean personas capacitadas sobre el manejo de la evidencia, ya que mediante un correcto desempeño de sus funciones se garantiza desde el inicio la

integridad de los distintos dispositivos que puedan ser incautados. El personal que accede a la escena debe contar con experiencia previa o estar capacitado en el manejo de la evidencia digital para adoptar mejores decisiones. Toda actividad llevada a cabo fuera de los protocolos establecidos podría alterar la evidencia.

Sequeiros (2016) presento una tesis para optar el título profesional de abogado en la Universidad de Huánuco, facultad de derecho y Ciencias Políticas, titulada *"Vacío legales que imposibilitan la sanción de los delitos informáticos en el nuevo Código Penal Peruano*", al respecto la tesis sustenta en relación al vacío legal o laguna jurídica en el Derecho a la ausencia de reglamentación legislativa en una materia concreta. Es una situación de vacío en la ley que ha sufrido omisión en su texto la regulación concreta de una determinada situación, que no encuentra respuesta legal específica; con ello se obliga a quienes aplican dicha ley (jueces, abogados, fiscales, y otros) al empleo de técnicas sustitutivas del vacío, con las cuales puedan obtener respuesta eficaz a tal ausencia. Ante esta situación, se hace necesario suplir la laguna jurídica a través de distintas herramientas tales como el Derecho Supletorio donde el juez acude a la regulación de una rama del derecho supletoria. La Interpretación extensiva el juez hace una interpretación lo más extensiva posible de una norma cercana. La Analogía el juez aplica normas que están dictadas para situaciones esencialmente parecidas. Acudir a otras fuentes del derecho como la costumbre o los principios generales del Derecho y la Norma Cruzada entre normas principales y otras supletorias, de modo que se sabe cuál debe aplicarse con preeminencia y al mismo tiempo, entre del derecho principal y el derecho supletorio.

1.2 Marco teórico referencial

Ciberdelincuencia.

Esta actividad delictiva se define como aquella acción en la que utilizando en el Internet, destruye o avería equipos de cómputo, y similares así como net de Internet. También buscan atentar la veracidad, la entereza de los sistemas

informáticos y sus redes, además podríamos agregar que son actividades que buscan robar información, suplantar la identidad de personas, generar fraudes a personas naturales y jurídicas, etc, entre otros. La ciberdelincuencia realiza distintas formas de acciones delictivas. Desarrolla la falsificación, engaño y por consiguiente el fraude por medio de sistemas de información. El segundo tiene que ver con la publicación de contenidos ilegales mediante el empleo de comunicación electrónica. El tercero aborda los ilícitos que se consuman en el internet.

Figura 1. Clases de ciberdelitos

Identificación de cibercriminales

Hacker, es una persona especializada en informática, sistemas de información o telecomunicaciones, pues siempre está en permanente actualización. También se les define como personas expertas en sistemas muy complejos. Con la tendencia moderna empiezan a centrarse en los sistemas informáticos y de telecomunicaciones. Les fascina ingresar en los ordenadores con el objetivo de poner en conocimiento de los demás que pudo vulnerar la seguridad, sin embargo en muchas oportunidades no vulneran el sistema, es decir dejan el sistema vulnerado sin modificaciones.

Cracker, Es aquel que tiene muchos conocimientos y habilidades de quebrar la parte lógica conocido como software, siendo su objetivo los grandes sistemas de información, ingresando a su estructura para generar el mayor daño posible. Virucker, es la persona que tiene conocimientos especiales en ingresar dolosamente a un ordenador, con la finalidad de anular, estropear información a través de la infección de virus. Spyware, Es un programa insertado en un ordenador con el objeto de seleccionar información de su computador para luego trasmitir información a una persona interesada u organismo con o sin el permiso del titular o dueño del computador.

El Ciberespacio y la Ciberseguridad.

Ciberespacio, Es el lugar virtual, ya que no tiene una locación física espacial, en ella interactúan usuarios, se explora información on line en páginas web, se comunican mediante redes sociales sin reparo de tiempos y distancias mediante el empleo del Internet. Ciberseguridad, es le estado de confianza que se tiene en el ciberespacio luego de habers adoptado medidas de seguridad capaces de resistir amenazas, responderlas y recuperarse. El insumo importante en la ciberseguridad, es el Internet, tanto las entidades del Estado como las privadas están expuestos a una serie de peligros que pueden causar daños considerables. La ciberseguridad, conocida también como seguridad digital, es hoy más actual que nunca y no solo hace referencia a la seguridad en Internet, sino también a otros aspectos y sectores de las TIC.

Para tener ese estado y confianza garantizando la seguridad informática de sus usuarios se puede emplear muchas formas como aquellas que van desde la explicación de los peligros en la red hasta la aplicación de herramientas y programas con los que el usuario puede protegerse de ataques en Internet, así como la capacitación de los cursos de formación sobre seguridad online. También los ciberataques no siempre tienen lugar en Internet, la ciberseguridad engloba la mitigación de los riesgos de los que se valen las modernas posibilidades de telecomunicación y de informática.

Figura 2. Representación del ciberespacio

La Ciberdelincuencia y el conflicto como delito transnacional.

Actualmente la ciberdelincuencia es uno de los delitos transnacionales que viene creciendo en forma alarmante, a ello contribuye la rápida evolución de Internet y la tecnología informática que paralelamente permiten el crecimiento económico y social, una mayor dependencia de Internet, convirtiéndolo en un medio de comunicación mundial, esto ha conllevado y generado más riesgos y vulnerabilidades, abriendo nuevas posibilidades para las actividades delictivas. Al no existir fronteras para este flagelo hoy más que nunca se hace necesario que los entes responsables al ejecutar la ley tengan problemas en actuar eficazmente, por la gran barrera que genera los límites en las investigaciones transfronterizas, a ello se suma problemas de tipo jurídico y la diversidad de capacidades en el mundo. Las fronteras nacionales, aunque se lea irónicamente, representan una dificultad para el tratamiento de los ciberdelincuentes.

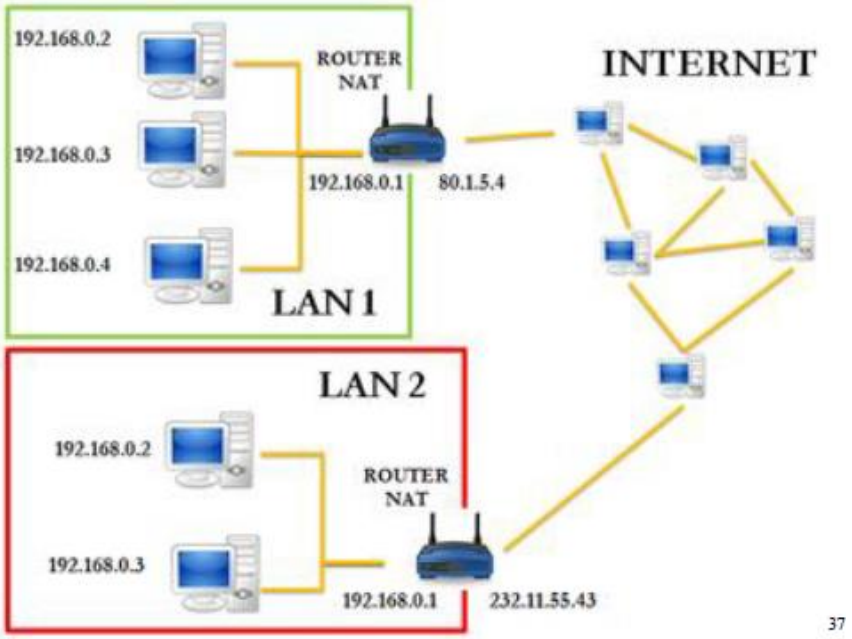


Figura 3. La Red Internet

Ciberdelitos en el mundo

Ataque masivo de hackers en Chile, bancos de Perú sufren ataque ransomware**.** De reportes en medios peruanos, tres bancos grandes fueron objeto de ataques cibernéticos de ransomware. Esto, luego de repetidos reportes de usuarios en redes sociales sobre problemas en los sistemas presenciales y online de las agencias bancarias, y del reporte de un organismo oficial del gobierno que reconoció que al menos dos bancos importantes fueron atacados. Este hecho ocurre a pocas semanas de una filtración grande de información de clientes de bancos en Chile y el robo de 10 millones de dólares en el Banco de Chile. De acuerdo al diario peruano La República, Maurice Fraisinet, jefe de Seguridad Informática de la SEGDI de la Presidencia del Concejo de Ministros, informó que es un ataque de ransomware y los afectados son Scotiabank e Interbank han recomendado a los trabajadores de diversas compañías no abrir joins externos recibidos a través de email y servicios de mensajería. Así también, trabajadores de Scotiabank reportaron haberse quedado sin sistema durante horas de la mañana.

Figura 4. Publicación del diario la republica el 18/08/2018

Ciberataques en cifras. El Jefe de operaciones de Asbanc, Giovanni Pichling, hizo de noción que en el universo, se producen 700 millones de ataques al año, aproximadamente sobre todo en los sectores económicos. Esto ubica a la ciberseguridad como un dificultad de gran posibilidad mundial, que genera la interés y quebradero de cabeza de todas las industrias sin pega, entre ellos la industria bancaria". Refiere que se estima que el 31% de los ataques que se dan hoy a altitud internacional están orientados contra los servicios financieros y ebanking. En los países del mundo, se produjeron más de 479 millones de ataques por phising en el año 2017. De los cuales, el 19.95% se direccionaron en dirección a Brasil, quien lidera el índice de naciones atacadas con este ilícito en el orbe. "Ese mismo año, más de 300 millones de puestos de trabajo y servidores fueron comprometidos con malware cotizable en 190 países de todo el mundo. Siendo China el primer puesto con el 35.75%" aseveró el representante de ASBANC.

22 Ago

ASBANC: La prevención y capacitación permanente permiten enfrentar los ciberataques y defender a los usuarios

- Los fraudes cibernéticos no sólo pueden dañar los sistemas informáticos y servidores sino también afectar los puestos de trabajo en la industria financiera.

El reciente ciberataque contra las entidades del sistema financiero

Figura 5. Publicación del portal de Asbanc el 22/08/2018

La industria que se avoca a la administración de la energía ha informado un alto registro de sucesos, ubicándose después del sector financiero. El "BlackEnergy" es un malware que desconectó a varias estaciones de la red eléctrica en Ucrania, generando un apagón de seis horas que afectó a miles de usuarios. El sector más afligido por el cibercrimen es el energético en el Perú, los ataques han generado un costo de pérdidas de US$ 17.20 millones al año aproximadamente. También indico que a medida que la renovación virtual ha aumentado, también creció el ilícito.

Figura 6. Publicación del diario Gestión el 31/07/2018

Conoce qué es la ‘Sextorsión’ y la ‘pornografía vengativa’. Muchas mujeres, han visto violada su intimidad al ver imágenes de encuentros sexuales con sus parejas en internet después de terminado la relación. Los casos de personas que son grabadas en la intimidad por sus parejas y luego las imágenes son publicadas en la red, a fin de extorsionarlas o por venganza, viene incrementándose en nuestro país, tal como se observa en las páginas pornográficas. Esto representa una violación a la intimidad y, por lo tanto, un delito. Por ello, la PNP combate este tipo de casos.

La Sextorsión tiene como objetivo que la persona le entregue un dinero, una ventaja o algo a cambio de que no divulgue las imágenes que él tiene en su poder. En cambio, la pornografía vengativa no busca que le des ninguna retribución, ningún dinero, ninguna ventaja, simplemente busca vengarse y hacer daño por despecho o por otra razón, consumiendo su objetivo, subiendo estas imágenes a diferentes redes sociales para que sean difundidas. Se indica que, en el Perú, la mayoría de víctimas son mujeres y que más de la mitad de ellas conocía a su acosador, ya que fue con quien tuvo una relación. Asimismo los sujetos que grabaron las escenas lo hicieron, en sus encuentros sexuales, en un motel y colocaron una cámara de video sin

que su pareja lo sepa. Así mismo en algunos casos, las personas se filman con el consentimiento de ambos, pero luego uno de ellos divulga el video como despecho al no poder superar la finalización de la relación.


El Comercio

Lo último · Opinión · Política · Economía · Perú · Lima · Mundo · Luces · DT · Somos · Ver Más · COLECCIONES · Club

MÁS EN POLICIALES

Lo que se sabe del asesinato del brazo derecho de 'Caracol' en sauna de San Isidro

¿Quién es Junior Tarazona? El sujeto asesinado en un sauna de San Isidro

Conoce la campaña que lucha contra los accidentes de tránsito

SJL: taxista fue asesinado a balazos por presuntos sicarios

San Isidro: asesinan a Junior Tarazona en un sauna de la calle Miguel Dasso

Asalto en Miraflores: policía herido por 'marcas' se encuentra estable

POLICIALES

Conoce qué es la 'sextorsión' y la 'pornografía vengativa'

Muchas personas, en su mayoría mujeres, han visto violada su intimidad al ver imágenes de encuentros sexuales con sus parejas en internet después de finalizada la relación.

CUARTO PODER

CORONEL PNP RAÚL ALFARO

JEFE DE LA DIVINDAT

En el reportaje de "Cuarto Poder" se señala que, en el Perú, la mayoría de víctimas son mujeres y que más de la mitad de ellas conocía a su acosador, ya que era alguien con quien tuvieron una relación.

ALDO & Co.

Figura 7. Publicación del diario El Comercio el 05/03/2018

Cuestionan ausencia de registro de evidencias digitales en Código Procesal Penal. Fernanda Ayasta Nassif asesora del Poder judicial, criticó que en el Nuevo Código Procesal Penal vigente no contempla un capítulo sobre el levantamiento, la conservación y el registro de las evidencias digitales o electrónicas. Refirió que dicho procedimiento es mucho más especializado que cualquier prueba material de las que estamos acostumbrados y no son consideradas por la legislación procesal, dificultando el trabajo de las autoridades encargadas de la investigación. Actualmente sólo se puede revisar el tema de la conservación y el registro de evidencias de manera analógica, así indico durante su participación del taller de investigación y persecución penal de delitos con evidencias digitales.

Figura 8. Publicación del portal web de Andina el 02/09/2018

Atacan web de la PNP. La Agrupación LulzSec atacó la página policial y dejaron un mensaje en el que critican la falta de compromiso de los efectivos de la PNP ante la creciente inseguridad ciudadana que afecta a los limeños.

Figura 9. Publicación del diario Perú 21el 18/11/2013

Sistema financiero del Perú repele ciberataques y suspenden temporalmente servicios. Autoridades del sistema financiero advirtieron que el pasado viernes se desarrollaban agresiones cibernéticas a las agencias bancarias a nivel mundial**.** Las entidades bancarias del país rechazaron las intrusiones e interrumpieron momentáneamente sus operaciones después de hacerles de conocimiento de la alarma de seguridad**,** informó la SBS, activando inmediatamente los protocolos establecidos de seguridad para salvaguardar la información bancaria de sus clientes, como medida preventiva.

Figura 10. Publicación del portal web infobae el 17/08/2013

Pérdidas económicas en el Perú por ciberdelincuencia ascienden a más de US$ 4,000 millones. Ante la falta de programas y políticas de seguridad informática en nuestro país, genero el aumento de los ciberdelitos en un 11,97% ubicando al sector financiero como el más afectado, en el último año. Según un análisis en Latinoamérica de la OEA y el BID, Perú no ha tomado un liderazgo en implementar un sistema de ciberseguridad, aseguró Andrés Galindo, director de negocios y alianzas estratégicas de Digiware. Además, índico en que no hay información al público sobre cuál es el rumbo del

gobierno sobre este tema. Las ganancias por ciberataques pueden ser de hasta 6350% de retorno a nivel global. Pues del impacto mundial que es US$ 3 trillones, el costo para el desarrollo de estos ataques puede ascender a más de US$ 47,000 mil millones. Esta industria va a crecer por el impacto económico que tiene, indica Galindo.

De manera concertada el gobierno, la empresa privada y las personas expertas en ciberseguridad se reúnan en mesas de trabajo para construir un plan para el país. Pues si el estado no asume, los gremios tienen la oportunidad para asociarse y desarrollar políticas de ciberseguridad. Y si los gobiernos ni la comunidad lo logran hacer, las empresas deben tener cada vez más material para que sepan que este riesgo no es efímero sino real, insiste Galindo.


GESTIÓN Tecnología • Portada • Economía • Tendencias • Tu Dinero • Gestión TV • Blogs

Perú registrará US$ 4,782 millones en pérdidas por ciberdelitos en 2017

El año pasado, Perú invirtió aproximadamente US$ 22 millones en servicios de ciberseguridad.

Compartir Compartir Compartir

(Foto: Difusión).

Figura 11. Publicación del diario Gestión el 10/08/2017

Perú se suma a la lista de los países víctimas de ciberataque. Desde los centros hospitalarios británicos hasta la empresa española Telefónica**,** pasando por la empresa de autos francesa Renault o la compañía publica ferroviaria alemana, son algunas de las empresas y organismos que han sido víctimas en todo el mundo por un masivo ataque informático. Perú no ha sido

ajeno a estos ciberdelitos. Un representante de la firma Kaspersky, indico que el Perú fue víctima del ataque conocido como ransomware Wanna Cry (secuestro de dato). Aseguró que varias decenas de empresas e instituciones peruanas, y una importante entidad financiera, fueron víctimas por el ataque al que calificó como el nuevo ISIS (terroristas del Estado Islámico).

Los cibercriminales se estima de China pidieron una recompensa por esa información. El ataque afectó a computadoras que no tienen la versión actualizada de un antivirus de Windows. Las computadoras muestran mensajes en diversos idiomas exigiendo el pago de dinero entre 300 y 600 dólares para desencriptar la información secuestrada de los equipos.

Figura 12. Publicación del portal Peru.com el 13/05/2017

Normatividad Jurídica Nacional.

La prueba en el Código Procesal Penal.

Esta nueva norma, constituye dentro del ordenamiento jurídico peruano un valioso instrumento de administración de justicia ya que ha implementado un sistema procesal penal acusatorio garantista, en la que define claramente la función persecutoria y la pesquisa del delito, encargado al Fiscal en la función del juzgamiento que estará a cargo de los Jueces, también se aprecia que brinda las garantías a quienes participan en esta fase penal, buscándose finalmente se logren los resultados optimo desde la perspectiva jurídica, concluyendo como resultado la resolución del conflicto materia del proceso. Para nuestro presente trabajo se extraído del Código Procesal Penal así como los articulados que relacionan al tratamiento de las evidencias. El Código Procesal Penal (2004) en su artículo 176° numeral 1, el perito tiene como derecho acceder al expediente penal a fin de conocer detalles del mismo así como también a las evidencias que se encuentren a cargo del Juez, todo ello para poder facilitar un buen análisis y desarrollo de su trabajo pericial, para ello deberá indicar la fecha en que inicia sus operaciones de análisis pericial y su continuación; es de vital importancia que el perito guarde reserva en todo lo que conozca.

El Código Procesal Penal (2004) en su artículo 378° numeral 5, prescribe: “El examen de los peritos se inicia con la exposición breve del contenido y conclusiones del dictamen pericial (…), explicaran las actuaciones periciales que ha efectuado (…)”. El Código Procesal Penal (2004), en su artículo 378° numeral 7, prescribe: “Los peritos podrán consultar documentos, notas escritas y publicaciones durante su interrogatorio. En caso sea necesario se realizará un debate pericial (…)”. El Código Procesal Penal (2004) en su artículo 378° numeral 8, prescribe: “Durante el contrainterrogatorio, las partes podrán confrontar al perito (…)”.

El Código Procesal Penal (2004), en su artículo 382° numeral 1, prescribe: “Los instrumentos o efectos del delito, y los objetos o vestigios

incautados o recogidos, que obren o hayan sido incorporados con anterioridad al juicio, siempre que sea materialmente posible, serán exhibidos (…)". El Código Procesal Penal (2004), en su artículo 511° numeral 1, prescribe: "Los actos de cooperación judicial internacional, sin perjuicio de lo que dispongan los Tratados, son (…), i) Facilitar información y elementos de prueba (…)". La cooperación judicial internacional, es una valiosa herramienta al alcance de los Estados en su tarea de combatir el delito y perseguir y sancionar a sus autores o partícipes, con una utilidad manifiesta sobre todo cuando se trata de ilícitos penales de carácter transnacional como el Tráfico Ilícito de Drogas, el Lavado de Activos, el Terrorismo, la Trata de Personas, la Corrupción de Funcionarios, Delitos informáticos entre otros, en cuya ejecución como en las tareas de esconder las ilícitas ganancias obtenidas y en la de evadir la acción de la justicia, las fronteras no constituyen un límite invencible. Precisamente por esta necesidad y como una de las expresiones del fenómeno de la globalización, los Estados vienen asumiendo compromisos de cooperación que se materializan en tratados multilaterales o bilaterales, mientras que en sus legislaciones internas van incluyendo disposiciones cada vez más precisas, con la finalidad de hacer de la Cooperación Judicial Internacional un mecanismo de ayuda mutua o recíproca más eficaz y expedito.

Actuación del Policía.

La legislación Procesal Penal (2004), en su articulado 67° numeral 1, refiere que el personal PNP dentro de sus atribuciones en una investigación, podrá por propia iniciación, agrupar y garantizar los componentes de prueba que puedan ayudar para el empleo de la Ley penal. El NCPP (2004), en su artículo 67° numeral 1, prescribe: "(…) tiene como atribuciones en otras: Proteger y vigilar la escena del delito con la finalidad que no se borre los indicios, restos o señales del delito asimismo reunir, agrupar y cuidar los objetos o dispositivos que relacionan con el delito, y todo aquello que sirva para la investigación (…)". Es de apreciarse que la norma procesal faculta a la Policía Nacional atribuciones en la investigación y el cuidado de la escena del delito.

La Prueba, la Pericia y la Prueba documental.

En relación al NCPP, se aprecia que respecto al término “evidencia”, como medio de prueba solo consigna el acceso al proceso de Reserva por parte del Perito así mismo tiene acceso a las evidencia que estén a disposición judicial para recabar información que considere, debiendo indicar la fecha que iniciara la operación pericial y su continuación. Respecto al término “prueba”, el Nuevo Código Procesal Penal establece procedimientos. El Código Procesal Penal (2004) en su artículo 155° numeral 2, prescribe: “Las pruebas se admiten a solicitud del Ministerio Público o de los demás sujetos procesales. El Juez decidirá su admisión mediante auto especialmente motivado, y sólo podrá excluir las que no sean pertinentes y prohibidas por la Ley (…)”. La norma Procesal Penal (2004), en su articulado 156° numeral 2, prescribe: “No son objeto de prueba las máximas de la experiencia, las Leyes naturales, la norma jurídica interna vigente, aquello que es objeto de cosa juzgada, lo imposible y lo notorio”. Son medios de prueba según el Código Procesal Penal (2004) en su artículo 157° numeral 1, prescribe: “Los hechos objeto de prueba pueden ser acreditados por cualquier medio de prueba permitido por la Ley. Excepcionalmente, pueden utilizarse otros distintos, siempre que no vulneren los derechos y garantías de la persona (…)”.

En la valoración de la prueba el Código Procesal Penal (2004) en su artículo 158° numeral 1 y 3, indica que el Juez deberá examinar las reglas de la lógica, la ciencia y las máximas de la experiencia, y explicara las conclusiones que obtenga y las apreciaciones aceptadas. La prueba por vestigios necesita: a) Que el indicio esté probado; b) Que la inferencia esté basada en las reglas de la lógica, la ciencia o la experiencia. La norma Procesal Penal (2004) en su articulado 159° numeral 1, refiere que la autoridad judicial no utilizara, inmediatamente o posteriormente las causas o recursos de evidencia obtenidas con trasgresión del asunto fundamental de su legitimidad esencial de la persona”.

En la Pericia, el Código Procesal Penal (2004) en su artículo 172° numeral 1, indica: “La pericia procederá siempre que, para la explicación y

mejor comprensión de algún hecho, se requiera conocimiento especializado de naturaleza científica, técnica, artística o de experiencia calificada". El Código Procesal Penal (2004) en su artículo 173° numeral 1, indica: "(…) la autoridad judicial nombrara un perito en la etapa de la Investigación Preparatoria, para lo cual elegirá a profesionales de preferencia que se hallen sirviendo al estado, o de aquellos que colaboran con el ente judicial sin costo para el Estado. Caso contrario elegirá de los que han sido nombrados o registrados, acorde a las normas de la Ley Orgánica del Poder Judicial". El Código Procesal Penal (2004) en su artículo 174° numeral 2, indica: "La disposición o resolución de nombramiento precisará el punto o problema sobre el que incidirá la pericia, y fijará el plazo para la entrega del informe pericial, escuchando al perito y a las partes (…)". El Código Procesal Penal (2004) en su artículo 176° numeral 1, indica: "El perito tiene acceso al expediente y demás evidencias que estén a disposición judicial a fin de recabar las informaciones que estimen convenientes para el cumplimiento de su cometido (…)".

La Prueba Documental según el Código Procesal Penal (2004) en su artículo 184° numeral 1, prescribe: "Se podrá incorporar al proceso todo documento que pueda servir como medio de prueba (…)". El Código Procesal Penal (2004), en su articulado 185°, indica: "Son documentos los hológrafos, folletos, reproducciones, fax, dispositivos magnéticos, películas, imágenes, gráficos, grabaciones magnetofónicas y otros que contengan registro de las actividades anteriormente descritas". El Código Procesal Penal (2004) en su artículo 186° numeral 2, prescribe: "También podrá acudirse a la prueba pericial cuando corresponda establecer la autenticidad de un documento".

Respecto a la Aportación y Admisión de la Prueba, se precisa que el primero se realiza por los sujetos procesales facultados legalmente para intervenir en la Litis penal. La admisión de la prueba se producirá cuando el aporte del sujeto del proceso se de en las condiciones que establecidas por la ley. Las pruebas se aceptan a solicitud del Fiscal o de los sujetos que interviene en el proceso. Como consecuencia de la aplicación de este principio se establece que las partes deben admitir la obligación de contribuir

al proceso las pruebas que consideren podrán ser atendidas. Representa una justificada excepción al principio de aportación de parte, pues la acción penal busca conocer la verdad; con mucha más razón si se encuentra de por medio el interés público en la persecución penal. No afecta la imparcialidad judicial. Requisitos: a. Debe tratarse de nueva prueba. b. Debe ejercitarse. c. Deben ser medios de prueba útiles.

La valoración de la prueba.

La valoración es el juicio de aceptabilidad de los resultados probatorios. La valoración constituye la medula del razonamiento probatorio; es decir, del razonamiento que orienta, a partir de las informaciones aportadas al proceso a través de los medios de prueba, a una afirmación sobre hechos controvertidos. Obando V. (2013*). La valoración de la prueba*. Recuperado de: https://bit.ly/2ouSAFA. En nuestro sistema jurídico, el derecho a la prueba, requiere el empleo de reglas epistemológicas o la coherencia para la acreditar el valor de la prueba. Conocer la verdad es el propósito principal de la diligencia probatoria en el juicio. Solo el juez tiene la obligación de descubrir la verdad, los abogados emplean las pruebas para defender la posición de su patrocinado, buscando, inducir al juez. El Juez está impedido de emplear su experiencia personal al valorar la prueba, y la responsabilidad de la prueba, debe concluir cuál de las partes asumirá los efectos de la falta de sustento en relación a la prueba en el hecho, y de conformidad al principio de equidad en el sentido y evaluación de la prueba, su valor deberá ser justo, proporcionado y equitativo.

La Cadena de Custodia en el NCPP.

Su marco normativo es el NCPP (Dec Leg Nº 957) Art. 220 º,Inc. 2, 5 y 318 º Inc.1. Resolución Nº 729-2006 que norma el reglamento para el cuidado de Elementos Materiales, Evidencias y Administración de Bienes Incautados.
Acuerdo Plenario Nro 6-2012. Este procedimiento garantiza, asegura y reserva las evidencias, halladas en la escena del delito, para que ingresen a la investigación en curso del ilícito, con el objetivo de asegurar su

autenticidad, en el proceso judicial. Se inicia con el ingreso del primer efectivo policial a la escena del Delito, que posteriormente seguirá un procedimiento de conformidad a lo que establece la Guía de Procedimientos de Criminalística**.** Ello permite acreditar que la evidencia sea la misma que fue recogida o analizada y que su totalidad no haya sido alterada durante el proceso penal (principio de mismidad). Asimismo trata de evitar suspicacia en la autenticidad y/o indemnidad de la evidencia.

Figura 13. La cadena de custodia

Protección y acordonamiento de la escena. Extracción o Recolección adecuada de los elementos materiales y evidencias. Embalaje, etiquetado y rotulado y Actas que acompañan al bien. Al Realizar las acciones pertinentes para no permitir que personas ajenas contaminen la escena del hecho ya sea alterándola, moviéndola, o destruyéndola, respecto a la prueba. El procedimiento e instrumentos por utilizar deben ser los idóneos, válidos y recomendados. Emplear embalajes requeridos de acuerdo a la naturaleza de los elementos o macro elementos. Seguidamente lacrar etiquetar y rotular, precintándolos según sea el caso. Acta de recojo de indicios y evidencias. Acta de Incautación. Acta de entrega.

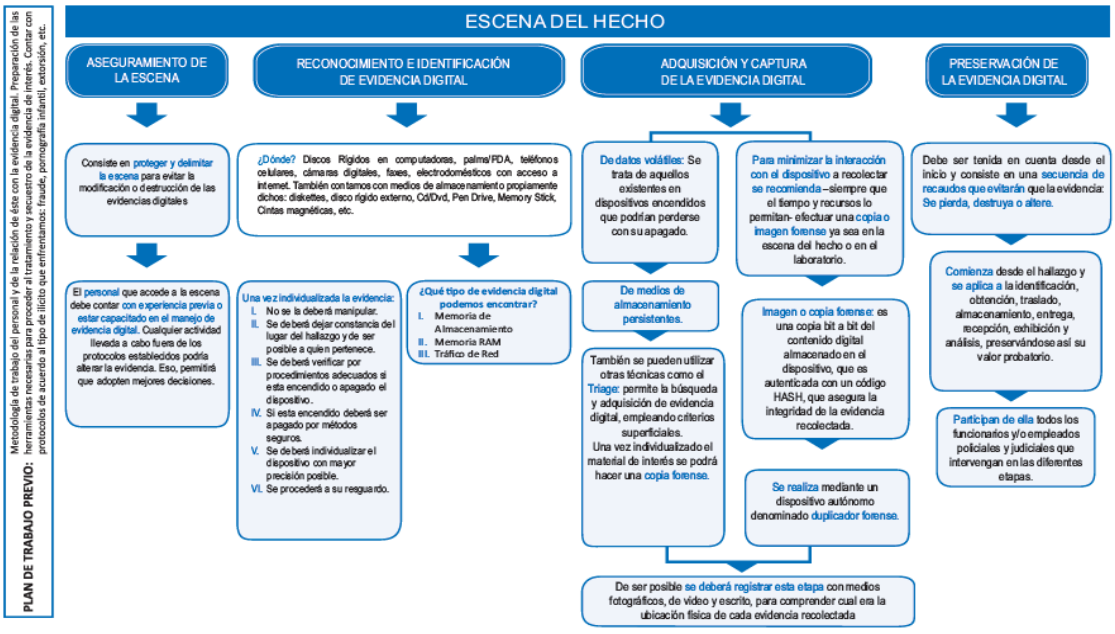


Figura 14. Procedimientos en la escena del hecho

Motivos de contaminación de evidencias.

Son muchísimos las circunstancias en la que una evidencia podría contaminarse, veamos algunas: Manipular las evidencias sin encontrarse protegidas. Juntar dos o varias evidencias, embalándolas en un solo depósito. Falta de cuidado en su conservación al no emplear envases requeridos. No brindar la seguridad adecuada. Empleo de equipo inadecuado para su tránsito.

Figura 15. Embalaje y rotulado

Decreto Legislativo N° 1412 Ley de Gobierno Digital.

Decreto Legislativo que aprueba la Ley de Gobierno Digital (2018) en su artículo 1°prescribe: “Esta norma busca instaurar un marco adecuado de trabajo en la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y asistencia de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno”. Decreto Legislativo que aprueba la Ley de Gobierno Digital (2018) en su artículo 4° numeral 4.1 y 4.2 prescribe: “Mejorar la prestación y acceso de servicios digitales en condiciones interoperables, seguras, disponibles, escalables, ágiles, accesibles, y que faciliten la transparencia para el ciudadano y personas en general. Promover la colaboración entre las entidades de la Administración Pública, así como la participación de ciudadanos y otros interesados para el desarrollo del gobierno digital y sociedad del conocimiento”.

Decreto Legislativo que aprueba la Ley de Gobierno Digital (2018) en su artículo 26° prescribe: “La Interoperabilidad es la capacidad de interactuar que tienen las organizaciones diversas y dispares para alcanzar objetivos que hayan acordado conjuntamente, a través del intercambio de información y conocimientos, mediante procesos interactivos entre sus sistemas de información”. Decreto Legislativo que aprueba la Ley de Gobierno Digital (2018) en su artículo 28° numeral 28.4 prescribe: “La Interoperabilidad a nivel legal, se ocupa de la adecuada observancia de la legislación y lineamientos técnicos con la finalidad de facilitar el intercambio de datos entre entes de la Administración Pública, así como el cumplimiento de los temas concernientes con el tratamiento de la información que se intercambia”. Decreto Legislativo que aprueba la Ley de Gobierno Digital (2018) en su artículo 30° refiere que la seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con

actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas. Decreto Legislativo que aprueba la Ley de Gobierno Digital (2018) en su artículo 32° prescribe: “El Marco de Seguridad Digital del Estado Peruano tiene los siguientes ámbitos: El Ministerio de Justicia y Derechos Humanos (MINJUS), el sector del Interior (MININTER), la PNP, la Fiscalía y el poder judicial en el marco de sus funciones y competencias dirigen, supervisan y evalúan las normas en materia de ciberdelincuencia”. Publicación oficial diario el peruano.

Delitos Informáticos.

En la actualidad como consecuencia del acentuado crecimiento de las TIC aparecen de nuevos ilícitos tipificados como delitos informáticos. Para frenar el creciente y alarmante hecho que involucra fundamental mente a la tecnología, se ha promulgado la Ley penal especial que busca prevenir y combatir las diferentes actividades ilícitas que dañan críticamente sistemas de información y por ende sus datos informáticos, sin dejar de lado el secreto de las comunicaciones, y los otros que como consecuencia de este ilícito resulten afectados. En la informática las principales vulnerabilidades son las siguientes: a. La falta de sistemas de control en la red, que genera dificultad para verificar la información. b. Aumento incontrolable de usuarios, y la libertad de acceder por herramientas de tecnología. c. La incógnita identificación de usuarios en la red que representa un obstáculo para su seguimiento al haber participado en un delito a través del internet. d. La sencillez para acceder a la información, con las posibilidades de modificar datos, arruinar sistemas informáticos.

Figura 16. Los delitos informáticos

Concepto y modalidades.

La ciberdelincuencia son comportamientos orientados a eludir los protocolos y medios de seguridad de las aplicaciones de información, entre ellas acceder ilícitamente a ordenadores a través de claves validas obtenidas de manera ilícita. En una percepción más amplia referimos que comprende a todas aquellas conductas en las que las TIC son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos; y que plantea problemas criminológicos y penales, originados por las características propias del lugar de comisión. De la creación de los delitos informáticos, se interpretar que no todo delito puede ser clasificado como delito informático por el solo hecho de haber empleado la computadora u otro medio tecnológico. “Es necesario determinar que conductas pueden ser clasificadas como delitos informáticos y cuáles no, a pesar de su vinculación con una computadora, un procesador de datos o la red de información”. Villavicencio F. (2014). *Delitos informáticos*. Recuperado de: https://bit.ly/2QcLkjb.

Finalidad - objeto.

La norma en referencia refiere en su artículo 1 que el fin que busca la norma es la prevención y la sanción del comportamiento ilícito que perjudican los sistemas, la información, el secreto de las comunicaciones así como los bienes jurídicos de importancia penal que resultaren dañados por medio del empleo de las TIC, y que garanticen las mínimos requisitos de que las personas disfruten del derecho a la libertad y al desarrollo. Esta norma busca asegurar la lucha eficaz contra la ciberdelincuencia. Es importante considerar la prevención esto ayudaría a evitar la comisión de ilícitos informáticos, teniéndose en consideración el creciente diario del avance de las TIC.

Los delitos informáticos ley 30096 y su modificación por la ley 30171.

La Ley 30171 que reformo la Ley 30096, ley de delitos informáticos, en su artículo 2° define el Acceso ilícito, como, el que en forma intencional y sin derecho ingresa a todo o parte de un sistema, teniéndose como requisito que esta se realice vulnerando las medidas de seguridad. El sustento legal, al respecto se encuentra en el Convenio de Budapest. Ley 30171, Ley que modifica la ley 30096, ley de delitos informáticos (2014) en su artículo 3° prescribe: “Atentado a la integridad de datos informáticos. El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesible datos informáticos (…)”.

Este licito penal castiga la actuación de dañar (causar pérdida, daño, deterioro), introducir, borrar (anular, impedir), deteriorar (perder, arruinar), alterar (deteriorar, destruir), suprimir (elimina, destruye) y hacer inaccesible los datos guardados en un sistema informático por medio del empleo de las Tic. Ley 30171, sobre los delitos informáticos (2014) en su artículo 4° prescribe: “Atentado a la integridad de sistemas informáticos. El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios (…)”. El presente articulado guarda similitud con el artículo 5 del Convenio Europeo de Budapest,

entendiéndose la obstaculización al acceso de un sistema informático con el daño total o parcial del sistema. Ley 30171, Ley que modifica la ley 30096, ley de delitos informáticos (2014) en su artículo 5° prescribe: “proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos. El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales (…)”.

Ley 30171 sobre los delitos informáticos (2014), en su artículo 7° prescribe: “Interceptación de datos informáticos. El que deliberadamente e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en unos sistemas informáticos o efectuados dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta dichos datos informáticos (…)”. Ley de delitos informáticos ley 30171 (2014), en su artículo 8° define la acción del Fraude informático, al que premeditadamente y sin derecho alguno busca para sí o para otro un beneficio ilícito en desmedro de un tercero a través de un plan, inserción, cambio, anulado, deleteo; clonación de datos o alguna interrupción o manejo en el funcionamiento de un sistema informático (…)”. Ley 30171, Ley que modifica la ley 30096, ley de delitos informáticos (2014), en su artículo 10° refiere sobre el abuso de mecanismos y dispositivos informáticos, que aquella persona que sin tener autorización y legitimidad construye, elabora, extiende, propaga, posibilita, reparte, importa u obtiene para su empleo, uno o más procesos, software informático, herramientas, códigos de acceso o cualquier otro dato informático, desarrollados especialmente para la comisión de estos ilícitos previstos en la presente ley.

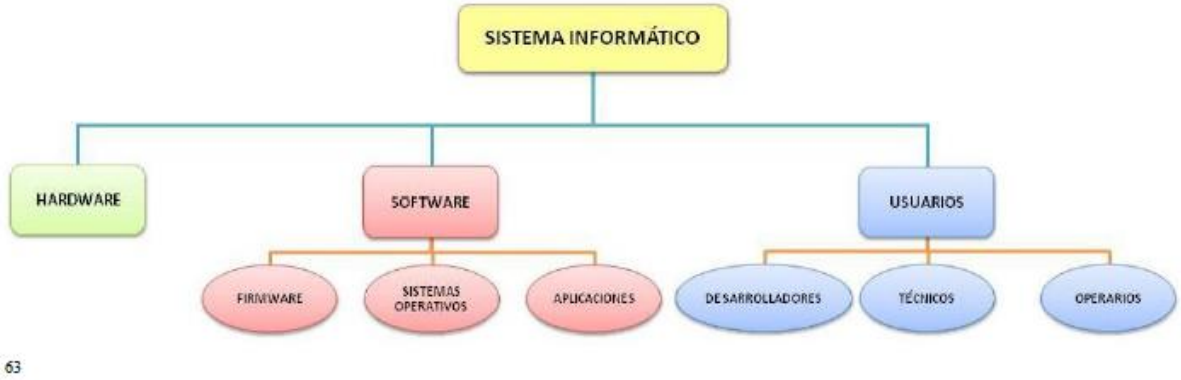


Figura 17. Composición de un sistema informático

Creación de la Divindat PNP.

La Dirección General de la PNP en el año 2005, creó la División de Investigación de Delitos de Alta Tecnología, unidad especializada que se encarga de investigar los ilícitos penales de delitos informáticos, así como los hechos en que se encuentre como medio de realización del delito un medio informático. Siendo una unidad que requiere de todo el apoyo de personal y logística para que cumpla con desarrollar un alto trabajo tecnológico lamentablemente, en la actualidad las instalaciones donde presta sus servicios es inadecuada, no cuenta con un selecto personal acorde a los conocimientos e exigencias que demanda el conocimiento de tecnologías, y lo más importante no tiene el equipamiento idóneo para realizar la exploración e indagación de las evidencias digitales. A continuación se presentan estadísticas en relación al trabajo que desarrolla la DIVINDAT en la lucha contra la ciberdelincuencia

Política Nacional de Ciberseguridad

El Estado Peruano para proteger sus datos, información así como su infraestructura tecnológica en previsión de amenazas internas o externas, preservando la confidencialidad, integridad, legalidad y confiablidad de su información, ha implementado normatividad referente a la seguridad de

información, basadas en políticas, partidas y recursos pertinentes a fin de tener un gobierno en el país de Ciberseguridad actual que busca también la participación de entes estatales y del entorno privado, así como representantes civiles y otros. Dentro de las políticas implementadas por el Estado en Ciberseguridad consideramos resaltar el Fortalecimiento de las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa. Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en materia de ciberseguridad dentro de la Administración Pública. Desarrollo de un Plan de sensibilización y capacitación a todos los ciudadanos respecto a la Ciberseguridad y fortalecer la legislación en materia de ciberseguridad, la cooperación internacional y propiciar la adhesión del Perú a los diferentes organismos internacionales en esta temática.

Figura 18. Seguridad de Información

Normatividad Jurídica Internacional.

Legislación sobre los Delitos Informáticos en Europa – España.

La carta magna española establece en su Articulado 18, numeral “4”, La norma restringirá el empleo de la tecnología buscando asegurar la dignidad y la confianza personal y familiar y el completo conocimiento de sus derechos,

como se aprecia en la acotada norma incide directamente en la regulación de los delitos realizados a través de la tecnología, apreciándose que el bien jurídico es el de la intimidad. Así mismo existe varias normas que regulan los actos en conductas en delitos informáticos como: Ley de Servicios de la Sociedad de la información y Comercio Electrónico. Ley General en Telecomunicaciones. Ley Orgánica en Protección de Datos. Ley sobre la Firma Electrónica. Reglamento sobre medidas en seguridad de archivos automatizados con información personal.

El Código Penal Español consigna conductas ilícitas en relación con los ilícitos informáticos, indica que esta tipificación se aproxima a la regulada por el Convenio de Budapest en la lucha contra la Ciberdelincuencia: Delitos contra la privacidad, la entereza y la disponibilidad de los datos y sistemas informáticos: Artículos 197, 278.1 y 264.2. Delitos informáticos: Artículos 248, 248.2, 249, 255 y 256. Delitos en relación con el contenido: Artículos 186 y 189.

Holanda (1993)

Cuenta con la Ley de Delitos Informáticos, penalizando las figuras de hacking, el phreaking (evasión de pago de servicios de telecomunicaciones), ingeniería social y la propalación de virus. Cabe resaltar que los virus son tratados de manera especial en la Ley. Adherido al convenio de ciberdelincuencia.

Austria (1987)

El Código Penal Austriaco contempla la figura de Delitos Informáticos de la siguiente forma: Destrucción de datos: Art. 126. Estafa informática: Art. 148. Adherido al convenio de ciberdelincuencia.

Portugal (1991)

Este país europeo cuenta con la una norma que protege datos personales Informatizados y se aplica de manera supletoria del Código Penal: Delito de falsedad informática: Artículo 4. Delito relativo a datos: Artículo 5. Sabotaje en con empleo de la informática: Artículo 6. Acceso ilegitimo: Artículo 7. Interceptación ilegitima: Artículo 8. Reproducción ilegitima de programas

protegidos: Artículo 9.

Legislación sobre los Delitos Informáticos en América

México

En América Latina, fue una de las primeras en conectarse a Internet en 1989. El Código Penal mexicano sanciona los delitos informáticos en lo siguiente: Ingreso no autorizado a sistemas de información y equipos tecnológicos. Sabotaje informático. Acceso ilegitimo a información. Adherido al convenio de ciberdelincuencia.

Venezuela (2001)

Promulgo una ley especial que reprime los ilícitos informáticos tipificando los siguientes delitos: Atentar contra los sistemas que emplean TIC. Los que atentan con la propiedad. Atentar contra las actividades privadas de las personas y las comunicaciones. Los que atentan contra los niños y adolescentes.

Argentina (2008)

En su legislación cuenta con una norma que reprime los delitos informáticos la misma que incorpora y rectifica el Código Penal Argentino. Incorpora los términos “documento”, “firma” y “suscripción” en lo que se refiere a firma digital y los términos “instrumento privado” y “certificado” que vendrían hacer los documentos digitales. Adherido al convenio de ciberdelincuencia.

Chile (1993)

País en Latinoamérica pionero en sancionar los delitos informáticos a través de una Ley. Cuenta con la Ley 19223 que sanciona lo relativo a los delitos informáticos. También cuenta con la Ley 20.009 que sanciona el robo y extravió de tarjetas bancarias y la Ley 18.168 que regula las telecomunicaciones.

Brasil (2012)

Mediante la Ley 12.737 tipifica los delitos informáticos que combaten la

elaboración, venta y reparación de pornografía infantil y pedofilia en internet. Sanciona también la invasión de los dispositivos informáticos, la interrupción o perturbar el servicio de telégrafo, radiotelegráfico o telefónico, impedir o dificultar su recuperación. La falsificación en su totalidad o parte de un documento o cambiar un documento concreto real.

Estados Unidos (1994)
Cuenta con el Acta Federal de abuso computacional que busca eliminar los argumentos de los virus informáticos; mediante un programa, dañar información, códigos o el interior de un ordenador, así como sistemas informáticos, redes, información de datos y otros. Así mismo cuenta con legislación que sanciona las estafas electrónicas. Cuenta con el Acta de firmas electrónicas en el comercio global y nacional, ley sobre la firma digital.

Budapest 2001 Concejo Europeo, Convenio sobre la ciberdelincuencia.

“Única norma internacional que cubre la legislación sobre ciberdelincuencia tanto penal como en su proceso y de cooperación internacional. Es el primer y único instrumento internacional que existe a la fecha**.** La misma que refiere que ante la amenaza de los ciberdelincuentes al emplear las redes tecnológicas para cometer ilícitos y que las evidencias se almacenen y transmitan por las redes; asimismo existiendo la exigencia de cooperar entre los gobiernos y el ámbito privado en el combate contra la ciberdelincuencia, siendo también imprescindible cuidar los genuinos intereses en el empleo y aumento de las TIC; conscientes de que la eficacia de esta batalla contra delincuentes informáticos, hace necesario establecer un canal internacional de cooperación para intercambiar normas sobre legislación penal, oportuna y operacional; significando que también los hechos contrarios a trasgredir lo confidencial, la probidad y la excedencia de los sistemas de información, redes y datos informáticos, y tal como define el Convenio, y la admisión de poderes idóneos para combatir de manera efectiva la ciberdelincuencia, ayudando a ello su descubrimiento, investigación y sanción, en el ámbito nacional así como internacional”. Ministerio de Asuntos Exteriores Madrid

España, Oficina de interpretación de lenguas (2001). Convenio sobre ciberdelincuencia. *Concejo de Europa*. Recuperado de https://bit.ly/2OU44PR.

El convenio de cibercriminalidad enfatiza tres objetivos bien marcados, el primero que armoniza el derecho penal, segundo establece medidas procesales y finalmente busca una política ágil y eficaz de cooperación internacional. Analizaremos algunos: Convenio de ciberdelincuencia Budapest (2001) en su artículo 14° numeral 1 y 2, prescribe: "Ámbito de aplicación de las disposiciones sobre procedimiento. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente sección para los fines de investigaciones o procedimientos penales específicos (…)". Convenio de ciberdelincuencia Budapest (2001) en su artículo 20° numeral 1 prescribe, que para los logros en tiempo real de datos, las partes adoptaran nuevas leyes y lo que resulte necesario, y que sus autoridades puedan; producir o guardar mediante el empleo de medios informáticos disponibles en su país. Convenio de ciberdelincuencia Budapest (2001) en su artículo 22° numeral 1 prescribe: "Jurisdicción. Cada país deberá legislar dentro de ámbito jurisdiccional afirmándolo ante cualquier ilícito (…), en su país, en buques y aeronaves (…)".

Convenio de ciberdelincuencia Budapest (2001) en su artículo 23° prescribe: "Principios generales relativos a la cooperación internacional. Las Partes cooperarán entre sí en la mayor medida posible, de conformidad con las disposiciones del presente capítulo, en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos". Convenio de ciberdelincuencia Budapest (2001) en su artículo 25° numeral 1 establece que los países miembros se asistirán mutuamente respecto a las investigaciones u operaciones contra la ciberdelincuencia en temas de protección de sistemas y

datos informáticos, así como en la adquisición de evidencias digitales de un delito. Convenio de ciberdelincuencia Budapest (2001) en su artículo 35° prescribe: “Cada Parte designará un punto de contacto disponible las veinticuatro horas del día, siete días a la semana, con objeto de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito. Dicha asistencia incluirá los actos tendentes a facilitar las siguientes medidas o su adopción directa, cuando lo permitan la legislación y la práctica internas: a. El asesoramiento técnico; b. La conservación de datos en aplicación de los artículos 29 y 30; y c. La obtención de pruebas, el suministro de información jurídica y la localización de sospechosos”. Convenio de ciberdelincuencia Budapest (2001) en su artículo 37° numeral 1 prescribe: “Adhesión al Convenio. Tras la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa, previa consulta con los Estados Contratantes del Convenio y una vez obtenido su consentimiento unánime, podrá invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo y que no haya participado en su elaboración. La decisión se adoptará por la mayoría establecida en el artículo 20.d) del Estatuto del Consejo de Europa y con el voto unánime de los representantes con derecho a formar parte del Comité de Ministros (…)”. Convenio de ciberdelincuencia Budapest (2001) en su artículo 46° numeral 1 refiere que los países integrantes efectuaran consultas permanentes para facilitar la interacción de información jurídica o tecnológica sobre la ciberdelincuencia y pruebas electrónicas.

Figura 19. Convenio de Budapest

La Evidencia Digital y el modelo Argentino

El estudio forense de este país en relación con la evidencia determina que ella es todo vestigio, signo, señal o rastro, que se abandona en la actuación de la escena del delito como muestra de prueba de haberse realizado un hecho. La mencionada evidencia indiciaria tiene un terceto de elementos: un hecho comprobado (situación que se demostrado, reconocido y demostrado, de naturaleza circunstancial), una acción lógica o un veredicto de argumento y, como resultado de esa deducción, un hecho indicado (es lo que se intenta acreditar y es fracción del propósito de la polémica). En la etapa de un proceso la evidencia necesita una apropiada manifestación y/o examen para transformarse en el origen de indicios. Son los deponentes y los peritos (y posteriormente las partes en sus argumentos) quienes hacen originar y descubrir a las evidencias, asignándoles un valor indiciario decisivo.

En el proceso, las evidencias permiten ejecutar dos funciones: Función orientadora: la evidencia produce una dirección que conduce hacia la investigación. Esta guía por sí sola no garantiza un límite del hecho investigado. Por ejemplo el logro de una dirección IP que nos encamine hacia la localización de la ubicación real. Función probatoria: puede acudirse como prueba aquellos hechos en que la evidencia ratifica una de las partes del proceso.

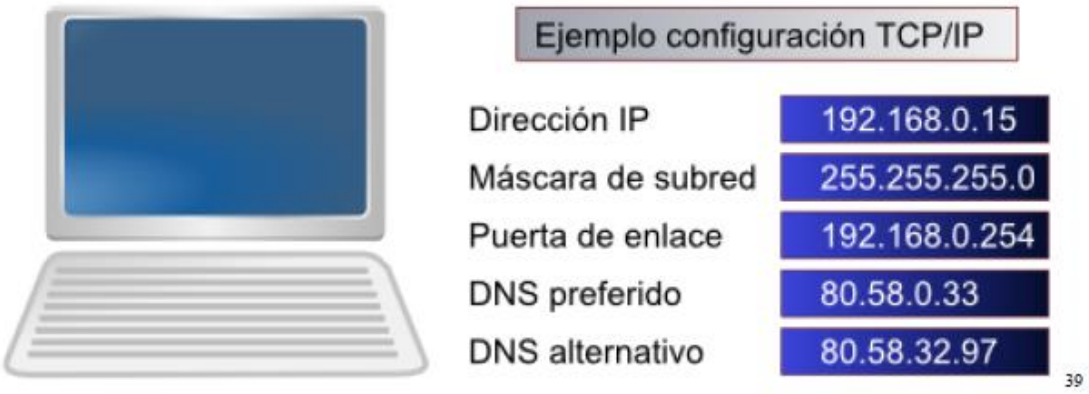


Figura 20. Configuración TCP/IP

Una evidencia tiene la posibilidad de efectuar continuamente las dos funciones. Es necesario tener presente que al pretender utilizar la evidencia en función probatoria, deberán cumplirse las formalidades de relevancia, idoneidad, confiabilidad y valor de esa prueba. En tal sentido el ingreso de las TIC a la actividad diaria ha determinado la obligación de insertar a los recursos tecnológicos como componentes de naturaleza investigatoria y/o probatoria, y, a su vez, la adquisición, comprobación, estudio, interpretación y exhibición de esta clase de evidencia, ha necesitado d la asistencia de peritos en la materia.

Resolución PGN Nro 756/16 de la Procuración General de la Nación Argentina.

Esta norma brinda directrices sobre la forma como se aborda, la conservación y el tratamiento de la evidencia digital respecto a cómo reprimir penalmente un proceso investigatorio fuera del país de este delito. Toma en consideración las recomendaciones dadas por la ONU en lo que se refiere a la transnacionalidad, su vínculo con el crimen organizado y la urgente atención de normas eficaces y estandarizadas para una buena cooperación internacional así como la atención del estado para la obtención de buenos resultados. Debe considerarse los siguientes principios, el primero es la relevancia jurídica que busca analizar e indagar con el objeto de acreditar una

hipótesis sobre un hecho. La segunda es la confiabilidad que indaga y busca homologar la repetibilidad y ser auditada, finalmente la suficiencia que en el proceso de recolección y análisis de las evidencias exista componentes hábiles para proteger los hallazgos del hecho investigado. Es importante que al llegar al lugar de hallazgo de la evidencia, evitarse que esta se contamine, proceder a retirar a las personas del área de trabajo. Tenerse cuidado que algún operador de seguridad modifique la información que se halla en el ordenador ya que ello luego constituirá los elementos de prueba. Es necesario que un perito con conocimiento en tecnologías acceda a la información que se halle en los ordenadores, afín de que explique las razones de interacción con la evidencia digital.

Delito transnacional. Jurisdicción y competencia.

En el 2017, Argentina aprobó la ley de ratificación de la Convención de Budapest, en la búsqueda de cooperación para la lucha contra delitos informáticos. El motivo importante de este documento es la cooperación entre los diferentes Estados de los países que lo integran y el sector privado. Ello conlleva y propone la integración de normas procesales y procedimientos para la investigación cooperativa de conductas ilegales en internet. La ley penal tendrá que modificarse algunas normas procesales. Por ejemplo, respecto a la evidencia digital se están utilizando las normas de códigos procesales diseñadas para la evidencia física. Uno de los beneficios de la cooperación es que cada país miembro tiene un contacto permanente todos los días durante las 24hs, para que países del Convenio se puedan comunicarse, informarse e intercambiar los diferentes procedimientos en la lucha contra la ciberdelincuencia.

La Evidencia Digital y el modelo Colombiano.

La Evidencia digital respecto a la normatividad en la que se desarrolla se ubica en el Derecho Colombiano, tal como lo tipifica según “el Código de Procedimiento Civil, Sección tercera, Título XIII. Adicionalmente, la Ley 527

de 1999, denominada Ley de Comercio Electrónico, reconoció como medios de prueba a los mensajes de datos, otorgándoles la fuerza probatoria establecida en el mencionado estatuto. Es un hecho entonces que tal disposición es un avance de la legislación colombiana tendiente a satisfacer las necesidades que el rápido avance de las Tecnologías de la Información exige". Moura W. (2012). Evidencia digital en Colombia: *Una reflexión práctica.* Recuperado de: https://bit.ly/2fmgvSL.

Ley 527 de 1999. Derecho Probatorio y Medios Electrónicos.

La Ley 527 de 1999, conocida como la ley de Comercio Electrónico, "tiene como aspecto relevante el de reconocer que no se le negará efectos jurídicos a cualquier tipo de información por el estricto hecho de constar en un mensaje de datos y en efecto, si una medida requiere que la información conste por escrito, dicho requerimiento quedará saciado por este medio, si la información que contiene es accesible para su postrera consulta. Respecto al valor probatorio de los mensajes de datos, los artículos 10 y 11 establecen que éstos serán admitidos como medios de prueba, teniendo como fuerza probatoria la otorgada por el Código de Procedimiento Civil. Asimismo, se establece que para su valoración deberá cumplir con las reglas de la sana crítica y los siguientes aspectos: La confiabilidad en que se haya generado, archivado o comunicado el mensaje de datos. La confiabilidad de cómo se haya cuidado la entereza de la información y la manera de identificar al que la origino". Moura W. (2012). Evidencia digital en Colombia: *Una reflexión práctica*. Recuperado de: https://bit.ly/2fmgvSL.

La Evidencia Digital comprende información en formato digital que establezca un vínculo. "Con el fin de garantizar su validez probatoria, los documentos deben cumplir con algunos requerimientos, estos son: Autenticidad: Satisfacer a una corte en que los contenidos de la evidencia no han sido modificados; la información proviene de la fuente identificada; la información externa es precisa. Precisión: debe ser relacionarla positivamente con el incidente. No debe haber ninguna duda sobre los procedimientos seguidos y las

herramientas utilizadas para su recolección, manejo, análisis y posterior presentación en una corte. Así mismo, los procedimientos deben ser seguidos por alguien que pueda explicar, en términos entendibles, cómo fueron realizados y con qué tipo de herramientas se llevaron a cabo. Suficiencia: Debe de propia forma presentar el espacio integro, y no una idea de un grupo individual de situaciones". Gutiérrez y Ribagorda (2004, p.295)

Requerimientos legales de la Evidencia Digital en Colombia.

La Ley 527 de 1999, reglamenta la admisibilidad y el valor probatorio de mensajes de datos, asimismo refiere criterios que dan valor probatorio. Comercio electrónico, Legislación Nacional Colombia Ley 527 (1999), en su artículo 5°, prescribe: "Reconocimiento Jurídico de los Mensajes de Datos. No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos". Comercio electrónico, Legislación Nacional Colombia Ley 527 (1999), en su artículo 8°, prescribe: "Original. Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si: a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma".

Comercio electrónico, Legislación Nacional Colombia Ley 527 (1999), en su artículo 9°, prescribe: "Integridad de un mensaje de datos. Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso".

Comercio electrónico, Legislación Nacional Colombia Ley 527 (1999), en su artículo 10, prescribe: "Admisibilidad y fuerza probatoria de los

mensajes de datos. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del capítulo VIII del título XIII, sección tercera, libro segundo del Código de Procedimiento Civil. En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original". Comercio electrónico, Legislación Nacional Colombia Ley 527 (1999), en su artículo 11, prescribe: "Criterio para valorar probatoriamente un mensaje de datos. Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas (…)".

La Protección al Dato Personal en Colombia. Los institutos más importantes, SANS16 y el NIST17.

"El interés del instituto es la difusión y cooperación en las técnicas y protocolos forenses aplicables en caso de delitos informáticos y los demás que involucren la aplicación de herramientas informáticas, con la finalidad de ayudar a los investigadores certificados, poniendo a disposición de forma gratuita documentos de investigación científica en lo referente a la informática forense y el derecho informático, temáticas que nutren el contexto total del campo de la investigación forense digital para la obtención de evidencia digital, con la aplicación de protocolo y herramientas forenses, no solo las consideradas por certificadas por un instituto reconocido como es SANS, sino también que permiten la obtención de la evidencia digital con características de autenticidad, integridad, originalidad, confiabilidad y no repudio". Mesa A. (2015). La evidencia digital eximente de violación a la protección del dato personal a partir de la autorregulación. *Revista Academia & Derecho Universidad Libre Seccional Cúcuta - Facultad de Derecho*. Recuperado de: https://bit.ly/2A8IJwB.

"En igual perspectiva frente a la utilidad y respaldo dado a la Evidencia Digital, se cuenta con el NIST: Para el campo de la informática o

computación forense promueve programas académicos de contenido novedoso y contemporáneo, satisfaciendo los retos diarios que la ciberdelincuencia plantea, entre los cuales podemos encontrar: Educación Nacional de Seguridad Cibernética de la Iniciativa (Niza), Biblioteca Nacional de referencia de Software es un proyecto apoyado por el Departamento de Justicia Estadounidense adscrita al Instituto Nacional de Justicia Federal, el Estado y Policía Local, además del National Institute of Standards y Tecnología-NIST, y las organizaciones de la industria para revisar los archivos de las computadoras, se puede definir esta cooperación como la forma eficiente y eficaz de usar tecnología informática “haciendo coincidir perfil de los archivos en el RDS, Esto ayudará a aliviar gran parte del esfuerzo necesario para determinar qué archivos son importantes como pruebas en los equipos o sistemas de archivos han sido incautados en el marco de las investigaciones penales” (NIST - National Institute of standards and technology), por ello se constituye como biblioteca dedicada al almacenaje de los tipos de software, Equipos forenses y referencia datos (CFReDS), permitiendo el desarrollo de equipos forenses de referencia Data Sets (CFReDS) para pruebas digitales”. Mesa A. (2015). La evidencia digital eximente de violación a la protección del dato personal a partir de la autorregulación. *Revista Academia & Derecho Universidad Libre Seccional Cúcuta - Facultad de Derecho.* Recuperado de: https://bit.ly/2A8IJwB.

Ambos institutos han determinado un marco mundial que garantiza la realización de actos de investigación con soporte a la resguardo de la privacidad, la intimidad y la protección del dato personal, respecto de lo recolectado en una prueba forense, en cuidado a los protocolos forenses digitales que administran y tienen estandarizados, permitiendo puntualizar los hechos sin que el presunto señalado, sea forzado en sus garantías constitucionales, ya que en atención a las normas legales, ellas en sí mismas poseen falencias en la sistemática, en la recogida de elementos, piezas y objetos de convicción, por consiguiente, debe respetar un doble filtro, atravesando inicialmente por las indicaciones legales del procesamiento y procedimiento sobre la etapa de hechos de investigación y finalmente la etapa de actos de prueba.

En lo que respecta a investigar este ilícito, es necesario efectuar un análisis juicioso referente a las reglas de indagación forense que se aplican en la adquisición de la evidencia digital, podemos apreciar en la revista académica lo siguiente: “Son elementos materiales probatorios y evidencia física. El mensaje de datos, como el intercambio electrónico de datos, internet, correo electrónico, telegrama, telefax o similar, regulados por la Ley 527 de 1999 o las normas que la sustituyan, adicionen o reformen; asimismo los demás elementos materiales que son encontrados, levantados y custodiados por el fiscal directamente o por conducto de la policía judicial o de peritos del Instituto Nacional de Medicina Legal y Ciencias Forenses, o de laboratorios aceptados oficialmente”. Mesa A. (2015). La evidencia digital eximente de violación a la protección del dato personal a partir de la autorregulación. *Revista Academia & Derecho Universidad Libre Seccional Cúcuta - Facultad de Derecho*. Recuperado de: https://bit.ly/2A8IJwB.

“La obtención de la evidencias responde a estándares de calidad formulados y certificados por entidades del ámbito privado, nacional e internacional, entre ellos ISO, SANS y NIST. En Colombia se cuenta con ICONTEC desde 1963, entidad que hace parte de IQNet18, que le da un alcance internacional a las certificaciones que ellos expiden en países donde se encuentran organismos de igual operatividad. Entre los servicios que se tiene la implementación, capacitación y formación, además de evaluación para certificación y recertificación en el cumplimiento de implementación en una norma ISO, son producto de la auto-regulación de organismos y empresas privadas, sin que previamente exista delegación por parte del Estado de esta función pública adscrita al Poder Judicial, constituyendo, en un indicador de pérdida de soberanía y control del Estado, al momento de regular los actos de investigación e indagación por entes públicos, toda vez que son normas que no se someten a control de legalidad, además quien determina su validez y eficacia jurídica, particularmente que no sea violatorias de la ley y la constitución, como si lo tiene el Código Penal, Procesal Penal”. Mesa A. (2015). La evidencia digital eximente de violación a la protección del dato personal a partir de la autorregulación. *Revista Academia & Derecho*

Universidad Libre Seccional Cúcuta - Facultad de Derecho. Recuperado de: https://bit.ly/2A8IJwB.

"Servicio de certificación y re-certificación en el cumplimiento de normas ISO para protocolos básicos de la evidencia. D NTC ISO 17025: Identifica lo que desarrolla la entidad así como las formalidades que debe cumplir en la norma. Evalúa la organización y la administración de laboratorios y órganos de inspección. Esta norma detalla las formalidades para constituir, establecer, elaborar, verificar, continuidad y mejorar un SGSI. Indica las formalidades para las aplicaciones de controles de seguridad acordes a las necesidades de la organización, así mismo busca proteger los activos de la información así como crear confianza a las partes interesadas. ISO/IEC 27037:2012: Esta norma está orientada al procedimiento de la actuación pericial en el lugar de los hechos del recojo, identificación y secuestro de la evidencia digital, no entra en la fase de Análisis de la evidencia. Las tipologías de dispositivos y entornos tratados en la norma son los siguientes: a. Equipos y medios de almacenamiento y dispositivos periféricos. b. Sistemas críticos c. Ordenadores y dispositivos conectados en red. d. Dispositivos móviles. y e. Sistema de circuito cerrado de televisión digital". Mesa A. (2015). La evidencia digital eximente de violación a la protección del dato personal a partir de la autorregulación. *Revista Academia & Derecho Universidad Libre Seccional Cúcuta - Facultad de Derecho*. Recuperado de: https://bit.ly/2A8IJwB.

La admisibilidad de evidencia digital y del criterio de expertos en un juicio, parten de la argumentación que de ello haga el representante del Ministerio Público a cargo del caso y finalmente el Juez, la forma de analizar su admisibilidad respondiendo a dos cuestiones en relación con la norma. En materia de la admisibilidad a un testigo técnico, quien debe ser capaz de testificar sobre cómo fue adquirida prueba, como la conservo en laboratorio, además de dar cuenta frente al tratamiento, integridad y originalidad, aspectos prevalentes para hacer frente a la idoneidad de los procesos sin que haya la necesidad de la calificación de otro experto en la materia, como lo plantea la

norma ISO / IEC 27042, el perito experto podría dar fe de los hechos técnicos aplicados.

El gobierno de Colombia promulgo la Ley 1928 del 24 de julio de 2018, mediante el cual se adhiere formalmente al Convenio, realizado en Budapest. Esta importante norma aporta un gran instrumento jurídico que contribuye a avanzar, con acciones decididas, contra la cibercriminalidad internacional y busca construir una política mundial común en la lucha contra la ciberdelincuencia. Por ejemplo una persona que reside en Colombia efectúa una compra en una tienda online que se encuentra ubicada en Chile y de la cual los dueños viven en Brasil, y el comprador es víctima de una estafa en ese sitio web, porque nunca le llega a su casa el producto que compró y al realizar el reclamo la tienda nunca le responde. Esta situación hace que la víctima efectué una denuncia por fraude en Colombia, pero el delito en sí se cometió desde Brasil y la evidencia se encuentra en Chile. Con la adhesión de Colombia al convenio de Budapest, se tendrían las herramientas necesarias para poder proceder ante casos como el expuesto anteriormente. Por lo tanto la adhesión al convenio representa un gran paso para Colombia en los procedimientos de investigación de delitos informáticos, ya que se beneficiara con herramientas para la lucha contra el cibercrimen.

International Organization on Computer Evidence (IOCE).

Este organismo internacional se organiza en agencias gubernamentales que llevan a cabo investigaciones referentes a evidencias digitales. Al respecto ha desarrollado seis principios. “Principios: 1. Cuando se maneje evidencia digital, deben ser aplicados todos los principios procedimentales y forenses generales. 2. Al obtener evidencia digital, las acciones que se hayan tomado, no pueden modificar esta evidencia. 3. Cuando sea necesario que una persona acceda a evidencia digital original, esa persona debe estar entrenada y calificada para este propósito. 4. Todas las actividades relacionadas con obtención, acceso, conservación y transferencia de evidencia digital, deben estar completamente documentadas, preservadas y disponibles para revisión. 5. El individuo es responsable por todas las acciones que realice con respecto

al manejo de evidencia digital mientras ésta esté bajo su cuidado. 6. Cualquier agencia gubernamental que sea responsable de obtener, acceder, conservar y transferir evidencia digital, es responsable de cumplir con estos principios". Moura W. (2012). Evidencia digital en Colombia: Una reflexión práctica. *Portal de e-gobierno, inclusión digital y sociedad del conocimiento*. Recuperado de: https://bit.ly/2fmgvSL.

La Evidencia Digital y el modelo Ecuatoriano.

Según el Código Orgánico de la función judicial, en su artículo 147, indica, que la validez y eficacia de un documento original, los archivos, mensajes, imágenes, bancos de datos y todo lo guardado o transmitido por medios de la electrónica, informática, dispositivos magnéticos, telemáticos, satelitales o producidos por nuevas TIC, destinadas a procesos judiciales. Sean actos o resoluciones judiciales. Igualmente los reconocimientos de firmas en documentos o la identificación de nombre de usuario, contraseñas, claves, utilizados para acceder a redes informáticas. Todo lo cual, siempre que cumplan con los procedimientos establecidos en las leyes de la materia.

Código Orgánico Integral Penal (2014) en su artículo 449 numeral 6, refiere que la prueba en documento podrá aceptarse como medio de prueba todo asunto digital. El COGEP (2015) en su artículo 196 numeral 3, dispone que la elaboración de la prueba en documento podrán ser fotografías, grabaciones, pruebas audiovisuales, de computación capaz de producir fe. Código Orgánico General del Procesos (2015) en su artículo 202 numeral 3, refiere sobre documentos digitales, se consideraran originales para todos los efectos legales. Las copias digitalizadas o escaneadas de documentos sean públicos o privados que se adicionen al expediente electrónico tendrán fuerza probatoria del original, dichos documentos serán serán cuidados por la titular y exhibidos en la audiencia de juicio.

El COIP, en su artículo 500 numeral 1, define que la evidencia digital es toda acción informática que simboliza acciones, información o definiciones guardados, procesados o transmitidos por un equipo de

tecnología que suministre un tratamiento informático, se incluye softwares hechos para un medio tecnológico separado, interconectado o relacionados entre sí. Asimismo para rescatar la integridad de la información se deberá realizar mediante técnicas digitales forenses. Para garantizar la integridad de lo que contiene los mensajes de textos, deberá emplearse los códigos de integridad que son algoritmos que evalúan un número único, a dicha función se les denomina HASH. El Código Orgánico Integral Penal, en su artículo 500 numeral 2, prescribe si la evidencia digital se ubique en dispositivos de almacenamiento sean discos duros, memorias y otros, se procederá a efectuar el acopio, en el mismo momento y espacio de la escena del hecho, empleando para ello métodos forenses digitales para cuidar la totalidad de su origen, debiéndose aplicar la cadena de custodia para su preservación y ulterior valor de su contenido.

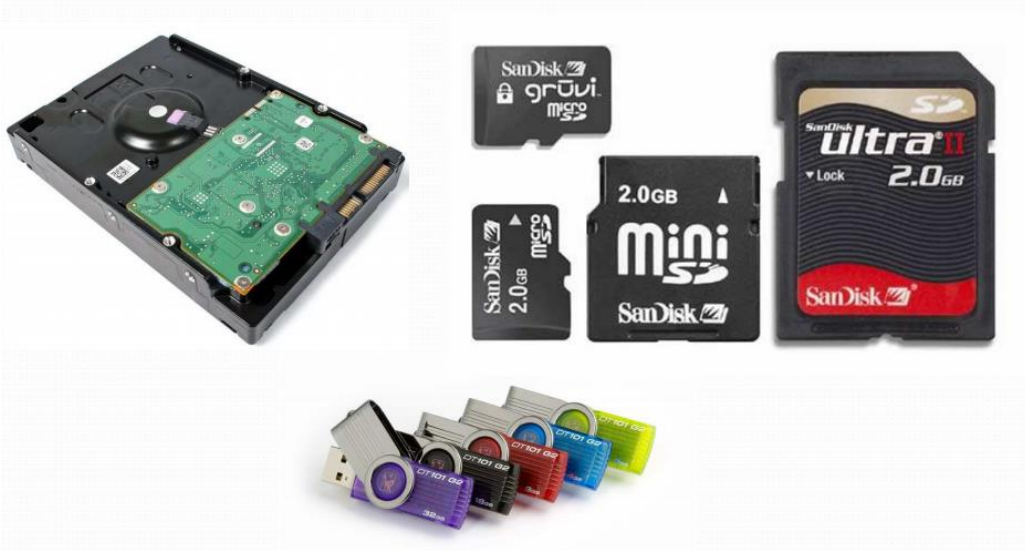


Figura 21. Dispositivos de almacenamiento

Legislación en España.

***Lucha contra la delincuencia informática - Aspectos generales*.**

El Internet ha supuesto una revolución tecnológica, pero al mismo tiempo, un problema para la represión de los delitos, “puesto que existe una especial dificultad para la búsqueda y persecución de los ilícitos informáticos, entre otros motivos, por el anonimato, la insuficiente conciencia de los usuarios

para mantener unas medidas preventivas de seguridad, o incluso el carácter transnacional de determinadas conductas delictivas". Fernández (2011 p.16). Las nuevas tecnologías e Internet constituyen unos de los principales impulsores de los cambios de muchas de las actividades desempeñadas por los ciudadanos, empresas, organizaciones y gobiernos en el actual mundo digital, convirtiéndoles en actores digitales cada vez más maduros e interactivos. "Actualmente existen unos 2.400 millones de usuarios conectados a la red, de los que 540 millones se conectan desde Europa, y entre ellos, unos 29 millones se conectan desde España". Gómez (2014 p. 81-82). "El coste que provoca la ciberdelincuencia en la economía es enorme. Según un informe cada año las víctimas pierden unos 388.000 millones USD en todo el mundo a causa de la ciberdelincuencia, lo que convierte a este tipo delictivo, en un negocio más rentable que el comercio global conjunto de marihuana, cocaína y heroína." Comisión Europea (2012 p. 2).

Para analizar la situación de la delincuencia organizada, y en concreto la ciberdelincuencia, son muy relevantes los datos brindados por el informe titulado *"Internet Organised Crime Threat Assessment* (IOCTA), valoración estratégica anual, realizado por Europol sobre los delitos informáticos, en virtud de la cual se podrán adoptar mejores decisiones y establecer prioridades en combatir los delitos informáticos, el abuso sexual infantil a través de Internet, los fraudes de pagos en la red, y otros tipos de delitos incluidos en este marco" Europol (2016 p. 19). La lucha contra la delincuencia informática se encuadra dentro del ámbito de la Europa de la Justicia, donde se articulan instrumentos y mecanismos para garantizar una cooperación judicial penal. "Actualmente la lucha contra la ciberdelincuencia se debe desarrollar en el marco de la Estrategia de Europol 2016-2020" Europol (2016 p. 5), en base a la cual deberán trabajar de forma coordinada las instituciones e entidades europeas, como Europol, para combatir cualquier tipo de delincuencia. La Comisión Europea ha mostrado en reiteradas ocasiones su compromiso para luchar contra la delincuencia informática o ciberdelincuencia y sofocar cualquier crisis de ciberseguridad, sosteniendo que "una respuesta eficaz en ciberseguridad requiere una cooperación rápida y eficaz entre todas las partes interesadas pertinentes y se basa en la

preparación y en las capacidades de cada uno de los Estados miembros, así como en una acción común coordinada apoyada en las capacidades de la Unión”. Comisión Europea (2017 p.2).

Los motivos que han provocado el aumento de la delincuencia informática son varios. Nos referimos a nuestras conductas, las cuales actualmente parece que únicamente se desarrollan en un contexto puramente digital, favorecidas por la absoluta digitalización de nuestra vida diaria, familiar, personal y profesional. “El anonimato en la red es otra circunstancia que motiva la comisión de estos tipos delictivos, ya que se pueden cometer con más facilidad, pueden ser ocultados y pasar inadvertidos, y en ocasiones puede haber más dificultades para perseguirlos ante los tribunales”. De la Mata (2010 p.19). La sensación de miedo y temor en la sociedad cuando se navega en Internet, utilizan las redes sociales o realizan transacciones comerciales electrónicas existe. Actualmente la percepción de inseguridad es un tema de interés para la investigación científica, para los medios informativos, y por supuesto para los ciudadanos” .De la Cuesta y San Juan (2010 p. 69-70). Por tanto, la sociedad percibe que ha aumentado el nivel de riesgo de ser una víctima, lo que les produce ansiedad, inseguridad y desconfianza cuando utilizan las TIC.

Se pueden señalar algunos bienes jurídicos a tutelar en el derecho informático, siendo cada vez más las voces académicas que sostienen que en el ámbito de la ciberdelincuencia debe crearse una nueva categoría jurídica penal que englobe las conductas vinculadas con el derecho informático, y en donde se lesionen no solamente los bienes jurídicos tradicionales, sino también unos nuevos bienes jurídicos protegidos propios de la era digital. La lucha contra la delincuencia informática se está desarrollando a nivel internacional, regional y nacional. La evaluación SOCTA UE de 2017 recomienda contemplar a la ciberdelincuencia como una de las cinco amenazas prioritarias. “En concreto, según este estudio, se consideran amenazas prioritarias las siguientes: la ciberdelincuencia; el tráfico y la distribución de droga; el tráfico ilícito de migrantes; los robos y asaltos organizados; y la trata de seres humanos” Comisión Europea (2017 p.7).

Medidas y mecanismos recientes para mejorar la ciberseguridad en la Unión Europea.

El pasado 13 de septiembre de 2017 se publicó la Comunicación de la Comisión Europea titulada “Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE” Comisión Europea (2017) donde se insta a mejorar la cooperación transfronteriza relativa a la preparación y prevención ante cualquier ciberincidente a gran escala. Por otro lado, se recuerda que sería conveniente establecer un “plan director” que creara un enfoque coordinado de la cooperación ante las crisis entre los diferentes elementos del ecosistema cibernético. “En la mencionada Comunicación se resalta la importancia que la ciberseguridad tiene para nuestra prosperidad y seguridad, ya que hoy las actividades de los ciudadanos europeos y la economía cada vez dependen más de las tecnologías digitales”. Comisión Europea (2017 p. 2-3).

“En definitiva, se requiere reforzar la resiliencia de la Unión Europea a los ciberataques, por lo que habrá que adoptar un enfoque colectivo y amplio, implantando medidas de diferente tipo”. Comisión Europea (2017 p.4-14): Creación de un mercado único de Ciberseguridad. Fortalecer las normas que regulan la ciberdelincuencia y ciberseguridad. Resiliencia mediante una respuesta rápida de emergencia. Es necesario tener respuestas rápidas y eficaces ante un ataque cibernético, para poder disminuir su impacto. Se ha propuesto la creación de un plan director que asegure un proceso eficaz de respuesta operativa a nivel de la Unión y Estados Europeos miembros, ante incidentes cibernéticos a gran escala. La capacidad de la ciberseguridad de la Unión Europea continuará reforzándose mediante la unión de centros de competencia en ciberseguridad, cuyo eje fomentara el desarrollo de tecnología en ciberseguridad y complementando los esfuerzos de capacitación en la UE. Creación de una base sólida de competencias cibernéticas de la UE. Deben adoptarse medidas para fomentar la educación en el ámbito de la ciberseguridad. Promover la ciberhigiene y la ciberconcienciación. Las Administraciones Públicas, las empresas y la ciudadanía deben tratar que todo el mundo entienda la amenaza que supone la ciberdelincuencia.

Por otra parte en la comunicación que estamos analizando se observa la necesidad de crear una ciberdisuasión efectiva en los Estados Europeos, mediante la aplicación de medidas que sean creíbles y disuasorias para potenciales ciberdelincuentes y ciberatacantes. Esta directiva supuso un gran avance en la lucha penal contra los ciberataques, no obstante, todavía se pueden mejorar los resultados en la aplicación de esta directiva. Sin embargo, la Comisión Europea plantea la aplicación de mejores medidas para reforzar la ciberseguridad: Identificar a los actores maliciosos. Reforzar la respuesta policial. A pesar de que la investigación y la adopción de acciones penales contra la ciberdelincuencia son eficaces, se debe mejorar el marco procesal para adaptarse mejor a las nuevas tecnologías y a Internet. Asimismo la Comisión Europea va a presentar propuestas para viabilizar el acceso transfronterizo a las pruebas electrónicas. Cooperación de los sectores público y privado contra la ciberdelincuencia. Es clave para que las autoridades públicas puedan luchar con eficacia contra la ciberdelincuencia. Reforzar la respuesta política. La colaboración política se consigue gracias a la aplicación del "conjunto de instrumentos de la ciberdiplomacia", para establecer vínculos de comunicación y diplomáticos en relación a las actividades cibernéticas maliciosas. Aumentar la disuasión de la ciberseguridad a través de la capacidad de defensa. Fortalecer la cooperación internacional en materia de ciberseguridad.

Directrices para la recopilación de evidencias y su almacenamiento. RFC 3227.

Los RFC (Request For Comments) son documentos que detalla cómo debe ser aceptado y pueda ser implementado sin ambigüedades una evidencia. Establece un procedimiento para recoger y guardar la evidencia. En ella podemos apreciar y describir la volatilidad de los datos, nos permite definir que recoger, así como que guardar y la documentación de los datos. "Principios en la recolección de evidencias: Capturar una imagen del sistema tan precisa como sea posible. Realizar notas detalladas, incluyendo fechas y horas indicando si se utiliza horario local o UTC. Minimizar los cambios en la información que se está recolectando y eliminar los agentes externos que

puedan hacerlo. En el caso de enfrentarse a un dilema entre recolección y análisis elegir primero recolección y después análisis y Recoger la información según el orden de volatilidad (de mayor a menor). Tener en cuenta que por cada dispositivo la recogida de información puede realizarse de distinta manera". Martínez A. (2014). RFC 3227 - Directrices para la recopilación de evidencias y su almacenamiento. Instituto Nacional de Ciberseguridad de España. Recuperado de: https://bit.ly/2QUi0Lj.

La prueba pericial informática.

En ocasiones se requiere la intervención de personal calificado, como los peritos informáticos, para darle legalidad y validez a la información que se encuentra en un dispositivo electrónico, para su admisibilidad en un proceso judicial. Para las pruebas electrónicas, la doctrina jurisprudencial exige la constatación de la existencia del hecho a través de periciales informáticas cuando aquellas sean contradichas, lo cual no implica que únicamente sea válida la prueba digital que haya sido confirmada por perito informático. Entonces, la prueba pericial informática será indispensable para los supuestos en que se impugne la veracidad de la prueba digital aportada, así como cuando se requiera el ingreso a la información contenida en un dispositivo y la misma haya sido encriptada o eliminada o, simplemente, cuando el acceso a dicha información sea difícil y se requiera por ello conocimientos técnicos.

Por lo expuesto, procede en este punto definir la prueba pericial informática como la prueba practicada por un perito con conocimientos especializados en la materia, quien emitirá un informe sobre unos hechos a través del cual aporta al juez conocimientos técnicos que éste no posee, permitiendo valorar la prueba. La prueba pericial informática, por tanto, no solo trata de una constatación de hechos, sino que requiere una valoración por parte del perito especializado que determine la veracidad, exactitud, inalterabilidad de los mismos. Cabe señalar que los datos informáticos pueden ingresarse en el proceso a través de distintos medios probatorios y no solo mediante la pericia informática: a través de documentos electrónicos, como un pdf.; una impresión en papel de una cadena de correos electrónicos;

la testifical, por ejemplo interrogando a un tercero que fue testigo de una conversación de Whatsapp que mantuvieron otras personas, etc. En definitiva, toda información de valor probatorio digital podrá aportarse como prueba en el marco de un proceso. Y, esta aportación podrá hacerse a través de pruebas tradicionales, no obstante, cuando se impugne la autenticidad de la misma, será necesario recurrir al informe emitido por un perito informático que dictamine sobre la exactitud, veracidad y origen del contenido de la misma.

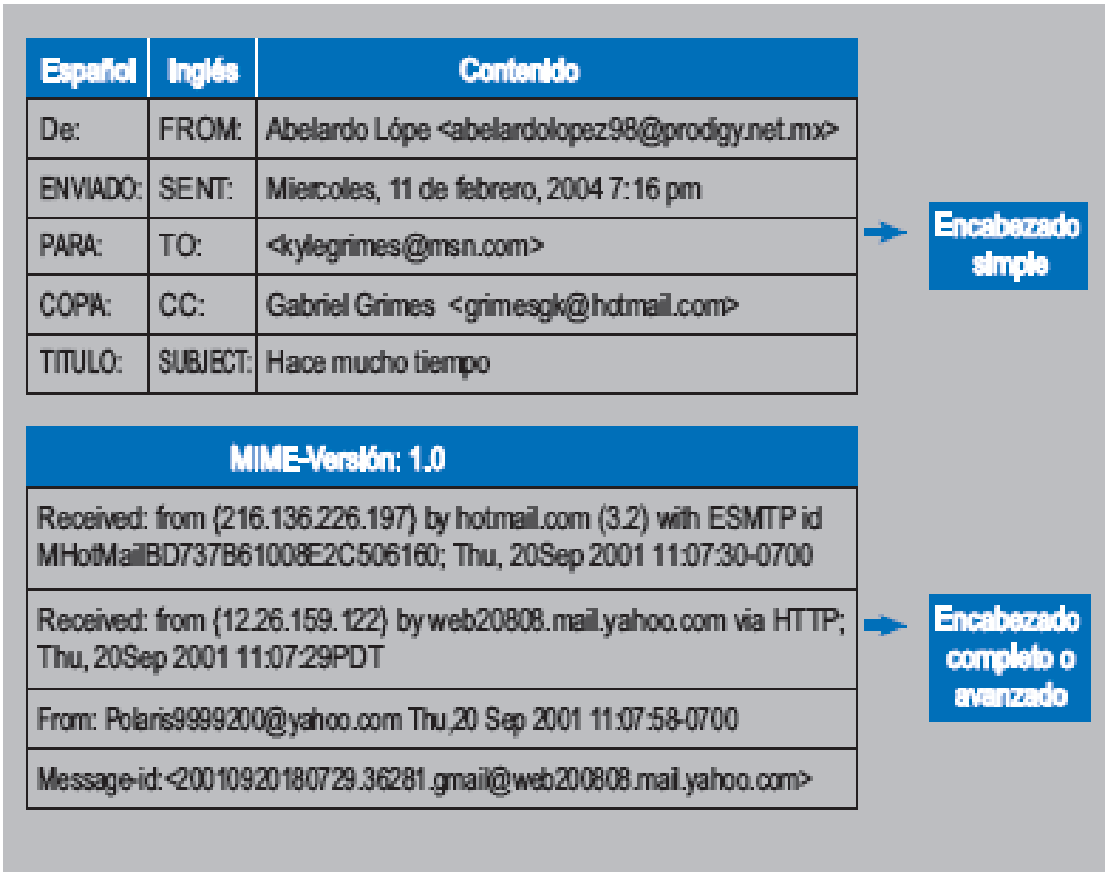


Figura 22. El Correo electrónico

El Proceso penal admisión de la prueba.

“La etapa oral es el lugar en que se practica la prueba en el proceso penal, respetando los principios de publicidad, oralidad, inmediación y contradicción. Además, con respecto al principio de contradicción, cabe señalar que para dar cumplimiento al mismo, la evidencia contenida en soportes magnéticos se reproducirá en el juicio oral”. Lluch y González (2013). *Estudios sobre prueba*

penal. Madrid: Wolters Kluwer. “El hecho electrónico puede incorporarse al proceso a través de un documento tradicional impreso o mediante la aportación del propio documento electrónico”. Navalón (2014) La prueba electrónica ante los tribunales. Valencia: Tirant lo Blanch.

Requisitos de acceso: necesidad, pertinencia y utilidad.

En la LEC el artículo 299, refiere a intervinientes en un procedimiento que aporten evidencias digitales, así como otros como medios donde se halla textos, sonidos e imágenes, y todos aquellos que posibiliten guardar, visualizar estos medios, importantes para la causa. En numerosas ocasiones estas pruebas ‘modernas’ son rechazadas, pero no se produce por su falta de encaje sino por motivos relacionados con su ilicitud o pertinencia. La admisión de la evidencia es el resultado del análisis hecho por el juez sobre las condiciones del medio o actividad probatoria propuestos para su admisión en el proceso. Deberá determinarse si la evidencia digital cumple los requerimientos de pertinencia, utilidad y legalidad. La prueba que pretenda ser incluida en el proceso ha de reunir necesariamente dichos requisitos, pues su incumplimiento será motivo de inadmisión de la misma.

Respecto a la utilidad de la prueba, el apartado segundo del art. 283 LEC señala que aquellas evidencias que no contribuyan a aclarar la situación polémica serán inútiles. Y, será inútil aquella prueba que, conforme a la experiencia, se pueda prever que no logrará el resultado pretendido y el requisito como prueba, se encuentra regulado en el apartado tercero del artículo 283 LEC, implica que cuando se pretenda acreditar un hecho por medio de una actividad contraria a la ley, tal actividad quedará prohibida y será inadmisible como medio de prueba, puesto que constituirá una prueba ilegal. Rodríguez (2018). La prueba digital en el proceso penal (tesis postgrado). Universidad de la Laguna, Tenerife, España.

La verificación por el juez del cumplimiento de estos requisitos para la admisibilidad de la prueba electrónica plantea ciertos problemas en ocasiones, motivo por el cual, autores como De Urbano Castrillo, establecen

una serie de puntos que han de observarse para la decisión sobre la admisibilidad: a) identificar el ordenador del que procede el documento electrónico, b) verificar que el funcionamiento del ordenador sea el correcto, c) demostrar que como consecuencia de los datos introducidos en el equipo se ha producido el resultado, d) explicar la fiabilidad del proceso de registro y salida de los datos obrantes en el equipo y e) acreditar quienes participaron en el procedimiento de elaboración del documento. El cumplimiento de lo señalado en los puntos expuestos, debido a su complejidad técnica, evidencia la necesidad en muchas ocasiones de aportar prueba pericial informática.

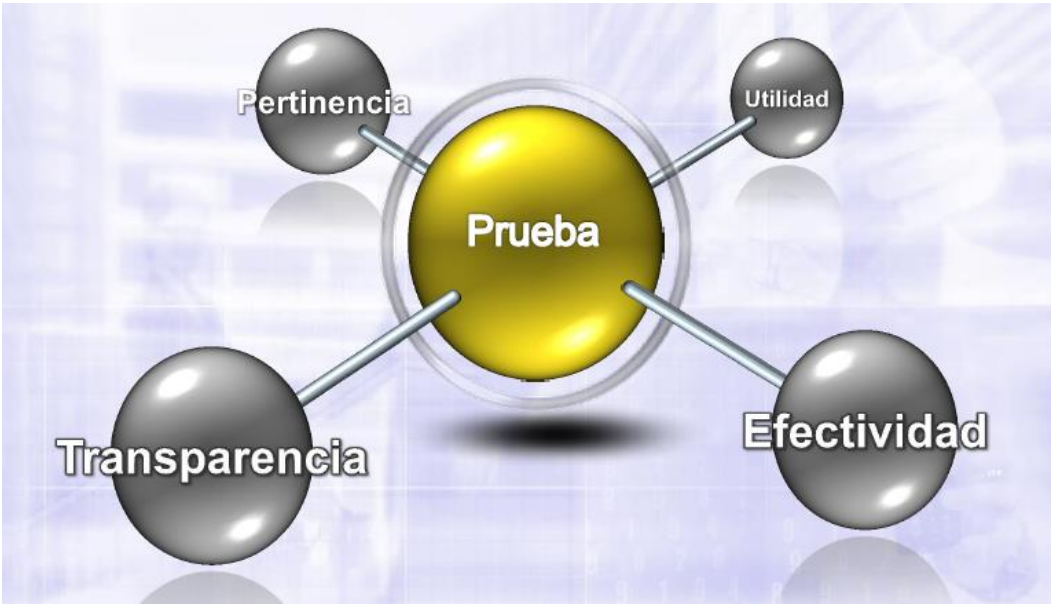


Figura 23. Legitimidad de la prueba

***Valoración de la prueba*.**

El tenor literal del art. 741 LEC dispone que “ apreciándose con consciencia las evidencias presentadas en el proceso, el Tribunal y además las deducciones disertadas por el fiscal y la defensa técnica y lo versado por las partes, emitirá sentencia en los plazos de ley”. Rodríguez (2018). La prueba digital en el proceso penal (tesis postgrado). Universidad de la Laguna, Tenerife, España. Así, la regla general para la valoración de la evidencia digital es el sistema de libre valoración, como lo dispone el art. 384.3 LEC. Los preceptos de la sana crítica se identifican con las máximas de

experiencia, que pueden ser definidas como propagaciones basadas en un cierto número de experiencias, considerándose que ellas denotan lo que suele ocurrir en casos análogos.

Este sistema de libre valoración no implica total discrecionalidad judicial ya que tal valoración ha de estar motivada pues ha de determinarse por el juzgador porqué otorga o no credibilidad a un concreto medio probatorio y, preservar la inocencia. Así, en lo se refiere a la libre valoración de la evidencia, es la apreciación de parte del juzgador de la prueba incriminatoria con arreglo a criterios de lógica y razonabilidad. Para tal valoración ha de tener en cuenta lo siguiente: a) Deberá analizarse si existe prueba de cargo; b) Realizar un 'juicio sobre la suficiencia' que implica que, de existir prueba de cargo, habrá de comprobar si la misma es capaz de desvirtuar su inocencia y; d) Deberá el juzgador motivar razonadamente el decaimiento de la presunción de inocencia. Como señalamos anteriormente, la información penal útil disponible en dispositivos electrónicos o alojada en servidores, podrá incorporarse al proceso mediante los medios probatorios oportunos. Pero para garantizar que los datos obtenidos en los registros hechos a dichos dispositivos o servidores permanecen inalterados o que son exactamente los contenidos en los mismos, se precisa de una serie de garantías.

Sobre el clonado de los datos.

La primera garantía, se refiere al proceso de clonado de la información. Ya que al accederse u obtener los datos del dispositivo, se procede al volcado o clonado, que es efectuar una reproducción idéntica de todo su contenido guardado. Básicamente lo que se realiza es una copia física del contenido del mismo. Pero es mediante el hash, una función basada en algoritmos que otorga al contenido de un archivo un valor numérico. "Mediante este procedimiento deberá originarse un original de los datos, una copia resultado del clonado que será sobre la cual se practicará la pericial informática, y una segunda copia para el propietario de los datos, para el caso de que fuese necesario que el mismo continuase con la actividad que viniese ejerciendo". Delgado (2016 p.4). El original, una vez hecha la copia o clonado, quedará

precintado y enviado al juzgado para que, en el caso de que se cuestionase en el seno del proceso sobre la autenticidad o exactitud de la copia, pudiera cotejarse la misma con el original.

Sobre la presencia del Letrado de la Administración de Justicia durante la práctica del clonado o volcado de datos.

En segundo lugar, los registros efectuados deben ser documentados. Esta función debe encargarse al Letrado, formulándose acta en la que se indique con precisión las actividades practicadas y quienes intervinieron en el registro. Cabe precisar que, en ocasiones, para asegurar la efectividad de la diligencia, la entrada en el domicilio se podrá practicar sin la presencia inmediata del Letrado aunque, posteriormente, la Policía Judicial deberá comunicar al mismo en qué circunstancias se produjo la entrada, qué Agente intervino, así como los efectos intervenidos.

En la indicada acta, deberá registrarse el IMEI del dispositivo, el número de serie del disco duro extraído (sin acceder a su contenido) y, de tratarse de portátiles, tablets o pendrives, se procederá a precintar los mismos. Ello es así en aras a preservar la cadena de custodia. En el material precintado firmará el Letrado de la Administración con rotulador permanente, en custodia policial. La policía deberá solicitar al juzgado el desprecinto y volcado de la información que se harán en sede judicial y de la que también se levantará acta. También será necesaria su presencia durante el desprecintado del dispositivo electrónico intervenido que se halla bajo custodia policial. Bastara la presencia del funcionario judicial durante la entrada y registro al lugar cerrado en que se halle el dispositivo, siendo dispensable durante el proceso de volcado de los datos que además, suele ser un proceso lento cuya duración puede alcanzar horas. En conclusión y, en consonancia con la jurisprudencia analizada, la presencia del fedatario judicial durante el volcado de datos obrantes en dispositivos electrónicos no actúa como presupuesto de validez de su práctica.

Sobre la presencia del investigado o su letrado durante el desprecintado y volcado de los dispositivos electrónicos.

Otra garantía que prevé la LEC, es la presencia del investigado y su letrado durante el desprecintado del dispositivo electrónico, tal y como se contempla en el artículo 476 de dicha norma legal, a fin de que esta parte pueda comprobar que el precinto está intacto y que, por tanto, no ha sido alterado el contenido del dispositivo. No obstante, a pesar de que el mencionado precepto contemple la posibilidad de que el investigado esté presente durante la práctica de tal diligencia, así como la posibilidad de que este pueda nombrar a un perito que comparezca a la misma, "tal presencia no constituye presupuesto de validez de la diligencia" y así lo dispone la Audiencia Nacional en sentencia núm. 34/2014 de 24 de julio (en el mismo sentido resuelve la STS 187/2015 de 14 de abril). Por lo que la ausencia del investigado durante el desprecinto del dispositivo electrónico, no invalida por sí misma el procedimiento y, por tanto, la autenticidad de la prueba sigue intacta.

Cadena de custodia.

Son las acciones y procedimientos que se ejecutan para garantizar la identidad e integridad de las evidencias obtenidas durante la investigación y garantizar así su total eficacia procesal. Su ruptura no permitiría afirmar la 'mismidad' de la prueba y, en consonancia, podría desvirtuar la misma. Los distintos tipos de prueba tecnológica se encuentran en constante movimiento, cambio e innovación al estar ligados a los cambios de las TIC. "Siendo las más comunes en los procesos penales las siguientes: Los email, mensajes multimedia en redes públicas. Los SMS y MMS de telefonía móvil, que consiste en la transmisión y recepción de mensajes de texto, particularmente los SMS que adicionalmente puede efectuar el mismo tráfico con archivos de tipo fotográfico, audios o películas. Los debates en línea, redes sociales, conversaciones, zonas de trabajo, estos se desarrollan en el ciberespacio donde las personas interactúan de diversas maneras, e intercambian distintas consideraciones, costumbres o reflexiones de distintas materias con una infinidad de usuarios de la red internet. El documento de identidad electrónico

empleado por las personas para todo tipo de trámite en línea, básicamente operaciones en tiempo real con entidades estatales o empresas particulares.

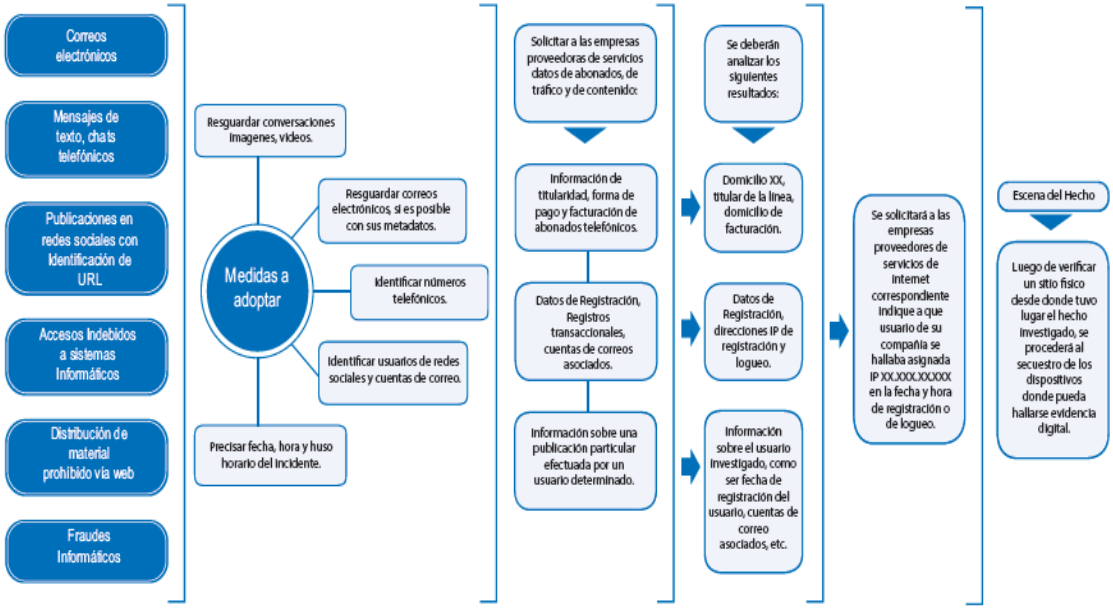


Figura 24. Investigaciones en entornos digitales

Aproximación al concepto de prueba electrónica.

Las apps, nos brinda el uso de aplicativos como: WhatsApp, Telegram, Hangouts, WeChat, BlackBerry, Messenger, Facebook y muchos otros que generan evidencias digitales utilizables en un proceso. En efecto, estas aplicaciones tecnológicas diseñadas para emplearse en teléfonos móviles, tablets u otros dispositivos, se presentan como medios de prueba. El concepto unánimemente aceptado, respecto a la evidencia digital lo precisa como una información que se ubica y obtiene en un dispositivo informático que puede evidenciar un hecho o acción con precisión, debiéndose para ello ser extraído conforme establece los procedimientos para su veracidad, integridad y traslado.

Sobre la naturaleza de la prueba electrónica.

Muchos estudios tratan de determinar que la evidencia digital se caracteriza como una evidencia documental e inclusive aplicándosele el principio de equivalencia funcional. Es preciso advertir que la evidencia digital representa una fundamento completamente independiente, con particularidades que la denotan como única. Las técnicas de capturas de pantalla tienen como objetivo brindar un sustento documental, mediante el congelamiento de pantallazos de diferentes situaciones como interacciones en diálogos o el intercambio de imágenes entre otros con la intensión de darle valor como prueba en un juicio. Es preciso indicar que en una causa penal se busca el debido proceso y por sobre todo la presunción de la inocencia, por lo que esta acción desbarata dichos mensajes que podrían ser ciertos ya que existe una alta posibilidad de ser adulterado por ser muy volátiles. Ante ello un Tribunal Supremo español determino que la veracidad de estos mensajes no pueden ser presentadas al proceso tan solo como impresiones, debe ser necesario una prueba pericial a fin de determinar su origen, la identificación de los intervinientes y por sobre todo la integridad de lo que contiene, solo de esa manera obtendrá valor probatorio.

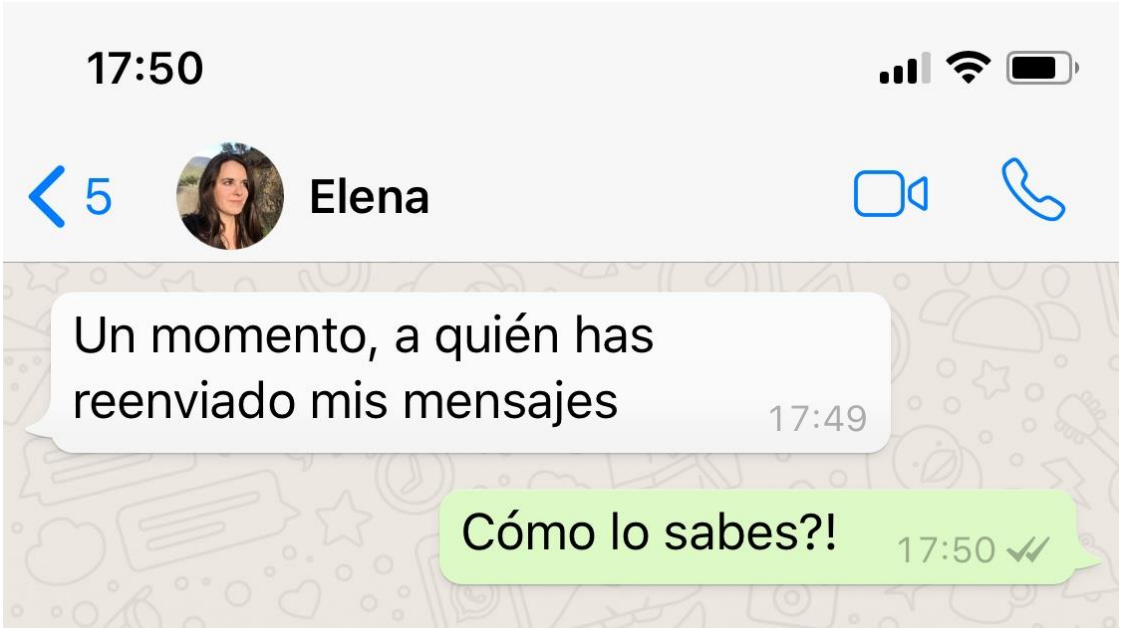


Figura 25. Congelamiento o pantallazos de mensajes

Es preciso indicar que el procedimiento de interrogar a los intervinientes del proceso, busca darle credibilidad y valor a la evidencia digital a través de la aceptación voluntaria de parte del autor de los mensajes de conversación que se presentan en el juicio. La técnica denominada prueba pericial informática tiene por objetivo examinar, descomponer un dispositivo a fin de saber si se realizó modificación o contaminación de la evidencia, se debe formular un informe donde se detalle los hechos y las acciones seguidas respecto a la evidencia para saber la certeza de la misma, que esta se encuentre en su estado original ya que es la mejor manera de saber si se produjo o no alteración a la misma. El examen del juez directamente a la evidencia digital a través del análisis pericial es conocido como reconocimiento judicial, y debido a ello se considera como prueba admisible ya que se demuestra la originalidad y legitimidad de la evidencia que finalmente puede concluir un juicio.

Procedimientos Tecnológicos de la Evidencia Digital

Normas estandarizadas sobre peritaje informático de la evidencia digital.

Norma UNE 71505 – 2013 define conceptos sobre la seguridad y controles de las evidencias informáticas. Indica las propiedades básicas de confiabilidad. Procesos de originalidad, reservas y cumplimiento. El periodo en que desarrolla la generación, guardado, comunicación y traslado de las evidencias digitales. Norma UNE 71505-2 2013 establece registros y desarrollo en la gerencia de seguridad de las evidencias, tales como la confiabilidad, la autenticación, y la integridad, asegurando el poder ser ubicada, rescatada y presentada y la completitud que nos muestra la publicación del contenido de la evidencia. La UNE 71505-3 2013 tiene como objetivo garantizar la legitimidad y plenitud de la evidencia digital conservando su legalidad probatoria ante el juez, brindando al perito informático el poder analizar y verificar, la validez y se encuentre intacta la evidencia. La firma electrónica y sello del tiempo son procedimientos en el que se aplican por ejemplo. UNE 71506 2013 esta procedimiento desarrolla un método cuyo objeto es la

preservación, adquirir, documentarla, analizarla y presentar las evidencias digitales.

La etapa de la preservación, trata en todo momento de preservar la validez y confianza de la originalidad de la evidencia. La adquisición es la etapa donde se efectúa una clonación de los datos primarios, mediante la documentación calculándose el código hash para cada evidencia. Cuando los sistemas se encuentran apagados, es necesario que el perito informático, suprima el soporte que contiene el clonado forense, debiendo emplear bloqueadores de escritura asegurando de esta forma que los datos primarios no se modifiquen, calculándose el hash de la evidencia original. Por el contrario cuando los sistemas se encuentran encendidos debe adquirirse volatilidad de más a menos.

En el análisis forense deberá documentarse todo proceso desde el principio hasta que este termine sobre la evidencia, el informe del perito debe precisar los procedimientos y medios empleados así como el tiempo en que se realizaron. La etapa del análisis se efectúa varios procesos que tienen como objetivo buscar soluciones a incógnitas respecto a la intrusión, su inicio, relación de sistemas dañados, los métodos empleados.

Figura 26. Sistemas operativos

El proceso de restauración de archivos suprimidos ya sea total o parcial ubicadas las diferentes áreas del dispositivo de almacenamiento no asignado por el sistema en ese instante y en el volumen sin emplear, restaurar carpetas y archivos perdidos, también hallar archivos completos o

partes de ellos de sus cabeceras. El sistema operativo deberá detallarse respecto a su información indicándose de que tipo es, usuarios que emplearon el mismo y sus direcciones de seguridad.

Estándares a nivel internacional.

La ISO/IEC 27037 2012 brinda patrones en las acciones del empleo de la evidencia digital, siendo entre ellos la de identificar, seleccionar, adquirir y preservar la evidencia. El ISO/IEC 27042 2015 tiene las características de una norma orientadora respecto al análisis así como interpretar la evidencia digital abordando conceptos de continuación, valor, reproducción y repetitividad. El documento RFC 3227 desarrolla una directiva en el procedimiento de recolectar y el almacenar las evidencias digitales. Respecto al procedimiento de adquirir una imagen o copia del sistema este debe realizarse de tal forma que se obtenga lo más idéntico posible al original, la misma que debe contener fechas, hora local UTC, análisis de volatilidad de las memorias cachés y de la memoria RAM y finalmente informe de los dispositivos de almacenamiento.

Mercosur: Principios de tratamiento de la evidencia digital.

Figura 27. Procedimientos para el tratamiento de la evidencia

Recolección y preservación de la evidencia digital.

En el lugar de los hechos y proceder a evaluar, es muy posible hallarse distintas situaciones, con diferentes resultados para cada momento que pueda elevar la calidad y cantidad datos a detener, es importante ante ello cuidar su originalidad para su posterior admisibilidad en un proceso judicial. Es muy necesario luego del cuidado del lugar, perennizar a través de documentos todas las acciones con respecto al ordenador, sus partes y los mecanismos de almacén de información, a continuación apreciar el estado del ordenador si está encendida o apagada, esto determinara el proceso que se adoptara, debiéndose tener cuidado que el ordenador este en modo suspendido o ahorro de energía. Debe tomarse en cuenta en el tratamiento de la evidencia que al iniciar contacto con un dispositivo tecnológico, perennizarlo mediante tomas fotográficas o películas caso contrario elaborar un mapa del lugar de los hechos sin depreciar nada, indicando cada uno de los dispositivos respecto al ordenador, hacer tomas fotográficas al frente y detrás las diversas de las conexiones y cables, así como lo que muestra en ese instante la pantalla. Esta situación generara distintos procedimientos para los casos del ordenador apagado o cuando este encendido.

Debemos tener mucho cuidado al desenchufar el ordenador, ya que los diferentes sistemas operativos cuentan con mecanismos y comandos que mantienen intacta información de mucho valor. Estos podrían ser la identificación de la última persona que ingreso al sistema indicándonos el nombre de user y clave de acceso, en que momento lo hizo día, hora y minuto; últimas acciones realizadas por el usuario; aplicativos accesados, documentos o archivos utilizados, etc. También se presenta situaciones cuando el ordenador esta encendido, sobre el particular no debe apagarse ya que la información que puede mostrarse en ese instante en el monitor es probable sea importante como evidencia en el proceso, asimismo debe tenerse cuidado de los programas o aplicativos que se encuentran abiertos así como documentos, hojas de cálculo o imágenes o hechos que podrían ser presuntamente ilegal; se recomienda perennizar la acción a desarrollar así

como emplear dispositivos que capturen datos o bloquee la escritura, para que no se altere la evidencia.

De anterior descrito es necesario tener mucho cuidado con lo que en adelante se hará respecto a la evidencia, en primera instancia el empaquetado, su traslado y la seguridad. Para ello verificar que la evidencia hallada este completamente documentada, precintada, señalada, fotografiada y con su respectivo mapa así como de haberse realizado un inventario de todo lo hallado. Otra de las consideraciones de mucho cuidado es la manipulación de los dispositivos que se hallen en el lugar de los hechos, los estudios y pruebas de estos medios magnéticos en los cuales se halla la información, es recomendable hacerlo en zonas acordes a las necesidades de preservación que reúna las condiciones de áreas seguras sin exposición de energía estática, debiéndose tener cuidado del ingreso por WI-FI u otra forma de ingreso remoto. Asimismo emplear implementos de látex como guantes o pulseras con descarga a tierra para prever alguna descarga ajena a nuestra voluntad que pudiera malograr o dejar inoperativo el equipo.

El procedimiento de imagen forense es el duplicado integro de un dispositivo magnético donde se guarda información, es un espejo idéntico y esta puede realizarse en forma externa, obteniéndose físicamente el disco del ordenador procediéndose a efectuar un copiado total; y la otra manera es interna conectándose un medio desde fuera del ordenador sin retirar físicamente el disco del ordenador, procediéndose mediante las conexiones de cables al medio, la extracción de la información. En ambos casos es muy importante este procedimiento ya que así se logra efectuar un análisis minucioso de la evidencia hallada permitiendo tener los metadatos, atributos y otros que contiene el dispositivo de almacenamiento sin alterar su originalidad.

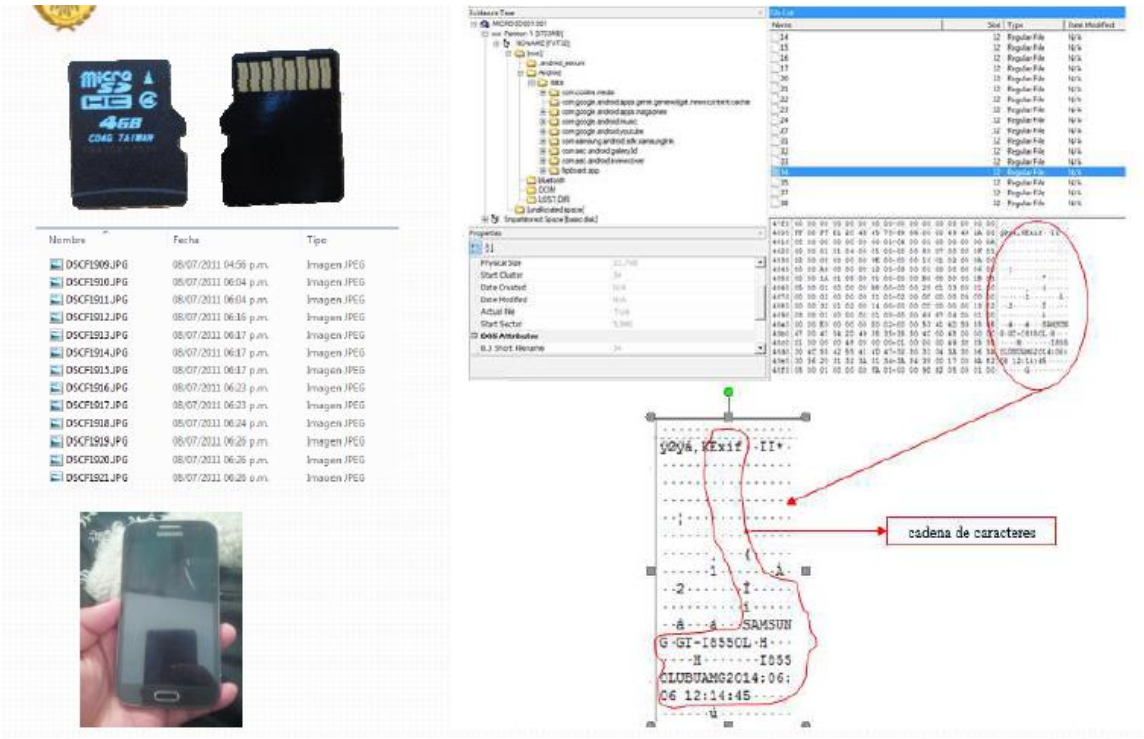


Figura 28. Metadato

Ciberseguridad judicial y sellado de tiempo.

En la evidencia digital el conocer el tiempo resulta gravitante cuando se requiere garantía y credibilidad respecto a la afirmación de la fecha y la hora, sobre todo cuando se necesite para ser presentada como aporte de prueba, así como garantizar el origen y la plenitud de los datos. Es por eso que se aplicó el método del sellado del tiempo, que en España se emplea en ciberseguridad jurídica. El sellado de tiempo es un método que sirve para mostrar que determinados datos existen y que no han sido modificados desde su origen. La base de este método implica la participación de la autoridad de certificación, de registro y otras entidades, así como una serie de políticas y actividades. El procedimiento determina la intervención de una entidad acreditada como Autoridad de Sellado de Tiempo, que genera y garantiza un resumen, la fecha y la hora de un documento, y que almacena los sellos emitidos para posteriores verificaciones.

“Múltiples aplicaciones: El sello del tiempo tiene muchas aplicaciones: factura electrónica, protección de la propiedad intelectual, registro electrónico, libros financieros, apuestas, pedidos, *logging* seguros, transacciones seguras de comercio electrónico, voto electrónico, transparencia. La fuga de datos es otro de los problemas que previene el uso del sellado del tiempo. ¿Cuántos despidos ha realizado una empresa? ¿Cuántos datos han circulado por una compañía de pendrive a pendrive o de ordenador a ordenador? ¿Y cuántos datos terminan en casa de un empleado, pareja o socio? Es posible que esta información aparezca en Internet sin saber exactamente de dónde proviene el ataque ante el que conviene reaccionar de forma efectiva lo antes posible. Otro ciberdelito muy común es el fraude que se realiza por vías informáticas y que tiene como objetivos destruir la información a través de medios electrónicos. Delitos como el sabotaje informático, la piratería, los robos de identidad, etc., están a la orden del día. Ante estos ciberataques es imprescindible detectar, procesar y certificar todo el proceso para evitar ser víctima de cualquier tipo de fraude informático; medidas que son relativamente fáciles de aplicar con la implementación del sello del tiempo”. Sánchez D. (2016). Revista especializada en seguridad de la información – Red Seguridad. Madrid, España. Recuperado de: https://bit.ly/2Ut0eB6.

El Análisis integral de la evidencia digital.

Existen varias técnicas y herramientas forenses que se utilizan para el análisis de la evidencia, estas deben cumplir las formalidades que exigen las normas estándares y procedimientos de buenas prácticas diseñados por entes del gobierno y autores reconocidos. Entre ellos tenemos: Computer Forensic, disciplina forense que, busca encontrar e interpretar la información en medios informáticos para constituir los hechos y enunciar las hipótesis que la relacionen con el caso. Móvil Forensic, Esta herramienta extrae, analiza e interpreta información guardada en dispositivos móviles entre ellos Smarphones, Tablet y otros. Network Forensic, es una herramienta de gran ayuda para analizar las operaciones en las redes informáticas en un ordenador, sigue los protocolos y la formación criminalística permite conocer

los rastros, movimientos y acciones que un ciberdelincuente ha ejecutado para acabar su acción. Database Forensic, efectúa un estudio forense detallado de bases de datos y sus metadatos. Las bases de datos son almacenes donde se aloja toda la información del sistema y esta herramienta nos brinda detalles como relaciones de información y volumen de datos. Live Forensics, se encarga de la recopilación y el análisis de la evidencia, mientras el sistema bajo investigación se encuentra operando en tiempo real. La implementación de esta rama se debe a que muchos casos al apagarse el sistema del ordenador en supervisión y control se pierde información importante que no puede ser recuperada con el análisis tradicional en el laboratorio.

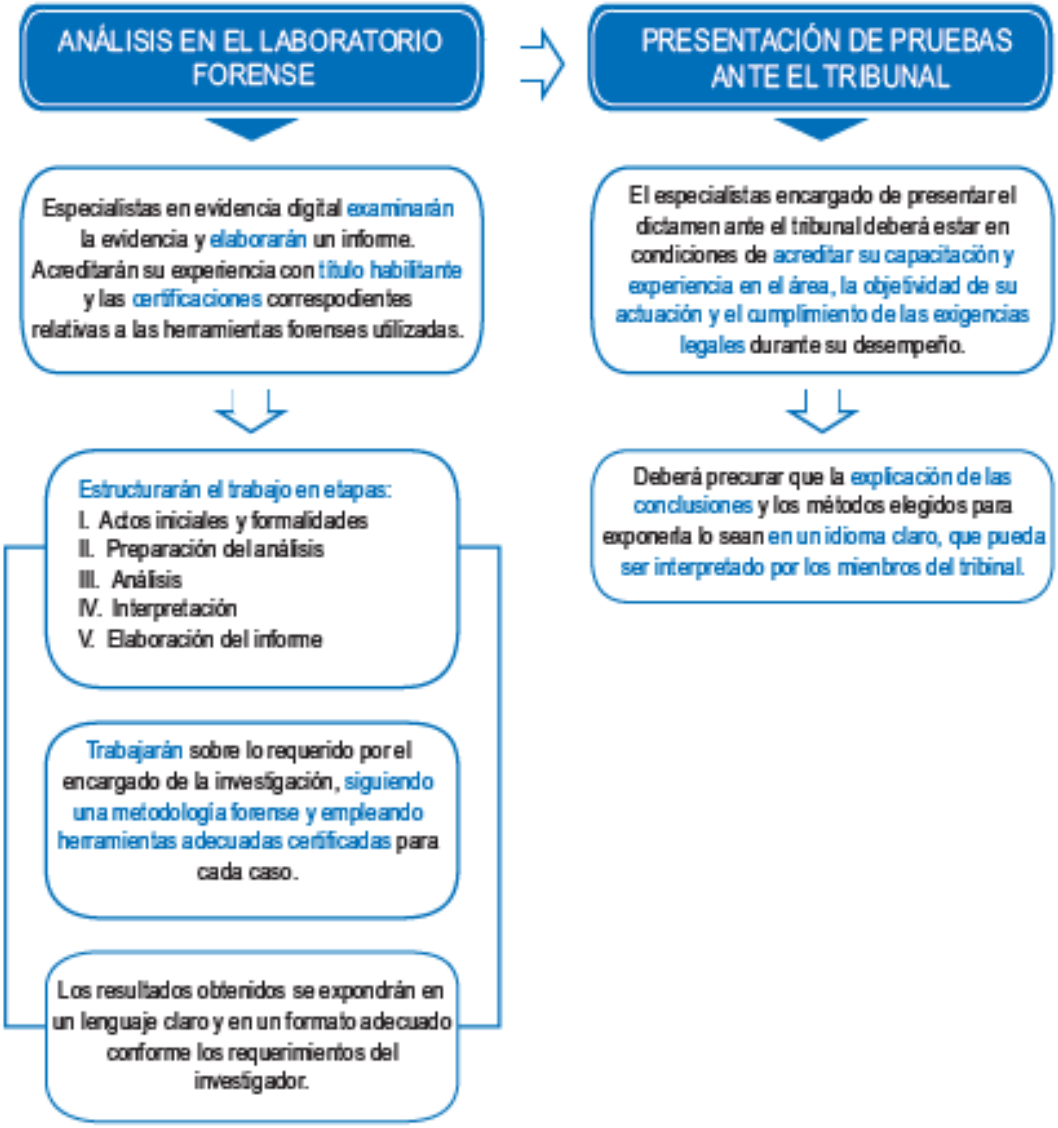


Figura 29. Proceso de la evidencia

Figura 30. Herramientas para el análisis de la evidencia.

Análisis de la evidencia digital definición de informática forense.

Constituyendo la misma una vez recopilada y procesada por un perito especialista evidencia física, puede ser esta contener: a. Registros diversos (Log files72) generados por el mismo sistema de manera automatizada, en el origen (en la Pc por el mismo software) o remota con datos enviados por medio de la red al terminal conectado a la red. b. Archivos diversos almacenados en equipos informáticos, creados por el propietario del hardware. c. Registros generados en el computador y externos, por ejemplo datos de tráfico generados en servidores de manera automatizada.

La participación de un perito informático es muy importante sobre todo en etapas tempranas de la investigación de un delito que contenga evidencia digital versa en que la misma: a. Puede alterarse fácilmente e impugnar su autenticidad. b. Se puede reproducir y con ello perjudicar su integridad. c. Puede duplicarse generando falsas pruebas. d. Nace “anónima” lo que se clarifica con el acceso a la fuente de manera rápida. e. Es importante obtener

rápidamente los medios por los que se crearon, modificaron, alteraron, suprimieron, entre otras actividades punibles. f. La evidencia requiere ser en algunos casos decodificada y certificar dicha conversión. g. El almacenamiento de la evidencia digital requiere condiciones especiales de almacenamiento y custodia. h. Requiere la protección del original de la muestra y trabajar con copias espejo, idénticas al original, certificada mediante software especializado. i. La información disponible en la red respecto a los datos de tráfico cuentan con regulación para su conservación, pero algunos de ellos por razones técnicas son temporales. j. Requiere una coordinación especializada en caso de recibir evidencia procedente de cooperación internacional.

Es importante realizar una tarea mediante procedimientos estandarizados siendo los recomendados: 1. Recolección de información**.-** de la fuente que origino, en tiempo real, o requiriendo información a empresas que almacenen por ejemplo datos de tráfico. 2. Examinar y clasificar la evidencia.- origen, procedencia, conexiones, redes, todo ello documentado mediante actas y dependiendo de la legislación, presencia de autoridades o veedores calificados. 3. Análisis.- consistente en una valoración de la evidencia obtenida atendiendo a los fines del proceso y los límites determinados por el juzgador. 4. Dictamen.- Conclusiones del análisis a consideración del juzgador o tribunal.

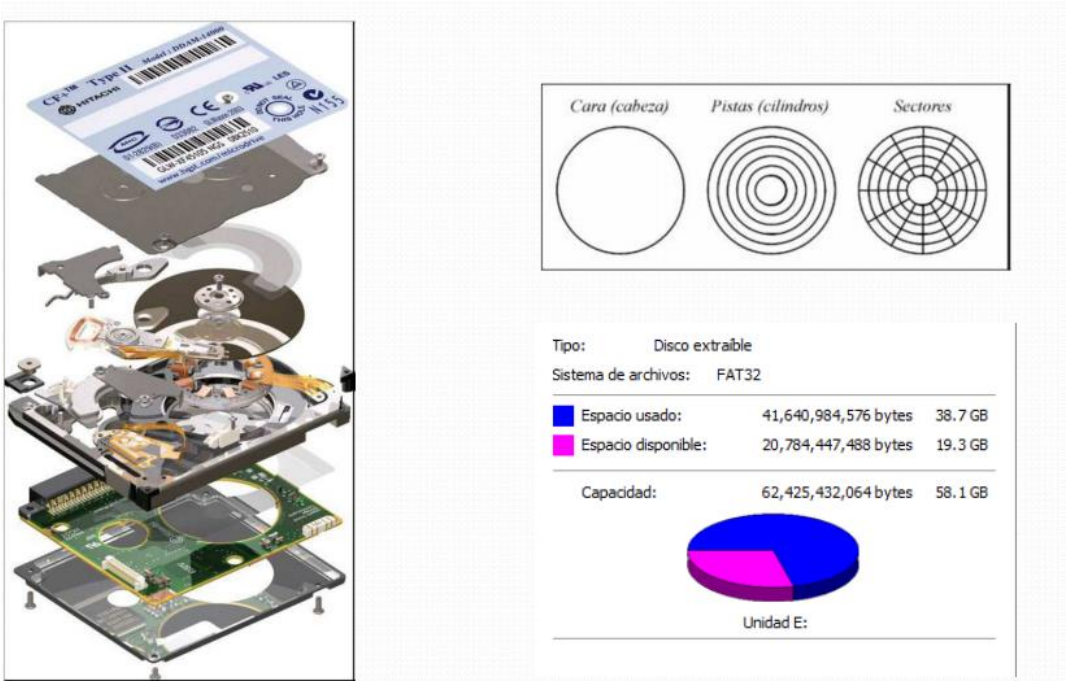


Figura 31. Como se obtiene los datos

Figura 32. Características de un disco

Criterios a considerar en la Evidencia Digital. Existen 4 criterios que se deben considerarse en la admisibilidad de la evidencia digital como son: a. Autenticidad: considerando situaciones como que la misma se haya generado y registrado en un lugar determinado y/o determinable que guarde vínculo con

el suceso que se investiga, asimismo que pueda probarse que no se ha alterado los medios originales, esto último puede acreditarse mediante software especializado, asimismo se puede llevar adelante un “lacrado digital” que permita la contratación de copias de trabajo utilizadas en el proceso penal. b. Confiabilidad.- atendiendo a la fuente de origen, que la misma en la creación de esta evidencia digital existan medios que permitan acreditar un funcionamiento adecuado, sin alteración en el sistema de origen. Los sistemas informáticos estos reportan por medio del denominado Log files, las acciones y comandos ejecutados en un sistema en tiempo real, y es almacenado de manera temporal. c. Suficiencia.- será suficiente la prueba si es completa, necesitamos mecanismos que nos permita determinar la integridad, sincronización de reportes y centralización de información, como reportes que emitan sistemas operativos o sistemas informáticos. d. Legalidad.- basados en la normativa especial y vigente respecto al tratamiento de evidencia digital de manera concordada con normas procesales y respeto a los derechos constitucionales desde su recopilación.

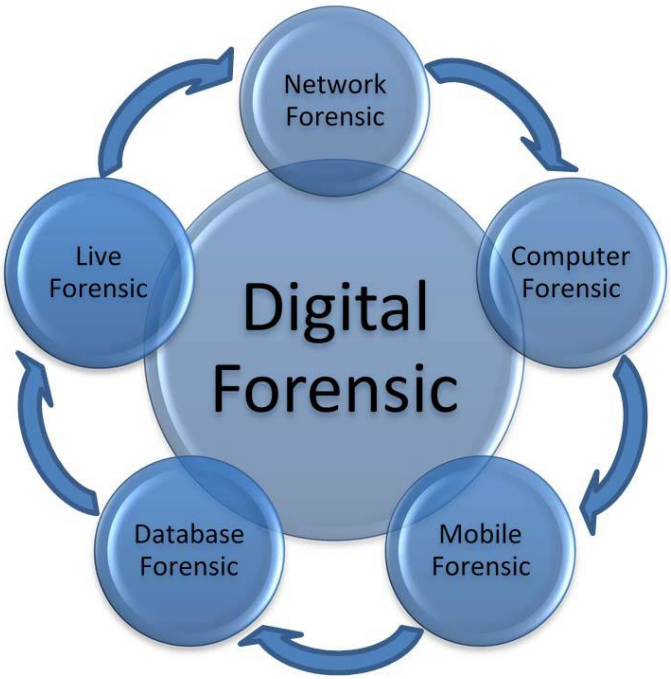


Figura 33. Forense digital

Cadena de Custodia. El objetivo es lograr garantizar los principios de autenticidad, identidad, estado original para ello es necesario cumplir el procedimiento y documentar información como: a. Identificación de las personas que intervienen tanto en calidad de peritos, partes, veedores, Fiscales, entre otros. b. Personal responsable del lacrado y envío de las evidencias, así como determinar el lugar de almacenamiento en condiciones de seguridad y buscando la conservación de los elementos físicos. c. Cambios en la custodia de los bienes. El proceso inicia desde el lugar donde se encuentre o ubique el medio físico que servirá como evidencia y culmina con pronunciamiento del Juez o administrativa.

Figura 34. Lacrado de equipos tecnológicos

Definiciones Técnicas en el análisis de evidencia digital. “Código Hash.- Es una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. Un hash es el resultado de dicha función o algoritmo”. Block Estructura de datos 7 Pato (2009). Método de búsqueda de Hashing. Colombia. Recuperado de: https://bit.ly/2BYhJSQ.

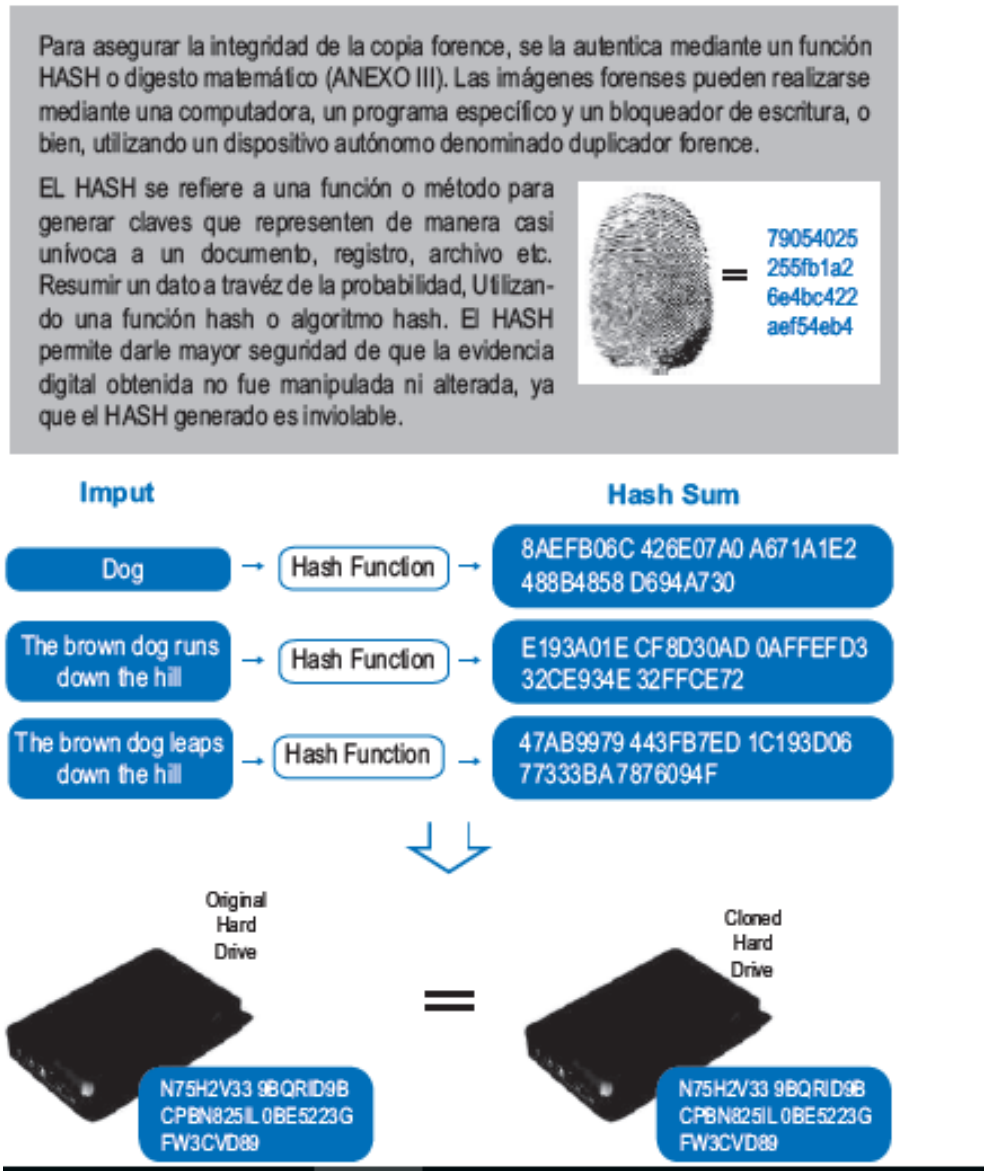


Figura 35. Función Hash

Copia espejo: Es la copia bit a bit de un archivo, carpeta ó volumen que contiene información grabada digitalmente, incluye los archivos y carpetas que pudieran encontrase ocultos ó marcados como borrados, así como cualquier otra información que forme parte del mismo.

Figura 36. Duplicado forense

Deslacrado de los dispositivos: Es el proceso de abrir los sobres ó cajas cerradas y aseguradas (“Lacrados”) y confrontar los dispositivos contenidos en ellos con las listas resultantes del “lacrado, en presencia de las partes interesadas. “Dispositivo bluetooth**:** Este dispositivo emplea la tecnología de Redes Inalámbricas de Área Personal (WPANs), posibilitando la emisión de voz y datos con otros dispositivos distintos, mediante un enlace por radiofrecuencia. Su principal objetivo es facilitar las comunicaciones entre equipos tecnológicos y por ende la eliminación de claves físicos y conectores”. Blog de WordPress.com (2009). Arquitectura de computadoras - Bluetooh. España. Recuperado de: https://bit.ly/2Qiprje.

Figura 37. Conectividad Bluetooth

1.3 Marco espacial

Siendo la evidencia digital un medio de prueba presente en la realización punible de un hecho delictivo, que incluye la participación de un medio tecnológico, la presente tesis se desarrollara y comprenderá la ciudad de Lima, debido a que registra la mayor incidencia de Delitos informáticos.

1.4 Marco temporal

La presente tesis se encuentra enmarcada dentro del periodo 2017 hasta el 2018, recopilándose información de hechos sucedidos en ciberdelincuencia y el estado de la normatividad en el Perú respecto al tratamiento de la evidencia digital

1.5 Contextualización: histórica, política, cultural, social

Contexto histórico.

El incontrolable avance de las tecnologías de la información y la comunicación del último siglo ha generado innumerables mejoras y avances para toda la humanidad, pero simultáneamente nuevos retos para las autoridades, legisladores e investigadores en el mundo, quienes actualmente deben ocuparse muy responsablemente en la persecución y sanción de los delitos cibernéticos, como por ejemplo la pornografía infantil, robo de identidad, acoso cibernético entre otros. Nuestro país no es ajeno a este hecho, históricamente con el avance de la tecnología y el uso del internet los ciberdelincuentes han propiciado innumerables hechos sobre todo contra las empresas nacionales quienes transformaron sus productos y servicios ofreciéndolo mediante plataformas online, facilitando la compra de productos, pagos de servicios o transacciones financieras para sus clientes, se tiene información que a la fecha superan los 4 mil millones de dólares en pérdidas encontrándose el Perú en el séptimo lugar entre los países más afectados por el cibercrimen en la región. Esto nos lleva a pensar el incremento de ilícitos que se producirán en los años sub siguientes con el auge de la tecnología en nuestro país y la necesidad de contar con leyes y autoridades que estén en capacidad de poder enfrentarlos.

Contexto político.

En el ámbito político es importante la apreciación que realiza Augusto Bequai, en su intervención Computer Related Crimes en el Consejo de Europa quien señala que: “Si prosigue el desorden político mundial, las redes de cómputo globales y los sistemas de telecomunicaciones atraerán seguramente la ira de terroristas y facinerosos. Las guerras del mañana serán ganadas o perdidas en nuestros centros de cómputo, más que en los campos de batalla. ¡La destrucción del sistema central de una nación desarrollada podría conducir a la edad del oscurantismo!. … En 1984, de Orwell, los ciudadanos de Oceanía vivían bajo la mirada vigilante del Hermano Grande y su policía secreta. En el mundo moderno, todos nos encontramos bajo el ojo

inquisidor de nuestros gigantes sistemas computacionales. En occidente, la diferencia entre el Hermano Grande y nuestra realidad es la delicada fibra política llamada democracia; de colapsarse ésta, el edificio electrónico para una implantación dictatorial ya existe. La revolución de la electrónica y la computación ha dado a un pequeño grupo de tecnócratas un monopolio sobre el flujo de información mundial. En la sociedad informatizada, el poder y la riqueza están convirtiéndose cada vez más en sinónimos de control sobre los bancos de datos. Somos ahora testigos del surgimiento de una elite informática". Comisión de las Comunidades Europeas. *Delitos relativos a las Computadoras. Bruselas*, (1996). El mejor hecho que hoy podemos apreciar se desarrolla en nuestro país, con la situación política que viene atravesando influenciado por problemas de corrupción que involucra a diferentes frentes políticos, en procesos judiciales mediáticos, apreciando que los medios de prueba en cuestión son correos electrónicos y mensajes de WhatsApp, que constituyen evidencias digitales, a través de las cuales se vienen dictando medidas coercitivas como prisiones preventivas o impedimentos de salida del país, generando un clima de inestabilidad política en nuestro país.

Contexto cultural.

El proceso cultural se encuentra muy íntimamente ligado al gran desarrollo de la tecnología de la Información y comunicación y que en la actualidad representa un importante desarrollo cultural. Las Tecnologías hoy brindan innumerables herramientas al servicio del hombre en las formas de transmisión, procesamiento y almacenamiento digital de información, que con el empleo de procesos y aplicaciones hacen más sencilla y fácil la interacción entre las personas. Es importante resaltar que las TIC alcanzaron poder gracias al internet mediante el empleo de correos electrónicos, redes sociales, páginas web en la forma de servicios y consultas de diversos tópicos del quehacer humano, rompiéndose el paradigma real del tiempo y espacio en la interacción humana. Por otro lado las aplicaciones de las TIC y el empleo del internet, en los denominados "cibergobierno", "cibereducacion" y "cibersalud", entre muchos otros son elementos muy importantes para el desarrollo social y cultural, ya que proporcionan un medio eficaz para brindar una variedad de

servicios básicos en zonas locales urbanas y rurales, pues estas aplicaciones facilitan el logro de los objetivos de desarrollo en mejoras de la población.

Contexto social.

El ser humano en la actualidad lleva una vida en sociedad natural y necesaria, mediante el cual se ajusta las funciones y actividades de cada individuo, con el objetivo de lograr una convivencia sana, evitando choques, resolviendo conflictos y fomentando la cooperación. La tecnología permite procesar y brindarnos una cantidad incalculable de información de toda naturaleza, a millones de personas y usuarios. Pero también esto viene afectando a las personas en las diferentes figuras de delitos con el empleo de tecnología que generan la inseguridad de las instituciones, y por consiguiente inestabilidad en las relaciones entre las personas, por ejemplo un mensaje anónimo por correo electrónico dentro de una organización, hogar, entre otros, acusando falsamente a ciertas personas, resultando con ello desconcierto, dudas sobre esas personas, lo cual crea una inestabilidad emocional, que desestabiliza el hogar, la familia, instituciones.

Ello se puede explicar por el problema de combatirla en forma internacional, ya que los usuarios están ubican por todo el mundo, conllevando a que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Si bien los acuerdos de cooperación internacional y/o tratados intentan solucionar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son muy limitadas.

Ante ello podemos concluir que las perspectivas de la tecnología no tienen límites previsibles, por ello se ha llegado a determinar que la informática es hoy una forma de poder social. Las capacidades puestas a disposición de Gobiernos y de particulares, de rapidez y ahorro de tiempo y energía, coluden una realidad de posibilidades de juegos lícitos e ilícitos, en donde se hace vital el derecho para reprimir y regular los efectos de situación, nueva y de tantas potencialidades en el medio social.

II. Problema de investigación

2.1. Aproximación temática: observaciones, estudios relacionados, preguntas orientadoras

Estudios relacionados al tema a nivel nacional, se tiene a Sequeiros (2015), en un estudio de tipo cualitativo, titulado “Vacíos legales que imposibilitan la sanción de los Delitos Informáticos en el nuevo Código Penal Peruano”. Concluyendo que La falta de una información adecuada sobre los límites de la tecnología informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones. Asimismo, nuevas modalidades de negocios por internet, como el comercio electrónico es un claro ejemplo de cómo los delitos pueden aparecer de diversas formas, por lo que se deben crear instrumentos legales efectivos que ataquen ésta problemática, con el único fin de tener un marco legal que se utilice como soporte para el manejo de éste tipo de transacciones. Asimismo los delitos informáticos no deben impedir que el usuario se prive de todo lo que proveen las tecnologías de información, sino por el contrario dicha situación debe plantear un reto a los profesionales de la informática, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad, controles, integridad de la información, etc. en las organizaciones.

Estudios a nivel internacional, se tiene a Ramírez y Castro (2018) realizaron un estudio titulado “Análisis de la Evidencia Digital en Colombia como soporte judicial de delitos informáticos mediante cadena de custodia” que tuvo como objetivo, identificar las falencias en el tratamiento de pruebas digitales que puedan ocasionar pérdidas, daños o destrucción de las mismas en procesos judiciales por medio del estudio del proceso de cadena de custodia en la investigación de delitos informáticos en Colombia. Concluyendo que en este proceso donde la investigación nos indica que la implementación y forma de realizar el levantamiento del material probatorio tecnológico no es óptimo ya que cuenta con falencias en sus procesos, por no contar con manuales, dotaciones y personal certificado y en constante actualización para no contaminar las evidencias a la hora de su recolección, embalaje, rotulado y

análisis. Asimismo se logró identificar las falencias y sus factores más relevantes que inciden en el proceso de cadena de custodia de evidencias digitales, las cuales son: Falta de capacitación o conocimiento de las metodologías. Dado que son muchas las formas y procedimientos para realizar procesos de custodia se debe contar con personal debidamente capacitado y que estén en constante retroalimentación ya que las tecnologías están en continuo desarrollo y esto permite el nacimiento de nuevas herramientas y formas de hackear o vulnerar la seguridad de la información. Uso de herramientas inadecuadas, se debe contar con tecnología de punta, la cual permite al perito y/o investigador forense realizar validación y rastreo a los procesos que hayan dado lugar a una posible vulnerabilidad en la información de un usuario, equipo o entidad. El manejo inadecuado, que en ocasiones por un mal procedimiento no cumple el marco normativo que dicta la ley, permite que este sea calificado por la contra parte como una prueba contaminada y que pierda su valides.

Queda las preguntas: ¿Cuál es el valor de la Evidencia digital para un proceso penal?, ¿Los operadores de justicia en el Perú están preparados y/o capacitados para el tratamiento de la evidencia digital?, ¿La evidencia digital en el Perú cuenta con la normatividad necesaria para ser admisible y tenga valor probatorio en un proceso penal?.

2.2. Formulación del problema de investigación

La Tecnología de Información y Comunicación es el medio por el cual hoy nos comunicamos sin ninguna barrera, ello forma parte indiscutible de nuestras vidas, al extremo de depender de ellas, hoy podemos con facilidad compartir información, imágenes, sonidos y otros inmediatamente, las distancias hoy se acortaron, solo basta conectarnos a internet y listo. Las Redes sociales hoy son parte de nuestra actividad diaria al igual que el Whatsapp, Skype y otros. El mal empleo de estas tecnologías por personas al margen de la ley como los ciberdelincuentes, abren el paso a la comisión de ilícitos denominados ciberdelitos, dejando como rastro de estas malas actividades las huellas del

delito que se denominan las evidencias digitales. Estas evidencias deben contar con el marco legal correspondiente para combatirlas eficazmente en los procesos judiciales, ante ello se plantea varias incógnitas.

Cabe resaltar que en la ciudad de Lima se concentra el índice delincuencial mayor, debido a existir una gran cantidad de denuncias penales, sobre todo que la gran mayoría de los agraviados presentan como elemento de prueba la evidencia, que se encuentra alojado en un medio electrónico o digital, Ante ello surge una serie de interrogantes, ¿son admitidas estas evidencias digitales? ¿El Ministerio Publico cuenta con la implementación tecnológica como para garantizar la autenticidad? ¿Son legítimas para que el juez pueda valorarlas? ¿Cuál es el tratamiento que brinda el Ministerio Publico para que estas pruebas electrónicas ofrecidas tengan valor probatorio? ¿Cuáles son los requisitos para obtener una evidencia digital?, ¿cuáles son los procedimientos para incorporar la evidencia digital? ¿Cuándo una evidencia digital es considerada ilícita o irregular? ¿Cuáles son las reglas o criterios de valoración para que sean admisibles por parte del juez?, este y otras interrogantes han sido desarrolladas y resueltas en el presente trabajo de investigación, gracias al aporte de los expertos en actividad en el campo jurídico, policial y expertos en tecnología.

Problema General.

¿De qué manera debe tratarse la evidencia digital en el Sistema Jurídico peruano, para que sea admisible y tenga el valor probatorio en un Proceso penal?

Problemas específicos.

Problema específico 1.

¿Cuál es la jurisdicción donde se cometen los delitos informáticos y si las leyes del país tienen el alcance jurídico para combatirlas?

Problema específico 2.

¿Qué normatividad jurídica tiene el Perú para acreditar la admisibilidad y valor probatorio de la evidencia digital?

Problema específico 3.

¿Cuáles son los procedimientos legales que aplican otros países para garantizar el valor probatorio de la evidencia digital como prueba en un proceso judicial?

Problema específico 4.

¿Qué tratamientos y procedimientos tecnológicos debe darse a la evidencia digital, para proteger su originalidad, desde su hallazgo, recojo, traslado y entrega final a la autoridad judicial, que garanticen su valor probatorio en un proceso judicial?

2.3. Justificación

Justificación teórica.

Las Tecnologías de la Información y la Comunicación cumplen un papel muy importante en el desarrollo de la sociedad, y por ende en las diferentes actividades que desarrolla el ser humano, siendo su empleo un gran aliado estratégico a los gobiernos del mundo y sus sectores como economía, educación, seguridad, salud, transporte y comunicaciones, administración pública, judicial, empleo, empresas, etc. Que refiere el uso de sus recursos respectivamente, en herramientas y aplicaciones que se utilizan para procesar, administrar, guardar y compartir información a través de soportes tecnológicos: computadoras, teléfonos móviles, tabletas electrónicas y otros, siendo para ello el elemento más importante de las TIC el Internet. Ello también involucra a la evidencia digital que se representa en cualquier valor probatorio de la información almacenada o transmitida en formato digital de tal manera que parte de ella o toda puede ser utilizada en un proceso judicial. Esta investigación se realiza con el propósito de aportar las consideraciones normativas de la evidencia digital afín de mantener la autenticidad, confiabilidad, suficiencia para su admisibilidad y valor probatorio en un

proceso judicial en el Sistema Jurídico Peruano.

Justificación metodológica.

Se han utilizado los métodos como el análisis, inducción y la comprensión, interpretación o la hermenéutica; así también las técnicas utilizadas como la entrevista semiestructurada, observación y análisis documental en la presente investigación (Ñaupas, Mejía, Novoa y Villagomez, 2014, p.98). Para ello analizaremos el contexto internacional sobre las normas legales y técnicas de procedimiento del tratamiento de la evidencia digital, a fin de identificar y acondicionarlas a la necesidad de nuestro país.

2.4 Relevancia

Con el avance de la tecnología en los últimos años, la sociedad ha experimentado un gran cambio, debido a que los dispositivos tecnológicos ayudan al mejoramiento de las organizaciones y empresas, ello conlleva también a la existencia de vulnerabilidades en su performance, que es bien aprovechado por delincuentes informáticos que buscan a como dé lugar apropiarse de información que es de vital importancia, es por ello que la evidencia digital, es la información almacenada en los dispositivos o medios electrónicos que puede ser alterada, modificada o eliminada sin dejar rastro. Por esta razón, las evidencias digitales, constituyen piezas probatorias importantes que requieren un tratamiento distinto al de cualquier otra evidencia en común que se presenta en la escena de un delito, necesita de una revisión detallada de cómo se crean, se recogen, se aseguran, se transportan y, finalmente, cómo se presentan ante la autoridad judicial, que contribuya a aportar con claridad y precisión la responsabilidad penal del infractor, así como oriente las decisiones como material probatorio.

2.5. Contribución

La contribución de esta investigación es, establecer las consideraciones que se deben de emplear al momento de localizar indicios que sean considerados como evidencia digital, en la escena del crimen. De esta manera se intenta dar un aporte en los procedimientos y lineamientos básicos para el trabajo que realiza el Ministerio Público, la Policía Nacional o los mismos particulares, quienes proporcionan indicios de investigación.

2.6. Objetivos

Objetivo General.

Describir alternativas de procedimientos legales e informáticos para el tratamiento de la evidencia digital, para que sean admisibles y tengan el valor probatorio en un proceso penal en el Sistema Jurídico Peruano.

Objetivos Específicos.

Oe1. Determinar cuál es la jurisdicción donde se comenten los delitos informáticos, y si las leyes del país tienen el alcance jurídico para combatirlas.

Oe2. Describir la normatividad jurídica que tiene el Perú para acreditar la admisibilidad y valor probatorio de la evidencia digital.

Oe3. Precisar los procedimientos legales que aplican otros países para garantizar el valor probatorio de la evidencia digital como prueba en un proceso judicial.

Oe4. Describir los tratamientos y procedimientos tecnológicos que debe darse a la evidencia digital, para proteger su originalidad, desde su hallazgo, recojo, traslado y entrega final a la autoridad judicial, que garanticen su valor probatorio en un proceso judicial.

III. Marco metodológico

3.1 Categorías y categorización

Para el reconocido Gomes el término categoría, se refiere principalmente a la clasificación de conceptos de manera que tenga una estructura jerarquizada, por lo que trabajar con ellas implica agrupar elementos, ideas y expresiones en torno a un concepto que responde a una estructura jerarquizada. Los agentes o sujetos que conforman el contexto u escenario de estudio de la presente investigación son representantes de Derecho Penal del Ministerio Público, representantes del orden y seguridad de la Policía Nacional del Perú y expertos en tecnologías de la información y comunicación del sistema financiero nacional, asimismo tienen la mayor potencialidad de emitir un juicio de valor, con un criterio pertinente sobre el tema, respaldado por su larga trayectoria y experiencia.

Straus y Corbin sostuvo que la categorización consiste en asignar conceptos a un nivel más abstracto, lo que refiere el autor, es que las categorías tienen un poder conceptual jerarquizado, puesto que estar organizada en grupos de conceptos denominados subcategorías, las cuales están relacionadas entre sí, los cuales emergen del fenómeno de estudio. Las categorías utilizadas en una investigación responden al marco teórico y conceptual de la investigación, esto a su vez los supuestos que orientan las categorías o instrumentos de investigación empleados en la presente investigación. Enseguida se considera la clasificación de conceptos y grupos de conceptos que responden a la investigación que tiene por título: La admisibilidad y el valor probatorio de la evidencia digital en el sistema jurídico peruano.

Tabla 1.

Categorías y sub categorías

Categorias	Sub categoria	Frases codificadas
A. Ciberdelincuencia y ciberespacio	A1. Canales de desarrollo	La ciberdelincuencia es la acción que utilizando el Internet, destruye o avería equipos de cómputo, redes de Internet. También atenta contra la veracidad, la integridad de los sistemas de información y redes, buscan robar información, suplantar la identidad de personas, generar fraudes a personas naturales y jurídicas.
	A2. Ambito	Lugar virtual, no tiene locación física espacial, interactúan usuarios, se explora información on line en páginas web, se comunican mediante redes sociales sin reparo de tiempos y distancias mediante el Internet
	A3. Jurisdiccion	La ciberdelincuencia es un delito transnacionales, no existe fronteras, genera límites en las investigaciones, se suma problemas de tipo jurídico y diversidad de capacidades en el mundo. Las fronteras nacionales, representa dificultad para el tratamiento de los ciberdelincuentes.
B. Valoracion legal de la evidencia digital en el Peru	B1. Bien juridico	Es el dato
	B2. Prevision	No se ha previsto en la legislacion peruana, ni la etapa procesal en el tratamiento a la evidencia digital, genera que los delitos informaticos en muchos de los casos queden impunes.
	B3. Sanciones	La Ley 30096 Ley de delitos informaticos sanciona ilicitos tecnologicos, la falta de precisiones en el Codigo Procesal Penal del tratamiento de la evidencia digital, las sanciones no se concretan.
	B4. Legalidad	La creciente incidencia de la Ciberdelincuencia hace necesario contar con ordenamiento jurídico que sancione la cibercriminalidad. En Perú se promulgo la Ley 30096 Ley de delitos informáticos, pero procesalmente existe vacíos que no brinda herramientas para la presentación de la evidencia digital durante un proceso judicial.
	B5. Definicion	Información obtenida de un dispositivo electrónico que sirve para el convencimiento de la certeza de un hecho, debe ser correctamente obtenida, constituye pruebas exactas, veraces y objetivas
	B6. Custodia	Este procedimiento, basado en el principio de la “mismidad”, debe garantizar la autenticidad e integridad de las evidencias encontradas.
	B7. Tratamient	En la escena, evitar su contaminación, retirar a las personas en el lugar. Ningún efectivo debe alterar los datos contenidos en la computadora o dispositivo de almacenamiento informático. La persona que accede a los datos contenida en las computadoras o dispositivos de almacenamiento debe tener conocimientos técnicos informáticos. Debe auditarse y registrar todo el proceso de manipulación de la evidencia digital, indicando las medidas y acciones llevadas a cabo así como su preservación mediante la cadena de custodia”
	B8. Atencion	Los aspectos esenciales de asegurar los medios y conservación de fuentes de prueba; es la cadena de custodia que permite la conservación, seguridad, custodia de la integridad de la prueba. Sobre la evidencia digital no existe pronunciamiento particular, no es lo mismo evidencia comun con evidencia digital.
C. Tratamiento de la evidencia digital en otros paises	C1. Convenios	No existe normas de carácter procesal que brinden el soporte legal a las evidencias digitales, ello contribuye que su valor probatorio sea complicado, resulta necesario adecuar el NCPP tomando como base leyes y normas de otros paises para distinguir la evidencia documental de la evidencia digital, el Peru debe adherirse al convenio de budapest.
	C2. Modelos	Se sugiere el modelo europeo para una actuación globalizada contra la ciberdelincuencia transnacional, tienen visión integradora, deseo común de llegar a conclusiones del tratamiento adecuado a los fenómenos para una mayor eficacia. Estas asistencias prevén soluciones concretas, intercambio de información, equipos de investigación conjuntos, transmisión de documentos, etc. Su incidencia en la persecución del ciberdelito queda bien acreditada.
	C3. Soluciones	Modelos Europeos como por ejemplo España o Americanos como Colombia, Chile, Mexico e inclusive Estados Unidos. Existe una gran disposicion por organizaciones privadas y/o particulares de acciones mas eficaces para combatir la ciberdelincuencia.
D. Proc. tecnologicos de la evidencia digital	D1. Procesos y Herramientas tecnologicas	Estandar internacional UNES, ISOS y hardware y Software que permiten la obtención de la evidencia digital con características de autenticidad, integridad, originalidad, confiabilidad y no repudio.

3.2 Metodología

Paradigma.

El presente estudio de investigación cualitativa busca realizar un análisis del tratamiento de la evidencia digital como medio de prueba en un proceso penal en el Perú, teniéndose en consideración los requisitos de admisibilidad y valor probatorio. Usa el Paradigma Interpretativo. La investigación busca describir, comprender e interpretar los distintos fenómenos que se desarrollan en ella. El investigador forma parte de lo que se quiere describir. Se centra en la descripción y comprensión de lo que es único y particular.

En la investigación cualitativa, observadores competentes y cualificados pueden informar con objetividad, claridad y precisión acerca de sus propias observaciones del mundo social, así como de las experiencias de los demás. El investigador se aproxima a un sujeto real, un individuo real, que está presente en el mundo y que puede, en cierta medida, ofrecer información sobre sus propias experiencias opiniones, valores, etc. Por medio de un conjunto de técnicas o métodos como las entrevistas, las historias de vida, el estudio de caso o el análisis documental, el investigador puede fundir sus observaciones con las observaciones aportadas por otros. Monje (2011)

Enfoque.

La presente investigación tuvo un enfoque cualitativo. La investigación cualitativa estudia la realidad en su contexto natural y cómo sucede, sacando e interpretando fenómenos de acuerdo con las personas implicadas. Utiliza variedad de instrumentos para recoger información como las entrevistas, imágenes, observaciones, historias de vida, en los que se describen las rutinas y las situaciones problemáticas, así como los significados en la vida de los participantes. El investigador tiende a sumergirse subjetivamente en el tema, en este método de investigación.

Diseño.

El presente trabajo de investigación tuvo por diseño el estudio de caso de la admisibilidad y valor probatorio de la evidencia digital en el Sistema Jurídico Peruano. El estudio de casos implica un proceso de indagación detallado, comprehensivo, sistemático y en profundidad del caso objeto de interés. El estudio de casos, estudia intensivamente un sujeto o situación única, permitiendo comprender a profundidad lo estudiado. Según Denny (1978, p. 370, citado en Rodríguez, Gil y García, 1996, p. 91) el estudio de caso es como “un examen completo e intenso de una faceta, una cuestión o quizás los acontecimientos que tiene lugar en un contexto geográfico a lo largo del tiempo”. Un caso puede ser una persona, una organización, un programa de enseñanza, una colección, un acontecimiento particular o un simple depósito de documentos. La única exigencia es que posea algún límite físico o social que le confiere entidad. En el entorno de gestión pública un trabajador, un funcionario, una institución, un proyecto de inversión, una determinada política de Estado, pueden constituir casos potenciales objeto de estudio. (Rodríguez, Gil y García, 1996, p. 92).

3.3 Escenario de estudio

Balcazar, Gonzáles-Arratia, Gurrola y Moysen (2013), manifestaron que: El escenario ideal para la investigación, en el cual, donde el observador obtiene fácil acceso, establece una buena relación inmediata con los informantes y obtiene datos directamente relacionados con el interés de la investigación. Por lo general, es muy difícil el acceso, se necesita diligencia y paciencia. No hay guías para saber cuándo renunciar a un escenario. Lo recomendable es que el investigador se abstenga estudiar escenarios donde tengan directa participación personal o profesional.

Para describir el escenario de estudio, se debe tener en cuenta el ambiente físico o entorno, describiendo tamaño, arreglo especial o distribución, señales, accesos, un elemento muy importante son nuestras impresiones iniciales. Para la presente investigación al tratarse de la

evidencia digital la cual que se produce por el empleo de un medio tecnológico por cualquier persona, sin importar edades, origen étnico, nivel socio económico, etc, ello se realiza en cualquier lugar del mundo y siendo nuestro estudio la admisibilidad y valor probatorio en el Sistema Jurídico Peruano, tomaremos como base a la ciudad de Lima.

3.4 Caracterización de sujetos

Al tratarse del estudio de la evidencia digital, el cual se origina al utilizar un dispositivo tecnológico sea Computadora personal, Laptop, Tablet, teléfonos celulares y otros, medios por los cuales se origina la evidencia en un determinado ilícito penal sea cual fuera la modalidad, los sujetos a intervenir de conformidad a las leyes y normas vigentes en nuestra legislación serían primeramente las personas que intervienen en el ilícito (agraviado y autor del hecho), la Policía Nacional del Perú, representado en efectivo policial interviniente, como autoridad que representa el orden y la seguridad, el Ministerio Publico representado en el Fiscal, encargado de investigar los delitos y acusar a los presuntos infractores ante los juzgados y tribunales y el Poder Judicial representado en el Juez, encargado de impartir justicia en la sociedad.

Tabla 2:

Caracterización de los Sujetos

Nro	Profesion	Grado Academico	cargo actual
1	Fiscal	Magister	Fiscalia Especializado Delitos Especiales
2	Policia	Magister	Investigacion Division de Alta Tecnologia
3	Ing. Sistemas	Magister	Gerente de Operaciones ASBANC

3.5 Procedimientos metodológicos de investigación

La trayectoria metodológica se desarrolló en cuatro etapas: la primera fue el diseño y construcción de los instrumentos de recojo de información, seguido fue la aplicación de los instrumentos a cada unidad de análisis; luego se

procedió a transformar en texto, los datos de las grabaciones realizadas, para codificarlas y categorizarlas y como etapa final, se realizó el análisis de la información a través de la triangulación. Para la credibilidad científica del estudio realizado, y el mejor entendimiento, es necesario explicar cada etapa mencionada.

Recogida de datos.

Esta primera etapa, se inició con el diseño y construcción de los instrumentos de recojo de información, como el cuestionario de preguntas, realizado a partir del diseño metodológico propio del estudio de caso. Se coordinó con los entrevistados, con la finalidad que nos conceda las entrevista planificadas, las coordinaciones se realizó a través de visita a sus centros de labores. Estas se llevaron a cabo a representantes del Ministerio Publico, Policía Nacional del Perú y un experto en el sistema bancario respecto al manejo de tecnologías en el sistema financiero, dichas entrevistas se realizaron durante el mes de Noviembre del presente año.

Las entrevistas que fueron grabadas, se realizaron en horas de la tarde y de la mañana dependió del tiempo disponible de los representantes. Se apreció buena disposición en las entrevistas, la ejecución de las mismas sirvió para comprender el fenómeno en estudio, ubicándonos en una posición más clara sobre el tema de investigación; la entrevista fue grabada y ayudo a percibir en mayor grado la importancia de la evidencia digital como medio de prueba. Con esta metodología de investigación se pudo entender mucho mejor la relevancia e importancia sobre la evidencia digital con posterioridad a muy próximos eventos de connotación sobre ataques de ciberdelincuentes sobre todo en el sistema financiero mundial.

Análisis de datos.

Para el análisis de datos se aplicará diferentes métodos los cuales nos permitirá responder apropiadamente al problema de investigación y obtener conclusiones. Método inductivo: “es una aproximación a la realidad mediante

el cual el investigador concreta los argumentos más concretos que van desde un aspecto particular a lo general, sustentada en una serie de evidencias eminentemente empíricas". (Ávila, 2006, p. 7). En este orden de ideas, este método ha permitido el uso de que los resultados obtenidos en la presente investigación de respectiva muestra sean generalizables a la población general estudiada.

Método Exegético: a través de este método se ha analizado las normas, tanto la constitución, el código penal procesal penal, como jurisprudencias se analizó manera aislada e independiente considerando su contenido con el tema de investigación. Método sistemático: a través de este método se ha analizado de manera sistemática con interpretación sistemática y articulada de norma, código penal, doctrina, jurisprudencia y aportes de los expertos de manera que permita una conclusión de la investigación.

Transcripción de los datos, codificación y categorización.

Gibb (2012), referido por Coaguila (2012), que la transcripción, es el proceso de cambio de medio, siendo necesario la exactitud, minuciosidad, fidelidad e interpretación. El autor refirió que hay que transformar en texto la información grabada, tal cual está en el instrumento, labor que fue realizada por el mismo investigador. La transcripción debe ser idéntica a lo manifestado por los informantes, para que no se pierda la fidelidad y autenticidad de lo grabado. En el presente estudio fue necesario quitar algunas palabras, frases repetidas en la misma oración, "no", "sigo adelante", "o sea", "hay que" asimismo se quitó algunas muletillas como "eh", "uhm". Gibbs (2012), referido por Coaguilla (2012), afirmó que en las investigaciones que están orientados a los hechos de lo expresado por los informantes, es justificable realizar correcciones de este tipo.

Con respecto a la codificación, Gibbs (2012) citado por Coaguilla (2012), refirió que es la forma en que se define de qué tratan los datos que se están analizando, para lo cual es necesario identificar y registrar uno o más pasajes de texto de los discursos transcritos, que de cierto modo guardan la misma idea teórica o descriptiva. Asimismo, Mejía (2011) citado por Coaguilla

(2012), que los códigos son principalmente etiquetas o abreviaturas que representan el contenido conceptual. Por tanto, en el presente estudio, se procedió a leer varias veces los discursos para identificar y clasificarlos según el parecido temático y asignarle un código, para la realización de esta tarea se usó la técnica del resaltado usando diferentes colores y numerando, de acuerdo al contenido temático mencionado.

Para terminar esta etapa, se realizó la categorización, según Mejía (2011) citado por Coaguilla (2012), consiste en dividir las unidades temáticas el texto transcrito y codificado. Es decir que categorizar es encontrar las unidades temáticas relacionadas al tema y objetivo de investigación. Las unidades temática identificadas, son las categorías emergentes (Cisterna, 2005 citado por coaguilla 2012). Según Mejía 2011 citado por Coaguilla 2012, se tuvo en cuenta el criterio inductivo-deductivo, para la elaboración de listas de categorías.

Triangulación.

Según Stake (2007) citado por Coaguilla (2012), triangulación de las fuentes de datos, es el esfuerzo por ver si aquello que observamos y de lo que informamos, contiene el mismo significado cuando lo encontramos en otras circunstancias. Según Cisterna (2005) citado por Coaguilla (2012), refiere a la triangulación como el proceso de reunión y cruce dialéctico de toda la información relacionado al fenómeno de estudio, que surgió en la investigación por medio de los instrumentos de recojo de información. Se realizó la triangulación de entrevistas de Fiscal, Policía y Experto en TIC se encontró más opiniones similares; se realizó la triangulación de las observaciones de expedientes judiciales, se obtuvo situaciones similares; finalmente se realizó la triangulación en el análisis documental, encontrando información similar.

3.6 Técnicas e Instrumentos de recolección de datos

Según el especialista metodólogo Valderrama (2013) sostuvo que las técnicas establecidas para llevar a cabo una investigación cualitativa son tres, tales como (a) Observación, (b) Entrevista, (c) Grupos de discusión

(Focus Groups) y los instrumentos de recolección de datos, más usados y conocidos por los investigadores, son: la guía de entrevista, ficha de observación, lista de cotejo check list entre otros. Para culminar con la presente investigación se recolecto los datos a través de las siguientes técnicas de recolección de datos:

Técnicas.

Entrevista. - Esta técnica permitió al investigador formular preguntas a un representante del Ministerio Publico Fiscal, Personal de la Policía Nacional del Perú de la división de Investigación de Delitos de Alta Tecnología – DIVINDAT-PNP, y el Gerente de Operaciones de la Asociación de Bancos del Perú experto en tecnologías del sistema financiero. Las preguntas de la entrevista fueron formuladas de acuerdo a los requerimientos de las categorías y sub categorías de la investigación, teniendo como eje central los problemas, los objetivos y los supuestos del estudio. Los datos recolectados mediante esta técnica fueron analizados mediante un cuadro comparativo para contrastar los supuestos.

Análisis documental: la presente técnica permitió analizar y sintetizar los conceptos más importantes de las fuentes bibliográfica documentales, conformado por Artículos, textos, revistas, casos y otras fuentes de naturaleza documental, y otras vinculadas con el tema de investigación, con la finalidad de determinar, si existe un tratamiento de la evidencia digital en el Sistema jurídico peruano - 2018. Así como las Responsabilidades del Estado respecto a la evidencia digital representadas en las Instituciones públicas, como son el Ministerio Publico, La Policía Nacional del Perú y El Poder Judicial.

Análisis de Jurisprudencial: esta técnica nos permitió analizar las tres sentencias que representan precedentes vinculantes sobre el tema de la evidencia digital en un proceso judicial, relacionada con el tema de investigación, estos casos son Business Track S.A. (Petro audios), sobre el manejo inadecuado que se le dio a la evidencia digital por parte del Fiscalía y Policía Nacional; Caso delitos de abusos sexuales, sobre el manejo de la

evidencia digital a través de conversaciones en cuenta Tuenti; y caso de delito de acoso sexual a través de cuenta de Facebook, siendo la primera sentencia en el Perú que se dio el 2018.

Instrumentos.

Cuestionario. - Este instrumento contiene preguntas abiertas, donde el entrevistado tenga la posibilidad de argumentar sus respuestas con mayor libertad de acuerdo a su experiencia. Estas preguntas, se plantearon partiendo del tema de sub preguntas del problema principal y de los objetivos y teniendo como horizonte los supuestos. El mismo que estuvo compuesta por 8 preguntas abiertas. Ficha de análisis de fuentes documentales: En aplicación de este instrumento de investigación se ha recopilado información valiosa sobre el tema objeto de estudio, esto es, el tratamiento que se ha hecho a nivel doctrinario por los especialistas en la materia. Ficha de análisis jurisprudencial: En aplicación de este instrumento de investigación se ha recopilado información acerca de la postura del Tribunal Constitución, sobre la validez de la prueba digital y sus excepciones establecidos en las jurisprudencias vinculantes.

3.7 Mapeamiento

La presente investigación se ha desarrollado en el Departamento de Lima, se escogió este escenario dado que la mayor parte de la criminalidad se realiza en Lima; también otro de los factores que influyeron para determinar el estudio fue la cercanía y las facilidades de mi persona como abogado en esta Jurisdicción y he visto casos respecto al fenómeno de estudio, asimismo cuento con relaciones amicales con fiscales, miembros de la Policía Nacional del Perú y expertos en tecnologías de información y comunicación, lo cuales son una ventaja para el recojo de la información con mayor facilidad y precisión. Esta se objetiviza mediante el siguiente mapa de procesos:

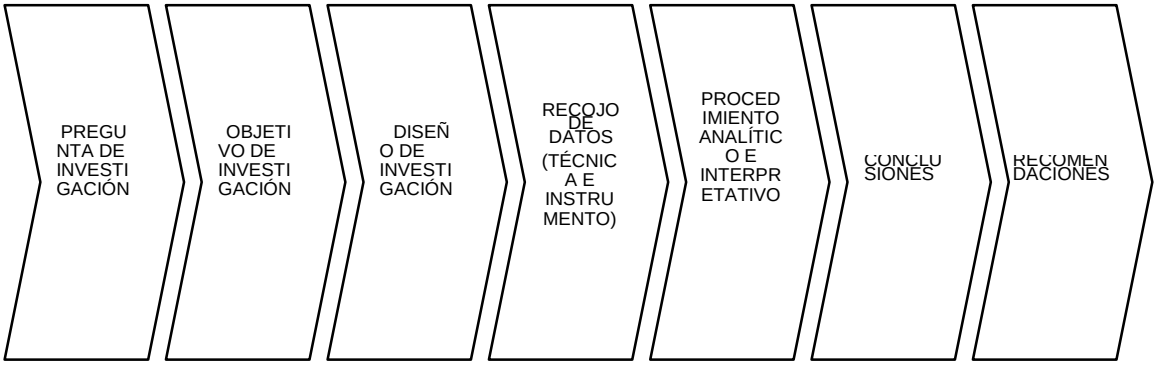


Figura 38. Mapeamiento

3.8 Rigor Científico

Según, Ramirez y Zwerg (2012), sostuvo que en el rigor científico "el investigador debe ser consciente en su forma de ver el mundo y sus limitaciones, cumplir con las condiciones que exige el método y la rigurosidad". (p.94). La presente investigación, ha respetado y respetara las normas establecidos por el método científico, de modo que nos desprenderemos de nuestros criterios personales para dar prevalencia el campo de mundo científico.

Credibilidad.

Según, Rodríguez Gómez, citado por Manuel Cortez, señaló; "la credibilidad es la confianza en la veracidad de los descubrimientos realizados en una investigación y hace referencia a la necesidad que exista isomorfismo entre los resultados de la investigación y las percepciones que los sujetos participan en la realidad estudiada". (p.43).

Transferibilidad.

Según, Palacios, B., Sánchez, y Gutiérrez, A (2011), señaló "este criterio corresponde a la validez externa en la investigación cualitativa. Se refiere al estudio que es representativo del universo al cual pueden extenderse los resultados obtenidos (p.583).

Seguridad.

Se ha redefinido la confiabilidad reliability, fiability como seguridad o auditabilidad dependability. La repetición de datos permite lograr la credibilidad fundamental de las ciencias exactas donde el investigador somete a distintas mediciones y repeticiones confiables.

Confirmabilidad.

El criterio objetivo del investigador está definido como confirmabilidad, de modo que el investigador va construyendo el conocimiento de investigación cualitativa. De manera que permite que otro investigador pueda continuar con complementar con nuevos conocimientos (Marshall y Rossman, 1999).

IV. Resultados

4.1 Descripción de los resultados

Para este proceso se han utilizado las técnicas de entrevista, observación, análisis documental y los instrumentos de recolección de datos, para dar respuesta al objetivo general que es describir alternativas de procedimientos legales e informáticos para el tratamiento de la evidencia digital, para que sean admisibles y tengan el valor probatorio en un proceso penal en el Sistema jurídico Peruano.

Entrevistas.

Para el recojo de información se aplicó una entrevista de tipo semiestructurada, dirigido a un representante del Ministerio Publico, un representante de la Policía Nacional del Perú y un representante experto en Tecnologías de la Información y la Comunicación; el tema central de la entrevista fue el conocer que es la Ciberdelincuencia y ciberespacio, la valoración legal de la evidencia digital en el Perú, el tratamiento de la evidencia digital en otros países y los procedimientos tecnológicos de la evidencia digital.

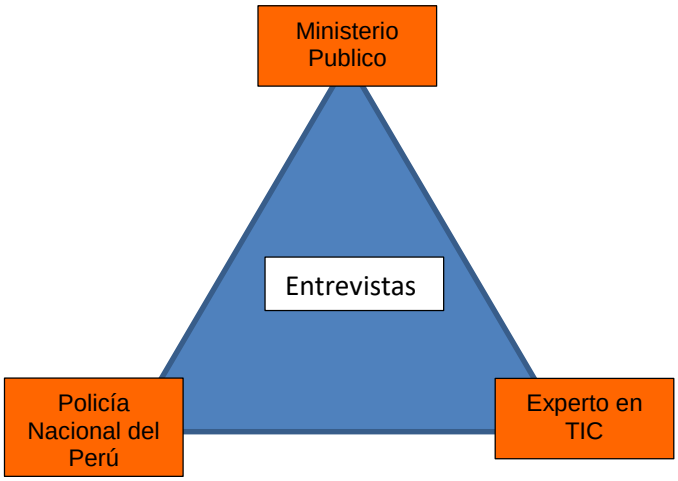


Figura 39. Triangulación de entrevistas de representantes

Análisis Documental.

Respecto al análisis documental, se efectuó una revisión de trabajos previos así como el Marco Teórico y las responsabilidades del Estado respecto a la evidencia digital representadas en las Instituciones públicas que intervienen en la misma, como son el Ministerio Publico, La Policía Nacional del Perú y El Poder Judicial.

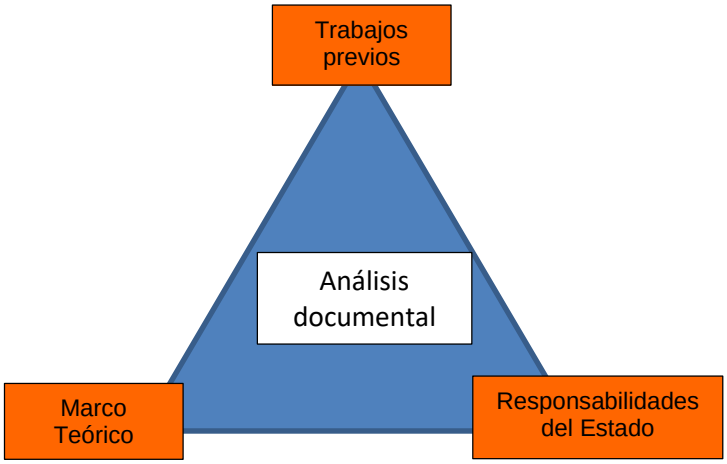


Figura 40. Triangulación de análisis documental

Observación.

Respecto a la observación se analizó sentencias judiciales sobre el tema de la evidencia digital en un proceso judicial, relacionada con el tema de investigación, siendo estos casos el de Business Track S.A. (Petro audios), sobre el manejo inadecuado que se le dio a la evidencia digital; Caso delitos de abusos sexuales, sobre el manejo de la evidencia digital a través de conversaciones en cuenta Tuenti; y caso de delito de acoso sexual a través de cuenta de Facebook.

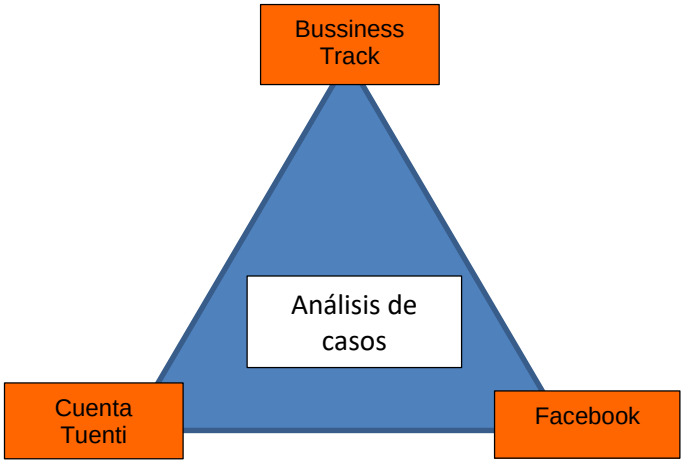


Figura 41. Triangulación de Observación

Resultado de Interpretación y análisis de las entrevistas.

Objetivo General.

Esta investigación se realizó con la finalidad de describir alternativas de procedimientos legales e informáticos para el tratamiento de la evidencia digital, para que sean admisibles y tengan el valor probatorio en un proceso penal en el Sistema Jurídico Peruano y para ello se han planteado los siguientes objetivos específicos:

Ministerio Público - Objetivo Especifico 1.

Determinar cuál es la jurisdicción donde se comenten los delitos informáticos, y si las leyes del país tienen el alcance jurídico para combatirlas.

Tabla 3.

Entrevista OE1 Ministerio Publico

Pregunta	Entrevistado 1 MP	conclusion
¿Qué es la ciberdelincuencia y si es una modalidad delictiva considerada en el Código Penal Peruano?	Consiste básicamente en cualquier delito o actividad ilegal cometido con la ayuda de un ordenador o internet contra una persona, sus bienes, negocios o el propio gobierno, y también se le conoce como delito informático. Existe una amplia variedad de cometer un delito informático. Si alguien piensa cometer un delito tradicional requiere de un montón de cosas y el riesgo es también muy alto sin embargo, para cometer un delito informático, la única necesidad está ahí, un ordenador con conexión a internet y las propias habilidades de la persona de tal forma que es capaz de hacerlo desde la intimidad de su propio hogar	Delito o actividad ilegal cometido con la ayuda de un ordenador o internet. contra una persona, sus bienes, negocios o el propio gobierno. Existe una amplia variedad de cometer un delito informático.

Análisis interpretativo.

La ciberdelincuencia es una modalidad delictiva ilegal, que se desarrolla en el ciberespacio, lugar donde no existe fronteras, presentándose la figura de ser un delito transnacional sin jurisdicción, esta actividad se lleva a cabo a través de medios tecnológicos como computadora, Teléfonos celulares, tabletas y otros, pero para ello básicamente estos dispositivos deben estar conectados a la red internet, lugar donde finalmente se consume el delito, que puede afectar a las personas mediante el acceso prohibido a información personal, así como sus bienes y negocios mediante el robo de información bancaria y operaciones en línea fraudulentas por citar un ejemplo, asimismo también puede afectar al gobierno mediante el acceso a información clasificada como secreto que podría poner en peligro la seguridad de la nación, entre otros. Es preciso indicar que existe una variedad y formas como se realiza los ilícitos por medio de la ciberdelincuencia.

Ministerio Público - Objetivo Especifico 2.

Describir la normatividad jurídica que tiene el Perú para acreditar la admisibilidad y valor probatorio de la evidencia digital.

Tabla 4

Entrevista OE2 Ministerio Publico

Pregunta	Entrevistado 1 MP	conclusion
¿Cree Ud. que la normatividad jurídica en el país, ha previsto el tratamiento de la evidencia digital?	Tratamiento especial de la prueba digital en el Código Procesal Penal del 2004 de manera puntual y especifica No existe, no hay regulación actual como prueba digital, sin embargo el Art. 185 del código procesal penal reconoce al contenido de un audio visual o audio grabado como prueba documental, si entre las fuentes de prueba de un hecho ilícito se encontrara un audio, o un video grabación u otro soporte digital o electrónico, simplemente el desahogo probatorio o actuación probatorio se efectúa en observación del artículo 382 del código procesal penal del 2004.	Tratamiento especial de la prueba digital en el Código Procesal Penal del 2004 de manera puntual y especifica No existe, no hay regulación actual como prueba digital. El Art. 185 del código procesal penal reconoce al contenido de un audio visual o audio grabado como prueba documenta., El desahogo probatorio o actuación probatorio se efectúa en observación del artículo 382 del código procesal penal del 2004.
¿Que significa para Ud. La cadena de custodia y si esta se aplica para la evidencia digital?	La Cadena de Custodia es el procedimiento destinado a garantizar la individualización, seguridad y preservación de los elementos materiales y evidencias, recolectados de acuerdo a su naturaleza o incorporados en toda investigación de un hecho punible, destinados a garantizar su autenticidad, para los efectos del proceso.	Procedimiento destinado a garantizar la individualización, seguridad y preservación de los elementos materiales y evidencias, recolectados. Destinados a garantizar su autenticidad, para los efectos del proceso.

Análisis interpretativo.

En el Nuevo código Procesal Penal no especifica puntualmente el tratamiento especial de la evidencia digital, en el Artículo 185 de la referida norma reconoce que este tipo de pruebas como pruebas documentadas. En el Artículo 382 habla de la incorporación al juicio de las pruebas entre ellas la documental tal como se pretende interpretar a la evidencia digital, las cuales serán exhibidos en el debate y podrán ser examinados por las partes. Respecto a la cadena de custodia indica que es un procedimiento que debe garantizar la individualización, seguridad y preservación de los elementos materiales, debe garantizarse su autenticidad para poder ser considerada en el proceso judicial.

Ministerio Público - Objetivo Especifico 3.

Precisar los procedimientos legales que aplican otros países para garantizar el valor probatorio de la evidencia digital como prueba en un proceso judicial.

Tabla 5

Entrevista OE3 Ministerio Publico

Pregunta	Entrevistado 1 MP	conclusion
¿Si conoce Ud. de algún país que actualmente viene enfrentando adecuadamente la lucha contra la ciberdelincuencia desde el ámbito judicial?	Si considero que Colombia y Argentina en América Latina vienen promulgándose leyes que contribuyen a mejorar y dotar de los instrumentos legales contra la lucha del cibercrimen.	Colombia y Argentina en América Latina. Leyes que contribuyen a mejorar y dotar de los instrumentos legales contra la lucha del cibercrimen

Análisis interpretativo.

Existe muchos países que en la actualidad enfrentan de la manera más acertada la ciberdelincuencia, citando en América Latina a Colombia y Argentina significando que estos países ya se han adherido al convenio internacional de lucha contra la ciberdelincuencia de Budapest. Así mismo en sus países han desarrollado toda una legislación que ha contribuido a mejorar y dotar de instrumentos legales en la lucha del cibercrimen entre ellos el tratamiento de la evidencia digital.

Ministerio Público - Objetivo Especifico 4.

Describir los tratamientos y procedimientos tecnológicos que debe darse a la evidencia digital, para proteger su originalidad, desde su hallazgo, recojo, traslado y entrega final a la autoridad judicial, que garanticen su valor probatorio en un proceso judicial.

Tabla 6

Entrevista OE4 Ministerio Publico

Pregunta	Entrevistado 1 MP	conclusion
¿Conoce de herramientas tecnológicas o jurídicas eficaces que ayuden a dar la legalidad a las evidencias digitales?	En materia procesal me documente sobre la utilización del remote forensic como herramientas de investigación. Ella sugiere a los países la adopción de una norma a nivel nacional que prevea estas técnicas de investigación previendo la excepcionalidad de la medida y un uso restrictivo atendiendo a la potencialidad de afectación a la intimidad que significa su uso.	Remote forensic como herramientas de investigación. Norma a nivel nacional que prevea estas técnicas de investigación

Análisis interpretativo.

En materia procesal tomo conocimiento que una de las herramientas tecnológicas jurídicas que ayuda a mejorar el tratamiento de la evidencia digital y que brindaría legalidad para un proceso judicial es la denominada Remote Forensic que es una herramienta de investigación que cuenta con

técnicas de investigación, adicionalmente existe normatividad en otros países que ayudan al tratamiento de la evidencia digital.

Conclusiones de resultado de Interpretación y análisis de entrevista al representante del ministerio Público.

La ciberdelincuencia es una modalidad delictiva, que se desarrolla en el ciberespacio. Se lleva a cabo empleando medios de tecnología que deben estar conectados a internet. Afecta a la personas, al Estado y también a la seguridad de la nación.

El NCPP no especifica el tratamiento de la evidencia digital, lo trata como prueba documentada. La cadena de custodia debe garantizar la autenticidad de la prueba para el proceso judicial.
Colombia y Argentina en Sudamérica son los países que se han adherido al Convenio de Budapest y han desarrollado mejor legislación dotando de instrumentos legales en el tratamiento de la evidencia digital.

La herramienta Remote Forensic es la que mejor se adecua al tratamiento de la evidencia digital.

Policía Nacional del Perú - Objetivo Especifico 1.
Determinar cuál es la jurisdicción donde se comenten los delitos informáticos, y si las leyes del país tienen el alcance jurídico para combatirlas.

Tabla 7
Entrevista OE1 Policía Nacional del Perú

Pregunta	Entrevistado 2 PNP	conclusion
¿Qué es la ciberdelincuencia y si es una modalidad delictiva considerada en el Código Penal Peruano?	La ciberdelincuencia es una actividad delictiva realizada mediante el uso de las TICs. Actualmente existe la Ley Nro. 30096 y su modificatoria 30171, que sanciona algunas conductas delictivas.	Actividad delictiva realizada mediante el uso de las TICs. Ley Nro. 30096 y su modificatoria 30171, que sanciona algunas conductas delictivas.

Análisis interpretativo.

Es una actividad delictiva que se realiza mediante el empleo de las Tecnologías de la Información y la Comunicación. Así mismo lamentablemente nuestras leyes que datan de muchos años atrás no han sido diseñadas y/o actualizadas para hacer frente a este modo de delincuencia ni a modo nacional que supone sanciones en el código penal mediante la Ley 30096 Ley de Delitos Informáticos, pero el Nuevo código Procesal Penal no ha sido adecuada para el tratamiento y empleo de la evidencia digital, tratándola como una evidencia común. En el ámbito transnacional no es posible sancionar estas conductas ya que las leyes peruanas solo tienen jurisdicción en el país y fuera de ella no.

Policía Nacional del Perú - Objetivo Especifico 2.

Describir la normatividad jurídica que tiene el Perú para acreditar la admisibilidad y valor probatorio de la evidencia digital.

Tabla 8

Entrevista OE2 Policía Nacional del Perú

Pregunta	Entrevistado 2 PNP	conclusion
¿Cree Ud. que la normatividad jurídica en el país, ha previsto el tratamiento de la evidencia digital?	No existe una normativa aborde sobre el tratamiento de la evidencia digital, sin embargo existe un manual de evidencia digital promovido por una ONG, que recoge las buenas prácticas de otros manuales para el manejo de la evidencia digital. En tanto, la PNP ha elaborado un manual para el recojo de la evidencia digital, que se encuentra a la espera de su aprobación.	No existe una normativa aborde sobre el tratamiento de la evidencia digital. Existe un manual de evidencia digital promovido por una ONG, que recoge las buenas prácticas de otros manuales para el manejo de la evidencia digital.
¿Que significa para Ud. La cadena de custodia y si esta se aplica para la evidencia digital?	Procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis, normalmente peritos, y que tiene fin no viciar el manejo que de ellos se haga y así evitar alteraciones, sustituciones, contaminaciones o destrucciones. La cadena de custodia se aplica tanto a la evidencia física así como a la evidencia digital.	Procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis. se aplica tanto a la evidencia física así como a la evidencia digital.

Análisis interpretativo.

En nuestro país no existe normatividad sobre el tratamiento de la evidencia digital, refiere que se ha formulado un manual de evidencia digital promovido por una ONG, en el cual se aprecia buenas practicas recogidas de otros manuales de otros países respecto al manejo de la evidencia digital, pero para un proceso judicial se requiere de normas puntales en el código Procesal Penal para cuidar el procedimiento de tratamiento de la evidencia digital, así mismo indica que la Policía Nacional del Perú ha formulado un manual de recojo de evidencias digital pero que a la fecha no ha sido aprobada por su Comando PNP. Respecto a la cadena de custodia lamentablemente se aplica el procedimiento controlado de la evidencia digital como una evidencia física de indicios materiales que relacionan al delito, en su localización, su valorización y su posterior análisis.

Policía Nacional del Perú - Objetivo Especifico 3.

Precisar los procedimientos legales que aplican otros países para garantizar el valor probatorio de la evidencia digital como prueba en un proceso judicial.

Tabla 9

Entrevista OE3 Policía Nacional del Perú

Pregunta	Entrevistado 2 PNP	conclusion
¿Si conoce Ud. de algún país que actualmente viene enfrentando adecuadamente la lucha contra la ciberdelincuencia desde el ámbito judicial?	Podría mencionar a España, que cuenta con personal contantemente capacitado y la tecnología adecuada, dentro de la región se encuentran Colombia y Brasil.	España, que cuenta con personal constantemente capacitado y la tecnología, de la región se encuentran Colombia y Brasil.

Análisis interpretativo.

Uno de los países que mejor se ha desarrollado en la lucha contra la ciberdelincuencia es España, tienen personal permanentemente entrenado, capacitado así como contar con tecnología adecuada y actual que les brinda un soporte técnico en esta lucha, así mismo indica que a nivel Sudamérica los países que mejor se han desarrollado para enfrentar estos ilícitos son Colombia y Brasil.

Policía Nacional del Perú - Objetivo Especifico 4.

Describir los tratamientos y procedimientos tecnológicos que debe darse a la evidencia digital, para proteger su originalidad, desde su hallazgo, recojo, traslado y entrega final a la autoridad judicial, que garanticen su valor probatorio en un proceso judicial.

Tabla 10

Entrevista OE4 Policía Nacional del Perú

Pregunta	Entrevistado 2 PNP	conclusion
¿Conoce de herramientas tecnológicas o jurídicas eficaces que ayuden a dar la legalidad a las evidencias digitales?	El Triage consiste en realizar una búsqueda rápida empleando criterios sencillos sobre la estructura del disco, evitando profundizar las búsquedas en áreas especiales del disco. La realización de una copia o imagen forense, en la escena de delito mediante una copia bloque a bloque bit a bit del contenido digital almacenado, el que es autenticado mediante una función HASH.	El Triage consiste en realizar una búsqueda rápida empleando criterios, La realización de una copia o imagen forense, en la escena de delito, función HASH.

Análisis interpretativo.

A nivel policial considera que la herramienta tecnológica denominada Triage ayuda a realizar una búsqueda rápida de la evidencia empleando criterios sobre estructura del disco donde se halla la información, así mismo brinda la realización de copias o imágenes forenses en la misma escena del delito

efectuado un copiado de bloque a bloque, de bit a bit del contenido de la información que es la evidencia almacenada y para darle mayor consistencia utiliza la función Hash que autentica la información.

Conclusiones de resultado de Interpretación y análisis de entrevista al representante de la Policía Nacional del Perú.

La ciberdelincuencia se realiza por medio de las TIC. Solo se tiene a la Ley 30096 Ley de delitos informáticos, el NCPP no ha sido adecuado para el tratamiento de la evidencia digital.

En el Perú no hay normatividad sobre el tratamiento de la evidencia digital. La cadena de custodia se realiza como si la evidencia digital fuese una evidencia física.

España es uno de los países que más se ha desarrollado en la lucha contra la ciberdelincuencia.

A nivel policial la herramienta Triage es la que se utiliza para la búsqueda de evidencias en las unidades de almacenamiento. Y se le da mayor consistencia con la función hash.

Experto en TIC - Objetivo Especifico 1.

Determinar cuál es la jurisdicción donde se comenten los delitos informáticos, y si las leyes del país tienen el alcance jurídico para combatirlas.

Tabla 11

Entrevista OE1 Experto TIC

Pregunta	Entrevistado 3 TIC	conclusion
¿Qué es la ciberdelincuencia y si es una modalidad delictiva considerada en el Código Penal Peruano?	La Ciberdelincuencia es un delito que está focalizado o se desarrolla en el ámbito del internet, generalmente es el canal que utiliza el delincuente para cometer delitos, claro se tipifica el delito cuando existe una norma una ley que así lo define, pero en nuestro país por ejemplo un botmaster no tendría ninguna sanción, en Estados Unidos un botmaster puede ser condenado a 15 años de prisión entonces, que es el ciberdelito son delitos que se realizan principalmente en el canal de Internet pero para ser considerados como delitos tiene que tener una tipificación.	Delito que está focalizado o se desarrolla en el ámbito del internet. Se tipifica el delito cuando existe una norma una ley que así lo define.

Análisis interpretativo.

La ciberdelincuencia se focaliza en el ámbito de internet, lugar donde se cometen los ilícitos. Así mismo en nuestro país no se tipifica este delito por no existir una Ley que la tipifique como tal y la sanciones, en otros países si se sanciona, por ejemplo una modalidad de ciberdelincuencia en otro país si se sanciona y en el nuestro no.

Experto en TIC - Objetivo Especifico 2.

Describir la normatividad jurídica que tiene el Perú para acreditar la admisibilidad y valor probatorio de la evidencia digital.

Tabla 12

Entrevista OE2 Experto TIC

Pregunta	Entrevistado 3 TIC	conclusion
¿Cree Ud. que la normatividad jurídica en el país, ha previsto el tratamiento de la evidencia digital?	Considero que eso es importante, pero que no exista en nuestro ordenamiento jurídico es un reflejo simplemente y de nuestra sociedad que nosotros nos gusta ir por el camino corto no respetamos las reglas; en la mañana estaba conversando con un taxista que me traía y hablábamos del callao, en el callao han puesto algo de tecnología con sistema de videocámaras, no es una ciudad inteligente sino que simplemente son cámaras que están conectadas a equipos para poder detectar la velocidad y todo el mundo anda 60 pero apenas cruza la línea que dice callao hacia lima, aumenta su velocidad a 80 o 90, cuál es la diferencia porque en dos cuadras uno puede ver ciudadanos yendo a 60 y a la siguiente cuadra a 80. Porque hay un sector, un territorio donde se cumple con la ley y esta se cumple con una sanción hay una pena en el otro lado no hay una sanción, entonces donde no se regula adecuadamente las cosas la gente hace lo que quiere, en el ciberespacio es exactamente es igual, porque nuestro país a esto el delincuente lo llama paraísos cibernético, es donde no hay la norma, no hay el procedimiento, no hay la pena entonces está libre y ejemplo de estos hay muchos en Argentina había un delincuente denominado el Gordo España, esta persona había cometido una cantidad de delitos terribles en España y le solicita a la Argentina la deportación, para ello argumentan todo y presentan sus leyes y lo demuestra muy bien todo perfecto, pero cuando llega a la Argentina dice no la puedo mandar porque eso aquí no es delito; y yo digo no había cometido el delito en Internet en Argentina. Entonces qué pasó, pasaron dos años o tres y Argentina actualiza su legislación, qué cosa crees que hizo	Considero que eso es importante, pero que no exista en nuestro ordenamiento jurídico es un reflejo simplemente y de nuestra sociedad que nosotros nos gusta ir por el camino corto no respetamos las reglas. En el ciberespacio es exactamente es igual, porque nuestro país a esto el delincuente lo llama paraísos cibernético, es donde no hay la norma, no hay el procedimiento, no hay la pena entonces está libre,

Análisis interpretativo.

Al no existir un ordenamiento jurídico sobre la evidencia digital es una muestra que en nuestro país no la tomamos en cuenta, lamentablemente nuestra sociedad no le gusta cumplir ni respetar las normas, se busca siempre lo más sencillo aun en contra de las normas, esto sucede en forma similar en el ciberespacio es por ello que el ciberdelincuente llama nuestro país el paraíso cibernético donde no hay norma, no hay procedimiento, hay libertad para hacer lo ilícito en esta modalidad delictiva. La cadena de custodia es muy importante no solo de tener personal preparado que realice este procedimiento de la forma correcta, si no de contar con equipos y programas legalmente constituidos con licencias, para darle la credibilidad legal en el cuidado y obtención de la evidencia digital.

Experto en TIC - Objetivo Especifico 3.

Precisar los procedimientos legales que aplican otros países para garantizar el valor probatorio de la evidencia digital como prueba en un proceso judicial.

Tabla 13

Entrevista OE3 Experto TIC

Pregunta	Entrevistado 3 TIC	conclusion
¿Si conoce Ud. de algún país que actualmente viene enfrentando adecuadamente la lucha contra la ciberdelincuencia desde el ámbito judicial?	Podemos mirar a Colombia que tiene una cuarta Fuerza Armada que es la ciberseguridad, pero la verdad que estaba pensando, en Argentina en Chile tú sabes que en una reunión que tuvimos de Celaes en Miami, se presentó la representante de seguridad del Banco Famérica y hablaba sobre ciberdelitos y ella manifestó que el problema más grande que tenía el banco era el phishing, yo me preguntaba el phishing será problema para un banco tan grande, después seguir escuchando dijo que el phishing que afectaba al banco famerica era el que provenía de Perú el problema más grande del banco famerica en ese momento era el phishing qué provenía de Perú y Cuál era el motivo la calidad del engaño del phishing, entonces los peruanos porque tienen mucha imaginación y el problema de Sudamérica relacionado con ciberdelitos son los hackers peruanos y brasileros. Porque algunos han estudiado en los países de Rusia antigua, terminaron fueron captados por las bandas rusas y ya están de regreso hablan el idioma y aprendieron la tecnología, yo estoy seguro si esas personas practicaran el bien tendrían unas empresas maravillosas y producirían muchos ingresos al país pero sin embargo, se van a lo fácil y te comento algo más en Cybertec de Israel en el 2017 Benjamín Netanyahu habla al empresariado de Israel y les dice hace 5 años yo propuse alcanzar estar entre las cinco primeras economías en ciberseguridad y en el 2017 les decía a todos tus empresarios que esa meta la habían alcanzado y el 20% de la facturación de ciberseguridad global es de Israel, dime tú si no es importante, si no es algo interesante para el país, poder darle la oportunidad los jóvenes orientarlos a estudiar temas de ciberseguridad de ciberdefensa para que puedan también generar empresas que a su vez generan ingresos y desarrollo para el país.	Colombia que tiene una cuarta Fuerza Armada que es la ciberseguridad. Es algo interesante para el país, poder darle la oportunidad los jóvenes orientarlos a estudiar temas de ciberseguridad de ciberdefensa para que puedan también generar empresas que a su vez generan ingresos y desarrollo para el país

Análisis interpretativo.

Considera que Colombia es uno de los países en Sudamérica que más ha desarrollado la lucha contra la ciberdelincuencia ya que ha creado su cuarta fuerza Armada encargada de la ciberseguridad, así mismo considera que nuestro país debería darle oportunidad a los jóvenes a involucrarse, estudiar y prepararse en temas de ciberseguridad, ya que generarían empresas competitivas y con altos ingresos pero por sobre todo seguras a esta modalidad delictiva, ello sería muy beneficioso y de gran desarrollo para nuestro país.

Experto en TIC - Objetivo Especifico 4.

Describir los tratamientos y procedimientos tecnológicos que debe darse a la evidencia digital, para proteger su originalidad, desde su hallazgo, recojo, traslado y entrega final a la autoridad judicial, que garanticen su valor probatorio en un proceso judicial.

Tabla 14

Entrevista OE4 Experto TIC

Pregunta	Entrevistado 3 TIC	conclusion
¿Conoce de herramientas tecnológicas o jurídicas eficaces que ayuden a dar la legalidad a las evidencias digitales?	Hay herramientas que están certificadas para poder extraer información del celular y preservarla como evidencia, son herramientas válidas para poder certificar y estas herramientas deben estar acompañadas de personal capacitado con el conocimiento y la certificación necesaria, con los protocolos de cadena de custodia y con la participación de la autoridad tanto de la denuncia y la de la investigación para darle el marco de la legalidad.	Hay herramientas que están certificadas para poder extraer información del celular y preservarla como evidencia. Estas herramientas deben estar acompañadas de personal capacitado con el conocimiento y la certificación necesaria, con los protocolos de cadena de custodia y con la participación de la autoridad tanto de la denuncia y la de la investigación para darle el marco de la legalidad

Análisis interpretativo.

El especialista en TIC refiere que hay varias herramientas tecnológicas que ayudan a la preservación de la evidencia digital, pero enfatiza que estas herramientas para que puedan brindar información legalmente valida deben de estar debidamente certificadas y autenticadas con las respectivas licencias, así mismo de contar con personal capacitado y entrenado con la certificación correspondiente y que en estos procesos es importante la participación de la autoridad que brinda la legalidad de los procedimiento como es el representante del Ministerio Publico, de esta manera estaríamos dándole la legalidad al tratamiento de la evidencia digital para su posterior utilización en el proceso judicial.

Conclusiones de resultado de Interpretación y análisis de entrevista al experto en tecnologías.

La ciberdelincuencia se focaliza en el internet donde se cometen los delitos.

No existe ordenamiento jurídico en el Perú sobre el tratamiento dela evidencia digital es considerado paraíso cibernético. La cadena de custodia debe hacerlo personal preparado, con equipos con licencias.

Colombia es uno de los países que más se ha desarrollado en la lucha contra la ciberdelincuencia, cuenta con la cuarta fuerza armada que se encarga de la ciberseguridad.

Existen varias herramientas tecnológicas para la preservación de la evidencia digital, estas deben estar certificadas con sus respectivas licencias y tener personal certificado en entrenamiento.

Conclusión de entrevistas.

La ciberdelincuencia se desarrolla en el ciberespacio por medio de las Tic conectados a internet.

En el Perú no hay normatividad jurídica sobre el tratamiento de la evidencia digital y la Cadena de Custodia se realiza como si fuese una evidencia física.

España, Colombia y Argentina son los países que mejor se han desarrollado en la lucha contra la ciberdelincuencia, además son parte del Convenio de Budapest.

Existen varias herramientas como el Remote Forensic, Triage para el tratamiento de la evidencia digital, estas deben estar certificadas con licencias y contar con personal capacitado.

Resultados del análisis documental.

Trabajos previos.

El presente trabajo de investigación abordó una importante fuente de trabajos previos realizados con cierto grado de similitud. Lo que permitió ahondar en la problemática, de modo que nos permitió comprender y analizar con mayor agudeza las dimensiones de la estructura del trabajo. Enseguida citaré los aportes de mayor relevancia:

Justo (2017), Policía Federal Argentina Área Digital Asociación por los Derechos Civiles elaboraron el trabajo *"Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal"*, correspondiente al proyecto financiado por Ford Foundation. Dicha investigación enfatiza la importancia y facultades en el ámbito procesal penal que deben de tener los investigadores en las diferentes modalidades del Cibercrimen tales como procesos, servicios, actividades o manejo de información que se realizan en línea, considerándose que un mismo ilícito se puede realizar en diferentes jurisdicciones (países), por la naturaleza del internet. Los operadores de justicia para tener éxito en sus investigaciones y decisiones, deben validar la información; móvil del ilícito, pero al involucrar diferentes países se presenta el problema de la jurisdiccionalidad o en su defecto la rogatoria internacional que se realiza para tener respuesta del pedido de información, conllevado a la demora de la investigación judicial incumpliéndose los plazos de investigación.

Análisis interpretativo.

La Asociación por los Derechos Civiles, durante una jornada de trabajo con la Policía Federal de Argentina realizaron un aporte muy beneficioso para todo el ecosistema de operadores que interactúa día a día en el quehacer de la investigación criminal, la Jornada de Trabajo contó con la participación de integrantes de los equipos y laboratorios forenses de las fuerzas policiales federales y provinciales, fiscales y miembros del poder judicial y reconocidos abogados penalistas. Se abordaron varios temas resaltando para la presente investigación el relacionado al desarrollo de investigaciones sobre cibercrimen

más exitosas, concluyeron que es necesario incorporar mejores herramientas judiciales y procesales que permitan proveer al perito de los elementos necesarios para que luego el operador judicial haga la valoración final de toda la actividad de investigación técnica. En este sentido, Estados Unidos y algunos países de Europa han adoptado herramientas que han sido útiles para ello. Es importante tener en cuenta las facultades procesales que deben tener los investigadores en cibercrimen cuando deben ocuparse de delitos online en los cuales existe una multiplicidad de jurisdicciones por la propia naturaleza de internet. De esta manera, si un operador judicial debe validar una información generada en otro país, debe esperar una rogatoria internacional que demora la investigación judicial.

Lasso (2017), presento una Monografía para optar al título de Especialista en Seguridad Informática de la Universidad Nacional abierta y a distancia, unad Escuela de Ciencias Básicas Tecnología e Ingeniería Especialización en Seguridad Informática Palmira, titulada *"Estado del peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia",* al respecto precisa que el estudio del fenómeno, denominado comúnmente delincuencia o criminalidad informática, y la motivación de contar con una capacidad de respuesta legal adecuada, ha permitido que se dé solución jurídica a muchos de los aspectos concernientes al cibercrimen tanto desde el Derecho Penal como desde el Derecho Procesal Penal, vinculándose el manejo ilícito de la informática con la protección de lo que se ha denominado bien jurídico tutelado de la información y de los datos mediante la expedición de la ley 1273 de 2009. La creciente incidencia de la Ciberdelincuencia a determinado la inminente necesidad de contar con un ordenamiento jurídico que sancione de forma adecuada a la cibercriminalidad, no solo desde la identificación de los delitos cometidos y el establecimiento de penas sino también desde el procedimiento penal admitido para dar solución a las investigaciones en las que se vea involucrada evidencia digital. En Colombia existen soportes constitucionales, el Derecho al Debido Proceso consagrado en el artículo 29 de la Constitución mediante la Sentencia C-980/10, Ley 527 de 1999 y la Ley 906 de 2004 en donde se expide el Código

de Procedimiento Penal, que brinda herramientas para la presentación de la evidencia digital durante un proceso judicial, aunque también dan a conocer la urgencia de la mejoría del Estatuto Procesal Penal de modo que sea suficiente y su interpretación y aplicación no sea incongruente.

Análisis interpretativo.

Lasso, en su Monografía para optar al título de Especialista en Seguridad Informática, de la Universidad Nacional abierta y a distancia, UNAD Escuela de Ciencias Básicas Tecnología e Ingeniería especialización en seguridad informática Palmira, Colombia, desarrollo el tema “Estado del peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia”. Concluye que el peritaje informático es una actividad de investigación que ha tomado fuerza a nivel internacional debido a la relevancia que tiene dentro de los procesos judiciales donde interviene la evidencia digital, a raíz del aumento de los ciberdelitos, pues permite esclarecer los hechos ocurridos en un caso específico, brindando las herramientas para dirimir y lograr la impartición de la justicia de manera adecuada. El órgano judicial en Colombia cuenta con un marco jurídico amplio en relación a los aspectos concernientes a la ciberdelincuencia, pero debido al desconocimiento por parte de los jueces, la impartición de la justicia flaquea y en ocasiones se pierde, dañando la confianza que la sociedad deposita en la justicia como medio para proteger sus derechos y castigar con rigor toda conducta ilícita.

Nessi (2017), presento el Proyecto de apoyo al sector Justicia American Bar Association Rule of law Initiative aba roli Perú, Ministerio Publico y Policía Nacional del Perú, titulada ***“Manual de Evidencia Digital”,*** al respecto precisa que debe tenerse en cuenta que quienes participen en los diferentes actos, ya sean estos, estrictamente de aseguramiento o análisis de la evidencia o de conducción de la investigación penal, lo harán bajo las prescripciones del Nuevo Código Procesal Penal Decreto Legislativo N° 957 el mismo que prescribe en su artículo 67, el aseguramiento de la escena del delito será llevado a cabo por funcionarios de la Policía Judicial que cuenten

con un conocimiento técnico avanzado en cuanto al manejo de la evidencia digital, debiendo dar inmediata noticia de ello al Fiscal. Es importante precisar que es de vital importancia que quienes intervengan en la escena del delito sean personas capacitadas sobre el manejo de la evidencia, ya que mediante un correcto desempeño de sus funciones se garantiza desde el inicio la integridad de los distintos dispositivos que puedan ser incautados. El personal que accede a la escena debe contar con experiencia previa o estar capacitado en el manejo de la evidencia digital para adoptar mejores decisiones. Toda actividad llevada a cabo fuera de los protocolos establecidos podría alterar la evidencia.

Análisis interpretativo.

La ONG American Bar Association Rule of law Initiative aba roli Perú, en un Proyecto de apoyo al Sector Justicia del Perú, con el auspicio del gobierno de EEUU, en el cual participo representantes del Ministerio Publico de la Fiscalía Especializada Delitos de Corrupción de Funcionarios y Delitos de Lavado de Activos y Pérdida de Dominio del Perú, así como y personal de la Policía Nacional del Perú de la Divindat PNP; elaboraron el “Manual de Evidencia Digital”, el cual busca reducir los errores frecuentemente cometidos al abordar una escena del crimen en el que se pueden encontrar medios de prueba altamente sofisticados y cuyo aseguramiento, protección y análisis exige conocimientos y técnicas avanzadas que impidan su alteración e, incluso, su destrucción. En este sentido, el Manual resulta útil para policías y fiscales en tanto se encuentran a cargo de la investigación y procesamiento de casos criminales así como de jueces quienes podrán advertir la complejidad que reviste el abordaje de un caso en el que las Nuevas Tecnologías se encuentran presentes. En ella se explica de manera sencilla, los términos que se emplean en el tratamiento de la evidencia digital. Para ello tuvo como referencia bibliográfica protocolos y guías de otros países, siendo sus principios básicos y generales fundamentalmente la capacitación y el entrenamiento de los investigadores, técnicos y fiscales para un correcto procedimiento, exento de falencias u objeciones procesales. El personal policial no debe adoptar ninguna decisión en la escena del delito que pueda

alterar o modificar los datos contenidos en los dispositivos de almacenamiento a utilizar sin previa consulta con el fiscal. Del mismo modo, las herramientas y metodologías a utilizar en la escena del delito, deben ser previamente acordadas con el director de la investigación.

Sequeiros (2016), presento una tesis para optar el título profesional de abogado en la Universidad de Huánuco, facultad de derecho y Ciencias Políticas, titulada *"Vacío legales que imposibilitan la sanción de los delitos informáticos en el nuevo Código Penal Peruano*"**,** al respecto la tesis sustenta en relación al vacío legal o laguna jurídica en el Derecho a la ausencia de reglamentación legislativa en una materia concreta. Es una situación de vacío en la ley que ha sufrido omisión en su texto la regulación concreta de una determinada situación, que no encuentra respuesta legal específica; con ello se obliga a quienes aplican dicha ley (jueces, abogados, fiscales, y otros) al empleo de técnicas sustitutivas del vacío, con las cuales puedan obtener respuesta eficaz a tal ausencia. Ante esta situación, se hace necesario suplir la laguna jurídica a través de distintas herramientas tales como el Derecho Supletorio donde el juez acude a la regulación de una rama del derecho supletoria. La Interpretación extensiva el juez hace una interpretación lo más extensiva posible de una norma cercana. La Analogía el juez aplica normas que están dictadas para situaciones esencialmente parecidas. Acudir a otras fuentes del derecho como la costumbre o los principios generales del Derecho y la Norma Cruzada entre normas principales y otras supletorias, de modo que se sabe cuál debe aplicarse con preeminencia y al mismo tiempo, entre del derecho principal y el derecho supletorio.

Análisis interpretativo.

Sequeiros (2016), en su tesis titulada *"Vacío legales que imposibilitan la sanción de los delitos informáticos en el nuevo Código Penal Peruano",* sustentada en la Universidad de Huánuco, presento las siguientes conclusiones que a modo de resumen se detallan; Dada la naturaleza virtual de los delitos informáticos, estos se pueden volver confusos en su tipificación, ya que a nivel general, se poseen pocos conocimientos y experiencias en el

manejo de ésta área. Nuevas modalidades de negocios por internet, como el comercio electrónico es un claro ejemplo de cómo los delitos pueden aparecer de diversas formas, por lo que se deben crear instrumentos legales efectivos que ataquen ésta problemática, con el único fin de tener un marco legal que se utilice como soporte para el manejo de éste tipo de transacciones. Los delitos informáticos no deben impedir que el usuario se prive de todo lo que proveen las tecnologías de información (comunicación remota, Interconectividad, comercio electrónico, etc.); sino por el contrario dicha situación debe plantear un reto a los profesionales de la informática, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad, controles, integridad de la información, etc. en las organizaciones.

Jiménez (2018) en su tesis titulada "*Desarrollo de una aplicación de uso didáctico para comunicación segura de datos a través de la red",* sustentada en la Escuela Politécnica Nacional de Quito; refiere en los servicios de integridad la función que cumple el algoritmo "Un algoritmo Hash es una función que toma una cadena o mensaje de longitud variable y produce un valor hash de longitud fija, también llamado resumen de mensaje, que se emplea para verificar la integridad de los datos y mensaje, que se emplea para verificar la integridad de los datos y mensajes, se representa como una cadena corta de letras aleatorias y números, es como una huella digital de un mensajes, es un proceso unidireccional, pues no es posible crear el texto original utilizando cualquier función del hash inverso, si los datos originales cambian incluso por un carácter, la función hash producirá un valor hash diferente, por lo tanto, el receptor sabrá que la información original ha cambiado" (p.33).

Análisis interpretativo.

En este trabajo se concluye que la aplicación Hash es una técnica informática que permite el asegurar de la integridad de las pruebas digitales. Ello resulta muy importante en la evidencia digital y están basadas en la obtención de datos de los medios de almacenamiento de un dispositivo electrónico mediante el procedimiento llamado copia espejo el que identifica el origen de

la información en los dispositivos electrónicos como una copia única. Esta función basada en algoritmos otorga al contenido de un archivo un valor numérico, corroborándose que los datos que se encontraban en el dispositivo original no han sido manipulados y, por tanto, son los mismos que los que se hallan en la copia. Mediante este procedimiento deberá originarse un original de los datos, una copia resultado del clonado que será sobre la cual se practicará la pericia informática, y una segunda copia para el propietario de los datos, para el caso de que fuese necesario.

Conclusiones del resultado de Interpretación y análisis de análisis documental.

En las investigaciones sobre cibercrimen la falta de herramientas judiciales y procesales, el desconocimiento de los jueces y fiscales sobre el tema, el personal policial que contamina la evidencia digital en la escena del hecho, la creciente demanda de comercio electrónico, negocios, operaciones, actividades diversas de las personas en línea que abren las puertas a los ciberdelincuentes y la multiplicidad de jurisdicciones por la naturaleza del internet donde se cometen estos ilícitos, se requiere que el operador judicial cuente con facultades procesales para que pueda validar la actividad de la investigación técnica. Es importante la actividad de investigación del perito informático, por el tratamiento que da a la evidencia digital y también la aplicación de procedimientos técnicos como el Hash en el aseguramiento de la integridad de evidencias digitales.

Marco Teórico.

El presente trabajo de investigación abordó una importante fuente de información referenciada en el Marco Teórico referencial que consistió en buscar las fuentes documentales que permitan detectar, extraer y recopilar la información de interés al problema de investigación planteado con cierto grado de similitud, organizado en cuatro sub capítulos que a continuación se detalla

La ciberdelincuencia.

Esta actividad delictiva se define como aquella acción en la que utilizando en el Internet, destruye o avería equipos de cómputo, y similares así como net de Internet. También buscan atentar la veracidad, la entereza de los sistemas informáticos y sus redes, además podríamos agregar que son actividades que buscan robar información, suplantar la identidad de personas, generar fraudes a personas naturales y jurídicas, etc, entre otros.

Ciberespacio, Es el lugar virtual, ya que no tiene una locación física espacial, en ella interactúan usuarios, se explora información on line en páginas web, se comunican mediante redes sociales sin reparo de tiempos y distancias mediante el empleo del Internet.

Al no existir fronteras para este flagelo hoy más que nunca se hace necesario que los entes responsables al ejecutar la ley tengan problemas en actuar eficazmente, por la gran barrera que genera los límites en las investigaciones transfronterizas, a ello se suma problemas de tipo jurídico y la diversidad de capacidades en el mundo. Las fronteras nacionales, aunque se lea irónicamente, representan una dificultad para el tratamiento de los ciberdelincuentes.

Análisis interpretativo.

En el marco teórico de la presente investigación llegamos a determinar que la ciberdelincuencia para ser considerado como ilícito necesariamente esta debe utilizar el internet, y las consecuencias que genera esta acción se evidencia en los medios o equipos tecnológicos que son utilizados como medios para consumar el ciberdelito. Asimismo los objetivos que tiene los ciberdelincuentes son atentar contra la integridad y veracidad de los sistemas informáticos que administran información sean estos públicos o privados, también buscan robar información personal con intenciones de suplantarlos generando inestabilidad entre las personas sean estas naturales o jurídicas. Además el medio o lugar donde se ejecutan estas acciones ilícitas se les conoce como el Ciberespacio que es un lugar virtual sin espacio físico, en ella

interactúan todos los usuarios conectados a internet donde navegan accediendo a todo tipo de actividad o información que se requiera, sin reparo de tiempos y distancias. No existe fronteras en el ciberespacio y ello hace más complicado la lucha contra la ciberdelincuencia debido a que cada país tiene sus propias leyes y procesos, existiendo su ámbito de jurisdicción para juzgar y sancionar los ilícitos, los delitos informáticos son delitos transnacionales.

Normatividad Jurídica Nacional.

La Policía Nacional del Perú según el NCPP (2004), en su artículo 67° numeral 1, prescribe: (…) tiene como atribuciones en otras: Proteger y vigilar la escena del delito con la finalidad que no se borre los indicios, restos o señales del delito asimismo reunir, agrupar y cuidar los objetos o dispositivos que relacionan con el delito, y todo aquello que sirva para la investigación. El artículo 155° numeral 2, prescribe: Las pruebas se admiten a solicitud del Ministerio Público o de los demás sujetos procesales. El Juez decidirá su admisión mediante auto especialmente motivado, y sólo podrá excluir las que no sean pertinentes y prohibidas por la Ley El artículo 172° numeral 1, indica: La pericia procederá siempre que, para la explicación y mejor comprensión de algún hecho, se requiera conocimiento especializado de naturaleza científica, técnica, artística o de experiencia calificada. El artículo 184° numeral 1, prescribe: Se podrá incorporar al proceso todo documento que pueda servir como medio de prueba, asimismo “Son documentos los hológrafos, folletos, reproducciones, fax, dispositivos magnéticos, películas, imágenes, gráficos, grabaciones magnetofónicas y otros que contengan registro de las actividades anteriormente descritas.

La valoración de la prueba es el juicio de aceptabilidad de los resultados probatorios. La valoración constituye la medula del razonamiento probatorio; es decir, del razonamiento que orienta, a partir de las informaciones aportadas al proceso a través de los medios de prueba, a una afirmación sobre hechos controvertidos. Obando V. (2013). La valoración de la prueba. *Jurídica Suplemento de análisis legal*. Recuperado de: https://bit.ly/2ouSAFA.

La Cadena de custodia es el procedimiento que garantiza, asegura y reserva las evidencias, halladas en la escena del delito, para que ingresen a la investigación en curso del ilícito, con el objetivo de asegurar su autenticidad, en el proceso judicial. Se inicia con el ingreso del primer efectivo policial a la escena del Delito, que posteriormente seguirá un procedimiento de conformidad a lo que establece la Guía de Procedimientos de Criminalística**.** Ello permite acreditar que la evidencia sea la misma que fue recogida o analizada y que su totalidad no haya sido alterada durante el proceso penal (principio de mismidad). Asimismo trata de evitar suspicacia en la autenticidad y/o indemnidad de la evidencia.

Ley 30096 Ley de delitos informáticos, en la actualidad como consecuencia del acentuado crecimiento de las TIC aparecen de nuevos ilícitos tipificados como delitos informáticos. Para frenar el creciente y alarmante hecho que involucra fundamental mente a la tecnología, se ha promulgado la Ley penal especial que busca prevenir y combatir las diferentes actividades ilícitas que dañan críticamente sistemas de información y por ende sus datos informáticos, sin dejar de lado el secreto de las comunicaciones, y los otros que como consecuencia de este ilícito resulten afectados. La norma en referencia refiere en su artículo 1 que el fin que busca la norma es la prevención y la sanción del comportamiento ilícito que perjudican los sistemas, la información, el secreto de las comunicaciones así como los bienes jurídicos de importancia penal que resultaren dañados por medio del empleo de las TIC, y que garanticen las mínimos requisitos de que las personas disfruten del derecho a la libertad y al desarrollo. Esta norma busca asegurar la lucha eficaz contra la ciberdelincuencia.

La Dirección General de la PNP en el año 2005, creó la División de Investigación de Delitos de Alta Tecnología, unidad especializada que se encarga de investigar los ilícitos penales de delitos informáticos, así como los hechos en que se encuentre como medio de realización del delito un medio informático. Siendo una unidad que requiere de todo el apoyo de personal y logística para que cumpla con desarrollar un alto trabajo tecnológico lamentablemente, en la actualidad las instalaciones donde presta sus

servicios es inadecuada, no cuenta con un selecto personal acorde a los conocimientos e exigencias que demanda el conocimiento de tecnologías, y lo más importante no tiene el equipamiento idóneo para realizar la exploración e indagación de las evidencias digitales.

El Estado Peruano para proteger sus datos, información así como su infraestructura tecnológica en previsión de amenazas internas o externas, preservando la confidencialidad, integridad, legalidad y confiablidad de su información, ha implementado normatividad referente a la seguridad de información, basadas en políticas, partidas y recursos pertinentes a fin de tener un gobierno en el país de Ciberseguridad actual que busca también la participación de entes estatales y del entorno privado, así como representantes civiles y otros.

Análisis interpretativo.

Es importante identificar a los diferentes actores que participan desde el descubrimiento de un ilícito informático hasta su posterior juzgamiento y aplicación de penas, siendo el medio utilizado por los ciberdelincuentes los diferentes equipos tecnológicos pero todos ellos con un común denominado evidencia digital ya que ahí se encuentra el inicio de la posible identificación de la persona que cometió el delito informático, es por ello que inicialmente en la escena del delito la Policía Nacional del Perú de conformidad al Nuevo Código Procesal Penal en su Art. 67 Num 1, refiere que tiene las atribuciones de proteger y vigilar la escena del delito, con el fin de que no se borre los indicios, restos o señales del delito y juntar de ser posible todo aquello que sirva para la investigación. Es importante establecer la norma en el tiempo, ya el NCPP se implementó en el año 2004 y de ahí para adelante no se ha actualizado para la aparición de los nuevos ilícitos delictivos como los delitos informáticos que las evidencias digitales requieren de un tratamiento especial muy distinto al que precisa la norma procesal. Seguidamente el siguiente actor es el fiscal quien es el titular de la acción penal y dirige la investigación en su etapa inicial o preparatoria, mucho dependerá como se haya ubicado, identificado, tratado y transportado la evidencia digital para que pueda ser

utilizada como medio de prueba y el fiscal la haga suyo para la acusación. El siguiente actor será el Juez quien determinará la admisión de la evidencia digital.

La valoración de la prueba dependerá de la aceptabilidad de los resultados probatorios, que las pruebas no hayan vulnerado los principios que regulan su admisibilidad, así mismo la cadena de custodia se haya efectuado respetando los procedimientos que garanticen la autenticidad de la evidencia, aquí también debe precisarse que el traslado de la evidencia digital es un proceso muy particular que el tratamiento que se le da a cualquier otra evidencia común, debe ser realizada por personal capacitado para garantizar la autenticidad e indemnidad de la evidencia digital. El Estado peruano como parte de no ser ajeno a este tipo de modalidad delictiva y en protección a la información en previsión de amenazas internas o externas, dicto la Ley 30096 Ley de delitos informáticos tipificando una serie ilícitos penales que tienen que ver con el uso de las TIC, asimismo ha creado la DIVINDAT unidad especializada de la Policía Nacional del Perú para que se encargue de investigar los ilícitos penales informáticos. Pero lo hecho hasta ahora resulta insuficiente falta regulación de normas de carácter procesal para el hallazgo, recojo, tratamiento y traslado de la evidencia digital, así mismo la Unidad Especializada de la Policía no cuenta con el personal y equipos necesarios para enfrentar eficazmente la lucha contra la ciberdelincuencia.

Normatividad Jurídica Internacional.

Convenio Internacional de Budapest, unica norma internacional que cubre la legislación sobre ciberdelincuencia tanto penal como en su proceso y de cooperación internacional. Es el primer y único instrumento internacional que existe a la fecha**.** La misma que refiere que ante la amenaza de los ciberdelincuentes al emplear las redes tecnológicas para cometer ilícitos y que las evidencias se almacenen y transmitan por las redes; asimismo existiendo la exigencia de cooperar entre los gobiernos y el ámbito privado en el combate contra la ciberdelincuencia, siendo también imprescindible cuidar los genuinos intereses en el empleo y aumento de las TIC; conscientes de

que la eficacia de esta batalla contra delincuentes informáticos, hace necesario establecer un canal internacional de cooperación para intercambiar normas sobre legislación penal, oportuna y operacional; significando que también los hechos contrarios a trasgredir lo confidencial, la probidad y la excedencia de los sistemas de información, redes y datos informáticos, y tal como define el Convenio, y la admisión de poderes idóneos para combatir de manera efectiva la ciberdelincuencia, ayudando a ello su descubrimiento, investigación y sanción, en el ámbito nacional así como internacional". Ministerio de Asuntos Exteriores Madrid España, Oficina de interpretación de lenguas (2001). Convenio sobre ciberdelincuencia. *Concejo de Europa*. Recuperado de https://bit.ly/2OU44PR.

En el modelo Argentino, el estudio forense de este país en relación con la evidencia determina que ella es todo vestigio, signo, señal o rastro, que se abandona en la actuación de la escena del delito como muestra de prueba de haberse realizado un hecho. Mediante la Resolución PGN Nro 756/16 de la Procuración General de la Nación Argentina, brinda directrices sobre la forma como se aborda, la conservación y el tratamiento de la evidencia digital respecto a cómo reprimir penalmente un proceso investigatorio fuera del país de este delito. Toma en consideración las recomendaciones dadas por la ONU en lo que se refiere a la transnacionalidad, su vínculo con el crimen organizado y la urgente atención de normas eficaces y estandarizadas para una buena cooperación internacional así como la atención del estado para la obtención de buenos resultados. Debe considerarse los siguientes principios, el primero es la relevancia jurídica que busca analizar e indagar con el objeto de acreditar una hipótesis sobre un hecho. La segunda es la confiabilidad que indaga y busca homologar la repetibilidad y ser auditada, finalmente la suficiencia que en el proceso de recolección y análisis de las evidencias exista componentes hábiles para proteger los hallazgos del hecho investigado.

En el modelo Colombiano la Evidencia digital respecto a la normatividad en la que se desarrolla se ubica en el Derecho Colombiano, tal

como lo tipifica según “el Código de Procedimiento Civil, Sección tercera, Título XIII. Adicionalmente, la Ley 527 de 1999, denominada Ley de Comercio Electrónico, reconoció como medios de prueba a los mensajes de datos, otorgándoles la fuerza probatoria establecida en el mencionado estatuto. La Evidencia Digital comprende información en formato digital que establezca un vínculo. “Con el fin de garantizar su validez probatoria, los documentos deben cumplir con algunos requerimientos, estos son: Autenticidad: Satisfacer a una corte en que los contenidos de la evidencia no han sido modificados; la información proviene de la fuente identificada; la información externa es precisa. Precisión: debe ser relacionarla positivamente con el incidente. No debe haber ninguna duda sobre los procedimientos seguidos y las herramientas utilizadas para su recolección, manejo, análisis y posterior presentación en una corte. Así mismo, los procedimientos deben ser seguidos por alguien que pueda explicar, en términos entendibles, cómo fueron realizados y con qué tipo de herramientas se llevaron a cabo. Suficiencia: Debe de propia forma presentar el espacio integro, y no una idea de un grupo individual de situaciones. Cuenta con institutos como el SANS16 y el NIST17, que buscan la difusión y cooperación en las técnicas y protocolos forenses aplicables en caso de delitos informáticos y los demás que involucren la aplicación de herramientas informáticas, con la finalidad de ayudar a los investigadores certificados, poniendo a disposición de forma gratuita documentos de investigación científica en lo referente a la informática forense y el derecho informático, temáticas que nutren el contexto total del campo de la investigación forense digital para la obtención de evidencia digital, con la aplicación de protocolo y herramientas forenses, no solo las consideradas por certificadas por un instituto reconocido como es SANS, sino también que permiten la obtención de la evidencia digital con características de autenticidad, integridad, originalidad, confiabilidad y no repudio. En igual perspectiva frente a la utilidad y respaldo dado a la Evidencia Digital, se cuenta con el NIST: Para el campo de la informática o computación forense promueve programas académicos de contenido novedoso y contemporáneo, satisfaciendo los retos diarios que la ciberdelincuencia. El gobierno de Colombia promulgo la Ley 1928 del 24 de julio de 2018, mediante el cual se adhiere formalmente al Convenio, realizado en Budapest. Esta importante

norma aporta un gran instrumento jurídico que contribuye a avanzar, con acciones decididas, contra la cibercriminalidad internacional y busca construir una política mundial común en la lucha contra la ciberdelincuencia.

Modelo Español, las nuevas tecnologías e Internet constituyen unos de los principales impulsores de los cambios de muchas de las actividades desempeñadas por los ciudadanos, empresas, organizaciones y gobiernos en el actual mundo digital, convirtiéndoles en actores digitales cada vez más maduros e interactivos. “Actualmente existen unos 2.400 millones de usuarios conectados a la red, de los que 540 millones se conectan desde Europa, y entre ellos, unos 29 millones se conectan desde España”. Gómez (2014 p. 81-82). “El coste que provoca la ciberdelincuencia en la economía es enorme. Según un informe cada año las víctimas pierden unos 388.000 millones USD en todo el mundo a causa de la ciberdelincuencia, lo que convierte a este tipo delictivo, en un negocio más rentable que el comercio global conjunto de marihuana, cocaína y heroína.” Comisión Europea (2012 p. 2).

Los RFC (Request For Comments) son documentos que detalla cómo debe ser aceptado y pueda ser implementado sin ambigüedades una evidencia. Establece un procedimiento para recoger y guardar la evidencia. En ella podemos apreciar y describir la volatilidad de los datos, nos permite definir que recoger, así como que guardar y la documentación de los datos.

La autenticidad de la prueba requiere la información penal útil disponible en dispositivos electrónicos o alojada en servidores, podrá incorporarse al proceso mediante los medios probatorios oportunos. Pero para garantizar que los datos obtenidos en los registros hechos a dichos dispositivos o servidores permanecen inalterados o que son exactamente los contenidos en los mismos, se precisa de una serie de garantías. La primera garantía, se refiere al proceso de clonado de la información. Ya que al accederse u obtener los datos del dispositivo, se procede al volcado o clonado, que es efectuar una reproducción idéntica de todo su contenido guardado. Básicamente lo que se realiza es una copia física del contenido del mismo. Pero es mediante el hash, una función basada en algoritmos que

otorga al contenido de un archivo un valor numérico. “Mediante este procedimiento deberá originarse un original de los datos, una copia resultado del clonado que será sobre la cual se practicará la pericial informática, y una segunda copia para el propietario de los datos, para el caso de que fuese necesario que el mismo continuase con la actividad que viniese ejerciendo”. Delgado (2016 p.4).

El concepto unánimemente aceptado, respecto a la evidencia digital lo precisa como una información que se ubica y obtiene en un dispositivo informático que puede evidenciar un hecho o acción con precisión, debiéndose para ello ser extraído conforme establece los procedimientos para su veracidad, integridad y traslado.

Las técnicas de capturas de pantalla tienen como objetivo brindar un sustento documental, mediante el congelamiento de pantallazos de diferentes situaciones como interacciones en diálogos o el intercambio de imágenes entre otros con la intensión de darle valor como prueba en un juicio. Es preciso indicar que en una causa penal se busca el debido proceso y por sobre todo la presunción de la inocencia, por lo que esta acción desbarata dichos mensajes que podrían ser ciertos ya que existe una alta posibilidad de ser adulterado por ser muy volátiles. Ante ello un Tribunal Supremo español determino que la veracidad de estos mensajes no pueden ser presentadas al proceso tan solo como impresiones, debe ser necesario una prueba pericial a fin de determinar su origen, la identificación de los intervinientes y por sobre todo la integridad de lo que contiene, solo de esa manera obtendrá valor probatorio.

Análisis interpretativo.

Para la lucha contra el cibercrimen a nivel internacional se tiene como único instrumento al Convenio de Budapest, el cual también promueve una cooperación entre los gobiernos y entes privados así como intercambiar normas sobre legislación penal y operacional entre sus miembros, y mantener un canal de comunicación permanente de asesoramiento y apoyo técnico en

la lucha contra la ciberdelincuencia en el mundo. El Perú a la fecha no se adherido a dicho convenio.

En Argentina existe normas que brindan directrices sobre el tratamiento y conservación de la evidencia digital, respecto a cómo reprimir penalmente un proceso investigatorio fuera del país de este delito. (Resolución PGN Nro 756/16) de la Procuración General de la Nación Argentina, toma la recomendación de la ONU sobre delitos transnacionales. Toma como principios la relevancia jurídica, la confiabilidad y la suficiencia que en el proceso de recolección y análisis de las evidencias exista componentes hábiles para proteger los hallazgos del hecho investigado.

En Colombia también se ha dado normas en el derecho en el cual dan la fuerza probatoria a la evidencia digital (CPC y Ley 527 Ley de Comercio Electrónico), con la finalidad de garantizar su validez probatoria, para ello los documentos deben cumplir con los requerimientos de Autenticidad, Precisión y Suficiencia. Así mismo Colombia cuenta con institutos como el SANS16 y el NIST17, que buscan la difusión y cooperación en las técnicas y protocolos forenses aplicables en caso de delitos informáticos y los demás que involucren la aplicación de herramientas informáticas, con la finalidad de ayudar a los investigadores certificados, poniendo a disposición de forma gratuita documentos de investigación científica en lo referente a la informática forense y el derecho informático, temáticas que nutren el contexto total del campo de la investigación forense digital para la obtención de evidencia digital, con la aplicación de protocolo y herramientas forenses así también permiten la obtención de la evidencia digital con características de autenticidad, integridad, originalidad, confiabilidad y no repudio.

En España se ha efectuado un estudio de las nuevas tecnologías e Internet como uno de los principales impulsores de los cambios de muchas de las actividades desempeñadas por los ciudadanos, empresas, organizaciones y gobiernos en el actual mundo digital, del cual se infiere que actualmente

existen unos 2.400 millones de usuarios conectados a la red, de los que 540 millones se conectan desde Europa, y entre ellos, unos 29 millones se conectan desde España, El coste que provoca la ciberdelincuencia en la economía es enorme. Según un informe cada año las víctimas pierden unos 388.000 millones USD en todo el mundo a causa de la ciberdelincuencia, lo que convierte a este tipo delictivo, en un negocio más rentable que el comercio global conjunto de marihuana, cocaína y heroína. Estudio efectuado por una comisión Europea (2012). Ante ello se ha implementado entre otras una herramienta denominada RFC (Request For Comments) son documentos que detalla cómo debe ser aceptado y pueda ser implementado sin ambigüedades una evidencia. Establece un procedimiento para recoger y guardar la evidencia. En ella podemos apreciar y describir la volatilidad de los datos, nos permite definir que recoger, así como que guardar y la documentación de los datos. Para ello debe precisar las siguientes garantías: el proceso de clonado de la información debe efectuarse una reproducción idéntica de todo su contenido guardado, básicamente lo que se realiza es una copia física del contenido del mismo; Las técnicas de capturas de pantalla tienen como objetivo brindar un sustento documental, mediante el congelamiento de pantallazos de diferentes situaciones como interacciones en diálogos o el intercambio de imágenes entre otros con la intensión de darle valor como prueba en un juicio. Para ello el Tribunal Supremo español determino que la veracidad de estos mensajes no pueden ser presentadas al proceso tan solo como impresiones, debe ser necesario una prueba pericial a fin de determinar su origen, la identificación de los intervinientes y por sobre todo la integridad de lo que contiene, solo de esa manera obtendrá valor probatorio.

Procedimientos Tecnológicos de la Evidencia Digital.

Norma UNE 71505 – 2013 define conceptos sobre la seguridad y controles de las evidencias informáticas. Indica las propiedades básicas de confiabilidad. Procesos de originalidad, reservas y cumplimiento. El periodo en que desarrolla la generación, guardado, comunicación y traslado de las evidencias digitales. Norma UNE 71505-2 2013 establece registros y desarrollo en la

gerencia de seguridad de las evidencias, tales como la confiabilidad, la autenticación, y la integridad, asegurando el poder ser ubicada, rescatada y presentada y la completitud que nos muestra la publicación del contenido de la evidencia. La UNE 71505-3 2013 tiene como objetivo garantizar la legitimidad y plenitud de la evidencia digital conservando su legalidad probatoria ante el juez, brindando al perito informático el poder analizar y verificar, la validez y se encuentre intacta la evidencia. La firma electrónica y sello del tiempo son procedimientos en el que se aplican por ejemplo. UNE 71506 2013 esta procedimiento desarrolla un método cuyo objeto es la preservación, adquirir, documentarla, analizarla y presentar las evidencias digitales.

La ISO/IEC 27037 2012 brinda patrones en las acciones del empleo de la evidencia digital, siendo entre ellos la de identificar, seleccionar, adquirir y preservar la evidencia. El ISO/IEC 27042 2015 tiene las características de una norma orientadora respecto al análisis así como interpretar la evidencia digital abordando conceptos de continuación, valor, reproducción y repetitividad. En la evidencia digital el conocer el tiempo resulta gravitante cuando se requiere garantía y credibilidad respecto a la afirmación de la fecha y la hora, sobre todo cuando se necesite para ser presentada como aporte de prueba, así como garantizar el origen y la plenitud de los datos. Es por eso que se aplicó el método del sellado del tiempo, que en España se emplea en ciberseguridad jurídica.

El sellado de tiempo es un método que sirve para mostrar que determinados datos existen y que no han sido modificados desde su origen. La base de este método implica la participación de la autoridad de certificación, de registro y otras entidades, así como una serie de políticas y actividades. El procedimiento determina la intervención de una entidad acreditada como Autoridad de Sellado de Tiempo, que genera y garantiza un resumen, la fecha y la hora de un documento, y que almacena los sellos emitidos para posteriores verificaciones.

Existen varias técnicas y herramientas forenses que se utilizan para el análisis de la evidencia, estas deben cumplir las formalidades que exigen las normas estándares y procedimientos de buenas prácticas diseñados por entes del gobierno y autores reconocidos. Entre ellos tenemos: Computer Forensic, disciplina forense que, busca encontrar e interpretar la información en medios informáticos para constituir los hechos y enunciar las hipótesis que la relacionen con el caso. Móvil Forensic, Esta herramienta extrae, analiza e interpreta información guardada en dispositivos móviles entre ellos Smarphones, Tablet y otros. Network Forensic, es una herramienta de gran ayuda para analizar las operaciones en las redes informáticas en un ordenador, sigue los protocolos y la formación criminalística permite conocer los rastros, movimientos y acciones que un ciberdelincuente ha ejecutado para acabar su acción. Database Forensic, efectúa un estudio forense detallado de bases de datos y sus metadatos. Las bases de datos son almacenes donde se aloja toda la información del sistema y esta herramienta nos brinda detalles como relaciones de información y volumen de datos. Live Forensics, se encarga de la recopilación y el análisis de la evidencia, mientras el sistema bajo investigación se encuentra operando en tiempo real. La implementación de esta rama se debe a que muchos casos al apagarse el sistema del ordenador en supervisión y control se pierde información importante que no puede ser recuperada con el análisis tradicional en el laboratorio.

Existen 4 criterios que se deben considerarse en la admisibilidad de la evidencia digital como son: a) Autenticidad: considerando situaciones como que la misma se haya generado y registrado en un lugar determinado y/o determinable que guarde vínculo con el suceso que se investiga, asimismo que pueda probarse que no se ha alterado los medios originales, esto último puede acreditarse mediante software especializado, asimismo se puede llevar adelante un “lacrado digital” que permita la contratación de copias de trabajo utilizadas en el proceso penal. b) Confiabilidad.- atendiendo a la fuente de origen, que la misma en la creación de esta evidencia digital existan medios que permitan acreditar un funcionamiento adecuado, sin alteración en el sistema de origen. Los sistemas informáticos estos reportan por medio del

denominado Log files, las acciones y comandos ejecutados en un sistema en tiempo real, y es almacenado de manera temporal. c) Suficiencia.- será suficiente la prueba si es completa, necesitamos mecanismos que nos permita determinar la integridad, sincronización de reportes y centralización de información, como reportes que emitan sistemas operativos o sistemas informáticos. d) Legalidad.- basados en la normativa especial y vigente respecto al tratamiento de evidencia digital de manera concordada con normas procesales y respeto a los derechos constitucionales desde su recopilación.

Análisis interpretativo.

En lo que respecta a los procedimientos tecnológicos de la evidencia digital existe una variada normatividad en Europa que permite brindar el valor probatorio de la evidencia digital, tenemos las siguientes: La Norma UNE 71505 – 2013 muy puntualmente esta norma define conceptos sobre la seguridad y controles de las evidencias informáticas. Indica las propiedades básicas de confiabilidad. Procesos de originalidad, reservas y cumplimiento. El periodo en que desarrolla la generación, guardado, comunicación y traslado de las evidencias digitales. Norma UNE 71505-2 2013 establece registros y desarrollo en la gerencia de seguridad de las evidencias, tales como la confiabilidad, la autenticación, y la integridad, asegurando el poder ser ubicada, rescatada y presentada y la completitud que nos muestra la publicación del contenido de la evidencia. La UNE 71505-3 2013 tiene como objetivo garantizar la legitimidad y plenitud de la evidencia digital conservando su legalidad probatoria ante el juez, brindando al perito informático el poder analizar y verificar, la validez y se encuentre intacta la evidencia. La firma electrónica y sello del tiempo son procedimientos en el que se aplican por ejemplo. UNE 71506 2013 esta procedimiento desarrolla un método cuyo objeto es la preservación, adquirir, documentarla, analizarla y presentar las evidencias digitales. También se tiene normas ISO establecidas por el Organismo Internacional de Estandarización y fueron creadas con la finalidad de ofrecer orientación, coordinación, simplificación y unificación de criterios a las empresas y organizaciones con el objeto de reducir costes y

aumentar la efectividad**,** así como estandarizar las normas de productos y servicios para las organizaciones internacionales. La ISO/IEC 27037 2012 brinda patrones en las acciones del empleo de la evidencia digital, siendo entre ellos la de identificar, seleccionar, adquirir y preservar la evidencia. El ISO/IEC 27042 2015 tiene las características de una norma orientadora respecto al análisis así como interpretar la evidencia digital abordando conceptos de continuación, valor, reproducción y repetitividad.

Otra herramienta es la llamada sellado de tiempo es un método que sirve para mostrar que determinados datos existen y que no han sido modificados desde su origen. La base de este método implica la participación de la autoridad de certificación, de registro y otras entidades, así como una serie de políticas y actividades. El procedimiento determina la intervención de una entidad acreditada como Autoridad de Sellado de Tiempo, que genera y garantiza un resumen, la fecha y la hora de un documento, y que almacena los sellos emitidos para posteriores verificaciones.

También se tiene herramientas como Computer Forensic, disciplina forense que, busca encontrar e interpretar la información en medios informáticos para constituir los hechos y enunciar las hipótesis que la relacionen con el caso. Móvil Forensic, extrae, analiza e interpreta información guardada en dispositivos móviles entre ellos Smarphones, Tablet y otros. Network Forensic, analiza las operaciones en las redes informáticas en un ordenador, sigue los protocolos y la formación criminalística permite conocer los rastros, movimientos y acciones que un ciberdelincuente ha ejecutado para acabar su acción. Database Forensic, efectúa un estudio forense detallado de bases de datos y sus metadatos. Las bases de datos son almacenes donde se aloja toda la información del sistema y esta herramienta nos brinda detalles como relaciones de información y volumen de datos. Los Metadatos son “datos acerca de los datos” y sirven para suministrar información sobre los datos producidos, consisten en información que caracteriza datos, describen el contenido, calidad, condiciones, historia, disponibilidad y otras características de los datos. Live Forensics, se encarga de la recopilación y el análisis de la evidencia, mientras el sistema bajo

investigación se encuentra operando en tiempo real. La implementación de esta rama se debe a que muchos casos al apagarse el sistema del ordenador en supervisión y control se pierde información importante que no puede ser recuperada con el análisis tradicional en el laboratorio.

Conclusiones del resultado de Interpretación y análisis del Marco Teórico.

La ciberdelincuencia utiliza el internet, a través de los medios o equipos tecnológicos donde se consuma el ciberdelito, el lugar donde se ejecutan estas acciones ilícitas es el Ciberespacio lugar virtual sin espacio físico. Atenta contra la integridad y veracidad de los sistemas informáticos y roba información personal de personas naturales o jurídicas. La huella de estos ilícitos es la evidencia digital, la Policía Nacional tiene la atribución de proteger y vigilar la escena del delito, las evidencias digitales requieren de un tratamiento especial muy distinto al que precisa la norma procesal. El fiscal dirige la investigación, mucho dependerá como haya ubicado, identificado, tratado y transportado la evidencia digital para que pueda ser utilizada como medio de prueba. El Juez determinará la admisión de la evidencia digital.

El Estado peruano dicto la Ley 30096 Ley de delitos informáticos tipificando una serie ilícitos penales que tienen que ver con el uso de las TIC, y creo la DIVINDAT unidad especializada de la Policía Nacional del Perú para que investigue los ilícitos penales informáticos.

El Convenio de Budapest, promueve cooperación así como intercambia legislación penal y operacional, mantiene comunicación permanente, asesora y da apoyo técnico en la lucha contra la ciberdelincuencia en el mundo. El Perú a la fecha no se adherido a dicho convenio.

Argentina, Colombia y España, cuentan con Leyes, normas, Institutos y herramientas que dan fuerza probatoria a la evidencia digital y garantizan la validez, cumpliendo con requisitos de Autenticidad, Precisión y Suficiencia.
Sobre los procedimientos tecnológicos de la evidencia digital se tiene varias

normas en Europa que brindan el valor probatorio de la evidencia digital, tales como las Normas UNE, las ISO y el sellado de tiempo.

Existen herramientas como Computer Forensic, Móvil Forensic, Network Forensic, Database Forensic y Live Forensics, son herramientas que ayudan al tratamiento de la evidencia digital.

Responsabilidades del Estado.

Debemos tener en cuenta que quienes participen en los diferentes actos, ya sean estos, estrictamente de aseguramiento o análisis de la evidencia o de conducción de la investigación penal, lo harán bajo las prescripciones del Nuevo Código Procesal Penal Decreto Legislativo n° 957. Resaltamos que es de vital importancia que quienes intervengan en la escena del delito sean personas capacitadas sobre el manejo de la evidencia, ya que mediante un correcto desempeño de sus funciones se garantiza desde el inicio la integridad de los distintos dispositivos que puedan ser incautados.

El Fiscal; Dirige la investigación desde su inicio planifica la estrategia acorde al caso, diseñando las acciones que lo conduzcan a sus objetivos, utilizando un método que le permita tener un orden y resultados con eficiencia y eficacia (art. 65.4 y 322 NCPP). Y Protección de los derechos y garantías en el proceso penal: debe respetar y garantizar el respeto a los derechos y garantías procesales de la víctima y del imputado (art. 65.4). y Poder coercitivo: puede disponer la conducción compulsiva de un omiso a una citación previo apercibimiento (art. 66). y Deber de la carga de prueba: el Fiscal al averiguar el hecho, recaba elementos de convicción de cargo y de descargo.

Adicionalmente el Artículo VIII del Título Preliminar tipifica sobre la legitimidad que debe cumplir la prueba. Es decir, en toda obtención de la prueba se debe haber tomado en cuenta el respecto de los principios y garantías constitucionales; de ser así cumplirá con el requisito de la legitimidad, asimismo su obtención e incorporación al proceso debe cumplir

con el procedimiento establecido en la normatividad. De caso contrario carecen de efecto legal y es materia de exclusión probatoria considerado como prueba ilícita por afectar y vulnerar derechos constitucionales. De la misma forma la inobservancia de cualquier regla de garantía constitucional favorece al imputado o procesado y que no podrá hacerse valer en su perjuicio.

La legislación peruana señaló tres tipos de prueba en el Código Procesal Penal: el primero es la prueba personal, segundo la prueba documental y por último la prueba técnica, de los cuales la prueba digital se encuentra regulado de manera implícita en la prueba documental tipificado en el Artículo 185º, respecto a las clases de documentos, lo que señala expresamente “son documentos los manuscritos, impresos, fotocopias, fax; luego hace mención a los dispositivos magnéticos como son los disquetes, los dispositivos electrónicos, ópticos como CD, DVD, USB, Pendrive, etc. los cuales pueden almacenar películas, fotografías, y otros medios con las cuales se pueda registrar o almacenar pruebas radiografías, representaciones gráficas, dibujos, grabaciones magnetofónicas, asimismo hace referente a otros medios que contienen registro de sucesos, imágenes, voces; y, otros similares”. En el caso de las evidencias digitales o pruebas digitales precisamente está considerado como prueba documental, y su tratamiento es bajo la observancia de este Artículo y en cuanto a las pruebas obtenidos por correos, paginas, Twitter, WhatsApp, Facebook, Instagram, Cloud Computing, y otros también están considerados dentro de las pruebas documentales. La prueba digital o prueba electrónica está tipificado expresamente en nuestro Código Procesal Penal, y su tratamiento está implícita dentro del Artículo 185º específicamente como pruebas documentales y tiene el mismo tratamiento que las pruebas tradicionales.

La actuación de los medios probatorios en el Proceso Penal peruano está garantizado por la carta magna, los tratados internacionales, a su vez ratificados por el Código Penal Peruano; donde se admiten a solicitud del Ministerio Publico o de los demás sujetos procesales, el juez de la investigación preparatoria decidirá la admisión o exclusión, tomando en

cuenta la afectación a los derechos fundamentales (Código Procesal Penal 2004, Art. 155º).

La Policía; Realiza la investigación operativa, al tomar conocimiento de los hechos delictivos, puede practicar actos urgentes e imprescindibles para asegurar el éxito de la investigación, dando cuenta inmediata al Fiscal (art. 67.1). y Apoyar al Fiscal en la investigación (art. 67.2). En la escena de la investigación, la Policía bajo la conducción del Fiscal podrá realizar: y Acciones para proteger y vigilar el lugar. y Recoger y conservar objetos e instrumentos relacionados con el hecho. y Levantar planos, tomar fotografías y realizar grabaciones. y Asegurar documentos que puedan servir a la investigación. y Efectuar bajo inventario secuestros e incautaciones. y Otras que le faculte la ley. El aseguramiento de la escena del delito será llevado a cabo por funcionarios de la Policía Nacional que cuenten con un conocimiento técnico avanzado en cuanto al manejo de la evidencia digital, debiendo dar inmediata noticia de ello al Fiscal. En cuanto a las atribuciones que le caben a funcionarios de la Policía Nacional, el artículo 68 establece, que bajo la conducción del Fiscal, podrán llevar a cabo numerosas tareas, siendo las más relevantes para este trabajo las que a continuación se detallan: a) Recoger y conservar los objetos e instrumentos relacionados con el delito, así como todo elemento material que pueda servir a la investigación; b) Levantar planos, tomar fotografías, realizar grabaciones en video y demás operaciones técnicas o científicas; c) Efectuar, bajo inventario, los secuestros e incautaciones necesarias en los casos de delitos flagrantes o de peligro inminente de su perpetración. El propio artículo 68 obliga a los funcionarios de la Policía Nacional que todo lo actuado quedará sentado en actas detalladas que se entregarán al Fiscal. Luego de ello, la investigación quedará en cabeza del Ministerio Público.

La División de Investigación de Delitos de Alta Tecnología es el órgano de ejecución de la Dirección de Investigación Criminal que tiene como misión, investigar, denunciar y combatir el crimen transnacional(Globalizado) y otros hechos trascendentes a nivel nacional en el campo de los Delitos contra la Libertad, Contra el Patrimonio, Seguridad Pública, Tranquilidad

Pública, Contra la Defensa y Seguridad Nacional, Contra la Propiedad Industrial y Otros, cometidos mediante el uso de la tecnología de la información y la comunicación, el aprehenso de los indicios, evidencias y pruebas, Identificando, ubicando y deteniendo a los autores con la finalidad de ponerlos a disposición de la autoridad competente.

El Juez de la Investigación; Los hechos objeto de prueba pueden ser acreditados por cualquier medio de prueba permitido por ley. (Libertad probatoria) En el proceso penal no se tendrán en cuenta los límites probatorios establecidos en las leyes. El juez no podrá utilizar directa o indirectamente las fuentes o medios de prueba obtenidos con vulneración del contenido esencial de derechos fundamentales.

El Juez Podrá limitar medios de prueba manifiestamente sobre abundantes o de imposible consecución. En la etapa intermedia el juez determina la admisión de la prueba. Limites la prueba ilícita.

Se advierte dos aspectos muy importantes relativos a quienes intervienen en el proceso: de un lado, las partes que tienen la facultad y el deber de poner en consideración del juez todo aquel material que sustenten sus hechos alegados en los actos postulatorios del proceso; y de otro lado, al juez, quien se encuentra en la obligación de sustentar su decisión en esos medios de prueba que han propuesto las partes en el proceso y han sido actuados por este, además de aquellos medios de prueba que de oficio haya incorporado al *iter* procesal.

Los medios probatorios tienen por finalidad acreditar los hechos expuestos por las partes, producir certeza en el Juez respecto de los puntos controvertidos y fundamentar sus decisiones. Debe tenerse en cuenta que la valoración de los medios probatorios aportados por las partes en el proceso y admitidos en la audiencia correspondiente deben destinarse a despejar la incertidumbre jurídica, en tal sentido la fijación de puntos controvertidos tiene entre sus objetivos determinar qué puntos van a ser materia de prueba.

El objeto de la prueba es el hecho que debe verificarse y sobre el cual el juez emite un pronunciamiento. Es demostrar la verdad de los hechos propuestos por las partes al momento de interponer la demanda y al momento de contestar la misma. Es todo aquello susceptible de demostración por las partes ante el juez, sobre la verdad o existencia de un hecho, materia de las pretensiones propuestas, pudiendo ser estos pasados, presentes o futuros. Sin embargo, el juez de acuerdo a las particularidades de cada caso y tomando en cuenta la normativa o sistema correspondiente podrá disponer la incorporación de determinada prueba al proceso, a esta figura excepcional, se le denomina prueba de oficio. El procedimiento de la prueba no es sino una manifestación particular del contradictorio y esta se realiza en la audiencia de pruebas que es fijada por el juez, la misma que es oral pero queda materializada en el acta correspondiente.

Análisis interpretativo.

El fiscal, dirige la investigación desde su inicio, planifica la estrategia, diseña las acciones que lo conduzcan a sus objetivos, debe respetar y garantizar el respeto a los derechos y garantías procesales de la víctima y del imputado y debe averiguar el hecho, recabar elementos de convicción de cargo y de descargo. En la obtención de la prueba debe tomarse en cuenta el respecto de los principios y garantías constitucionales, caso contrario carece de efecto legal y es materia de exclusión probatoria considerado como prueba ilícita por afectar y vulnerar derechos constitucionales.

La legislación peruana señala tres tipos de prueba en el Código Procesal Penal: el primero es la prueba personal, segundo la prueba documental y por último la prueba técnica, de los cuales la prueba digital se encuentra regulado de manera implícita en la prueba documental tipificado en el Artículo 185º, como; documentos manuscritos, impresos, fotocopias, fax; los dispositivos magnéticos como dispositivos electrónicos, ópticos como CD, DVD, USB, Pendrive, etc. los cuales pueden almacenar información. En el caso de las evidencias digitales o pruebas digitales precisamente está considerado como prueba documental, y su tratamiento es bajo la

observancia de este Artículo y en cuanto a las pruebas obtenidos por correos, paginas, Twitter, WhatsApp, Facebook, Instagram, Cloud Computing, y otros también están considerados dentro de las pruebas documentales. La prueba digital o prueba electrónica está tipificado expresamente en nuestro Código Procesal Penal, y su tratamiento está implícita dentro del Artículo 185º específicamente como pruebas documentales y tiene el mismo tratamiento que las pruebas tradicionales. Particularmente considero que tratar a una evidencia digital al igual que una evidencia documental es un gran error, ya que requiere de un tratamiento especial desde el momento de su hallazgo, levantamiento, análisis y traslado, ya que una mala manipulación del mismo lo contamina y no podrá ser utilizado en un proceso judicial.

La Policía, realiza la investigación operativa, puede practicar actos urgentes e imprescindibles para asegurar el éxito de la investigación, dando cuenta inmediata al Fiscal y Apoyar al Fiscal en la investigación. En la escena de la investigación, la Policía bajo la conducción del Fiscal podrá realizar: Acciones para proteger y vigilar el lugar, recoger y conservar objetos e instrumentos relacionados con el hecho, levantar planos, tomar fotografías y realizar grabaciones, asegurar documentos que puedan servir a la investigación y efectuar bajo inventario secuestros e incautaciones. El aseguramiento de la escena del delito lo efectuara personal de la Policía Nacional que cuenten con un conocimiento técnico avanzado en cuanto al manejo de la evidencia digital, debiendo dar inmediata noticia de ello al Fiscal. Finalmente todo lo actuado quedará sentado en actas detalladas que se entregarán al Fiscal. Luego de ello, la investigación quedará en cabeza del Ministerio Público.

La División de Investigación de Delitos de Alta Tecnología es el órgano especializado que tiene como misión, investigar, denunciar y combatir el crimen transnacional y otros hechos trascendentes a nivel nacional, cometidos mediante el uso de la tecnología de la información y la comunicación, el aprehenso de los indicios, evidencias y pruebas, Identificando, ubicando y deteniendo a los autores con la finalidad de ponerlos a disposición de la autoridad competente.

El Juez determina la admisión de la prueba. Limites la prueba ilícita. Asimismo las partes que tienen la facultad y el deber de poner en consideración del juez todo aquel material que sustenten sus hechos alegados en los actos postulatorios del proceso; y también el juez, se encuentra en la obligación de sustentar su decisión en esos medios de prueba que han propuesto las partes en el proceso y han sido actuados por este, también de acuerdo a las particularidades de cada caso y tomando en cuenta la normativa o sistema correspondiente podrá disponer la incorporación de determinada prueba al proceso. Los medios probatorios tienen por finalidad acreditar los hechos expuestos por las partes, producir certeza en el Juez respecto de los puntos controvertidos y fundamentar sus decisiones.

Conclusiones del resultado de Interpretación y análisis de responsabilidades del Estado.

El Fiscal, dirige la investigación desde su inicio, debe averiguar el hecho, recabar elementos de convicción de cargo y de descargo. En la obtención de la prueba debe respetarse los principios y garantías constitucionales, caso contrario carece de efecto legal y es materia de exclusión probatoria.

En la legislación peruana la evidencia digital se encuentra regulado de manera implícita en la prueba documental y tiene el mismo tratamiento que las pruebas tradicionales. Esto es un error tratar a una evidencia digital al igual que una evidencia documental, esta requiere de un tratamiento especial desde el momento de su hallazgo, levantamiento, análisis y traslado.

La mala manipulación de la evidencia digital lo contamina y no puede ser utilizado en un proceso judicial. La Policía, realiza la investigación operativa, en la escena de la investigación, la Policía bajo la conducción del Fiscal realiza acciones para proteger y vigilar el lugar, recoger y conservar objetos e instrumentos relacionados con el hecho, que puedan servir a la investigación.

Realiza el aseguramiento de la escena del hecho y es necesario que cuenten

con un conocimiento técnico avanzado en cuanto al manejo de la evidencia digital, la investigación quedará en cabeza del Ministerio Público.

La División de Investigación de Delitos de Alta Tecnología es el órgano especializado que investigar y combate los ilícitos cometidos mediante el uso de las TIC.

El Juez determina la admisión de la prueba. Tiene la obligación de sustentar su decisión de los medios de prueba propuesta por las partes en el proceso, tomando en cuenta la normativa o sistema correspondiente podrá disponer la incorporación de determinada prueba al proceso. La admisibilidad y valor probatorio de la evidencia digital dependerá del tratamiento efectuado por la Policía y el Fiscal que permita acreditar los hechos expuestos por las partes, producir certeza en el Juez respecto de los puntos controvertidos y fundamentar sus decisiones.

Conclusión de análisis documental.

Es un error tratar a una evidencia digital como una evidencia documental, esta requiere de un tratamiento especial desde el momento de su hallazgo, levantamiento, análisis y traslado. La mala manipulación de la evidencia digital lo contamina y no puede ser utilizado en un proceso judicial.

El Fiscal, dirige la investigación desde su inicio, debe averiguar el hecho, recabar elementos de convicción de cargo y de descargo. En las investigaciones sobre cibercrimen la falta de herramientas judiciales y procesales, el desconocimiento de los jueces y fiscales sobre el tema, el personal policial que contamina la evidencia digital en la escena del hecho, la creciente demanda de comercio electrónico, negocios, operaciones, actividades diversas de las personas en línea que abren las puertas a los ciberdelincuentes y la multiplicidad de jurisdicciones por la naturaleza del internet donde se cometen estos ilícitos, se requiere que el operador judicial cuente con facultades procesales para que pueda validar la actividad de la investigación técnica.

La ciberdelincuencia utiliza el internet, se ejecuta en el Ciberespacio lugar virtual sin espacio físico. La huella de estos ilícitos es la evidencia digital, la Policía Nacional tiene la atribución de proteger y vigilar la escena del delito, las evidencias digitales requieren de un tratamiento especial muy distinto al que precisa la norma procesal. El Juez determinará la admisión de la evidencia digital.

El Estado dicto la Ley 30096 Ley de delitos informáticos tipificando una serie ilícitos penales que tienen que ver con el uso de las TIC, creo la DIVINDAT unidad especializada de la PNP para que investigue los ilícitos penales informáticos. El Convenio de Budapest, promueve cooperación, asesoramiento técnico, intercambio de legislación penal y operacional. El Perú a la fecha no se adherido a dicho convenio.

Argentina, Colombia y España, cuentan con Leyes, normas, Institutos y herramientas que dan fuerza probatoria a la evidencia digital y garantizan la validez. En procedimientos tecnológicos la evidencia digital en Europa cuenta con Normas UNE, ISO y el sellado de tiempo.

Existen herramientas como Hash, Computer Forensic, Móvil Forensic, Network Forensic, Database Forensic y Live Forensics, son herramientas que ayudan al tratamiento de la evidencia digital.

Resultados de Observaciones.

Proceso Business Track S.A. (Petro audios).

Corte superior de justicia de Lima Segunda Sala Especializada en lo penal para procesos con reos en carcel. exp. N° 99-09 (527-09). Audiencia Oral y Pública, el juzgamiento incoado contra: Elías Manuel Ponce Feijoo, Carlos Alberto Tomasio de Lambarri, Giselle Mayra Giannotti Grados, Martín Alberto Fernández Virhuez, Jesús Manuel Ojeda Angles, Jesús Juan Tirado Seguín,

Alberto Oswaldo Salas Cortez y Pablo Eriks Martell Espinoza, por el delito Contra la Libertad - Violación del Secreto de las Comunicaciones – Interceptación Telefónica en calidad de integrantes de una organización criminal en agravio de Rómulo Augusto León Alegría, Alberto Quimper Herrera, Alberto Fortunato y otros. Por el delito contra la Libertad - Violación del Secreto de las Comunicaciones – Interceptación Telefónica en calidad de integrantes de una organización criminal en agravio del Estudio Jurídico Fernández Concha SCRL (Estudio Fernández – Concha Sociedad Civil de Responsabilidad Limitada), Empresa Trupal S.A., Alexander Martín Kouri Bumachar, Municipalidad Provincial del Callao. Por el delito contra la Libertad – Violación del Secreto de las Comunicaciones – Violación de Correspondencia en calidad de integrantes de una organización criminal en agravio de Rómulo Augusto León Alegría, Alberto Alfonso Borea Odría, Francisco Ricardo Soberón Garrido y otros y por el delito contra la Tranquilidad Pública – Asociación Ilícita para Delinquir en agravio del Estado.

El día domingo 05 de octubre del 2008 en el Programa Dominical “Cuarto Poder” de América Televisión se difundió audios en las que se registraba supuestamente conversaciones sostenidas entre Alberto Quimper Herrera – Ejecutivo de Perú- Petro, entidad estatal a cargo de promover la inversión extranjera en el sector petrolero y Rómulo León Alegría- Ex Ministro Aprista, discutiendo sobre pagos para favorecer a la empresa noruega Discover Petroleum para ganar contratos.

El Presidente de la República Alan García Pérez anunció la destitución de Alberto Quimper Herrera como miembro del Directorio de PERÚ-PETRO y la suspensión del contrato petrolero adjudicado a la Compañía Discover Petroleum. Asimismo aceptó la renuncia del Ministro de Energía y Minas Juan Valdivia Cano. A los pocos días el Premier Jorge del Castillo Gálvez, anuncio la renuncia del Gabinete Ministerial, que fue aceptado por el Presidente de la República.

La Fiscalía de la Nación mediante Resolución N ° 1419-2008-MP-FN de fecha 20 de octubre del 2008, dispuso que por excepción la Fiscalía

Provincial Especializada en Criminalidad Organizada se avoque al conocimiento de la interceptación telefónica difundidos en los medios de comunicación. El Fiscal Superior Mateo Castañeda Segovia, Coordinador de las Fiscalías Especializadas en Criminalidad Organizada con fecha 31 de octubre 2008, designó a la Tercera Fiscalía Provincial Especializada contra la Criminalidad Organizada, a cargo del doctor Orestes Walter Milla López, para que se encargue de la investigación. La Tercera Fiscalía Provincial Especializada contra la Criminalidad Organizada a cargo del Fiscal Milla López , mediante resolución de fecha 22 de noviembre del 2008- fojas 3077 del anexo J – designo a la Dirección Nacional Antidrogas de la Policía Nacional del Perú – Dirandro para que realicen las indagaciones orientadas a determinar quién o quiénes están dedicados a las actividades de interceptación telefónica y por qué razones se realiza esta práctica ilegal; debiendo con dicho conformar un equipo especial.

Mediante Resolución N ° 01 de fecha 07 de enero del 2009 – fojas 71 a 90 del anexo 99-09-09 - emitida por el señor Juez Penal de Turno, doctor Edwin Elmer Yalico Contreras resolvió: Autorizar: la detención preliminar por el término de diez días de Elías Manuel Ponce Feijoo, Carlos Alberto Tomasio De Lambarri, Giselle Mayra Giannotti Grados, Martín Alberto Fernández Virhuez, Jesús Manuel Ojeda Ángles y Jesús Juan Tirado Seguín y su correspondiente registro personal, incautación de soportes electrónicos, informáticos y/o magnéticos de comunicaciones y telecomunicaciones, documentos públicos o privados, objetos, instrumentos y efectos vinculados al delito materia de la presente investigación que pudieran tener u ocultar al momento de la detención; el Descerraje y Allanamiento de inmuebles y ambientes interiores con fines de detención de los ciudadanos en mención; así como el registro domiciliario y de sus distintos ambientes e Incautación de bienes, documentos públicos y privados, equipos informáticos, soportes electrónicos e informáticos y/o magnéticos, equipos de comunicaciones y telecomunicaciones y otros objetos, instrumentos y/o efectos relacionados con la presente investigación.

Iniciado el Juicio Oral, la Sala Penal ante los cuestionamientos

formulados por algunos de los acusados respecto a la intangibilidad de la cadena de custodia , mediante Resolución de fecha 25 de mayo de 2011.- fojas 109877 del tomo 189, resolvió excluir del debate probatorio aquellas muestras que a criterio del Colegiado no contaban con un margen de seguridad y autenticidad en su recojo o custodia, siendo estos: Bienes de la acusada Giannotti Grados: 02 USB Boston Technologies , precisando que mantienen validez de las actas del deslabrado y las actas de obtención de muestras de imagen, visualización, impresión de archivos y escucha de audios que se consignan en el cuaderno 49, al estar premunidas de las garantías que el debido proceso requiere; tanto más , que los cuestionamientos a dichos USBs están referidos al momento de la entrega de dichas muestras de la custodia policial al Ministerio Público y posteriormente al Poder Judicial, esto es con posterioridad a fecha de incautación , del inicial deslacrado de obtención de muestras que reprodujeron a partir del 08 de enero al 13 de enero del 2009 . Los USB Marca Memorex, debido a las diferencias en la descripción de dichos bienes al momento de su incautación y al momento de su entrega a la autoridad judicial, así como contradicción en cuanto a su contenido. Bienes del acusado Carlos Alberto Tomasio De Lambarri: discos compactos y diskettes que se encontraban contenidos en la Caja 01, debido a que difieren en número.

En la declaración de testigos en el juicio oral a los miembros de la Policía Nacional del Perú que participaron en la intervención se tiene lo siguiente: Remigio Hernani Meloni, Ministro del Interior; Respecto al caso Business Track, señala que se enteró por medio de la prensa, no conocía detalles sobre el mismo, al perecer el General Hidalgo Medina recibió un documento de un Fiscal para que se haga cargo de investigarlo. Precisa que desconoce porque la investigación policial del caso Business Track fue derivada a la Dirandro, es un hecho totalmente raro. Agrega que la Dirandro no era la dependencia policial que debía llevar a cabo estas investigaciones toda vez que la institución policial tiene sus leyes y reglamento, que establecen que hay estamentos, así como la Dirincri no puede investigar drogas, la Dirandro no puede investigar hechos que se investigan en la DIRINCRI, a no ser que haya algún interés particular. “llame usted al General

Hidalgo Medina", lo llamaron, se apersono y le pregunto, directamente "General, que pasó con este caso, qué me puede informar" y me dijo "yo he hecho una investigación ordenada por el Presidente de la República Alan García Pérez estrictamente reservada y que yo no debo darle cuenta a usted señor Ministro, ni a usted señor Director General, solamente debo darle cuenta directamente al Presidente de la República", "¿está usted seguro de lo que dice?" Le pregunté y me respondió "efectivamente estoy seguro", ante esta respuesta yo opté por quedarme callado y ver como se desarrollaban las cosas posteriormente. Señala que la investigación del delito de interceptación telefónica le correspondía a la División de Alta Tecnología de la Dirincri. Refiere que la investigación no le correspondería a la Dirandro y en el caso que se le asigne a esta un caso de investigación criminal es irregular y no dar cuenta a sus Jefes. En el caso del General Hidalgo Medina debió dar cuenta a sus superiores, ha debido manifestar a la Fiscalía que investiga drogas y que no le corresponde investigar interceptación telefónica, ya que le corresponde a la Dirincri, devolver el oficio y comunicarle al señor Director General de la Policía Nacional del Perú.

Mauro Walter Remicio Maguiño, Director General de la PNP; Refiere que este caso por tratarse de un delito común (interceptación telefónica) debería ser investigado por la Dirección de Investigación Criminal por intermedio de la División de Alta Tecnología.

Elmer Miguel Hidalgo Medina, General Director de la Dirandro; Refiere que tomó conocimiento sobre la existencia del caso BTR al momento de recepcionar la Resolución Fiscal emitida por la 13° Fiscalía de Crimen Organizado el 22 ó 23 de octubre del 2008 donde dispone que la Dirección Antidrogas por su capacidades, por el nivel profesional de su personal y otros fundamentos ha sido designada para poder investigar un caso de interceptación de las telecomunicaciones con la reserva que el caso amerita. Niega que el Presidente de la República Alan García Pérez le haya ordenado avocarse a esta investigación. Asimismo desconoce la participación de Jorge Del Castillo Gálvez, Hernán Garrido Lecca, Mateo Castañeda en esta investigación.

Carlos Moran Soto, Coronel Jefe de la División de Investigaciones Especiales de la Dirección Antidrogas, estuvo a cargo de la investigación del caso Business Track; Preciso que mientras se estuvo visualizando un disco duro respecto a la información de los USBs surgió la información del Mayor Soller, el Fiscal y el señor Ponce que estaban presentes donde dijeron “es la voz del Presidente de la República”, dicha información me la comunica el Mayor a cargo de la visualización. Detalla el deponente que procedió a escuchar el audio conjuntamente con el Mayor y otro personal técnico, sin la presencia del procesado, su defensa, ni el Fiscal. Detalla que de dicho audio se tenía dudas si era la voz o no del Presidente porque era muy parecida, “el audio era corto donde hablaba con una dama y le lanzaba un piropo y que se iban a encontrar más tarde”, al parecer se trataba de un audio del ex Presidente de la Confiep Raymundo Morales, pero en ese momento la preocupación era si se trataba de la voz del Presidente de la República o no y se descartó que no era. Precisa que no se puede contaminar la muestra porque se trataba de un espejo. Detalló que luego hablo con Ponce Feijoo.

Walter Enrique Capa Gurbillón; Precisa haber participado en el caso Business Track ostentando el grado de Sub Oficial Superior, siendo su participación en la obtención de imagen y visualización de archivos de una memoria USB que pertenecía al procesado Tomasio De Lambarri que se realizó en enero del año dos mil nueve. Precisa además que del resultado del proceso de obtención de imagen, este da un informe en donde arroja un valor algoritmo que es el código hash e indica que la integridad de la imagen no ha sido adulterada.

Raúl Felipe Del Castillo Vidal, Comandante de la Policía Nacional del Perú; Se continuó con el registro en ese ambiente quien lo hace son Oficiales femeninas, durante toda esa búsqueda en ese cuarto ambiente, aproximadamente a las dieciocho horas, es donde se encuentra los USB posteriormente se continua con la diligencia no produciendo ninguna novedad; precisa que los CDs encontrados fueron lacrados en el cuarto ambiente, en el ambiente donde se encuentra, pero se hace al final del registro de cada ambiente; en el quinto ambiente, en su “walking closet” se

encontró una caja fuerte en cuyo interior se encontró dinero que por indicación de la señora Giannotti Grados se entrega a su abogada, lo que se consigna al final del acta; en este ambiente la señora Giannotti participó activa y normalmente en la diligencia; en el último ambiente, se encuentran las computadoras las que fueron desconectadas y lacradas, nadie manipulo nada, estaban presentes todas las personas, nadie entraba a los ambientes que aún faltaba revisar, una vez que se terminaba de registrar un ambiente, se lacraba, se sellaba, firmaban todos los participantes o algunos de los participantes y se pasaba al siguiente ambiente y eso ya estaba cerrado, lacrado con la firma de los que estábamos realizando esa diligencia. Sobre los USBs Marca “Memorex”, precisa eran de color plomo de plástico, que de las vistas fotográficas que se le pone a la vista y que obran a fojas 190656 del Tomo 189, reconoce como los incautados y entregados los que se ven encima de la tablilla; si en el Acta de entrega a la Fiscalía se describe con tapa de plástico transparente se debe a un error; desconoce lo que ha sucedido después del veintitrés de enero, lo que sé es que los dos USB que visualizamos y los dos USB que no visualizamos, los cuatro no son los que tiene el Poder Judicial, si tenemos en cuenta los Boston Technologies que nosotros entregamos uno de uno y uno de dos y el Poder Judicial tiene “dos” de “dos” y a nuestro cargo está de “uno” y de “dos”, estos USB eran amarillos con un borde de metal, en la marca venía la cantidad de GB que tenía, uno era de 1GB y el otro de 2 GB, precisando que adicionalmente tenían en manuscrito una marca que decía uno y dos; estos USBs se lacran el día que se incautan, se guardan lacrados hasta el día doce, el día doce se deslacran y se visualizan, se iba a continuar al día siguiente pero tal como quedaron se guardaron, el día trece se retiran del ambiente de seguridad y se continúa con la visualización, se termina el día trece y tal como quedaron se guardaron y de ahí no se continuó con ninguna diligencia de visualización y así es como se llevan a la fiscalía el día veintitrés; no se volvieron a lacrar porque la Fiscal dispuso que se continuara con la diligencia lo más que se pueda, pero ese mas que se pueda estaba supeditado a tener el perito el único software que había validado y las demás diligencias que pudieran hacer entonces el día trece se comienza la manifestación de la señora Giannotti que se prolonga hasta el quince. No se sacó código Hash a todas las evidencias debido a los

pocos días que tenían, se sacó a los que se le pudo sacar, no tenía todos los días y el único perito no era para la señora Giannotti y para mi grupo, estaba el grupo del Almirante Ponce y el Comandante Tomasio, todos tenían que trabajar y solamente había un perito que tenía un software.

Ruth Amparo Tenicela Calderón, Oficial de Inteligencia Operativa y labora en la Dirandro de la Policía Nacional del Perú; habiéndose encontrado en el cuarto ambiente o dormitorio de la señora Giannotti Grados los USBs, (3 dentro de un sobre blanco y 1 suelto; cree que dos de ellos son amarillo con soporte de metal, uno de 1GB y el otro de 2GB; y, los otros dos de marca Mémorex, de color plomo, creo que cada uno era de dos GB o algo así); así como CDs, respecto de los cuales la señora Giannotti decía que eran películas, que podían comprobar su dicho viéndolas en su DVD, pero como no funcionaba el Comandante Del Castillo trajo su Laptop para visualizarlos, el cual se prendió y permaneció así por espacio de diez a veinte minutos, pero no se llegó a visualizar nada debido a que a la señora Giannotti Grados le bajó la presión, por lo que indicó la Fiscal que se llevarían todos; precisa que el único que manipuló la laptop fue el Comandante Del Castillo; quien optó por llamar a los médicos de la Policía para que auscultaran a la señora Giannotti Grados, quienes llegaron luego de una hora; que como la señora Giannotti dijo que se podía continuar con la diligencia, prosiguieron con el registro conjuntamente con su abogada. todos los bienes incautados fueron trasladados al sexto piso de la Dirandro, donde funcionaba las oficinas del grupo de investigaciones especiales cuyo acceso es restringido sólo para los que pertenecen a dicha área y mediante huella digital, cuya llave estaba a cargo del Comandante Del Castillo; de tal manera que para acceder a cualquier bien incautado el Comandante Del Castillo abría la puerta y el gavetero lo abría, ya sea la Capitana Portocarrero o ella, siendo por tanto los tres responsables de la seguridad. en cuanto a los USBs que aparece en la vista fotográfica que obran a fojas 109656, dijo que cree que son los “Memorex” plomos, los cuales reconoce como los que encontró en la casa de la señora Giannotti Grados, que de la vista fotográfica que obra a fojas 109655, reconoce dos memorias USBs de color plomo con una inscripción que dice “Memorex”.

Luis Vicente López Ruiz, Comandante de la Policía Nacional del Perú; precisa que cuando se encontraba un dispositivo de almacenamiento de información como una laptop o un dispositivo externo de disco duro o USB o CD, se procedía a describir para que la persona encargada lo anote en el acta respectiva; se procedía a lacrar utilizando unas bolsas (las que se usan para envolver las maletas en el aeropuerto) a las que se les ponía un papel y firmaban los que estaban en ese momento y se procedía a guardar momentáneamente en ese mismo ambiente y cuando se terminaba se procedía a llevar a otro ambiente ubicado en el primer piso donde había personal de seguridad. En cuanto a las diligencias de cómputo forense realizado a los dispositivos incautados, señala en el caso de un USB para obtener la imagen se volvía a obtener el código Hash para verificar que era el mismo dispositivo; normalmente no se trabaja directamente en el dispositivo incautado porque se puede cometer errores, modificar la evidencia, o puede suceder algún desperfecto del equipo y se malogra la evidencia; por lo que se estila obtener una imagen de esa evidencia de tal manera, que si antes había información, también se está copiando en la imagen para que después se pueda recuperar si es que ha sido eliminado algún archivo; para lo cual se utilizó el Software Encase Forensic y un maletín que contenía diferentes dispositivos de bloqueo de escritura. Precisa que cada vez que se obtiene la imagen de un dispositivo el Software Encase arroja treinta y dos caracteres que es el Código Hash. Reconoce el Acta de Obtención de Imagen de USB, Visualización, Impresión de Archivos y Escucha de Audios de fecha 12 de enero de 2009 obrante a fojas 1163 a 1173 del anexo C en su contenido y firma de acuerdo a lo que se consigna en el foja 1164 (refiriéndose al ícono de disco duro que dice Giselle Giannotti USB 2GB – 12-01-2009), se verificó que el código hash de verificación es igual al código hash del original, lo que significa que la imagen que se está abriendo es idéntica a la que se obtuvo originalmente; lo que aparece en el foja 1166, es la estructura de carpetas que tenía ese dispositivo, no se muestra ahí los archivos que contiene cada carpeta, solo se muestra las carpetas que existía o existen en ese dispositivo; en cuanto a la denominación “música” señala que es el nombre de la carpeta; el archivo número seis, es un archivo empaquetado, en ese caso se abre el archivo que contenía varios archivos que tenía varios correos, entonces se

habría un correo y dependiendo de lo que indicaba la Fiscal, se seguía ahondando si no se tomaba una vista del correo y se capturaba en la pantalla; el archivo número 08, contiene la carpeta “Música con fechas”, que contiene otra carpeta llamada “Rey 22” y dentro de esa carpeta había un archivo “punto doc” que es una extensión de Word con ese nombre “36 Rómulo y Paola” (Agenda); de acuerdo a los datos obtenidos el archivo “Música con fecha” fue creado el 11 de junio del 2008 y fue accedido por última vez el 27 de julio del 2008, y como fecha de creación del archivo el 06 de abril del 2008; dicho archivo contenía un archivo Word se imprimió y se colocó el título que tenía el documento, por lo que supone que la hoja que se imprimió está junta al acta; el archivo 07 es la misma ruta pero en ese caso es un archivo WAV (archivo de sonido), es un audio de la conversación entre “Paola y Rómulo”, el cual se imprimió; lo mismo ocurre con el archivo 09, en el que se constató que si bien dice “música ” se trata de un audio de conversación; en cuanto al archivo 15 (Observaciones de la Cooperación Cimpor a la Operación de Cementos Otorongo) señala que cuando se imprimía algún archivo Word o PDF se solía colocar entre paréntesis el título del documento y se adjuntaba ahí, no es que solamente era visualizado sino que se imprimía y se adjuntaba al acta; en cuanto al archivo 13 es una carpeta llamada “música con fechas” dentro de la cual había otra carpeta llamada “Rey30” y dentro estaba recién el archivo de audio; el archivo 21 era un correo electrónico, que contiene otros correos electrónicos y se capturó esa pantalla. En cuanto a la constancia de que en una de las imágenes se hace referencia a un dispositivo marca Boston Technologies de 2GB, cuando en realidad posee una capacidad de almacenamiento de 1GB, señala que el nombre de las carpetas y de las imágenes lo asigna el operador, es decir se puedo crear una carpeta y asignarle el nombre que se desea, también a la imagen se le puede poner el nombre que se desee, eso no significa que se esté alterando el contenido de la imagen; entonces para evitar cualquier suspicacia en la parte final del documento, se hace constar que si bien es cierto dice 2GB, la capacidad de almacenamiento de ese dispositivo era de 1GB, lo que se puede verificar con la pantalla en donde se capturó, ahí dice que la capacidad de almacenamiento redondeando es de 1GB, entonces todos los que estuvieron constataron eso y firmaron en señal de conformidad. Respecto al punto Sobre

manipulación de fechas, refiere que existen software que permiten manipular fechas, por ejemplo si se cambian la fecha de esa computadora (refiriéndose a la computadora de la Sala de Audiencias) todos los documentos que se creen, que se grabe, es con la fecha alterada; si ese archivo se copia o se empaqueta, lo que cambia es la fecha de creación, la fecha de creación será la fecha en el cual estoy haciendo esa acción, por ejemplo si yo creo un archivo hace diez días y en este momento lo copio a un USB, la fecha de creación no me aparece la de hace diez días pero la fecha de último acceso si se sigue manteniendo y cuando son empaquetados mantienen y restauran igualito a como lo tenía originalmente.

Yonhy Lescano Ancieta Congresista de la República; Señala que formó parte de la Comisión integrada por los Congresistas Walter Menchola, Juan Carlos Eguren, Freddy Otárola, José Vargas, Falla Lamadrid y el deponente, la misma que fuera designada por el Pleno del Congreso de la República para investigar si los USBs incautados en la casa de la señora Giannotti Grados se perdieron o no, se cambiaron o no, ese era el objetivo principal y único de la investigación realizada en el Parlamento; de tal manera que se investigó cómo ingresó la Policía, cómo ingresaron Fiscales, cómo se guardaron las pruebas, cómo se guardaron los USBs, quiénes eran los Fiscales, quiénes eran los miembros de la Policía Nacional. Refiere que el Dictamen en Mayoría no establece los presuntos autores y el Dictamen en Minoría, sí; que de la casa de la señora Giselle Giannotti se incautaron 02 USBs Memorex color plomo entero y, finalmente en la entrega de la Policía a la Fiscalía, se entregaron dos USBs totalmente distintos porque tenían tapa transparente y, de eso sí hay pruebas contundentes porque están las actas de incautación, las tomas fotográficas y eso sí llegó a determinar la Comisión, que se habían cambiado los USBs e, incluso los USBs Boston Technologies, cuando se hace un examen tecnológico a estos otros USBs, se establece que inicialmente uno, tenía supuestamente una capacidad de 01 GB y otro de 02 GB; pero, aparentemente los incautados tenían 02 GB, cada uno; de manera tal que eso suponía que también habían sido cambiados y eso demuestra, dentro de la investigación parlamentaria, que estos USBs están en poder de alguien y que no fueron los originalmente entregados, eso sí determinó la

Comisión; y, luego se entregó estos USBs, se pusieron en una bolsa, sin el debido cuidado y el día 12 o 13 del mismo mes que se hizo la incautación, fueron visionados sin autorización judicial, eso está también acreditado en la investigación, recién el catorce llega una orden judicial que permite la visualización de estos USBs, pero los USBs ya habían sido manipulados. Señala que no han realizado ningún tipo de indagación sobre otros hechos, que eran los USB que se suponía que ahí se había grabado todas las conversaciones donde se habrían hecho negociados por parte de algunos miembros del Ejecutivo con otras personas, ese era el objetivo de la investigación. Refiere que 02 USBs eran visiblemente cambiados; y los otros 02 mediante el examen técnico, también se llega a determinar que fueron cambiados porque el código Hash, los archivos y todo lo demás no coincidían con los USBs que se habían incautado. En esas fotografías, en esos registros que se tomó al momento de la intervención en la casa de la señora Giselle Giannotti aparecen USBs de un color, luego cuando la Policía le hace entrega a la Fiscalía, aparecen dos USBs de otro color; eso es una clara demostración que se cambiaron los USBs, groseramente, yo creo que cómo van a incurrir en una irregularidad de esta naturaleza, miembros de la Policía Nacional con Fiscales que intervinieron conjuntamente la casa de la señora Giselle Giannotti, consecuentemente, ese solo hecho involucra la responsabilidad de los miembros de la Policía Nacional y los Fiscales que estuvieron a cargo de la investigación, es una primera evidencia que nosotros hemos establecido. Más adelante señaló que el objetivo de la investigación era establecer si había actos de corrupción o no y ese objetivo era verificar si en esa investigación que se había llevado a cabo, se practicaron actos de corrupción o no para hacer desaparecer pruebas; y si usted verifica que un USB incautado es distinto al entregado, es obviamente un acto de corrupción, porque no tendría otra finalidad hacer desaparecer un USB, que tapar algún tipo de información.

Solicitado por la defensa de Fernández Virhuez; Acta de apertura de lacrado Obtención de imagen de USB visualización y escucha de audios de fecha 10 de enero del año 2009; acreditándose que no se preservó la cadena de custodia; precisa la defensa que en esta Acta no consta la firma de su

patrocinado, pese habérsele incautado el USB en su registro personal, ni de su abogado, aparte de eso el disco duro marca Western Digital, donde se almacenó las imágenes de USB no se lacró para preservar la inalterabilidad, ya que quedó en poder del Mayor De la Cruz; no se preservó ese disco duro en donde se almacenaron las imágenes del USB 256 MBT; asimismo, la apertura se hizo violando la resolución N ° 1, del Juez Yalico, que prohibía la visualización del material incautado, que recién se autorizó el 13 de enero; resaltando los colores de los celulares que se han incautado, acá dice, un Motorola plateado (singular) y otro Nextel de color gris oscuro con negro.

Solicitado por la defensa de Tomasio De Lambarri, “Acta de Obtención de Imagen del USB, donde la policía designa códigos a los bienes incautados; donde la defensa de Tomasio de Lambarri se retiró de esa diligencia, no participando en ella, sino para solicitar que mi patrocinado sea retirado de la misma; al USB incautado a mi patrocinado se le consignó dos Códigos Hash el MD-5 y el SHA-1, que al haberse impuesto conjuntamente son irrompibles, cosa que no sucedió con las demás muestras de los demás procesados, a los cuales se les impuso sólo un código hash, el MD-5 el cual hace muchos años es vulnerable y fácil de penetrar. (Fojas 547 – 548 anexo B). “Acta de Visualización del USB”, donde se hace la verificación del Código Hash; a dicha muestra se le consignó “dos códigos Hash” se precisa que dicho USB estaba totalmente vacío, por eso se le consigno “dos códigos Hash”.

Solicitado por la defensa de la acusada Giannotti Grados; “Acta de Obtención de imagen de USB”, su fecha 13 de enero de 2009, este USB, no puede ser ningún medio de prueba de la acusación, debido a que ya desde el nivel policial se comprobó que este dispositivo se encontraba malogrado y no podía ser leído por el Software Encase Forensic; en dicha acta se aprecia que el bien incautado no contenía ningún elemento relevante que pueda ser materia de la acusación. Acta de audiencia de visualización del día 05/03/2010, se acredita la observación que hace la señora Giannotti, sobre un CPU y un disco extraíble que tenía su dispositivo y que no aparece el día que realizamos el deslacrado; se verifico los códigos hashes y el contenido de los

USB; en esta diligencia, después que se comprueba que las muestras MGG-102 y MGG-103, no contaban con el sistema operativo Linux que era el originario sino con el Windows, el Juzgado dispone la impresión de los reportes del Encase acreditándose las fechas de manipulación y modificaciones que se han realizados en los mismos. Recortes de la muestra MGG-93, no presentan ninguna fecha, estas serían pruebas nuevas y por ende no corresponden a las incautadas, ese es el archivo de origen, ejecutable con la que vienen todos los USBs que son nuevos, con la cual se acredita que no corresponde al USB que le fue incautada a mi patrocinada de los USBs plomos de 4GB. La muestra MGG-94 que corresponde al USB Memorex de color plomo de 4GB, fecha de último acceso, escritura y creación; igual que el anterior, este USB se encuentra vacío y no corresponde al USB que fue incautado a la señora Giannotti Grados; precisando que son los USB Memorex de color plomo, a nivel policial, el día que se incautaron tenían una tapa toda de plástico color plomo y a nivel judicial se ha evidenciado que morfológicamente son distintos, son alargados con un círculo en medio y tienen una tapa de plástico transparente, con lo que se acredita que no son los mismos USBs que le fueron incautados el 08 de enero del año 2009. Acta de Audiencia de fecha 08 de marzo del año 2010, acreditándose con la verificación del contenido de los bienes que supuestamente fueron incautados a Giannotti Grados corresponden a CDs, los que han sido cuestionados desde el inicio, al no coincidir en número, verificación realizada el 13 de mayo del 2009 y sometida al Encase se evidenció la diferencia de los Códigos Hash, la diferencia de capacidad de almacenamiento de las muestras MGG95 y MGG96, que corresponden a dos USBs Boston Technologies; se acredita la rotura de la cadena de custodia, no se pudo realizar la comparación, pues la generación del Código Hash, a la que hace referencia esta acta del 08 de marzo, sólo corresponde a la verificación del Código Hash obtenido siempre a nivel judicial, ya que a nivel policial no se les asignó ningún código de seguridad; por lo tanto, habiendo sido incautado un número de CDs menor al que aparece a nivel judicial, no se puede comparar ni corroborar.

Prueba pericial: La Defensa de la Procesada Giannotti Grados,

presenta como prueba el informe de Pericia de Parte elaborada por el ingeniero Enrique Segundo Suárez Guimarey, el mismo que existe manipulación de los archivos antes de pasar el examen del Software Encase 6.1 en el 34 Juzgado Penal de Lima, asimismo que de los archivos analizados se ha encontrado diferencias en los segundos de las horas de ultimo acceso (un segundo), considerando que al tratase de un atributo más de los mencionado archivos los harían diferentes, por lo que considera que el Código Hash Debería ser distinto, pero a pesar de dicha diferencia el código Hash es el mismo, por lo que sustenta la existencia de una colisión de Hash, con la cual se puede alterar un archivo o muestra y mantener el Código Hash original, caso que se presenta en las siguientes muestras: USB2 12 enero2009, Giselle Giannotti USB 2 GB -1 12ene2009. Que de la revisión del acta de obtención de imagen de USB, visualización e impresión de archivos y escucha de audios se observan diferencias en la cantidad de objetos entre lo que reporta el software Encase Forensics con lo que se consigna en el acta, esto sucede en las siguientes muestras: Giselle Giannotti, USB2 12 enero2009, Giselle Giannotti USB 2 GB -1 12ene2009. Incongruencias en las fechas de ultima escritura y de creación en las muestras MGG95, MGG96, asimismo que estas modificaciones han sucedido entre archivo y archivo son de segundos por lo que presume se haya alterado dicha propiedad en cada uno de los archivos o que estos archivos originariamente no hayan estado en ese medio, ni generados en el medio examinado sino copiados o migrados mediante el empleo de otro medio como (USB, CD, portable, etc). Respecto a la muestra Giannotti USB 2GB 12ENE2009 manifiesta que el archivo Roleon 010408.zip no se encuentra y aparentemente fe sustraído o borrado de la muestra, por lo que se evidencia manipulación y no debería tener el mismo código Hash.

Fiscalía Superior Especializada en Crimen Organizado presenta una pericia elaborada por el Ingeniero Santos Alejandro Camarena Ames, indica que De las diez muestras analizadas Giselle Giannotti Memory Card 3, Giselle Giannotti USB2GB, Giselle Giannotti USB 2GB-1 , MGG95, MGG96, MGG101, MGG102, MGG103, MOA19, MBT260, solo las muestras denominadas MGG95, MGG96 son las que contienen fecha de creación

posteriores al 8 de Enero del 2009, de la lectura de dicho listado se aprecia que las fechas de creación de dichos archivos registran 4 de Mayo del 209 entre las 01:05:59am y 01:37:42 por que las demás muestras analizadas no han sido alteración posterior al 8 de enero del 2009.

Análisis de las conclusiones arribadas por ambos peritos: Respecto a la precisión presentada por el perito Enrique Segundo Suárez Guimarey en las que aprecia que existe manipulación de los archivos antes de pasar el examen del Software Encase 6.1 en el 34 Juzgado Penal de Lima, asimismo que de los archivos analizados se ha encontrado diferencias en los segundos de las horas de ultimo acceso de un segundo en algunas muestras, es de precisar que de lo analizado en el expediente y del informe presentado por el Ingeniero Arturo Garro Morey se puede apreciar que existen diferencias respecto a la versión del software utilizado tanto para la diligencia de toma de muestras que arroja en la emisión del código Hash que la versión utilizada para dicha diligencia sería la 4.20 a diferencia de la reciente versión utilizada para esta diligencia 6.0 por lo que la precisión del procedimiento llevado adelante en la pericia realizada tanto por el perito presentado por la Defensa de la procesada Giselle Giannotti y Ponce Feijoo, así como por la Segunda Fiscalía Superior Especializadas, atendiendo al avance de la tecnología y mejora en las versiones hace sostenible la posibilidad de un mejor cálculo y precisión de la hora y fecha de los archivos presentados, asimismo teniendo en consideración el informe final presentado por el perito veedor del Poder Judicial Ingeniero Arturo Garro Morey precisa que el código Hash tomado tanto a las copias espejo mediante el software Encase Forensics Versión 6.0 con los detallados en el expediente resultaron ser idénticos, por lo que se confirma que las copias espejo utilizadas para las pericias de la fiscalía y de la defensa son Bit a Bit idénticas a las copias espejo obtenidas directamente de las muestras originales, por lo que la posibilidad de colisión de hash argumentada por el perito Suarez Guimarey sustentado en el Anexo I de su informe, no prueba la vulnerabilidad en el uso del software Encase Forensics al no haberse demostrado con el uso de dicho software dicha posibilidad real de colisión. Puesto que el Código Hash obtiene de procesar “Bit a Bit” las pistas de un dispositivo (disco duro, CD, USB, etc.) no siendo posible obtener

dos Códigos Idénticos para dos dispositivos con contenidos diferentes. Se concluye que la aseveración presentada por el perito de la Defensa de Giselle Giannotti en su pericia de parte carece de sustento técnico que permita identificar diferencias o manipulación en las muestras analizadas. Respecto afirmación del perito de la Procesada Giselle Giannotti que manifiesta que en la muestra Giannotti USB 2GB 12ene2009 el archivo Roleon 010408.zip no se encuentra y aparentemente fue sustraído o borrado de la muestra, por lo que se evidencia manipulación y no debería tener el mismo código Hash, de la misma manera estando a la consideración sustentada por el Perito Informático Garro Morey y las especificaciones técnicas del Software Encase Forensics, No es posible que dos muestras puedan contener un numero diferente de archivos y mantener el mismo "Código Hash". Puesto que el En Case Forensic no permite modificar las "Copias Espejo" obtenidas de los dispositivos y mucho menos actualizar las pistas del dispositivo al recuperarse un archivo borrado o "malogrado". La defensa dice que un archivo recuperado "Roleon 010408.ZIP" se contabilizó en la pericia de la policía, pero no así en la última pericia. Esta afirmación no tiene sustento técnico porque de lo que obra en el expediente a fojas 1172. Se aprecia el archivo denominado, \Recovered Folders\Folder3\Roleon 010408.ZIP, ha sido obtenido mediante un proceso de recuperación, labor que no se manifiesta se haya realizado por el perito informático Suarez Guimarey para certificar la existencia real de dicho archivo en la muestra USB2 GB-1 12ENE2009, por lo que no queda establecido con esta afirmación del perito una modificación o borrado de archivos de la "Copia Espejo" porque el software En Case Forensic no se lo permite al operador y reiteramos que en base a la opinión del Perito Informático Garro Morey respecto a la generación de código hash las "Copias Espejo", son idénticas "Bit a Bit" y la constatación de su integridad se hace con la verificación de sus códigos hash , realizado en las diligencias periciales y como consta en las actas adjuntadas por los peritos.

Podemos concluir en términos definitivos que las apreciaciones que hacen los peritos, necesariamente encuentran explicación lógica y técnica, lo que deriva en considerar que tanto las conclusiones del perito de parte como las conclusiones del perito del Ministerio Público, tienen deficiencias, puesto

que su capacidad de determinar técnicamente y en términos incuestionables si se produjeron manipulaciones o no en los contenidos de los archivos analizados, no es plena, tanto así que la única vertiente segura es que el En Case Forensic que consiste en otorgar un Código Hash a una muestra constituye hasta el momento el único mecanismo seguro para proteger la muestra y si bien es verdad existe la posibilidad de la manipulación de dicho Código Hash, la posibilidad de lograr es virtualmente inexistente, porque las cifras que garantiza el Código son combinaciones de muchas cifras , consecuencia de diversos cálculos y conclusiones lógicas que establece el En Case que sería extremadamente complicado duplicar, en consecuencia aquello que está protegido con un Código Hash y se vuelve a verificar su autenticidad, si el Código coincide tenemos el 99.99% de seguridad que se trata de la misma muestra, de tal manera que su validez probatoria resulta incuestionable. Evidentemente la dialéctica de un debate penal puede conducirnos a cuestionamientos fáciles sin razón técnica o científica, de ahí que la opinión de los técnicos y la información técnica existente es lo que prevalece y todos los técnicos y conocedores de esta materia afirman que no hay mejor seguridad que el Código Hash para garantizar la autenticidad de una muestra de esta naturaleza, por esa razón la copia espejo que ha servido como referencia para hacer los peritajes tiene la misma calidad que el original y no se ha usado dicho original por los riesgos que implica el reiterado uso de una muestra original que puede derivar inclusive en la perdida de la muestra.

Tacha de documentos: La Sala, al resolver la apelación interpuesta contra la resolución de la A Quo que declara Infundada las tachas formuladas por los procesados Giannotti Grados, Ponce Feijoo y Tomasio De Lambarri, dispuso que se resuelvan conjuntamente con la sentencia; no obstante, iniciado el Juicio Oral en atención a que los cuestionamientos están referidos al rompimiento de la cadena de custodia, mediante Resolución de fecha 25 de Mayo del 2011 excluyó del debate probatorio: i) los USBs marca Mémorex y los USBs marca Boston Technologies incautados a la procesada Giannotti Grados, precisando que las Actas de Deslacrado y las Actas de Obtención de muestra de imagen, visualización, impresión de archivos y escucha de audio realizados hasta el 13 de enero del 2009, respecto de los USBs Boston

Technologies mantienen validez; y, ii) los CDs y Diskettes hallados en la Caja 1, correspondiente al procesado Tomasio de Lambarri; de otro lado, se declaró la validez del Registro Vehicular del procesado Ponce Feijoo. En tal sentido, no nos pronunciaremos sobre los USBs de la procesada Giannotti Grados ni de los CDs y Diskettes de la Caja 1 incautado al procesado Tomasio De Lambarri al haber sido excluidos del debate, ni sobre el Acta de Registro Vehicular del procesado Ponce Feijoo al haberse declarado su validez.

Por lo que concluimos que las Tachas propuestas por la defensa de los procesados Giannotti Grados y Tomasio De Lambarri se declaren Fundados, con excepción de la tacha contra el USB, cassettes y discos duros cuestionados por la defensa del procesado Tomasio de Lambarri.

Evaluación de la prueba y Determinación de la Responsabilidad; Se ha alegado también que la cadena de custodia ha sido rota y en todo caso no ha sido debidamente preservado, lo que habría originado que se manipule indebidamente todos los bienes incautados. Al respecto tenemos que señalar que en situaciones específicas se advierte deficiencias en la custodia de los bienes, falta de precisión en la descripción del bien, inseguridad en su lacrado y manifiesto descuido en una adecuada preservación e intangibilidad del bien; lo que ha originado que se declare fundadas las tachas que han planteado los abogados de la defensa de los acusados, sin embargo tenemos que destacar que los actos iniciales de acopio de elementos, así como la obtención de muestras realizado los primeros días en las oficinas de la Dirandro están premunidos de razonables seguridades y garantías que nos permite evaluar legal y válidamente dichos elementos hallados y descubiertos inicialmente; ya que en todo caso manipulaciones indebidas se habrían producido durante la posterior permanencia de dichos elementos bajo custodia policial o en todo caso en la demora en entregar al Ministerio Publico y posteriormente al juzgado; lo que ciertamente origina dudas sobre la autenticidad de algunos elementos hallados que han originado que antes de iniciar el juicio oral, éste Colegiado haya excluido de la evaluación dos USB que habrían sido cambiados y otros elementos tratados de manera displicente o tal vez

deliberadamente manipulados con propósitos ilícitos; hechos que se vienen investigando y que han merecido que las tachas se declaren fundadas por parte de éste Colegiado; lo que nos remite a evaluar única y exclusivamente aquello que inicialmente se recogió y que inmediatamente se obtuvo muestras, hasta el día 13 de Enero del año 2009 inclusive; porque lo ocurrido posteriormente no tiene los márgenes de garantía y seguridad que la validez del mantenimiento probatorio requiere en los términos que exige el reglamento de cadena de custodia aprobado por resolución N° 729-2006MP-FN del 15 de junio del 2006.

Si esto es así y según la defensa se ha cambiado USB, los CPU no son los mismos o aun siendo los mismos se habrían cambiado los discos duros, habrían desaparecido CD o habrían sido cambiados, la pregunta fluye evidente, por qué se hizo eso, evidentemente porque esos dispositivos contenían información sensible que comprometía al gobierno y sus altos funcionarios, lo que nos lleva a concluir de manera totalmente lógica y congruente que la información que poseían los dispositivos encontrados en posesión de Giannotti Grados, de Tomasio De Lambarri, Ponce Feijoo, lo que se encontró en BTR y todas las demás muestras, no fue lícitamente obtenida, no fue información de fuente abierta; sino más bien información reservada, producto de violaciones de correos e interceptaciones telefónicas; pues de no haber contenido esa información, no había razón para cambiar, borrar, manipular, sobrescribir, infectar y utilizar cualquier otro mecanismo para descartar determinada información; entonces la tesis que con tanto entusiasmo sostiene la defensa determina que los acusados estaban en posesión de valiosa información, que fue obtenida de manera ilícita.

Resuelven: Declararon Fundadas las Tachas planteadas por Giselle Mayra Giannotti Grados y Carlos Alberto Tomasio De Lambarri, respecto de los elementos referidos en la parte considerativa respectiva, con excepción de la tacha contra el USB, cassettes y discos duros cuestionados por éste.

Análisis interpretativo.

El caso Busisnes Track más conocido como los petro audios, fue un caso mediático ya que involucraba a políticos del partido Aprista e inclusive al Presidente de la Republica Sr. Alan García Pérez en ese entonces 2008, y otras personas influyentes del medio, que tuvo como consecuencia la destitución de cargos públicos e inclusive de ministros de estado y el premier del PCM, el caso se dio a raíz de que se difundió audios en el que supuestamente se detallaba conversaciones sobre la inversión extranjera en el sector petróleo y pagos para favorecer contratos.

Para ello la Fiscalía Provincial Especializada en Crimen organizado designa al General PNP Miguel Hidalgo Director de la DIRANDRO para que se encargue de las investigaciones quien nombra un equipo de trabajo al mando del Coronel Carlos Moran Soto, Aquí es importante aclarar conforme lo manifestó el Ministro del Interior Sr. Remigio Hernani Meloni y el Director de la PNP General Mauro Remicio Maguiño, que sobre este caso no tuvieron conocimiento y el General Miguel Hidalgo no les informo al respecto ya que el Presidente de la Republica Alan García le había dado órdenes estrictas de no darles cuenta y solo debería hacerlo a él, esta actitud tomada por el General Hidalgo no es la correcta ya que en la Policía existe el llamado “conducto regular” y que todo hecho que suceda o este por suceder debe dársele cuenta para su conocimiento y estar en condiciones de informar cuando se les requiera, por ello resulta extraño ello.

Segundo, también resulta extraño que la Dirandro que es una Unidad especializada de la PNP en la lucha contra las drogas, investigue casos sobre crimen organizado, ya que funcionalmente esto le correspondía a la Dirección de Investigación Criminal tal como lo refiere el Ministro del Interior y el Director de la PNP.

Tercero, el General Miguel Hidalgo no tenía experiencia en este tipo de investigaciones por ello designa al Coronel PNP Carlos Moran y un equipo de Oficiales para que investiguen el caso. El Fiscal autoriza la detención

preliminar de varias personas vinculadas a la empresa Business Track, así como el descerraje y allanamiento de inmuebles y ambientes interiores de varias personas que tenían nexo en este caso y también dispone la incautación de bienes, documentos, equipos informáticos, soportes electrónicos y de comunicación y otros relacionados a la investigación. El Coronel Carlos Moran indica que mientras se está visualizando un disco duro respecto a la información de los USB, el Mayor PNP Soller, el Fiscal y el Sr. Ponce presentes indicaron “Es la voz del Presidente de la Republica”, ante ello volvió a escuchar el audio sin la presencia del procesado, su abogado ni el fiscal, preocupado por tratarse del Presidente de la Republica, aquí preciso de manera personal que se dio un hecho de contaminación de la evidencia digital ya que para que tenga valor probatorio debieron estar presentes las personas antes referidas y haberse levantado el acta de audio de ese USB.

Como cuarto punto podemos indicar que de conformidad a la declaración del Comandante PNP Raúl Del Castillo encargado de la intervención del domicilio de la Sra Giselle Mayra Giannotti al mando de personal de Oficiales femeninas hallan USBs entre otros bienes y equipos tecnológicos, estos USBs era de marca Memorex, color plomo de plástico, plasmándolo en el acta con esas características siendo incautados y entregados, pero posteriormente al visualizarse los mismos se dan cuenta que era de marca Boston Technologies uno era de 1GB y otro de 2Gb que eran de color amarillo con borde de metal, a ello indican que se trató de un error del acta de entrega al fiscalía. Así mismo indica que no se sacó código Hash a todas las evidencias, solo se hizo a los que se pudieron.

Quinto, respecto al lugar donde se trasladó y guardo las evidencias, según la declaración de la Oficial PNP Ruth Amparo Tenicela, indica que fueron trasladados al sexto piso de la Dirandro en una de las oficinas del grupo de investigaciones especiales cuyo acceso es restringido y se hace mediante huella digital cuya llave estaba a cargo del Comandante PNP Del Castillo, si se quería acceder a algún bien incautado el Comandante tenía que autorizarlo o en su defecto a ella o la Capitán Portocarrero quienes eran los responsables de la seguridad.

Sexto, El Congresista Yonhy Lescano señalo que se formó una comisión integrada por Congresistas designada por el pleno del Congreso de la Republica para investigar si los USBs incautados a la Sra. Giannotti Grados se perdieron o no, se cambiaron o no; se investigó como ingreso la Policía, los Fiscales, como se guardaron las pruebas los USBs, que de la casa de la señora Giselle Giannotti se incautaron 02 USBs Memorex color plomo entero y, finalmente en la entrega de la Policía a la Fiscalía, se entregaron dos USBs totalmente distintos porque tenían tapa transparente y, de eso sí hay pruebas contundentes porque están las actas de incautación, finalmente la comisión determino que se habían cambiado los USBs e, incluso los USBs Boston Technologies, cuando se hace un examen tecnológico a estos otros USBs, se establece que inicialmente uno, tenía supuestamente una capacidad de 01 GB y otro de 02 GB; pero, aparentemente los incautados tenían 02 GB, cada uno; de manera tal que eso suponía que también habían sido cambiados y eso demuestra, dentro de la investigación parlamentaria, que estos USBs están en poder de alguien y que no fueron los originalmente entregados, asi mismo se entregó estos USBs, se pusieron en una bolsa, sin el debido cuidado y el día 12 o 13 del mismo mes que se hizo la incautación, fueron visionados sin autorización judicial, recién el catorce llega una orden judicial que permite la visualización de estos USBs, pero los USBs ya habían sido manipulados. Consecuentemente, ese solo hecho involucra la responsabilidad de los miembros de la Policía Nacional y los Fiscales que estuvieron a cargo de la investigación, es una primera evidencia que nosotros hemos establecido.

Septimo, de las pruebas periciales efectuadas tanto por la defensa de la procesada Giannotti Grados y la Fiscalía Superior Especializada en Crimen Organizado respecto a los dispositivos de almacenamiento USBs y otros en el análisis se concluye que las apreciaciones que hacen los peritos, necesariamente encuentran explicación lógica y técnica, lo que deriva en considerar que tanto las conclusiones del perito de parte como las conclusiones del perito del Ministerio Publico, tienen deficiencias, puesto que su capacidad de determinar técnicamente y en términos incuestionables si se produjeron manipulaciones o no en los contenidos de los archivos analizados,

no es plena, tanto así que la única vertiente segura es que el En Case Forensic que consiste en otorgar un Código Hash a una muestra constituye hasta el momento el único mecanismo seguro para proteger la muestra y si bien es verdad existe la posibilidad de la manipulación de dicho Código Hash, la posibilidad de lograr es virtualmente inexistente, porque las cifras que garantiza el Código son combinaciones de muchas cifras , consecuencia de diversos cálculos y conclusiones lógicas que establece el En Case que sería extremadamente complicado duplicar, en consecuencia aquello que está protegido con un Código Hash y se vuelve a verificar su autenticidad, si el Código coincide tenemos el 99.99% de seguridad que se trata de la misma muestra, de tal manera que su validez probatoria resulta incuestionable.

Octavo, en su análisis el colegiado concluye que las Tachas propuestas por la defensa de los procesados Giannotti Grados y Tomasio De Lambarri se declaren Fundados. Se ha alegado también que la cadena de custodia ha sido rota y en todo caso no ha sido debidamente preservado, lo que habría originado que se manipule indebidamente todos los bienes incautados. Al respecto tenemos que señalar que en situaciones específicas se advierte deficiencias en la custodia de los bienes, falta de precisión en la descripción del bien, inseguridad en su lacrado y manifiesto descuido en una adecuada preservación e intangibilidad del bien; lo que ha originado que se declare fundadas las tachas que han planteado los abogados de la defensa de los acusados. Finalmente el Colegiado determina que haya excluido de la evaluación dos USB que habrían sido cambiados y otros elementos tratados de manera displicente o tal vez deliberadamente manipulados con propósitos ilícitos; hechos que se vienen investigando y que han merecido que las tachas se declaren fundadas por parte de éste Colegiado.

Noveno, la Corte Superior resuelve declarar fundada las tachas planteadas Giselle Mayra Giannotti Grados y Carlos Alberto Tomasio De LambarrI, respecto de los elementos referidos en la parte considerativa respectiva.

Conclusiones del resultado de Interpretación y análisis del proceso Business Track S.A. (Petro audios).

Fue un caso que involucro al Presidente de la Republica Alan García, ministros, políticos, a raíz de que se difundió audios en el que supuestamente se detallaba conversaciones sobre la inversión extranjera en el sector petróleo y pagos para favorecer contratos. La Fiscalía Provincial Especializada en Crimen organizado encargada de la investigación designo al General PNP Miguel Hidalgo Director de la Dirandro para que se encargue de las investigaciones y este a su vez a varios Oficiales PNP.

Se dieron varias incongruencias como solicitar a la Dirandro Unidad especializada en lucha contra las drogas, se encargue de investigar mas no a la Dirincri Unidad especializada en estos ilícitos. Se dispuso descerraje y allanamiento de inmuebles y ambientes interiores de varias personas entre ellas de la Sra. Giselle Mayra Giannotti hallando USBs, a los cuales no se les dio el tratamiento técnico, no aplicándoseles procedimientos mediante herramientas para preservar la originalidad y autenticidad del contenido de información. De ahí que se cuestionó características, colores, marcas y capacidad de almacenamiento. La cadena de custodia fue deficiente se visualizaron videos sin presencia de los propietarios, abogados y fiscal del contenido de los USBs en la Dirandro donde se le daba custodia.

El Congreso de la Republica efectuó una investigación sobre los USBs determinando que estos fueron cambiados, ya que aparentemente fueron incautados y que días después se cambiaron. También fueron manipulados y visualizados sin autorización judicial siendo responsabilidad de la Policía a cargo de la investigación. De los exámenes periciales se determinó que existió deficiencias en la capacidad de terminar técnicamente si se produjeron manipulaciones en los USBs, esto finalmente determino para que la Corte Superior declare fundada las tachas planteada por la Sra. Giselle Mayra Giannotti Grados respecto a los USBs.

Proceso Delito de abusos sexuales – cuenta Tuenti.

Procedimiento: Penal - Procedimiento Abreviado/Sumario Tribunal Supremo. Sala de lo Penal Madrid. recurso de casación interpuesto por la representación legal de Luis Francisco, contra la sentencia dictada por la Audiencia Provincial de Valladolid, de fecha 19 de noviembre de 2014 en causa seguida contra Luis Francisco, por un delito de abusos sexuales.

"Ana María, nacida el NUM000 de 2000, es hija de Don Abilio y doña Belén, que se separaron de mutuo acuerdo en el año 2005, pasando a residir con la madre tanto Ana María como su hermana Micaela, en la vivienda sita en la CALLE000 nº NUM001, NUM002, de la localidad de Villanubla (Valladolid). Don Luis Francisco, mayor de edad y sin antecedentes penales, inició hace años una relación sentimental con Doña Belen, comenzando a convivir con ésta y sus hijas en el domicilio indicado en el año 2006 ó 2007. Por problemas de convivencia con su madre y con Don Luis Francisco, Micaela en el mes de Octubre de 2012 se marchó a vivir con su padre en la calle CAMINO000 nº NUM003, NUM004 de la localidad de Villanubla (Valladolid), estando de acuerdo con este cambio su madre, de tal forma que ni siquiera se comunicó al Juzgado que había conocido de la separación matrimonial, llevándose el cambio de residencia de Micaela, que era menor de edad, de forma consensuada entre sus progenitores. A principios del mes de Abril de 2013, Don Luis Francisco, en fecha que no ha sido exactamente concretada, aprovechando la relación de convivencia con Doña Belen y Ana María, y con la excusa de ayudar a esta última en sus tareas escolares, accedió a la habitación en la que se encontraba Ana María estudiando, mientras su madre estaba en la planta baja de la vivienda, se colocó detrás de Ana María mientras ésta se encontraba sentada delante del ordenador y la tocó el pecho por encima de la ropa, diciéndole Ana María que parase, sin que Don Luis Francisco continuara con estos tocamientos.

El día 31 de Mayo de 2013, alrededor de las 20 horas, Ana María estaba manteniendo una conversación a través de Tuenti con su amigo Constancio, al que le contó que el novio de su madre "le tocaba las..." y que la

decía que le enseñara su sujetador nuevo, que la había intentado subir la camiseta y que la tocaba, que la había tocado "sus partes", afirmando que "la había tocado las de arriba" y que "la de abajo se la tocó dos veces o así", que el día de las comuniones intentó subir su camiseta, insistiendo Constancio en que se lo contara a su madre.

La Audiencia Provincial de Valladolid, Sección Segunda, dictó el siguiente pronunciamiento: "Fallamos: Que debemos Condenar Y Condenamos a Don Luis Francisco como autor de un delito continuado de abuso sexual sobre una menor de trece años, con prevalimiento derivado de su situación de superioridad, a la pena de Cinco Años y un día de prisión.

La representación legal del recurrente Luis Francisco, basa su recurso en los siguientes motivos de casación: Las conversaciones mantenidas entre Ana María e Constancio, incorporadas a la causa mediante "pantallazos" obtenidos a partir del teléfono móvil de la víctima, no son propiamente documentos a efectos casacionales. Se trata de una prueba personal que ha sido documentada a posteriori para su incorporación a la causa. Y aquéllas no adquieren de forma sobrevenida el carácter de documento para respaldar una impugnación casacional. Así lo ha declarado de forma reiterada esta Sala en relación, por ejemplo, con las transcripciones de diálogos o conversaciones mantenidas por teléfono, por más que consten en un soporte escrito o incluso sonoro.

Se reacciona también frente a la incondicional aceptación probatoria del diálogo mantenido entre Ana María y su amigo Constancio, que fue incorporado a la causa mediante pantallazos de la cuenta de Tuenti. Apunta la defensa que "... se desconoce el contexto en que se desenvuelven y si alguna frase fue eliminada".

Respecto a la queja sobre la falta de autenticidad del diálogo mantenido por Ana María con Constancio a través del Tuenti, la Sala quiere puntualizar una idea básica. Y es que la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería

instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido. Pues bien, en el presente caso, dos razones son las que excluyen cualquier duda. La primera, el hecho de que fuera la propia víctima la que pusiera a disposición del Juez de instrucción su contraseña de Tuenti con el fin de que, si esa conversación llegara a ser cuestionada, pudiera asegurarse su autenticidad mediante el correspondiente informe pericial.

La segunda, el hecho de que el interlocutor con el que se relacionaba Ana María fuera propuesto como testigo y acudiera al plenario. Allí pudo ser interrogado por las acusaciones y defensas acerca del contexto y los términos en que la víctima Ana María y el testigo Constancio mantuvieron aquel diálogo. Con toda claridad lo explican los Jueces de instancia en el FJ 2º de la resolución combatida: "... respecto de la conversación de Tuenti cuya impresión fue aportada por la Acusación Particular, porque las dos personas que la mantuvieron, Ana María y su amigo Constancio, en el plenario han manifestado que efectivamente mantuvieron esa conversación y en esos términos, sin que ninguno de los dos hiciera referencia a que se hubiera producido ninguna manipulación en la impresión de dicha conversación, que consta no solamente aportada por la Acusación Particular en los folios 178 a 190 sino también en las fotografías que del teléfono móvil de la menor adjuntó la Guardia Civil (folios 199 y siguientes), ya que según consta en el oficio, Ana María accedió en su presencia a su cuenta de Tuenti a través de un ordenador, pero el historial

solo permitía retroceder hasta el 26 de Octubre de 2013, por lo que únicamente pudieron visualizarlo a través de la aplicación de Tuenti para teléfonos móviles, haciendo los agentes fotografías de las pantallas correspondientes a la conversación, que coinciden exactamente con las hojas impresas que fueron aportadas por la Acusación Particular. Precisamente, en el escrito con el que se adjuntaban estas impresiones, la Acusación Particular facilitó las claves personales de Ana María en Tuenti y solicitaba que, si había alguna duda técnica o probatoria, que se oficiara a "Tuenti España", indicando su dirección, para que se certificara el contenido de esa conversación, sin que la Defensa haya hecho petición alguna al respecto. Teniendo en cuenta que tanto Ana María como Constancio han reconocido el contenido de la conversación que se ha facilitado tanto por la Acusación Particular como por la Guardia Civil, no puede estimarse la impugnación de la Defensa, quedando dicha documental dentro del acervo probatorio para su valoración con el conjunto de las restantes pruebas que han sido practicadas".

Fallo: Lo Que debemos declarar y declaramos No Haber Lugar al recurso de casación, interpuesto por Luis Francisco contra la sentencia de fecha 19 de noviembre de 2014, dictada por la Sección Segunda de la Audiencia Provincial de Valladolid , en la causa seguida por el delito de abusos sexuales y condenamos al recurrente al pago de las costas causadas.

Análisis interpretativo.

Este es un caso de procedimiento abreviado o sumario como se le conoce en Perú, del Tribunal Supremo de Madrid, respecto a un recurso de casación interpuesto por Luis Francisco contra la sentencia dictada por la Audiencia Provincial de Valladolid por delito de abusos sexuales.

Los hechos datan que Luis Francisco es conviviente de Doña Belén madre de Ana María quien es una menor de edad en etapa escolar, el imputado con el pretexto de ayudarle con sus tareas escolares accedió a la habitación de la menor Ana María, se colocó detrás de ella delante del ordenador donde ella se encontraba y le toco el pecho por encima de la ropa,

indicándole Ana María que parase.

El 31 de Mayo del 2013, Ana María mantenía una conversación a través de Tuenti con su amigo Constancio, a quien le conto que el novio de su madre le había tocado sus partes las de arriba y las de abajo en más de una oportunidad.

Al respecto en primera instancia la Audiencia Provincial de Valladolid, fallo condenando a Luis Francisco como autor del delito continuado de abuso sexual sobre la menor de 13 años a la pena de 5 años y 1 día de prisión. Luis Francisco basa su recurso de casación indicando que las conversaciones mantenidas entre Ana María y Constancio fue incorporado mediante “pantallazos”, obtenidos del teléfono móvil de la víctima, no son propiamente documentos a efectos casacionales, y se trata de una prueba personal que ha sido documentada a posteriori para su incorporación a la causa. También refiere el imputado que los pantallazos de la cuenta de Tuenti "...se desconoce el contexto en que se desenvuelven y si alguna frase fue eliminada". Al respecto reclama la falta de autenticidad del diálogo mantenido por Ana María con Constancio a través del Tuenti, la Sala puntualiza que la prueba de una comunicación bidireccional mediante sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido.

En el presente caso, hay dos razones que excluyen cualquier duda, que la propia víctima puso a disposición del Juez de instrucción su contraseña de Tuenti con el fin de que, si esa conversación llegara a ser cuestionada, pudiera asegurarse su autenticidad mediante el correspondiente informe pericial. La segunda, el hecho de que el interlocutor con el que se relacionaba Ana María fuera propuesto como testigo y acudiera al plenario. Allí pudo ser interrogado por las acusaciones y defensas acerca del contexto y los términos en que la víctima Ana María y el testigo Constancio mantuvieron aquel diálogo. Ana María accedió en su presencia a su cuenta de Tuenti a través de la aplicación de Tuenti para teléfonos móviles, haciendo los agentes fotografías de las pantallas correspondientes a la conversación, que coinciden exactamente con las hojas impresas que fueron aportadas por la Acusación Particular.

En ese sentido el Tribunal falla no haber lugar al recurso de casación interpuesto por Luis Francisco contra la sentencia dictada por la Sección Segunda de la Audiencia Provincial de Valladolid, en la causa seguida por el delito de abusos sexuales y condenamos al recurrente al pago de las costas causadas.

Conclusiones del resultado de Interpretación y análisis del proceso Delito de abusos sexuales – cuenta Tuenti.

Recurso de casación interpuesto por Luis Francisco contra la sentencia dictada por la Audiencia Provincial de Valladolid por delito de abusos sexuales. El imputado es conviviente de Doña Belén madre de Ana María quien es una menor de edad en etapa escolar, y con el pretexto de ayudarle en sus tareas escolares accedió a la habitación de la menor Ana María, se colocó detrás de ella delante del ordenador donde ella se encontraba y le toco el pecho por encima de la ropa. Ana María a través de su cuenta en Tuenti con su amigo Constancio, le conto que el novio de su madre le había tocado sus partes las de arriba y las de abajo en más de una oportunidad.

En primera instancia falla condenándolo como autor del delito

continuado de abuso sexual a la pena de 5 años y 1 día de prisión. El imputado basa su recurso de casación cuestionando la falta de autenticidad de los “pantallazos”, obtenidos del teléfono móvil de la víctima, de la conversación de la menor con Constancio y que se desconoce el contexto en que se desenvuelven y si alguna frase fue eliminada.

La Sala puntualiza que la prueba que proviene de sistemas de mensajería instantánea debe ser abordada con cautela, ya que existe posibilidad de manipulación de los archivos digitales. El anonimato que brinda la libre creación de cuentas con una identidad fingida, dan la posibilidad de aparentar una comunicación en la que un único usuario se relaciona consigo mismo. En estos casos es indispensable la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido. Para este caso, hay dos razones que excluyen cualquier duda, que la propia víctima puso a disposición del Juez de instrucción su contraseña de Tuenti con el fin de que, si esa conversación llegara a ser cuestionada, pudiera asegurarse su autenticidad mediante el correspondiente informe pericial. La segunda, el hecho de que el interlocutor con el que se relacionaba Ana María fuera propuesto como testigo y acudiera al plenario. En ese sentido el Tribunal falla no haber lugar al recurso de casación interpuesto por Luis Francisco.

Proceso delito de Acoso Sexual Agravado – vía Facebook.

Corte Superior de Justicia de Madre de Dios Tercer Juzgado de Investigación Preparatoria de Tambopata Cuaderno Nro. 01328-2018-0-2701-JR-PE-02 Puerto Maldonado, octubre, uno del año dos mil dieciocho. Sentencia de terminación anticipada. Audiencia de Proceso Inmediato, en la investigación seguida contra de Parizaca Puma, Edwar Alex, por la presunta comisión del delito de Acoso Sexual Agravado en agravio de la menor de iniciales G.M.B.M de 15 años.

El imputado le envía una solicitud de amistad por medio de la red social Facebook a la menor agraviada, con fecha 18 de Setiembre 2018 acepta la solicitud, procediendo el imputado a preguntarle si era soltera y si iba a las discotecas, respondiendo la menor que no lo hacía por ser menor de edad. Al día siguiente el imputado continuo asediando a la menor preguntándole “amiga te gustaría entrar a un grupo de chicas sexis de servicios discretos”, “te pago 50 soles”, posteriormente le pregunta “Me gustaría follarte si gustas claro”, la menor le increpa indicando “que te pasa”, el imputado insiste “Me gustas, me gustaría tener una noche erótica contigo” por lo que la menor le dice que podría denunciarlo, pidiéndole el imputado que no lo haga. Días después le continua escribiendo “Te ves bellísima”.

El día 28 de Setiembre 2018 al descubrir su progenitora de la menor estas conversaciones, pregunto al imputado por ese mismo medio si seguía en pie su propuesta, quien le indico que sí, aclarándole el nuevamente que todo sería discreto y que podían encontrarse en el cementerio. Es así que a horas 13.30 aprox. La menor concurrió al cementerio, indicándole al imputado por Facebook que está dentro al lado derecho, la menor ingreso y luego vio llegar al imputado aproximársele.

La progenitora de la menor acompañada de unos familiares, observaron desde afuera del cementerio la llegada del imputado en motokar y cómo es que ingresaba detrás de la menor al cementerio, se le acercó y le reclamo al imputado iniciándose una discusión conglomerándose un grupo de personas. Al notar el tumulto dos policías que se encontraban de franco se aproximaron, siendo informados de lo sucedido, interviniendo al imputado, identificándolo y encontrando entre sus pertenencias el teléfono desde el que conversaba con la menor por las redes sociales.

Se formularon varias actas entre ellas el acta de visualización de mensajes y conversaciones en cuenta Messenger del equipo telefónico usado por la menor agraviada, verificándose y extrayéndose las capturas de la totalidad de conversaciones que sostuvo el imputado desde su equipo telefónico, verificándose como es que en dicho equipo estaba abierta la

aplicación de Facebook con el usuario “Jimi Castro de la Vega”, encontrándose la última conversación que sostuvo con la menor, advirtiéndose que las anteriores fueron borradas.

El Juez resuelve declarar fundada la incoación del proceso inmediato, por el delito en flagrancia en contra de Edwar Alex Parisaca Puma por el delito de acoso sexual agravado, en agravio de la menor de iniciales G.M.B.M. señalando el imputado que se encuentra conforme en todo los extremos y que no desea pasar a la siguiente etapa. Sobre el control de legalidad, en la suficiencia y elementos de convicción; El sustento no solo está amparado en el reconocimiento que ha hecho el imputado en esta audiencia sino también a los suficientes elementos de convicción que le dan sostenibilidad a la imputación.

Resuelve: Declarar a de Edwar Alex Parisaca Puma, autor del delito contra la Libertad en su modalidad de violación de la libertad sexual, sub tipo Acoso Sexual Agravada, en agravio de la menor de iniciales G.M.B.M. y como tal se le impone Tres años y seis meses de pena privativa de la libertad suspendida, en su ejecución por el plazo de dos años. Así como a reglas de conducta.

Análisis interpretativo.

Esta es la primera sentencia en el Perú que condenan a sujeto por acoso sexual. La Corte Superior de Justicia de Madre de Dios con fecha 08 de Octubre del 2018 en la Audiencia de Proceso inmediato en la investigación seguida contra de Parizaca Puma, Edwar Alex, por la presunta comisión del delito de Acoso Sexual Agravado en agravio de la menor de iniciales G.M.B.M de 15 años.

Los hechos se dan cuando el imputado envía una solicitud de amistad por medio de la red social Facebook a la menor agraviada, aceptando la solicitud, preguntándole si era soltera y si iba a las discotecas, respondiendo la menor que no lo hacía por ser menor de edad. Días

posteriores el imputado continuaba asediando a la menor preguntándole “amiga te gustaría entrar a un grupo de chicas sexis de servicios discretos”, “te pago 50 soles”, posteriormente le pregunta “Me gustaría follarte si gustas claro”, la menor le increpa indicando “que te pasa”, el imputado insiste “Me gustas, me gustaría tener una noche erótica contigo” por lo que la menor le dice que podría denunciarlo, pidiéndole el imputado que no lo haga. Días después le continua escribiendo “Te ves bellísima”.

Con fecha 28 de Setiembre 2018 la madre de la menor descubre estas conversaciones, y decide preguntarle al imputado por ese mismo medio si seguía en pie su propuesta, quien le indico que sí, aclarándole el nuevamente que todo sería discreto y que podían encontrarse en el cementerio. Es así que a horas 13.30 aprox. La menor concurrió al cementerio, indicándole al imputado por Facebook que está dentro al lado derecho, la menor ingreso y luego vio llegar al imputado aproximársele. La progenitora de la menor observo desde afuera del cementerio la llegada del imputado y vio como ingresaba detrás de la menor al cementerio, ante ello se le acercó y le reclamo al imputado iniciándose una discusión conglomerándose un grupo de personas. Al notar el tumulto dos policías se aproximaron, siendo informados de lo sucedido, interviniendo al imputado, identificándolo y encontrando entre sus pertenencias el teléfono desde el que conversaba con la menor por las redes sociales.

Se formula el acta de visualización de mensajes y conversaciones en cuenta Messenger del equipo telefónico usado por la menor agraviada, verificándose y extrayéndose las capturas de la totalidad de conversaciones que sostuvo el imputado desde su equipo telefónico, verificándose que la aplicación de Facebook con el usuario “Jimi Castro de la Vega”, se encontraba activa. Observándose la última conversación que sostuvo con la menor, advirtiéndose que las anteriores fueron borradas. Sobre el control de legalidad, el sustento no solo está amparado en el reconocimiento que ha hecho el imputado en la audiencia sino también a los suficientes elementos de convicción que le dan sostenibilidad a la imputación. Por lo que se resuelve, declarar a Edwar Alex Parisaca Puma, autor del delito contra la Libertad en su

modalidad de violación de la libertad sexual, sub tipo Acoso Sexual Agravada, en agravio de la menor de iniciales G.M.B.M. y se le impone Tres años y seis meses de pena privativa de la libertad suspendida, en su ejecución por el plazo de dos años. Así como a reglas de conducta.

Conclusiones del resultado de Interpretación y análisis del proceso delito de Acoso Sexual Agravado – vía Facebook.

El Imputado Parizaca Puma, Edwar Alex, envía una solicitud de amistad en la red social Facebook a la menor agraviada quien lo acepta, le pregunta si era soltera y si iba a las discotecas, respondiendo la menor que no lo hacía por ser menor de edad. Posteriormente le pregunta si le gustaría entrar a un grupo de chicas sexis de servicios discretos, con el pago de 50 soles, y que le gustaría follarla insistiendo que le gustaría tener una noche erótica. La menor le dice que podría denunciarlo, pidiéndole el imputado que no lo haga.

Días después la madre de la menor descubre estas conversaciones, y decide preguntarle al imputado por ese mismo medio si seguía en pie su propuesta, quien le indico que sí, aclarándole el nuevamente que todo sería discreto y que podían encontrarse en el cementerio. Ante ello la menor concurre al cementerio y el imputado también. La progenitora en el lugar se le acerca y le reclama al imputado iniciándose una discusión conglomerándose un grupo de personas. Personal de la policía interviene al imputado, encontrando entre sus pertenencias el teléfono desde el que conversaba con la menor por las redes sociales.

En el acta de visualización de mensajes y conversaciones en cuenta Messenger del equipo telefónico usado por la menor agraviada, se verifica las capturas de la totalidad de conversaciones que sostuvo el imputado desde Facebook con el usuario “Jimi Castro de la Vega”. Sobre el control de legalidad, el sustento no solo está amparado en el reconocimiento que ha hecho el imputado en la audiencia sino también a los suficientes elementos de convicción que le dan sostenibilidad a la imputación. Por lo que se resuelve, declarar a Edwar Alex Parisaca Puma, autor del delito contra la Libertad en su

modalidad de violación de la libertad sexual, sub tipo Acoso Sexual Agravada, en agravio de la menor de iniciales G.M.B.M.

Conclusión de Análisis de Observaciones.

La falta de tratamiento especializado en el recojo de evidencias digitales en la escena del hecho, por parte del personal policial resulta gravitante en la preservación de la originalidad y autenticidad del contenido de información.

La presentación de evidencias digitales en impresiones de papel de mensajes escritos en redes sociales, no resulta suficiente, en casos de flagrancia es importante incautar el medio tecnológico de donde se hizo la afectación el cual será un elemento de convicción contundente.

Los pantallazos obtenidos de conversaciones en redes sociales de medios tecnológicos deben estar acompañados de elementos que aseguren su autenticidad, ya que existe la posibilidad de manipulación del archivo o la identidad fingida.

V. Discusión

Respecto a la discusión de los resultados de la investigación, Lerma (2011) señala que el objetivo de la discusión es "(…) mostrar las concordancias y diferencias de los propios resultados con los encontrados por otros investigadores, y que ya fueron mencionados en el marco de referencia del estudio (…)" (p. 70). En este orden de ideas, tomando en cuenta que la discusión es el contraste crítico de los resultados de la investigación con los antecedentes o trabajos previos respecto al problema de estudio, así como con las teorías relacionadas al tema, el cual, en la presente investigación se presenta de la siguiente manera.

Los delitos informáticos se desarrollan dentro de un lugar virtual sin espacio físico denominado ciberespacio, empleando como medio un dispositivo tecnológico (PC, Tablet, ipod, etc), y además que debe estar conectado a internet, ello implica al usuario que hace uso de esta tecnología que resulta ser víctima, al afectarse sus bienes, negocios y otros, si hablamos de empresas privadas o estatales la pérdida de credibilidad en su servicio y la inseguridad de parte de sus clientes generando por consiguiente mala imagen y desprestigio (por ejemplo información bancaria), instituciones del Estado que estarían expuestas al secuestro de información personal de los ciudadanos del país (por ejemplo Reniec), o contra la seguridad del país al exponer información clasificada de la seguridad del país (por ejemplo información secreta de seguridad FFAA), y a ello el avance incontrolable de las Tecnologías de Información y Comunicación que sin lugar a dudas hoy resulta una necesidad imprescindible en todas las actividades del ser humano y la falta de conciencia en seguridad informática.

Los ilícitos informáticos que se cometen en el ciberespacio, resultan muy complejos debido no existe límites ni espacios físicos definidos donde las leyes de los países no tienen alcance de jurisdicción, generándose que estos delitos sean transnacionales, este factor contribuye fundamentalmente en no poder sancionarlos, y que los ciberdelincuentes gocen de impunidad, nuestro país es uno de ellos, siendo considerado como paraíso de la ciberdelincuencia por la impunidad que genera el no tener normas que sancionen los delitos transnacionales, por citar un ejemplo pornografía infantil en internet, el

servidor donde se halla las fotografías se ubica en Chile, el proveedor y comercializador de estas imágenes lo hace desde su equipo de cómputo de Colombia y un comprador de ese material lo hace en Perú, a través de pago on line. En este caso personas de tres países son parte de un mismo ilícito, el poder sancionar esta inconducta es compleja ya que no hay leyes que nos permita poder aplicar sanciones a estas personas debido a la soberanía de jurisdicción en aplicación de la Ley penal.

Los ilícitos informáticos en el proceso de su ejecución y consumación, dejan como rastro las llamadas evidencias digitales, que son los puntos de partida para la acción de los operadores encargados de la lucha contra la ciberdelincuencia como son la Policía Nacional del Perú, el Ministerio Publico y el Poder Judicial. En nuestro país el Nuevo Código Procesal Penal no regula específicamente su tratamiento, trata de darle una similitud como si fuese una prueba documental reconocida en el Art. 185 de la referida norma, lo cual es un grave error, muy por el contrario ello contribuye a que la evidencia digital se contamine y no pueda emplearse en un proceso judicial, al haberse vulnerado los principios que se exige. La valoración de la prueba dependerá de la aceptabilidad de los resultados probatorios, que las pruebas no hayan vulnerado los principios que regulan su admisibilidad.

El procedimiento que garantiza la individualización, seguridad y preservación de la evidencia digital recolectado, se denomina la cadena de custodia que busca garantizar la autenticidad para los efectos de un proceso judicial. Al respecto se señala que no existe en nuestro ordenamiento jurídico acciones concretas respecto al procedimiento de la cadena de custodia de la evidencia digital, esta se realiza como si se tratase de una evidencia física en común, a ello se suma la falta de personal tanto policial y de fiscales que no están capacitados y en condiciones de recolectar técnicamente una evidencia digital, ello conlleva a que esta se contamine y no pueda emplearse en el proceso judicial, más aun al no existir conciencia de seguridad informática se emplean en el mejor de los casos equipos, softwares que no tienen reconocimiento legal, no tienen las licencias o no se encuentran autorizadas por los organismos que regulan su el empleo, por lo general son de otros

países.

El Estado peruano en previsión de amenazas internas o externas, dicto la Ley 30096 Ley de delitos informáticos tipificando una serie ilícitos penales que tienen que ver con el uso de las TIC, asimismo ha creado la DIVINDAT unidad especializada de la Policía Nacional del Perú para que se encargue de investigar los ilícitos penales informáticos. Pero lo hecho hasta ahora resulta insuficiente falta regulación de normas de carácter procesal para el hallazgo, recojo, tratamiento y traslado de la evidencia digital, así mismo la Unidad Especializada de la Policía no cuenta con el personal y equipos necesarios para enfrentar eficazmente la lucha contra la ciberdelincuencia.

Otros países han desarrollado mejores condiciones respecto al tratamiento de la evidencia digital, desde el punto de vista legal y capacitación, entre ellos tenemos en Sudamérica a Colombia y Argentina, en Europa España que es uno de los referentes en esta lucha. Colombia ha creado su cuarta fuerza armada encargada de ciberseguridad y la ciberdefensa de su país, esto genera un gran impacto de confiabilidad de las personas en los ámbitos privados y estatales en el empleo de las Tecnologías de Información y Comunicación ya sea de forma personal, empresarial o institucional generando mejores ingresos y desarrollo para su país.

En la actualidad existe una variedad de herramientas tecnológicas y jurídicas que ayudan a mantener la originalidad de la evidencia digital, entre las que podemos citar el Remote Forensic que es una herramienta de investigación, el Triage que realiza una búsqueda rápida de información sobre la estructura de los dispositivos de almacenamientos que servirán posteriormente para la realización de copias forenses de la evidencia digital, es necesario precisar que para que para darle valor probatorio a los resultados que se obtiene del empleo de estas herramientas ellas deben estar certificadas avaladas por normas que respalden su empleo así como contar con personal capacitado con conocimiento y certificados.

De una jornada hecha por la Asociación por los Derechos Civiles,

con la Policía Federal de Argentina realizaron un aporte muy beneficioso para todo el ecosistema de operadores que interactúa día a día en el quehacer de la investigación criminal informática, concluyeron que es necesario incorporar mejores herramientas judiciales y procesales que permitan proveer al perito de los elementos necesarios para que luego el operador judicial haga la valoración final de toda la actividad de investigación técnica. La actividad de investigación que realiza el perito ha tomado fuerza a nivel internacional debido a la relevancia que tiene dentro de los procesos judiciales la evidencia digital, Las facultades procesales que deben tener los investigadores en cibercrimen se hace necesario cuando deben ocuparse de delitos online en los cuales existe una multiplicidad de jurisdicciones por la propia naturaleza de internet. De esta manera, si un operador judicial debe validar una información generada en otro país, debe esperar una rogatoria internacional que demora la investigación judicial.

La ONG American Bar Association Rule of law Initiative aba roli Perú, con el auspicio del gobierno de EEUU, en el cual participo representantes del Ministerio Publico de la Fiscalía Especializada Delitos de Corrupción de Funcionarios y Delitos de Lavado de Activos y personal de la Policía Nacional del Perú de la Divindat PNP; elaboraron el “Manual de Evidencia Digital”, el cual busca reducir los errores frecuentemente cometidos al abordar una escena del crimen en el que se pueden encontrar medios de prueba altamente sofisticados y cuyo aseguramiento, protección y análisis exige conocimientos y técnicas avanzadas que impidan su alteración e, incluso, su destrucción. En ella se explica de manera sencilla, los términos que se emplean en el tratamiento de la evidencia digital. Pero a nivel policial este manual no está aprobada para su empleo.

El Convenio de Budapest, es la única norma internacional que aborda legislación sobre ciberdelincuencia, en lo penal así como en procedimientos y de cooperación internacional, mantiene comunicación permanente, asesora y da apoyo técnico en la lucha contra la ciberdelincuencia en el mundo. El Perú a la fecha no se adherido a dicho convenio.

Existen normas como el modelo argentino del PGN Nro. 756/16 de la Procuraduría General de la Nación Argentina, brinda directrices sobre la forma como se aborda, la conservación y el tratamiento de la evidencia digital respecto a cómo reprimir penalmente un proceso investigatorio fuera del país de este delito. Toma en consideración las recomendaciones dadas por la ONU en lo que se refiere a la transnacionalidad, su vínculo con el crimen organizado y la urgente atención de normas eficaces y estandarizadas para una buena cooperación internacional así como la atención del estado para la obtención de buenos resultados.

En Colombia se crearon los institutos que buscan la difusión y cooperación en las técnicas y protocolos forenses aplicables en caso de delitos informáticos y los demás que involucren la aplicación de herramientas informáticas, con la finalidad de ayudar a los investigadores certificados, poniendo a disposición de forma gratuita documentos de investigación científica en lo referente a la informática forense y el derecho informático, temáticas que nutren el contexto total del campo de la investigación forense digital para la obtención de evidencia digital, con la aplicación de protocolo y herramientas forenses, no solo las consideradas por certificadas por un instituto reconocido como es SANS16, sino también que permiten la obtención de la evidencia digital con características de autenticidad, integridad, originalidad, confiabilidad y no repudio. En igual perspectiva frente a la utilidad y respaldo dado a la Evidencia Digital, se cuenta con el NIST17: Para el campo de la informática o computación forense promueve programas académicos de contenido novedoso y contemporáneo, satisfaciendo los retos diarios que la ciberdelincuencia.

En España Los RFC (Request For Comments) son documentos que detalla cómo debe ser aceptado y pueda ser implementado sin ambigüedades una evidencia. Establece un procedimiento para recoger y guardar la evidencia. En ella podemos apreciar y describir la volatilidad de los datos, nos permite definir que recoger, así como que guardar y la documentación de los datos.

Respecto a los procedimientos tecnológicos en la evidencia digital, existen normas de la Unión Europea que brindan valor probatorio a la evidencia digital tales como La Norma UNE 71505 – 2013 que define conceptos sobre la seguridad y controles de las evidencias informáticas. Indica las propiedades básicas de confiabilidad. Procesos de originalidad, reservas y cumplimiento. El periodo en que desarrolla la generación, guardado, comunicación y traslado de las evidencias digitales. Norma UNE 71505-2 2013 establece registros y desarrollo en la gerencia de seguridad de las evidencias, tales como la confiabilidad, la autenticación, y la integridad, asegurando el poder ser ubicada, rescatada y presentada y la completitud que nos muestra la publicación del contenido de la evidencia. La UNE 71505-3 2013 tiene como objetivo garantizar la legitimidad y plenitud de la evidencia digital conservando su legalidad probatoria ante el juez, brindando al perito informático el poder analizar y verificar, la validez y se encuentre intacta la evidencia. UNE 71506 2013 esta procedimiento desarrolla un método cuyo objeto es la preservación, adquirir, documentarla, analizarla y presentar las evidencias digitales. También se tiene normas ISO establecidas por el Organismo Internacional de Estandarización y fueron creadas con la finalidad de ofrecer orientación, coordinación, simplificación y unificación de criterios a las empresas y organizaciones**,** así como estandarizar las normas de productos y servicios para las organizaciones internacionales. La ISO/IEC 27037 2012 brinda patrones en las acciones del empleo de la evidencia digital, siendo entre ellos la de identificar, seleccionar, adquirir y preservar la evidencia. El ISO/IEC 27042 2015 tiene las características de una norma orientadora respecto al análisis así como interpretar la evidencia digital abordando conceptos de continuación, valor, reproducción y repetitividad.

Otra herramienta es el sellado de tiempo es un método que sirve para mostrar que determinados datos existen y que no han sido modificados desde su origen, esto implica la participación de la autoridad de certificación, de registro y otras entidades, así como políticas y actividades. El procedimiento determina la intervención de una entidad acreditada como Autoridad de Sellado de Tiempo, que genera y garantiza un resumen, la fecha y la hora de un documento, y que almacena los sellos emitidos para

posteriores verificaciones. Existen herramientas como Computer Forensic, Móvil Forensic, Network Forensic, Database Forensic y Live Forensics, son herramientas que ayudan al tratamiento de la evidencia digital.

En el caso Business Track, se pudo apreciar que en el proceso de hallazgo, recojo y traslado de la evidencia digital se cometieron grandes errores, en principio el Personal de la Policía Nacional, le dio un tratamiento a la evidencia digital como si fuese una evidencia común (USBs), en el momento de formulación de la cadena de custodia no se precisó detalles como colores, características, marcas, capacidad de almacenamiento, pero aún más importante es que no se aplicó la generación de los códigos hash para cada dispositivo USB, esta técnica informática permite el aseguramiento de la integridad de las pruebas digitales. La función que cumple es mitigar las dificultades o errores de los sectores de los dispositivos de almacenamiento de la información que pudieran afectar la integridad de los datos, dando una alta fiabilidad de autenticidad e integridad de la información, la aplicación de esta herramienta hubiera permitido tener la seguridad que se trataban de los mismos dispositivos y evitar la suspicacia que planteo la defensa técnica de los procesados, por lo que la autoridad judicial dispuso que dichas pruebas no sean consideradas en el proceso.

En el empleo de pruebas mediante impresos o pantallazos de aplicativos de redes sociales o sistemas de mensajería instantánea, debe ser abordada con cautela y mucho cuidado ya que existe la posibilidad de manipulación de los archivos digitales, debido al anonimato que autorizan estos sistemas y la libre creación de cuentas con una identidad fingida, hacen la posibilidad de aparentar una comunicación, es por ello que es necesario la práctica de una prueba pericial que identifique que sea el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido.

VI. Conclusiones

Primera conclusión.

Los delitos informáticos se desarrollan en el ciberespacio en conexión con internet, la ciberdelincuencia ha dado lugar a los delitos transnacionales donde las leyes no tiene alcance y jurisdicción al involucrar a varios países en un solo hecho, quedando impunes y sin sanción penal, ello también viene generando grandes pérdidas a personas e instituciones públicas y privadas tanto económicas así como de credibilidad en los servicios a sus clientes. Los ciberdelincuentes en el desarrollo de su actividad ilícita dejan las evidencias digitales, que son los rastros o huellas del delito, siendo el origen de la investigación con participación de la Policía y los operadores de justicia.

Segunda conclusión.

A pesar de que el Derecho Penal ha cedido la presión del avance tecnológico de la informática no existe un tratamiento especial de la evidencia digital en el Nuevo Código Procesal Penal, ya que el manejo se da bajo la observancia del Art. 185º dentro de la prueba documental; es decir, las evidencias de los delitos que se cometen a través de los correos, publicaciones a través de páginas web, WhatsApp, redes sociales como Twitter, Facebook, entre otros que constituyen evidencia digital, son tratados como prueba documental, a ello se suma los operadores de justicia jueces, fiscales, abogados litigantes y el personal de la Policía Nacional no están capacitados en el manejo de procedimientos de hallazgo, recojo, tratamiento y traslado de las evidencias digitales que es la Cadena de custodia ya que la evidencia digital es tratada como una evidencia física en común, al no existir procedimientos establecidos en nuestro ordenamiento jurídico, no se garantiza la preservación de su integridad y autenticidad, muy por el contrario se contamina, perdiendo su valor probatorio para un proceso judicial. Actualmente existe un Manual de evidencia digital, en nuestro país formulado por representantes del Ministerio Publico y la Divindat PNP auspiciado por el gobierno de EEUU. En donde se ha diseñado procedimientos y acciones sofisticadas en aseguramiento, protección y análisis, con conocimientos y técnicas avanzadas en impedir la

alteración y destrucción de la evidencia digital. Actualmente no está autorizado su empleo en la PNP.

Tercera conclusión.

Países como España, Colombia y Argentina son referentes en el tratamiento de la evidencia digital y la lucha contra la ciberdelincuencia, al haber desarrollado mejores condiciones de legalidad y capacitación, habiendo generado mejores ingresos, confiabilidad y desarrollo para sus países. Asi mismo emplean herramientas tecnológicas que ayudan a mantener la originalidad de la evidencia digital las cuales son respaldadas en su empleo con personal capacitado y certificado, así como el empleo de equipos tecnológicos con aplicaciones licenciadas. El Convenio de Budapest, es la única norma internacional sobre legislación en ciberdelincuencia, en lo penal así como en procedimientos y de cooperación internacional, con comunicación permanente, asesoramiento y apoyo técnico en la lucha contra la ciberdelincuencia en el mundo. El Perú a la fecha no se adherido a dicho convenio.

Cuarta conclusión.

Existe normas internacionales en la Unión Europea (UNES), así como del Organismo Internacional de Estandarización (ISOS) que brindan procedimientos tecnológicos para el valor probatorio de la evidencia digital, así como ofrece orientación, coordinación, simplificación y unificación de criterios a las empresas y organizaciones. Herramientas como el sellado del tiempo que sirven para mostrar que determinados datos existen y que no han sido modificados desde su origen, Computer Forensic, Móvil Forensic, Network Forensic, Database Forensic, los Metadatos, Live Forensics, todas ellas buscan preservar integridad y originalidad a la evidencia digital**.**

VII. Recomendaciones

Primera recomendación.

Que el Congreso de la República como institución con iniciativa legislativa, apruebe la adhesión del Perú al convenio de Budapest, la misma que esta lista para ser aprobada por el pleno del Congreso con dictamen favorable, puesto que en América solo lo han ratificado: USA, Canadá, Panamá, República Dominicana , Chile, Argentina y Colombia, ya que al no existir una legislación uniforme en delitos informáticos genera dualidad de delitos y problemas de interpretación dogmática, y además, la migración de la ciberdelincuentes a esta parte del planeta ya que la ciberdelincuencia, sabe que la legislaciones diferentes en cada país latinoamericano son una ventaja para que estas nuevas conductas delictivas sigan cubiertas bajo el manto de la impunidad al ser considerados delitos transnacionales.

Segunda recomendación.

Teniendo en cuenta que la evidencia digital no cuenta con un tratamiento especial en el Nuevo Código Procesal Penal del 2004, y su regulación está implícito dentro de la prueba documental tipificado en el Artículo 185º del Código Procesal Penal; sugerimos una regulación especial, sobre el tratamiento adecuado de la evidencia digital, respecto a su independencia y autonomía, con la finalidad de garantizar la autenticidad y valoración procesal. Sugerimos que el Ministerio Publico y la Policía Nacional del Perú gestionen una partida presupuestal, tanto para la implementación de equipos tecnológicos como capacitación, debidamente acreditados y licenciadas con tecnología de punta que permita crear instrumentos de control y seguridad en el tratamiento de la evidencia digital. Así mismo debe dársele mayor apoyo a la División de Investigación de Delito de Alta tecnología de la PNP; en capacitar al personal en el manejo tecnológico de la evidencia digital, y que el Comando de la Policía Nacional apruebe y disponga el uso del Manual de evidencia digital diseñado con apoyo del gobierno de EEUU.

Tercera recomendación.

Se deben crear Fiscalías especializadas en delitos informáticos para que la investigación y sanción de estos delitos sea eficiente, más cuando el avance de la informática es mucho más acelerado, son delitos emergentes en aumento y la comisión suele ser cada vez más sofisticados. Así mismo en todas las Universidades se debe incluir en la malla curricular de la carrera de derecho en el pre y postgrado, un curso obligatorio de derecho informático, y el estudio de la ciberdelincuancia y ciberdefensa, de igual manera en el nivel de formación escolar tanto de primaria y secundaria se debe incluir en las unidades de aprendizaje el curso de informática, no solo de como utilizar equipos o programas sino tener un énfasis en la prevención de todo tipo de delitos informáticos.

Cuarta recomendación.

Si bien es cierto que en la actualidad hay entidades privadas en el Perú, que hacen los mejores esfuerzos para protegerse del ataque de la ciberdelincuencia, como por ejemplo la Asociación de Bancos del Perú, que sin tener el respaldo legal que el Estado tiene por obligación que brindarles por falta de normas que protejan el tratamiento de la evidencia digital ante acciones delictivas en contra del sistema financiero tal como lo evidencia las estadísticas presentada por la División de Alta Tecnología del Perú; se recomienda que la Presidencia de Concejo de Ministros a través de la Secretaria de Gobierno Digital, tome los modelos que las entidades privadas vienen empleando para proveer y combatir los ciberdelitos, basados en el cumplimiento de normas de la Unión Europea así como normas ISO respecto a los procedimientos de preservación y el cuidado de la integridad de la evidencia digital y lo aplique a las entidades del Estado, ya en realidad se encuentran totalmente desprotegidas y que en un posible ciberataque las consecuencias serían muy lamentables para el país.

VIII. Referencias bibliográficas

Di lorio, A. y Castallote, M. (2016). *El rastro digital del delito. Aspectos técnicos, legales y estratégicos de la Informática Forense*. Universidad FASTA ediciones Mar del Plata. Recuperado de https://bit.ly/2SqOKw8.

Diario Oficial No. 43.673. (1999). *Ley 527*. Colombia. Recuperado de https://bit.ly/2Dyl4Ic.

Ediciones legales. (2015). *Código Orgánico General de Procesos*. Recuperado de https://bit.ly/2KlJeIl.

E-gobierno, inclusión digital y sociedad del conocimiento. (2012). *Evidencia Digital en Colombia: Una reflexión en la práctica*. Recuperado de https://bit.ly/2fmgvSL.

Fiscalía de la Nación. (15 de junio de 2006). *Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados*. Recuperado de https://bit.ly/2RZy6Ua.

Instituto Nacional de Ciberseguridad. (2014). RFC 3227 - *Directrices para la recopilación de evidencias y su almacenamiento. España*. Recuperado de https://bit.ly/2QUi0Lj.

Jiménez, J. (2017). *Manual de Derecho Penal Informático*. (1.a ed.). Perú: Jurista Editores

Justo, M. (2017). *Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal*. (Proyecto financiado por Ford Foundation). Recuperado de https://bit.ly/2RumV9F.

Lasso, V. (2017). *Estado del peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia.* (Monografía para optar al título de Especialista en Seguridad Informática. Universidad Nacional abierta y a distancia, Escuela de Ciencias Básicas Tecnología e Ingeniería Especialización en Seguridad Informática, Palmira).

Recuperado de https://bit.ly/2RzcxgQ.

Lexis. S. A. (2009). *Código Orgánico de la función Judicial*. Recuperado de https://bit.ly/29funy2.

Ministerio de Asuntos Exteriores Madrid España. (2002). *Convenio sobre ciberdelincuencia*. Recuperado de https://bit.ly/2OU44PR.

Ministerio de Justicia, Derechos Humanos y Cultos. (2014). *Código Orgánico Integral Penal*. Recuperado de https://bit.ly/2twibTE.

Obando, V. (2013). *La valoración de la prueba*. Recuperado de: https://bit.ly/2ouSAFA.

Porta de e-gobierno, inclusión digital y sociedad del conocimiento. (2012). *Evidencia digital en Colombia: Una reflexión práctica*. Recuperado de https://bit.ly/2fmgvSL.

Proyecto de apoyo al sector justicia EEUU y Ministerio de Justicia y DDHH del Perú. (2017). *Manual de evidencia digital*. Recuperado de https://bit.ly/2TCWnAr.

Publicación oficial diario el peruano. (13 de setiembre de 2018). *Ley de gobierno digital*. Recuperado de https://bit.ly/2xgErSo

Publicación oficial diario el peruano. (2014). *Ley que modifica la ley 30096, Ley de Delitos Informáticos*. Recuperado de https://bit.ly/2AaF0yL.

Rodríguez, M. (2018). *La prueba digital en el proceso penal.* (Tesis de maestría. Ilustre Colegio de Abogados de Santa Cruz de Tenerife). Recuperada de https://bit.ly/2TCdLoW.

Revista Academia & Derecho Universidad Libre Seccional Cúcuta - Facultad de Derecho (2016). *La evidencia digital eximente de violación a la*

protección del dato personal a partir de la autorregulación. Recuperado de https://bit.ly/2A8IJwB.

Sequeiros, I. (2015). *Vacíos legales que imposibilitan la sanción de los delitos informáticos en el Nuevo Código Penal Peruano-201*5. (Tesis para optar el Título profesional de Abogado. Universidad de Huánuco). Recuperado de https://bit.ly/2Fa4Kjy.

Villavicencio, F. (Diciembre 2014). Delitos Informáticos Revista PUC ius et veritas, N° 49. Recuperado de https://bit.ly/2QcLkjb.

IX. Anexos

Instrumentos

Guía de entrevista semiestructurada a representante del Ministerio Público

Fecha:	**Lugar:**
Hora de inicio de grabación:	Hora de término de grabación:
Entrevistado:	**Entrevistador:**

Introducción:
Señor representante del Ministerio Publico, le solicité esta entrevista por la importancia que tiene el analizar y determinar la importancia de la evidencia digital, como medio de prueba en los procesos judiciales en la lucha contra los delitos informáticos, teniéndose en consideración que son tratadas como evidencias documentales comunes, al no existir normas jurídicas para su admisibilidad y valor probatorio. Le realizaré algunas preguntas a los cuales les pido me respondan con confianza, y para no perder ningún detalle de sus respuestas se grabará la entrevista. Agradezco su colaboración.

Preguntas
1. ¿Qué es la ciberdelincuencia y si es una modalidad delictiva considerada en el Código Penal Peruano?
2. ¿Qué es el ciberespacio o el territorio donde se desarrolla la ciberdelincuencia?
3. ¿Qué son delitos transnacionales?
4. ¿Cuál es bien jurídico protegido en los delitos informáticos?
5. ¿Al ser los delitos informáticos delitos transnacionales, las leyes peruanas que han previsto para que estos no queden impunes?
6. ¿El Perú se encuentra en condiciones jurídicas de poder sancionar los delitos informáticos?
7. ¿Cree Ud. que la normatividad jurídica en el país, ha previsto el tratamiento de la evidencia digital?
8. ¿Conoce Ud. el convenio de Budapest?
9. ¿Cuál es el concepto de la evidencia digital en el ámbito jurídico?
10. ¿Qué significa para Ud. La cadena de custodia y si esta se aplica para la evidencia digital?
11. ¿Considera Ud. que el personal de la Policía Nacional del Perú está en condiciones de tratar adecuadamente la evidencia digital?
12. ¿Considera Ud. si el Estado está abordando la lucha de ciberdelincuencia de manera eficaz?
13. ¿Si conoce Ud. de algún país que actualmente viene enfrentando adecuadamente la lucha contra la ciberdelincuencia desde el ámbito judicial?
14. ¿Cree Ud. que organizaciones privadas y/o particulares vienen aplicando soluciones para contrarrestar la ciberdelincuencia?
15. ¿Conoce de herramientas tecnológicas o jurídicas eficaces que ayuden a dar la legalidad a las evidencias digitales?

Instrumentos

Guía de entrevista semiestructurada a representante de la Policía Nacional del Perú

Fecha:	**Lugar:**
Hora de inicio de grabación:	Hora de término de grabación:
Entrevistado:	**Entrevistador:**

Introducción:

Señor representante de la Policía Nacional del Perú, le solicité esta entrevista por la importancia que tiene el analizar y determinar la importancia de la evidencia digital, como medio de prueba en los procesos judiciales en la lucha contra los delitos informáticos, teniéndose en consideración que son tratadas como evidencias documentales comunes, al no existir normas jurídicas para su admisibilidad y valor probatorio. Le realizaré algunas preguntas a los cuales les pido me respondan con confianza, y para no perder ningún detalle de sus respuestas se grabará la entrevista. Agradezco su colaboración.

Preguntas

1. ¿Qué es la ciberdelincuencia y si es una modalidad delictiva considerada en el Código Penal Peruano?
2. ¿Qué es el ciberespacio o el territorio donde se desarrolla la ciberdelincuencia?
3. ¿Qué son delitos transnacionales?
4. ¿Cuál es bien jurídico protegido en los delitos informáticos?
5. ¿Al ser los delitos informáticos delitos transnacionales, las leyes peruanas que han previsto para que estos no queden impunes?
6. ¿El Perú se encuentra en condiciones jurídicas de poder sancionar los delitos informáticos?
7. ¿Cree Ud. que la normatividad jurídica en el país, ha previsto el tratamiento de la evidencia digital?
8. ¿Conoce Ud. el convenio de Budapest?
9. ¿Cuál es el concepto de la evidencia digital en el ámbito policial?
10. ¿Qué significa para Ud. La cadena de custodia y si esta se aplica para la evidencia digital?
11. ¿Considera Ud. que el personal de la Policía Nacional del Perú está en condiciones de tratar adecuadamente la evidencia digital?
12. ¿Considera Ud. si el Estado está abordando la lucha de ciberdelincuencia de manera eficaz?
13. ¿Si conoce Ud. de algún país que actualmente viene enfrentando adecuadamente la lucha contra la ciberdelincuencia desde el ámbito policial?
14. ¿Cree Ud. que organizaciones privadas y/o particulares vienen aplicando soluciones para contrarrestar la ciberdelincuencia?
15. ¿Conoce de herramientas tecnológicas o jurídicas eficaces que ayuden a dar la legalidad a las evidencias digitales?

Instrumentos

Guía de entrevista semiestructurada a experto en Tecnología de la información y comunicación en el Sistema Financiero Nacional

Fecha:	**Lugar:**
Hora de inicio de grabación:	Hora de término de grabación:
Entrevistado:	**Entrevistador:**

Introducción:
Señor representante del Sistema financiero nacional, le solicité esta entrevista por la importancia que tiene el analizar y determinar la importancia de la evidencia digital, como medio de prueba en los procesos judiciales en la lucha contra los delitos informáticos, teniéndose en consideración que son tratadas como evidencias documentales comunes, al no existir normas jurídicas para su admisibilidad y valor probatorio. Le realizaré algunas preguntas a los cuales les pido me respondan con confianza, y para no perder ningún detalle de sus respuestas se grabará la entrevista. Agradezco su colaboración.

Preguntas
1. ¿Qué es la ciberdelincuencia y si es una modalidad delictiva considerada en el Código Penal Peruano?
2. ¿Qué es el ciberespacio o el territorio donde se desarrolla la ciberdelincuencia?
3. ¿Qué son delitos transnacionales?
4. ¿Cuál es bien jurídico protegido en los delitos informáticos?
5. ¿Al ser los delitos informáticos delitos transnacionales, las leyes peruanas que han previsto para que estos no queden impunes?
6. ¿El Perú se encuentra en condiciones jurídicas de poder sancionar los delitos informáticos?
7. ¿Cree Ud. que la normatividad jurídica en el país, ha previsto el tratamiento de la evidencia digital?
8. ¿Conoce Ud. el convenio de Budapest?
9. ¿Cuál es el concepto de la evidencia digital en el ámbito de la tecnología?
10. ¿Qué significa para Ud. La cadena de custodia y si esta se aplica para la evidencia digital?
11. ¿Considera Ud. que el personal de la Policía Nacional del Perú está en condiciones de tratar adecuadamente la evidencia digital?
12. ¿Considera Ud. si el Estado está abordando la lucha de ciberdelincuencia de manera eficaz?
13. ¿Si conoce Ud. de algún país que actualmente viene enfrentando adecuadamente la lucha contra la ciberdelincuencia desde el ámbito financiero?
14. ¿Cree Ud. que organizaciones privadas y/o particulares vienen aplicando soluciones para contrarrestar la ciberdelincuencia?
15. ¿Conoce de herramientas tecnológicas o jurídicas eficaces que ayuden a dar la legalidad a las evidencias digitales?

Transcripción de datos

Entrevista Nro 1 RMP

1. **¿Qué es la ciberdelincuencia y si es una modalidad delictiva considerada en el Código Penal Peruano?**

Consiste básicamente en cualquier delito o actividad ilegal cometido con la ayuda de un ordenador o internet contra una persona, sus bienes, negocios o el propio gobierno, y también se le conoce como delito informático. Existe una amplia variedad de cometer un delito informático. Si alguien piensa cometer un delito tradicional requiere de un montón de cosas y el riesgo es también muy alto sin embargo, para cometer un delito informático, la única necesidad está ahí, un ordenador con conexión a internet y las propias habilidades de la persona de tal forma que es capaz de hacerlo desde la intimidad de su propio hogar.

2. **¿Qué es el ciberespacio o el territorio donde se desarrolla la ciberdelincuencia?**

El Ciberespacio se ha constituido como un nuevo mundo digital o virtual, sin fronteras físicas. Un nuevo mundo que no puede ser ajeno al derecho y a los distintos ordenamientos jurídicos que vertebran nuestro civilizado y moderno mundo. Pero claro, en un mundo donde el espacio físico no existe pero sí el tiempo Inmaterial, carente de materia. No hay fronteras físicas, sin Gobiernos o Estados democráticos o autoritarios, en él conviven ciberciudadanos y ciberorganizaciones y coexisten conductas aceptables y otras no aceptables éticamente por los ciudadanos del otro mundo.

3. **¿Qué son delitos transnacionales?**

Cuando el delito informático es trasnacional cualquier intento regulatorio Estatal es ineficaz, por ende se patentiza la necesaria aprobación de un tratado internacional que unifique criterios, tanto sustanciales como procesales y establezca las pautas a seguir en tema de cooperación judicial internacional, de lo contrario, será imposible disminuir los altos índices de impunidad registrados en esta materia.

4. **¿Cuál es bien jurídico protegido en los delitos informáticos?**

El bien jurídico que pone en peligro el delito informático es 'la información: (almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos).

5. **¿Al ser los delitos informáticos delitos transnacionales, las leyes peruanas que han previsto para que estos no queden impunes?**

En los delitos informáticos se necesita trabajar en conjunto con otros países ya que no es un delito solo local, también es transnacional. Actualmente el tratado internacional que rige es el Convenio de Budapest o Convenio sobre ciberdelincuencia, creado para combatir el delito informático y generar la cooperación entre los países al cual aún el Perú no se adherido. El aumento de la criminalidad informática en el Perú y a nivel mundial trae consigo consecuencias económicas y numerosos fraudes cometidos por organizaciones delictivas que muchas veces no son denunciados o cuyos delitos son cometidos en el exterior sin que muchas veces exista una sanción.

6. **¿El Perú se encuentra en condiciones jurídicas de poder sancionar los delitos informáticos?**

La legislación existente resulta insuficiente, toda vez que continuamente se renuevan las modalidades delictivas en el ámbito informático, asimismo si se tiene presente que en nuestro país las herramientas existentes para contrarrestar dichos ilícitos no resultan ser suficientes, y que poco es el efecto disuasivo en la proliferación del mismo. Aún falta no solo legislar sobre las nuevas actividades delictivas, sino también difundir y explicar la nueva criminalidad informática en su connotación holística.

7. **¿Cree Ud. que la normatividad jurídica en el país, ha previsto el tratamiento de la evidencia digital?**

Tratamiento especial de la prueba digital en el Código Procesal Penal del 2004 de manera puntual y especifica No existe, no hay regulación actual como prueba digital, sin embargo el Art. 185 del código procesal penal reconoce al contenido de un audio visual o audio grabado como prueba documental, si entre las fuentes de prueba de un hecho ilícito se encontrara un audio, o un video grabación u otro soporte digital o electrónico, simplemente el desahogo probatorio o actuación

probatorio se efectúa en observación del artículo 382 del código procesal penal del 2004.

8. ¿Conoce Ud. el convenio de Budapest?

El Convenio de Budapest es un tratado internacional creado por los países miembros del Consejo de Europa con el fin de hacer frente a los delitos informáticos a través de mecanismos de homologación de normas de derecho penal sustantivo, estandarización de procesos penales y cooperación internacional.

9. ¿Cuál es el concepto de la evidencia digital en el ámbito jurídico?

La evidencia digital como un tipo de prueba física en donde sus datos pueden ser recolectados, almacenados y analizados con herramientas informáticas forenses y técnicas especiales. Si se la compara con otras formas de evidencia, la prueba digital es única. Si la evidencia fue presentada de manera correcta y su cadena de custodia no fue alterada, puede llegar a ser crucial para resolver cualquier clase de delitos.

10. ¿Que significa para Ud. La cadena de custodia y si esta se aplica para la evidencia digital?

La Cadena de Custodia es el procedimiento destinado a garantizar la individualización, seguridad y preservación de los elementos materiales y evidencias, recolectados de acuerdo a su naturaleza o incorporados en toda investigación de un hecho punible, destinados a garantizar su autenticidad, para los efectos del proceso.

11. ¿Considera Ud. que el personal de la Policía Nacional del Perú está en condiciones de tratar adecuadamente la evidencia digital?

Existe una una insuficiencia de implementación de laboratorios a nivel nacional y existe un centralismo en todo el Perú para las pericias de pruebas digitales y de las tradicionales, para los delitos más comunes se sigue haciendo en Lima. Incluso para los delitos informáticos es más complejo se tiene que remitir a DIVINDAT-PNP de la Av. España y dicha división no existe en el Callao.

12. ¿Considera Ud. si el Estado está abordando la lucha de ciberdelincuencia de manera eficaz?

Considero que necesitamos promover la creación e implementación de Fiscalías Especializadas en Cibercrimen a fin de enfrentar adecuadamente los diversos delitos informáticos a fin de llevar a cabo investigaciones eficientes. El Perú requiere de una política de estado sobre el manejo de internet y desarrollar una campaña de educación entre escolares y adolescentes para que sepan proteger su información en la red.

13. ¿Si conoce Ud. de algún país que actualmente viene enfrentando adecuadamente la lucha contra la ciberdelincuencia desde el ámbito judicial?

Si considero que Colombia y Argentina en América Latina vienen promulgándose leyes que contribuyen a mejorar y dotar de los instrumentos legales contra la lucha del cibercrimen.

14. ¿Cree Ud. que organizaciones privadas y/o particulares vienen aplicando soluciones para contrarrestar la ciberdelincuencia?

Las empresas tecnológicas son un aliado indispensable en la lucha contra la ciberdelincuencia. Es necesario aumentar la participación de los sectores público y privado para abordar inquietudes comunes como mejorar la educación y poner freno al material de abuso en línea.

15. ¿Conoce de herramientas tecnológicas o jurídicas eficaces que ayuden a dar la legalidad a las evidencias digitales?

En materia procesal me documente sobre la utilización del remote forensic como herramientas de investigación. Ella sugiere a los países la adopción de una norma a nivel nacional que prevea estas técnicas de investigación previendo la excepcionalidad de la medida y un uso restrictivo atendiendo a la potencialidad de afectación a la intimidad que significa su uso.

Transcripción de datos

Entrevista Nro 2 PNP

1. **¿Qué es la ciberdelincuencia y si es una modalidad delictiva considerada en el Código Penal Peruano?**

La ciberdelincuencia es una actividad delictiva realizada mediante el uso de las TICs. Actualmente existe la Ley Nro. 30096 y su modificatoria 30171, que sanciona algunas conductas delictivas.

2. **¿Qué es el ciberespacio o el territorio donde se desarrolla la ciberdelincuencia?**

Se podría decir que es espacio virtual, sin límites, donde se puede interactuar con otras personas únicamente a través de una conexión a la red.

3. **¿Qué son delitos transnacionales?**

Son aquellos delitos que se comente en dos o más países, por ejemplo un fraude informático que se comete desde Perú a una entidad financiera extranjera.

4. **¿Cuál es bien jurídico protegido en los delitos informáticos?**

La información de manera general es el valor jurídico protegido pero existen otros como la indemnidad sexual, intimidad y el patrimonio.

5. **¿Al ser los delitos informáticos delitos transnacionales, las leyes peruanas que han previsto para que estos no queden impunes?**

Ninguna, ya que el Perú aun no forma parte del Convenio sobre ciberdelincuencia (Convenio de Budapest).

6. **¿El Perú se encuentra en condiciones jurídicas de poder sancionar los delitos informáticos?**

No, para que suceda ello tendría que crearse una Fiscalía Especializada.

7. **¿Cree Ud. que la normatividad jurídica en el país, ha previsto el tratamiento de la evidencia digital?**

No existe una normativa aborde sobre el tratamiento de la evidencia digital, sin embargo existe un manual de evidencia digital promovido por una ONG, que recoge las buenas prácticas de otros manuales para el manejo de la evidencia digital. En tanto, la PNP ha elaborado un manual para el recojo de la evidencia digital, que se encuentra a la espera de su aprobación.

8. **¿Conoce Ud. el convenio de Budapest?**

Es un Convenio sobre ciberdelincuencia o llamado Convenio de Budapest, firmado en el 2001 que busca hacer frente a los delitos cometidos a través de la Internet, mediante la cooperación de los países que la integran y el sector privado.

9. **¿Cuál es el concepto de la evidencia digital en el ámbito policial?**

Cualquier registro generado por o almacenado en un sistema informático o dispositivo digital que pueda ser utilizado como prueba en un proceso legal.

10. **¿Que significa para Ud. La cadena de custodia y si esta se aplica para la evidencia digital?**

Procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis, normalmente peritos, y que tiene fin no viciar el manejo que de ellos se haga y así evitar alteraciones, sustituciones, contaminaciones o destrucciones. La cadena de custodia se aplica tanto a la evidencia física así como a la evidencia digital.

11. **¿Considera Ud. que el personal de la Policía Nacional del Perú está en condiciones de tratar adecuadamente la evidencia digital?**

Si, la Policía Nacional del Perú, cuenta con personal capacitado que viene laborando en la División de Investigación de Delitos de Alta Tecnología -DIRINCRI.

12. **¿Considera Ud. si el Estado está abordando la lucha de ciberdelincuencia de manera eficaz?**

Considero que el Estado tiene mucho por hacer en materia de ciberdelincuencia, modalidad

delictiva que viene creciendo debido a que las personas emplean hoy más que ayer tecnología en su vida personal así como laboral, esto conlleva a las posibilidades de ilícitos informáticos.

13. **¿Si conoce Ud. de algún país que actualmente viene enfrentando adecuadamente la lucha contra la ciberdelincuencia desde el ámbito judicial?**

Podría mencionar a España, que cuenta con personal contantemente capacitado y la tecnología adecuada, dentro de la región se encuentran Colombia y Brasil.

14. **¿Cree Ud. que organizaciones privadas y/o particulares vienen aplicando soluciones para contrarrestar la ciberdelincuencia?**

Las empresas privadas en los últimos años han tomado conciencia de los peligros a los que se encuentra expuesto su información, para ello vienen implementando políticas de seguridad para proteger sus activos.

15. **¿Conoce de herramientas tecnológicas o jurídicas eficaces que ayuden a dar la legalidad a las evidencias digitales?**

El Triage consiste en realizar una búsqueda rápida empleando criterios sencillos sobre la estructura del disco, evitando profundizar las búsquedas en áreas especiales del disco. La realización de una copia o imagen forense, en la escena de delito mediante una copia bloque a bloque bit a bit del contenido digital almacenado, el que es autenticado mediante una función HASH.

Transcripción de datos

Entrevista Nro 3 TIC

1. **¿Qué es la ciberdelincuencia y si es una modalidad delictiva considerada en el Código Penal Peruano?**

La Ciberdelincuencia es un delito que está focalizado o se desarrolla en el ámbito del internet, generalmente es el canal que utiliza el delincuente para cometer delitos, claro se tipifica el delito cuando existe una norma una ley que así lo define, pero en nuestro país por ejemplo un botmaster no tendría ninguna sanción, en Estados Unidos un botmaster puede ser condenado a 15 años de prisión entonces, que es el ciberdelito son delitos que se realizan principalmente en el canal de Internet pero para ser considerados como delitos tiene que tener una tipificación.

2. **¿Qué es el ciberespacio o el territorio donde se desarrolla la ciberdelincuencia?**

El ciberdelito qué va por el internet es global, la razón es muy simple para poder comunicarnos entre nuestras redes locales en nuestro país y con otros países, tenemos que usar la misma tecnología, al usar la misma tecnología usamos equipos de comunicación, medios de enlace, protocolos de comunicación y configuraciones eso hace que todos nosotros nos podamos comunicar. Entonces tu pregunta iba sobre el ciberespacio que es el ámbito en el cual se desarrolla o se transmite información piezas de información usando protocolos, equipos y medios de comunicación estándar.

3. **¿Qué son delitos transnacionales?**

Las redes están conectadas a nivel global y no tienen un problema de idioma, porque ellos usan su propio mecanismo de entendimiento, los equipos, los medios de comunicación, los protocolos son estándar es lo que permite el sistema de comunicación, entonces tú pregunta era las fronteras, no hay fronteras porque todo es relativo o sea él delito se puede producir aquí o en un país de Sudamérica o en Europa o en Estados Unidos y eso se hacen milisegundos, porque estamos en la misma red. Aquí no hay un tema de países porque si hablamos de territorialidad los conceptos hay que cambiarlos, que sucede antes por ejemplo para proteger el dinero de un banco se hacían grandes bóvedas, se ponían medidas de seguridad electrónicas las llaves y los discos para proteger puertas muy pesadas, paredes de concreto para proteger el dinero pero ahora en el ciberespacio ese dinero que hay en una bóveda de un banco no lo puedes consumir, entonces lo que tratan de hurtar es la información, el activo se convierte de un medio físico papel, barra de oro o un artículo valioso, hoy se convierte en números de cuenta códigos de acceso identidad de las personas etc. y ahí hay una gran vulnerabilidad que nace desde el diseño de la red, porque la red a estado preparada para identificar equipos, medios de comunicación, protocolos y eso en 7 capas que la última era la interface y los programas que te dan acceso al manejo de todas estas anteriores, pero nunca estuvo pensado, la red para identificar a personas, entonces ahora se está trabajando, esta es información ultima que pocas personas la conocen, se está desarrollando últimamente la capa 8 que va a identificar a las personas como parte de la información que circula por internet por eso que es cuando se habla del ciberdelincuente, se habla del ciberespacio, se habla del ámbito jurisdiccional o sea se habla de cosas que no identifican a las personas se está hablando de medios, se está hablando de equipos, se está hablando de otras cosas y no se hablan de la persona, entonces si estamos hablando del ciberdelincuente cómo puedes identificarlo, porque ahora los ataques los hacen robots, piezas de Software que son los que hacen los ataques, sobre qué jurisdicción estamos hablando, cuál es la jurisdicción que estamos protegiendo, entonces todo estado unido es una sola pieza es una sola jurisdicción, porque en el concepto de la red es precisamente global es como decir que yo puedo respirar aire de Perú si voy a otro país No puedo respirar el aire, porque tengo que ser ciudadano ese país para poder respirar ese aire es un derecho, entonces estamos hablando de la vida, entonces el concepto de jurisdicción cambia por eso es que nosotros hemos impulsado, los acuerdos internacionales. Por eso que es importante y siempre lo hemos dicho que Perú se suscriba a la comisión de Budapest y como todavía tenemos representantes que no entienden este tema de la jurisdicción y la necesidad de establecer alianzas e iniciativas globales. La asociación de bancos si lo ha entendido y nosotros nos hemos suscrito “el llamamiento de Paris para la confianza y la seguridad del ciberespacio” iniciativa del presidente francés Emmanuel Macron, que ha invitado a grandes empresas globales, asociaciones y empresas que trabajan en el internet para generar espacios que sean seguros, porque son iniciativas que debemos hacer, si el país no lo entiende así y también sus representantes, las instituciones tienen que volverse globales.

4. **¿Cuál es bien jurídico protegido en los delitos informáticos?**

Es el dato, lo que hay que proteger es el dato, porque la información ya son los datos que ya están procesados Entonces el bien jurídico protegido es el dato.

5. **¿Al ser los delitos informáticos delitos transnacionales, las leyes peruanas que han previsto para que estos no queden impunes?**

Mira hay un antecedente que te pueden interesar en el 2008, Estonia sufrió el ataque más grande de ciberdelincuencia, cuando se hizo el análisis resulta que fue en el Perú donde se había generado la mayoría de ataques, entonces Estonia fue a las naciones Europeas a solicitar una sanción para Perú, pero justamente haciendo el análisis se demostró que no se podía sancionar a nuestro país porque no había un tema intencional de ataque de un país hacia otro. el presidente Obama en una de sus edictos o pronunciamiento síndico de qué Estados Unidos podría repeler con la fuerza de sus fuerzas armadas un ataque Cibernético identificado en otro país, entonces ahí te doy dos ejemplos y el otro tema es del china con las elecciones de Estados Unidos donde se puede apreciar de que se puede influir desde un país hacia otro, usando las redes sociales, el internet, la información no precisa y técnicas de ingeniería social que son los que más se utiliza para engañar a las personas.

6. **¿El Perú se encuentra en condiciones jurídicas de poder sancionar los delitos informáticos?**

Considero que no, esté es muy simple, tenemos 3 artículos del año 2000 y la ley delitos informáticos del año 2013, que salió después de 8 años porque nosotros insistimos en la necesidad de que haya una ley, pero eso fue producto del hackeo de una cuenta de la esposa de un funcionario del Estado, eso fue el motivo por el cual se buscó, cuál proyecto había para aprobarlo; cuando nosotros proponemos que Perú se adhiera al a la convención de Budapest, no solamente estamos hablando de una iniciativa que nos pone a nivel Global en el primer mundo, estamos hablando de que el consejo de Europa tiene destinado fondos para qué países como los nuestros, puedan adecuar su legislación y puedan tipificar y sancionar efectivamente los delitos informáticos, nosotros no entendemos que cosa es un delito informático en el Perú no se entiende que es un delito informático, porque no saben en donde nos estamos desarrollando en donde nos desenvolvemos, entonces mal podemos nosotros tipificar y sancionar algo como que te comentaba que en Estados Unidos pueden sancionar a un botmaster 15 años y en el Perú no exista, hemos tenido casos de ciudadanos de otras nacionalidades en Sudamérica con más de 100 tarjetas en un cajero automático y no se le pudo detener por delito informático porque acá ese señor es coleccionista de tarjeta y no es un clonador.

7. **¿Cree Ud. que la normatividad jurídica en el país, ha previsto el tratamiento de la evidencia digital?**

Considero que eso es importante, pero que no exista en nuestro ordenamiento jurídico es un reflejo simplemente y de nuestra sociedad que nosotros nos gusta ir por el camino corto no respetamos las reglas; en la mañana estaba conversando con un taxista que me traía y hablábamos del callao, en el callao han puesto algo de tecnología con sistema de videocámaras, no es una ciudad inteligente sino que simplemente son cámaras que están conectadas a equipos para poder detectar la velocidad y todo el mundo anda 60 pero apenas cruza la línea que dice callao hacia lima, aumenta su velocidad a 80 o 90, cuál es la diferencia porque en dos cuadras uno puede ver ciudadanos yendo a 60 y a la siguiente cuadra a 80. Porque hay un sector, un territorio donde se cumple con la ley y esta se cumple con una sanción hay una pena en el otro lado no hay una sanción, entonces donde no se regula adecuadamente las cosas la gente hace lo que quiere, en el ciberespacio es exactamente es igual, porque nuestro país a esto el delincuente lo llama paraísos cibernético, es donde no hay la norma, no hay el procedimiento, no hay la pena entonces está libre y ejemplo de estos hay muchos en Argentina había un delincuente denominado el Gordo España, esta persona había cometido una cantidad de delitos terribles en España y le solicita a la Argentina la deportación, para ello argumentan todo y presentan sus leyes y lo demuestra muy bien todo perfecto, pero cuando llega a la Argentina dice no la puedo mandar porque eso aquí no es delito; y yo digo no había cometido el delito en Internet en Argentina. Entonces qué pasó, pasaron dos años o tres y Argentina actualiza su legislación, qué cosa crees que hizo España mando de nuevo el pedido porque ahora si lo consideraba y lo capturaron y lo deportaron y Argentina ya está suscrito el convenio de Budapest.

8. **¿Conoce Ud. el convenio de Budapest?**

Mira aquí te doy un ejemplo clarísimo en Colombia tuve la oportunidad de conversar con el jefe de la policía de investigaciones de delitos cibernéticos para Europa, entonces les manifesté nuestro interés de tener contacto y poder compartir información y él también se mostró muy interesado por qué era de Perú, le dije tenemos información de ciudadanos búlgaros que han cometido delitos en Perú, como puedo hacer para pasarte esa información, me respondió y me dijo mira no puedo recibirlo porque estás en un país que no ha suscrito la convención de Budapest; yo al principio no lo entendía y luego entendí claramente lo que me estaba diciendo, ellos respetan mucho las normas y los procedimientos y recibir la información que le daba podría contaminar la evidencia o el contaminarse para poder dar testimonios posteriores, hay que tener respeto por los procedimientos y seguir los protocolos y esas cosas no las entendemos; Entonces yo le dije mira yo soy ciudadano europeo también, tengo doble nacionalidad yo como ciudadano comunitario no te puedo pasar la información y me dijo no te la puedo recibir porque estás en un país que no ha suscrito la convención de Budapest. Bueno y qué hacemos y cómo te puedo dar esa información yo quiero colaborar, entonces me dijo si la captura de esos delincuentes ha sido registrada en algún periódico, correcto donde aparezcan los nombres, tú me puedes pasar eso y yo verificar que esa información sea correcta, como es de un medio de prensa y eso poder compartirlo con la comunidad. Entonces mira la dificultad que tenemos nosotros de enfrentar a una delincuencia que es global con las limitaciones de nuestra legislación local.

9. **¿Cuál es el concepto de la evidencia digital en el ámbito de la tecnología?**

La evidencia digital es un elemento que debería tener mucha importancia, pero aquí no le dan importancia y te lo digo porque yo he visto manipular evidencias que cualquier abogado podría fácilmente solicitar que no forme parte del proceso, porque esto debe ser formalizado. Por ejemplo la persona que recolecta información o evidencia digital debe tener una certificación, debe tener una profesión, debe tener procedimientos, debe ser una autoridad y debe estar acompañado de la fiscalía; ninguna de esas cosas se dan entonces por eso te digo la evidencia digital en nuestro país lamentablemente no es de interés por falta de conocimiento.

10. **¿Qué significa para Ud. La cadena de custodia y si esta se aplica para la evidencia digital?**

La cadena de custodia es importantísimo, fíjate en el momento de recolectar la información también tienes que demostrar que tienes equipo, que has comprado con factura, que tienes software que es legal, que tiene licencia, que tienes el mecanismo utilizando software especializado para la captura de datos, no puede usar cualquier cosa como Encase o herramientas libres, porque para los procesos judiciales la evidencia tiene que ser recolectada de manera autorizada.

11. **¿Considera Ud. que el personal de la Policía Nacional del Perú está en condiciones de tratar adecuadamente la evidencia digital?**

Sobre los delitos financieros no es DIVINDAT la primera que interviene, tenemos a las Águilas Negras, porque ellos lo que van a hacer es aislar la zona y si están preparados; pero representa al 3 por 1000 de la policía, también ellos cuando van al lugar las evidencias lo derivan a la DIVINDAT.

Las Águilas Negras para algunas cosas si está preparado, pero mira los delitos informáticos cambia muy rápido es muy dinámico, entonces no estamos preparados para enfrentarlos; nosotros tenemos otra estrategia, tenemos apoyo de un Cecyt Financiero Europeo y ha sido calificado por dos años consecutivos como el mejor en Europa, entonces eso sí nos da un respaldo para poder enfrentar a una delincuencia internacional que estoy seguro que aquí podríamos hacerlo pero nos tardaríamos demasiado.

12. **¿Considera Ud. si el Estado está abordando la lucha de ciberdelincuencia de manera eficaz?**

Si claro definitivamente ahora el estado tiene personas capacitadas para enfrentar, pero creo que no están en el lugar indicado, tampoco tiene lo básico que es la norma, que se está construyendo pero lamentablemente el ambiente político influye mucho en este tema.

13. **¿Si conoce Ud. de algún país que actualmente viene enfrentando adecuadamente la lucha contra la ciberdelincuencia desde el ámbito financiero?**

Podemos mirar a Colombia que tiene una cuarta Fuerza Armada que es la ciberseguridad, pero la verdad que estaba pensando, en Argentina en Chile tú sabes que en una reunión que tuvimos de

Celaes en Miami, se presentó la representante de seguridad del Banco Famérica y hablaba sobre ciberdelitos y ella manifestó que el problema más grande que tenía el banco era el phishing, yo me preguntaba el phishing será problema para un banco tan grande, después seguir escuchando dijo que el phishing que afectaba al banco famerica era el que provenía de Perú el problema más grande del banco famerica en ese momento era el phishing qué provenía de Perú y Cuál era el motivo la calidad del engaño del phishing, entonces los peruanos porque tienen mucha imaginación y el problema de Sudamérica relacionado con ciberdelitos son los hackers peruanos y brasileros. Porque algunos han estudiado en los países de Rusia antigua, terminaron fueron captados por las bandas rusas y ya están de regreso hablan el idioma y aprendieron la tecnología, yo estoy seguro si esas personas practicaran el bien tendrían unas empresas maravillosas y producirían muchos ingresos al país pero sin embargo, se van a lo fácil y te comento algo más en Cybertec de Israel en el 2017 Benjamín Netanyahu habla al empresariado de Israel y les dice hace 5 años yo propuse alcanzar estar entre las cinco primeras economías en ciberseguridad y en el 2017 les decía a todos tus empresarios que esa meta la habían alcanzado y el 20% de la facturación de ciberseguridad global es de Israel, dime tú si no es importante, si no es algo interesante para el país, poder darle la oportunidad los jóvenes orientarlos a estudiar temas de ciberseguridad de ciberdefensa para que puedan también generar empresas que a su vez generan ingresos y desarrollo para el país.

14. **¿Cree Ud. que organizaciones privadas y/o particulares vienen aplicando soluciones para contrarrestar la ciberdelincuencia?**

Si tú quieres identificar algo y darle validez en el internet o de un medio cibernetico lo que hay que usar es certificado digital porque siempre identifica la persona, va apunta a la capa 8 que te estaba diciendo de identificación de personas, pero el certificado lo que te garantiza es que esa persona que genero el documento es quien dice ser y funciona para los teléfonos, laptops o cualquier computadora, lo importante es que tú puedas obtener ese certificado con una entidad en registro que es la que te va a identificar como persona, que tengas una identidad certificadora y que tengas una identidad nacional, son tres niveles ahora el notario digital es eso la entidad certificadora, es el notario y si quieres ir más allá, ahora los sistemas están cambiando para usar tecnología Blockchain de alguna forma también se vuelven como notario básicamente es algo que lo llaman el General electry o sea es el libro contable donde se registra todas las modificaciones o alteraciones de la data y si a eso tú le pones un certificado digital ya lo estás garantizando que la información sea legal.

15. **¿Conoce de herramientas tecnológicas o jurídicas eficaces que ayuden a dar la legalidad a las evidencias digitales?**

Hay herramientas que están certificadas para poder extraer información del celular y preservarla como evidencia, son herramientas válidas para poder certificar y estas herramientas deben estar acompañadas de personal capacitado con el conocimiento y la certificación necesaria, con los protocolos de cadena de custodia y con la participación de la autoridad tanto de la denuncia y la de la investigación para darle el marco de la legalidad.

Anexo 3. Matriz de categorización

MATRIZ DE CONSTRUCCION DE CATEGORIAS Y SUB CATEGORIAS APRIORISTICA

AMBITO TEMATICO	PROBLEMA DE INVESTIGACION	PREGUNTAS DE INVESTIGACION	OBJETIVO GENERAL	OBJETIVOS ESPECIFICOS	CATEGORIAS	SUB CATEGORIA
Tratamiento de la evidencia digital en el Sistema Jurídico Peruano	¿De qué manera debe tratarse la evidencia digital en el Sistema Jurídico peruano, para que sea admisible y tenga el valor probatorio en un Proceso penal?	¿Cuál es el tratamiento de la evidencia digital en la ciudad de Lima y si en la legislación nacional brinda el sustento legal?	Describir y plantear alternativas de procedimientos legales e informáticos para el tratamiento de la evidencia digital, a fin que sean admisibles y tengan el valor probatorio en un proceso penal en el Sistema Jurídico Peruano 2018.	Determinar cuál es el tratamiento de la evidencia digital en la ciudad de Lima y si la legislación nacional brinda el sustento legal.	Ciberdelincuencia y Ciberespacio	• Canales de desarrollo • Ámbito • Jurisdicción
		¿Qué legislación internacional protege la evidencia digital respecto a su tratamiento y que procedimientos legales protegen su valor probatorio?		Describir la legislación internacional que protege la evidencia digital respecto a su tratamiento y que procedimientos legales protegen su valor probatorio.	Valoración	•Bien jurídico • Previsión • Sanciones • Legalidad • Definición • Custodia • Tratamiento • Atención
		¿Cuáles son los procedimientos tecnológicos y guías del tratamiento de la evidencia digital desde su hallazgo hasta su presentación como prueba en un proceso judicial?		Precisar los procedimientos tecnológicos y guías del tratamiento de la evidencia digital desde su hallazgo hasta su presentación como prueba en un proceso judicial.	Tratamiento	• Convenios • Modelos • soluciones
		¿Qué propuestas legales así como técnicas se darían para el tratamiento de la evidencia digital, protegiendo su originalidad para ser admisibles y tengan el valor probatorio en un proceso judicial en el Sistema Jurídico Peruano?		Proponer alternativas legales así como técnicas para el tratamiento de la evidencia digital, protegiendo su originalidad y sean admisibles y tengan el valor probatorio en un proceso judicial en el Sistema Jurídico Peruano.	Procedimientos	• Procesos y Herramientas tecnológicas

Preguntas formuladas

Categoría	Sub categoría	Preguntas y sub preguntas
Ciberdelincuencia y Ciberespacio	• Canales de • Desarrollo • Ámbito • Jurisdicción	**¿Qué es la ciberdelincuencia y si es una modalidad delictiva considerada en el Código Penal Peruano?**
		¿Qué es el ciberespacio o el territorio donde se desarrolla la ciberdelincuencia?
		¿Qué son delitos transnacionales?
Valoración legal de la evidencia digital en el Perú	• Bien jurídico • Previsión • Sanciones • Legalidad • Definición • Custodia • Tratamiento • Atención	**¿Cree Ud. que la normatividad jurídica en el país, ha previsto el tratamiento de la evidencia digital?**
		¿Qué significa para Ud. La cadena de custodia y si esta se aplica para la evidencia digital?
		¿Cuál es bien jurídico protegido en los delitos informáticos?
		¿Al ser los delitos informáticos delitos transnacionales, las leyes peruanas que han previsto para que estos no queden impunes?
		¿El Perú se encuentra en condiciones jurídicas de poder sancionar los delitos informáticos?
		¿Cuál es el concepto de la evidencia digital en el ámbito jurídico?
		¿Considera Ud. que el personal de la Policía Nacional del Perú está en condiciones de tratar adecuadamente la evidencia digital?
		¿Considera Ud. si el Estado está abordando la lucha de ciberdelincuencia de manera eficaz?
Tratamiento de la evidencia digital en otros países	• Convenios • Modelos • soluciones	**¿Si conoce Ud. de algún país que actualmente viene enfrentando adecuadamente la lucha contra la ciberdelincuencia desde el ámbito judicial?**
		¿Conoce Ud. el convenio de Budapest?
		¿Cree Ud. que organizaciones privadas y/o particulares vienen aplicando soluciones para contrarrestar la ciberdelincuencia?
Procedimientos tecnológicos de la evidencia digital	• Procesos y • Herramientas • Tecnológicas	**¿Conoce de herramientas tecnológicas o jurídicas eficaces que ayuden a dar la legalidad a las evidencias digitales?**

Anexo 4. Proceso de codificación

Categorías	Preguntas	Entrevistado 1 MP	Frases codificadas	Sub categorías
A. Ciberdelincuencia y ciberespacio	1. ¿Qué es la ciberdelincuencia y si es una modalidad delictiva considerada en el Código Penal Peruano?	Consiste básicamente en cualquier delito o actividad ilegal cometido con la ayuda de un ordenador o internet contra una persona, sus bienes, negocios o el propio gobierno, y también se le conoce como delito informático. Existe una amplia variedad de cometer un delito informático. Si alguien piensa cometer un delito tradicional requiere de un montón de cosas y el riesgo es también muy alto sin embargo, para cometer un delito informático, la única necesidad está ahí, un ordenador con conexión a internet y las propias habilidades de la persona de tal forma que es capaz de hacerlo desde la intimidad de su propio hogar.	Delito o actividad ilegal cometido con la ayuda de un ordenador o internet. contra una persona, sus bienes, negocios o el propio gobierno. Existe una amplia variedad de cometer un delito informático.	Canales de desarrollo
	2. ¿Qué es el ciberespacio o el territorio donde se desarrolla la ciberdelincuencia?	El Ciberespacio se ha constituido como un nuevo mundo digital o virtual, sin fronteras físicas. Un nuevo mundo que no puede ser ajeno al derecho y a los distintos ordenamientos jurídicos que vertebran nuestro civilizado y moderno mundo. Pero claro, en un mundo donde el espacio físico no existe pero sí el tiempo Inmaterial, carente de materia. No hay fronteras físicas, sin Gobiernos o Estados democráticos o autoritarios, en él conviven ciberciudadanos y ciberorganizaciones y coexisten conductas aceptables y otras no aceptables éticamente por los ciudadanos del otro mundo.	Nuevo mundo digital o virtual, sin fronteras físicas. Espacio físico no existe pero sí el tiempo Inmaterial, carente de materia. Sin Gobiernos o Estados democráticos o autoritarios, en él conviven ciberciudadanos y ciberorganizaciones	Ámbito
	3. ¿Qué son delitos transnacionales?	Cuando el delito informático es trasnacional cualquier intento regulatorio Estatal es ineficaz, por ende se patentiza la necesaria aprobación de un tratado internacional que unifique criterios, tanto sustanciales como procesales y establezca las pautas a seguir en tema de cooperación judicial internacional, de lo contrario, será imposible disminuir los altos índices de impunidad registrados en esta materia.	Intento regulatorio Estatal es ineficaz. Necesaria aprobación de un tratado internacional que unifique criterios, tanto sustanciales como procesales y establezca las pautas a seguir en tema de cooperación judicial internacional,.	Jurisdicción

B. Valoración legal de la evidencia digital en el Perú	4. ¿Cuál es bien jurídico protegido en los delitos informáticos?	El bien jurídico que pone en peligro el delito informático es 'la información: (almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos).	La información: (almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos).	Bien jurídico
	5. ¿Al ser los delitos informáticos delitos transnacionales, las leyes peruanas que han previsto para que estos no queden impunes?	En los delitos informáticos se necesita trabajar en conjunto con otros países ya que no es un delito solo local, también es transnacional. Actualmente el tratado internacional que rige es el Convenio de Budapest o Convenio sobre ciberdelincuencia, creado para combatir el delito informático y generar la cooperación entre los países al cual aún el Perú no se adherido. El aumento de la criminalidad informática en el Perú y a nivel mundial trae consigo consecuencias económicas y numerosos fraudes cometidos por organizaciones delictivas que muchas veces no son denunciados o cuyos delitos son cometidos en el exterior sin que muchas veces exista una sanción.	Se necesita trabajar en conjunto con otros países ya que no es un delito solo local, también es transnacional. Consecuencias económicas y numerosos fraudes cometidos por organizaciones delictivas que muchas veces no son denunciados o cuyos delitos son cometidos en el exterior sin que muchas veces exista una sanción.	Previsión
	6. ¿El Perú se encuentra en condiciones jurídicas de poder sancionar los delitos informáticos?	La legislación existente resulta insuficiente, toda vez que continuamente se renuevan las modalidades delictivas en el ámbito informático, asimismo si se tiene presente que en nuestro país las herramientas existentes para contrarrestar dichos ilícitos no resultan ser suficientes, y que poco es el efecto disuasivo en la proliferación del mismo. Aún falta no solo legislar sobre las nuevas actividades delictivas, sino también difundir y explicar la nueva criminalidad informática en su connotación holística.	La legislación existente resulta insuficiente, toda vez que continuamente se renuevan las modalidades delictivas en el ámbito informático. Falta no solo legislar sobre las nuevas actividades delictivas, sino también difundir y explicar la nueva criminalidad informática.	Sanciones

	7. ¿Cree Ud. que la normatividad jurídica en el país, ha previsto el tratamiento de la evidencia digital?	Tratamiento especial de la prueba digital en el Código Procesal Penal del 2004 de manera puntual y especifica No existe, no hay regulación actual como prueba digital, sin embargo el Art. 185 del código procesal penal reconoce al contenido de un audio visual o audio grabado como prueba documental, si entre las fuentes de prueba de un hecho ilícito se encontrara un audio, o un video grabación u otro soporte digital o electrónico, simplemente el desahogo probatorio o actuación probatorio se efectúa en observación del artículo 382 del código procesal penal del 2004.	Tratamiento especial de la prueba digital en el Código Procesal Penal del 2004 de manera puntual y especifica No existe, no hay regulación actual como prueba digital. El Art. 185 del código procesal penal reconoce al contenido de un audio visual o audio grabado como prueba documenta., El desahogo probatorio o actuación probatorio se efectúa en observación del artículo 382 del código procesal penal del 2004.	Legalidad
	8. ¿Conoce Ud. el convenio de Budapest?	El Convenio de Budapest es un tratado internacional creado por los países miembros del Consejo de Europa con el fin de hacer frente a los delitos informáticos a través de mecanismos de homologación de normas de derecho penal sustantivo, estandarización de procesos penales y cooperación internacional.	tratado internacional creado por los países miembros del Consejo de Europa con el fin de hacer frente a los delitos informáticos, a través de mecanismos de homologación de normas de derecho penal sustantivo, estandarización de procesos penales y cooperación internacional	Definición
	9. ¿Cuál es el concepto de la evidencia digital en el ámbito jurídico?	La evidencia digital como un tipo de prueba física en donde sus datos pueden ser recolectados, almacenados y analizados con herramientas informáticas forenses y técnicas especiales. Si se la compara con otras formas de evidencia, la prueba digital es única. Si la evidencia fue presentada de manera correcta y su cadena de custodia no fue alterada, puede llegar a ser crucial para resolver cualquier clase de delitos.	prueba física en donde sus datos pueden ser recolectados, almacenados y analizados con herramientas informáticas forenses y técnicas especiales. Prueba digital es única. Crucial para resolver cualquier clase de delitos.	Custodia
	10. ¿Qué significa para Ud. La cadena de custodia y si esta se aplica para la evidencia digital?	La Cadena de Custodia es el procedimiento destinado a garantizar la individualización, seguridad y preservación de los elementos materiales y evidencias, recolectados de acuerdo a su naturaleza o incorporados en toda investigación de un hecho punible, destinados a garantizar su autenticidad, para los efectos del proceso.	Procedimiento destinado a garantizar la individualización, seguridad y preservación de los elementos materiales y evidencias, recolectados. Destinados a garantizar su autenticidad, para los efectos del proceso.	Tratamiento

	11. ¿Considera Ud. que el personal de la Policía Nacional del Perú está en condiciones de tratar adecuadamente la evidencia digital?	Existe una una insuficiencia de implementación de laboratorios a nivel nacional y existe un centralismo en todo el Perú para las pericias de pruebas digitales y de las tradicionales, para los delitos más comunes se sigue haciendo en Lima. Incluso para los delitos informáticos es más complejo se tiene que remitir a DIVINDAT-PNP de la Av. España y dicha división no existe en el Callao.	Insuficiencia de implementación de laboratorios a nivel nacional y existe un centralismo en todo el Perú para las pericias de pruebas digitales. Se tiene que remitir a DIVINDAT-PNP	Atención
C. Tratamiento de la evidencia digital en otros países	12. ¿Considera Ud. si el Estado está abordando la lucha de ciberdelincuencia de manera eficaz?	Considero que necesitamos promover la creación e implementación de Fiscalías Especializadas en Cibercrimen a fin de enfrentar adecuadamente los diversos delitos informáticos a fin de llevar a cabo investigaciones eficientes. El Perú requiere de una política de estado sobre el manejo de internet y desarrollar una campaña de educación entre escolares y adolescentes para que sepan proteger su información en la red.	Necesitamos promover la creación e implementación de Fiscalías Especializadas en Cibercrimen. El Perú requiere de una política de estado sobre el manejo de internet y desarrollar una campaña de educación entre escolares y adolescentes para que sepan proteger su información en la red.	Convenios
	13. ¿Si conoce Ud. de algún país que actualmente viene enfrentando adecuadamente la lucha contra la ciberdelincuencia desde el ámbito judicial?	Si considero que Colombia y Argentina en América Latina vienen promulgándose leyes que contribuyen a mejorar y dotar de los instrumentos legales contra la lucha del cibercrimen.	Colombia y Argentina en América Latina. Leyes que contribuyen a mejorar y dotar de los instrumentos legales contra la lucha del cibercrimen	Modelos
	14. ¿Cree Ud. que organizaciones privadas y/o particulares vienen aplicando soluciones para contrarrestar la ciberdelincuencia?	Las empresas tecnológicas son un aliado indispensable en la lucha contra la ciberdelincuencia. Es necesario aumentar la participación de los sectores público y privado para abordar inquietudes comunes como mejorar la educación y poner freno al material de abuso en línea.	Aliado indispensable en la lucha contra la ciberdelincuencia. Aumentar la participación de los sectores público y privado para abordar inquietudes comunes como mejorar la educación y poner freno al material de abuso en línea.	Soluciones

D. Procedimientos tecnológicos de la evidencia digital	15. ¿Conoce de herramientas tecnológicas o jurídicas eficaces que ayuden a dar la legalidad a las evidencias digitales?	En materia procesal me documente sobre la utilización del remote forensic como herramientas de investigación. Ella sugiere a los países la adopción de una norma a nivel nacional que prevea estas técnicas de investigación previendo la excepcionalidad de la medida y un uso restrictivo atendiendo a la potencialidad de afectación a la intimidad que significa su uso .	Remote forensic como herramientas de investigación. Norma a nivel nacional que prevea estas técnicas de investigación	Procesos y Herramientas tecnológicas

Categorías	Preguntas	Entrevistado 2 PNP	Frases codificadas	Sub categorías
A. Ciberdelincuencia y ciberespacio	1. ¿Qué es la ciberdelincuencia y si es una modalidad delictiva considerada en el Código Penal Peruano?	La ciberdelincuencia es una actividad delictiva realizada mediante el uso de las TICs. Actualmente existe la Ley Nro. 30096 y su modificatoria 30171, que sanciona algunas conductas delictivas.	Actividad delictiva realizada mediante el uso de las TICs. Ley Nro. 30096 y su modificatoria 30171, que sanciona algunas conductas delictivas.	Canales de desarrollo
	2. ¿Qué es el ciberespacio o el territorio donde se desarrolla la ciberdelincuencia?	Se podría decir que es espacio virtual, sin límites, donde se puede interactuar con otras personas únicamente a través de una conexión a la red.	Espacio virtual, sin límites. Interactuar con otras personas únicamente a través de una conexión a la red.	Ámbito
	3. ¿Qué son delitos transnacionales?	Son aquellos delitos que se comente en dos o más países, por ejemplo un fraude informático que se comete desde Perú a una entidad financiera extranjera.	Delitos que se comente en dos o más países,	Jurisdicción
B. Valoración legal de la evidencia digital en el Perú	4. ¿Cuál es bien jurídico protegido en los delitos informáticos?	La información de manera general es el valor jurídico protegido pero existen otros como la indemnidad sexual, intimidad y el patrimonio.	La información. La indemnidad sexual, intimidad y el patrimonio.	Bien jurídico
	5. ¿Al ser los delitos informáticos delitos transnacionales, las leyes peruanas que han previsto para que estos no queden impunes?	Ninguna, ya que el Perú aun no forma parte del Convenio sobre ciberdelincuencia (Convenio de Budapest).	Ninguna, ya que el Perú aun no forma parte del Convenio sobre ciberdelincuencia.	Previsión
	6. ¿El Perú se encuentra en condiciones jurídicas de poder sancionar los delitos informáticos?	No, para que suceda ello tendría que crearse una Fiscalía Especializada.	No, para que suceda ello tendría que crearse una Fiscalía Especializada.	Sanciones
	7. ¿Cree Ud. que la normatividad jurídica en el país, ha previsto el tratamiento de la evidencia digital?	No existe una normativa aborde sobre el tratamiento de la evidencia digital, sin embargo existe un manual de evidencia digital promovido por una ONG, que recoge las buenas prácticas de otros manuales para el manejo de la evidencia digital. En tanto, la PNP ha elaborado un manual para el recojo de la evidencia digital, que se encuentra a la espera de su aprobación.	No existe una normativa aborde sobre el tratamiento de la evidencia digital. Existe un manual de evidencia digital promovido por una ONG, que recoge las buenas prácticas de otros manuales para el manejo de la evidencia digital.	Legalidad

	8. ¿Conoce Ud. el convenio de Budapest?	Es un Convenio sobre ciberdelincuencia o llamado Convenio de Budapest, firmado en el 2001 que busca hacer frente a los delitos cometidos a través de la Internet, mediante la cooperación de los países que la integran y el sector privado.	Convenio sobre ciberdelincuencia. Busca hacer frente a los delitos cometidos a través de la Internet, mediante la cooperación de los países que la integran y el sector privado.	Definición
	9. ¿Cuál es el concepto de la evidencia digital en el ámbito jurídico?	Cualquier registro generado por o almacenado en un sistema informático o dispositivo digital que pueda ser utilizado como prueba en un proceso legal.	Registro generado por o almacenado en un sistema informático. Dispositivo digital que pueda ser utilizado como prueba en un proceso legal.	Custodia
	10. ¿Que significa para Ud. La cadena de custodia y si esta se aplica para la evidencia digital?	Procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis, normalmente peritos, y que tiene fin no viciar el manejo que de ellos se haga y así evitar alteraciones, sustituciones, contaminaciones o destrucciones. La cadena de custodia se aplica tanto a la evidencia física así como a la evidencia digital.	Procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis. se aplica tanto a la evidencia física así como a la evidencia digital.	Tratamiento
	11. ¿Considera Ud. que el personal de la Policía Nacional del Perú está en condiciones de tratar adecuadamente la evidencia digital?	Si, la Policía Nacional del Perú, cuenta con personal capacitado que viene laborando en la División de Investigación de Delitos de Alta Tecnología -DIRINCRI.	Si, la Policía Nacional del Perú, cuenta con personal capacitado, División de Investigación de Delitos de Alta Tecnología -DIRINCRI	Atención
C. Tratamiento de la evidencia digital en otros paises	12. ¿Considera Ud. si el Estado está abordando la lucha de ciberdelincuencia de manera eficaz?	Considero que el Estado tiene mucho por hacer en materia de ciberdelincuencia, modalidad delictiva que viene creciendo debido a que las personas emplean hoy más que ayer tecnología en su vida personal así como laboral, esto conlleva a las posibilidades de ilícitos informáticos.	el Estado tiene mucho por hacer en materia de ciberdelincuencia, personas emplean hoy más que ayer tecnología en su vida personal así como laboral.	Convenios

	13. ¿Si conoce Ud. de algún país que actualmente viene enfrentando adecuadamente la lucha contra la ciberdelincuencia desde el ámbito judicial?	Podría mencionar a España, que cuenta con personal constantemente capacitado y la tecnología adecuada, dentro de la región se encuentran Colombia y Brasil.	España, que cuenta con personal constantemente capacitado y la tecnología, de la región se encuentran Colombia y Brasil.	Modelos
	14. ¿Cree Ud. que organizaciones privadas y/o particulares vienen aplicando soluciones para contrarrestar la ciberdelincuencia?	Las empresas privadas en los últimos años han tomado conciencia de los peligros a los que se encuentra expuesto su información, para ello vienen implementando políticas de seguridad para proteger sus activos.	Las empresas privadas en los últimos años han tomado conciencia de los peligros a los que se encuentra expuesto su información, vienen implementando políticas de seguridad para proteger sus activos.	Soluciones
D. Procedimientos tecnológicos de la evidencia digital	15. ¿Conoce de herramientas tecnológicas o jurídicas eficaces que ayuden a dar la legalidad a las evidencias digitales?	El Triage consiste en realizar una búsqueda rápida empleando criterios sencillos sobre la estructura del disco, evitando profundizar las búsquedas en áreas especiales del disco. La realización de una copia o imagen forense, en la escena de delito mediante una copia bloque a bloque bit a bit del contenido digital almacenado, el que es autenticado mediante una función HASH.	El Triage consiste en realizar una búsqueda rápida empleando criterios, La realización de una copia o imagen forense, en la escena de delito, función HASH.	Procesos y Herramientas tecnológicas

Categorías	Preguntas	Entrevistado 3 TIC	Frases codificadas	Sub categorías
A. Ciberdelincuencia y ciberespacio	1. ¿Qué es la ciberdelincuencia y si es una modalidad delictiva considerada en el Código Penal Peruano?	La Ciberdelincuencia es un delito que está focalizado o se desarrolla en el ámbito del internet, generalmente es el canal que utiliza el delincuente para cometer delitos, claro se tipifica el delito cuando existe una norma una ley que así lo define, pero en nuestro país por ejemplo un botmaster no tendría ninguna sanción, en Estados Unidos un botmaster puede ser condenado a 15 años de prisión entonces, que es el ciberdelito son delitos que se realizan principalmente en el canal de Internet pero para ser considerados como delitos tiene que tener una tipificación.	Delito que está focalizado o se desarrolla en el ámbito del internet. Se tipifica el delito cuando existe una norma una ley que así lo define.	Canales de desarrollo
	2. ¿Qué es el ciberespacio o el territorio donde se desarrolla la ciberdelincuencia?	El ciberdelito qué va por el internet es global, la razón es muy simple para poder comunicarnos entre nuestras redes locales en nuestro país y con otros países, tenemos que usar la misma tecnología, al usar la misma tecnología usamos equipos de comunicación, medios de enlace, protocolos de comunicación y configuraciones eso hace que todos nosotros nos podamos comunicar. Entonces tu pregunta iba sobre el ciberespacio que es el ámbito en el cual se desarrolla o se transmite información piezas de información usando protocolos, equipos y medios de comunicación estándar.	Va por el internet es global. Es el ámbito en el cual se desarrolla o se transmite información piezas de información usando protocolos, equipos y medios de comunicación estándar.	Ámbito
	3. ¿Qué son delitos transnacionales?	Las redes están conectadas a nivel global y no tienen un problema de idioma, porque ellos usan su propio mecanismo de entendimiento, los equipos, los medios de comunicación, los protocolos son estándar es lo que permite el sistema de comunicación, entonces tú pregunta era las fronteras, no hay fronteras porque todo es relativo o sea él delito se puede producir aquí o en un país de Sudamérica o en Europa o en Estados Unidos y eso se hacen milisegundos, porque estamos en la misma red. Aquí no hay un tema de países porque si hablamos de territorialidad los conceptos hay que cambiarlos, que sucede antes por ejemplo para proteger el dinero de un banco se hacían grandes bóvedas, se ponían medidas de seguridad electrónicas las llaves y los discos para proteger puertas muy pesadas, paredes de concreto para proteger el dinero pero ahora en el ciberespacio ese dinero que hay en una bóveda de un banco no lo puedes consumir, entonces lo que tratan de hurtar es la información, el activo se convierte de un medio físico papel, barra de oro o un artículo valioso, hoy se convierte en números de cuenta códigos de acceso identidad de las personas etc. y ahí hay una gran vulnerabilidad que nace desde el diseño de la red, porque la red a estado preparada para identificar equipos, medios de comunicación, protocolos y eso en 7 capas que la última era la interface y los programas que te dan acceso al manejo de todas estas anteriores, pero nunca estuvo pensado, la red para identificar a personas, entonces ahora se está trabajando, esta es información ultima que pocas personas la conocen, se está desarrollando últimamente la capa 8 que va a identificar a las personas como parte de la información que circula por internet por eso que es cuando se habla del ciberdelincuente, se habla del ciberespacio, se habla del ámbito jurisdiccional o sea se habla de cosas que no identifican a las personas se está hablando de medios, se está hablando de equipos, se está hablando de otras cosas y no se hablan de la persona, entonces si estamos hablando del ciberdelincuente cómo puedes identificarlo, porque ahora los ataques los hacen robots, piezas de Software que son los que hacen los ataques, sobre qué jurisdicción estamos hablando, cuál es la jurisdicción que estamos protegiendo, entonces todo estado unido es una sola pieza es una sola jurisdicción, porque en el concepto de la red es precisamente global es como decir que yo puedo respirar aire de Perú si voy a otro país No puedo respirar el aire, porque tengo que ser ciudadano ese país para poder respirar ese aire es un derecho, entonces estamos hablando de la vida, entonces el concepto de jurisdicción cambia por eso es que nosotros hemos impulsado, los acuerdos internacionales. Por eso que es importante y siempre lo hemos dicho que Perú se suscriba a la comisión de Budapest y como todavía tenemos representantes que no entienden este tema de la jurisdicción y la necesidad de establecer alianzas e iniciativas globales.	No hay fronteras porque todo es relativo o sea él delito se puede producir aquí o en un país de Sudamérica o en Europa o en Estados Unidos y eso se hacen milisegundos, porque estamos en la misma red. Lo que tratan de hurtar es la información, el activo se convierte de un medio físico papel, barra de oro o un artículo valioso, hoy se convierte en números de cuenta códigos de acceso identidad de las personas etc. Cuando se habla del ciberdelincuente, se habla del ciberespacio, se habla del ámbito jurisdiccional o sea se habla de cosas que no identifican a las personas se está hablando de medios, se está hablando de equipos, se está hablando de otras cosas y no se hablan de la persona, entonces si estamos hablando del ciberdelincuente , Es importante y siempre lo hemos dicho que Perú se suscriba a la comisión de Budapest y como todavía tenemos representantes que no entienden este tema de la jurisdicción y la necesidad de establecer alianzas e iniciativas globales.	Jurisdicción

B. Valoración legal de la evidencia digital en el Perú	4. ¿Cuál es bien jurídico protegido en los delitos informáticos?	Es el dato, lo que hay que proteger es el dato, porque la información ya son los datos que ya están procesados Entonces el bien jurídico protegido es el dato	Es el dato, lo que hay que proteger es el dato.	Bien jurídico
	5. ¿Al ser los delitos informáticos delitos transnacionales, las leyes peruanas que han previsto para que estos no queden impunes?	Mira hay un antecedente que te pueden interesar en el 2008, Estonia sufrió el ataque más grande de ciberdelincuencia, cuando se hizo el análisis resulta que fue en el Perú donde se había generado la mayoría de ataques, entonces Estonia fue a las naciones Europeas a solicitar una sanción para Perú, pero justamente haciendo el análisis se demostró que no se podía sancionar a nuestro país porque no había un tema intencional de ataque de un país hacia otro. el presidente Obama en una de sus edictos o pronunciamiento síndico de qué Estados Unidos podría repeler con la fuerza de sus fuerzas armadas un ataque Cibernético identificado en otro país, entonces ahí te doy dos ejemplos y el otro tema es del china con las elecciones de Estados Unidos donde se puede apreciar de que se puede influir desde un país hacia otro, usando las redes sociales, el internet, la información no precisa y técnicas de ingeniería social que son los que más se utiliza para engañar a las personas	Estonia sufrió el ataque más grande de ciberdelincuencia. Fue en el Perú donde se había generado la mayoría de ataques. Estonia fue a las naciones Europeas a solicitar una sanción para Perú. No se podía sancionar a nuestro país porque no había un tema intencional de ataque de un país hacia otro	Previsión
	6. ¿El Perú se encuentra en condiciones jurídicas de poder sancionar los delitos informáticos?	Considero que no, esté es muy simple, tenemos 3 artículos del año 2000 y la ley delitos informáticos del año 2013, que salió después de 8 años porque nosotros insistimos en la necesidad de que haya una ley, pero eso fue producto del hackeo de una cuenta de la esposa de un funcionario del Estado, eso fue el motivo por el cual se buscó, cuál proyecto había para aprobarlo; cuando nosotros proponemos que Perú se adhiera al a la convención de Budapest, no solamente estamos hablando de una iniciativa que nos pone a nivel Global en el primer mundo, estamos hablando de que el consejo de Europa tiene destinado fondos para qué países como los nuestros, puedan adecuar su legislación y puedan tipificar y sancionar efectivamente los delitos informáticos, nosotros no entendemos que cosa es un delito informático en el Perú no se entiende que es un delito informático, porque no saben en donde nos estamos desarrollando en donde nos desenvolvemos, entonces mal podemos nosotros tipificar y sancionar algo como que te comentaba que en Estados Unidos pueden sancionar a un botmaster 15 años y en el Perú no exista, hemos tenido casos de ciudadanos de otras nacionalidades en Sudamérica con más de 100 tarjetas en un cajero automático y no se le pudo detener por delito informático porque acá ese señor es coleccionista de tarjeta y no es un clonador.	Considero que no. Nosotros insistimos en la necesidad de que haya una ley, pero eso fue producto del hackeo de una cuenta de la esposa de un funcionario del Estado, eso fue el motivo por el cual se buscó, cuál proyecto había para aprobarlo. Proponemos que Perú se adhiera al a la convención de Budapest. Europa tiene destinado fondos para qué países como los nuestros, puedan adecuar su legislación y puedan tipificar y sancionar efectivamente los delitos informáticos. No entendemos que cosa es un delito informático en el Perú,	Sanciones
	7. ¿Cree Ud. que la normatividad jurídica en el país, ha previsto el tratamiento de la evidencia digital?	Considero que eso es importante, pero que no exista en nuestro ordenamiento jurídico es un reflejo simplemente y de nuestra sociedad que nosotros nos gusta ir por el camino corto no respetamos las reglas; en la mañana estaba conversando con un taxista que me traía y hablábamos del callao, en el callao han puesto algo de tecnología con sistema de videocámaras, no es una ciudad inteligente sino que simplemente son cámaras que están conectadas a equipos para poder detectar la velocidad y todo el mundo anda 60 pero apenas cruza la línea que dice callao hacia lima, aumenta su velocidad a 80 o 90, cuál es la diferencia porque en dos cuadras uno puede ver ciudadanos yendo a 60 y a la siguiente cuadra a 80. Porque hay un sector, un territorio donde se cumple con la ley y esta se cumple con una sanción hay una pena en el otro lado no hay una sanción, entonces donde no se regula adecuadamente las cosas la gente hace lo que quiere, en el ciberespacio es exactamente es igual, porque nuestro país a esto el delincuente lo llama paraísos cibernético, es donde no hay la norma, no hay el procedimiento, no hay la pena entonces está libre y ejemplo de estos hay muchos en Argentina había un delincuente denominado el Gordo España, esta persona había cometido una cantidad de delitos terribles en España y le solicita a la Argentina la deportación, para ello argumentan todo y presentan sus leyes y lo demuestra muy bien todo perfecto, pero cuando llega a la Argentina dice no la puedo mandar porque eso aquí no es delito; y yo digo no había cometido el delito en Internet en Argentina. Entonces qué pasó, pasaron dos años o tres y Argentina actualiza su legislación, qué cosa crees que hizo España mando de nuevo el pedido porque ahora si lo consideraba y lo capturaron y lo deportaron y Argentina ya está suscrito el convenio de budapest	Considero que eso es importante, pero que no exista en nuestro ordenamiento jurídico es un reflejo simplemente y de nuestra sociedad que nosotros nos gusta ir por el camino corto no respetamos las reglas. En el ciberespacio es exactamente es igual, porque nuestro país a esto el delincuente lo llama paraísos cibernético, es donde no hay la norma, no hay el procedimiento, no hay la pena entonces está libre,	Legalidad

	8. ¿Conoce Ud. el convenio de Budapest?	Mira aquí te doy un ejemplo clarísimo en Colombia tuve la oportunidad de conversar con el jefe de la policía de investigaciones de delitos cibernéticos para Europa, entonces les manifesté nuestro interés de tener contacto y poder compartir información y él también se mostró muy interesado por qué era de Perú, le dije tenemos información de ciudadanos búlgaros que han cometido delitos en Perú, como puedo hacer para pasarte esa información, me respondió y me dijo mira no puedo recibirlo porque estás en un país que no ha suscrito la convención de Budapest; yo al principio no lo entendía y luego entendí claramente lo que me estaba diciendo, ellos respetan mucho las normas y los procedimientos y recibir la información que le daba podría contaminar la evidencia o el contaminarse para poder dar testimonios posteriores, hay que tener respeto por los procedimientos y seguir los protocolos y esas cosas no las entendemos; Entonces yo le dije mira yo soy ciudadano europeo también, tengo doble nacionalidad yo como ciudadano comunitario no te puedo pasar la información y me dijo no te la puedo recibir porque estás en un país que no ha suscrito la convención de Budapest. Bueno y qué hacemos y cómo te puedo dar esa información yo quiero colaborar, entonces me dijo si la captura de esos delincuentes ha sido registrada en algún periódico, correcto donde aparezcan los nombres, tú me puedes pasar eso y yo verificar que esa información sea correcta, como es de un medio de prensa y eso poder compartirlo con la comunidad. Entonces mira la dificultad que tenemos nosotros de enfrentar a una delincuencia que es global con las limitaciones de nuestra legislación local.	Hay que tener respeto por los procedimientos y seguir los protocolos y esas cosas no las entendemos. Dificultad que tenemos nosotros de enfrentar a una delincuencia que es global con las limitaciones de nuestra legislación local.	Definición
	9. ¿Cuál es el concepto de la evidencia digital en el ámbito jurídico?	La evidencia digital es un elemento que debería tener mucha importancia, pero aquí no le dan importancia y te lo digo porque yo he visto manipular evidencias que cualquier abogado podría fácilmente solicitar que no forme parte del proceso, porque esto debe ser formalizado. Por ejemplo la persona que recolecta información o evidencia digital debe tener una certificación, debe tener una profesión, debe tener procedimientos, debe ser una autoridad y debe estar acompañado de la fiscalía; ninguna de esas cosas se dan entonces por eso te digo la evidencia digital en nuestro país lamentablemente no es de interés por falta de conocimiento.	Es un elemento que debería tener mucha importancia. He visto manipular evidencias que cualquier abogado podría fácilmente solicitar que no forme parte del proceso, porque esto debe ser formalizado. Persona que recolecta información o evidencia digital debe tener una certificación, debe tener una profesión, debe tener procedimientos, debe ser una autoridad y debe estar acompañado de la fiscalía. La evidencia digital en nuestro país lamentablemente no es de interés por falta de conocimiento.	Custodia
	10. ¿Que significa para Ud. La cadena de custodia y si esta se aplica para la evidencia digital?	La cadena de custodia es importantísimo, fíjate en el momento de recolectar la información también tienes que demostrar que tienes equipo, que has comprado con factura, que tienes software que es legal, que tiene licencia, que tienes el mecanismo utilizando software especializado para la captura de datos, no puede usar cualquier cosa como Encase o herramientas libres, porque para los procesos judiciales la evidencia tiene que ser recolectada de manera autorizada.	Es importantísimo. En el momento de recolectar la información también tienes que demostrar que tienes equipo, que has comprado con factura, que tienes software que es legal, que tiene licencia, que tienes el mecanismo utilizando software especializado para la captura de datos	Tratamiento

	11. ¿Considera Ud. que el personal de la Policía Nacional del Perú está en condiciones de tratar adecuadamente la evidencia digital?	Sobre los delitos financieros no es DIVINDAT la primera que interviene, tenemos a las Águilas Negras, porque ellos lo que van a hacer es aislar la zona y si están preparados; pero representa al 3 por 1000 de la policía, también ellos cuando van al lugar las evidencias lo derivan a la DIVINDAT. Las Águilas Negras para algunas cosas si está preparado, pero mira los delitos informáticos cambia muy rápido es muy dinámico, entonces no estamos preparados para enfrentarlos; nosotros tenemos otra estrategia, tenemos apoyo de un Cecyt Financiero Europeo y ha sido calificado por dos años consecutivos como el mejor en Europa, entonces eso sí nos da un respaldo para poder enfrentar a una delincuencia internacional que estoy seguro que aquí podríamos hacerlo pero nos tardaríamos demasiado.	La primera que interviene, tenemos a las Águilas Negras, porque ellos lo que van a hacer es aislar la zona y si están preparados; pero representa al 3 por 1000 de la policía. Lo derivan a la DIVINDAT. No estamos preparados para enfrentarlos. Tenemos apoyo de un Cecyt Financiero Europeo y ha sido calificado por dos años consecutivos como el mejor en Europa, entonces eso sí nos da un respaldo para poder enfrentar a una delincuencia internacional	Atención
C. Tratamiento de la evidencia digital en otros países	12. ¿Considera Ud. si el Estado está abordando la lucha de ciberdelincuencia de manera eficaz?	Si claro definitivamente ahora el estado tiene personas capacitadas para enfrentar, pero creo que no están en el lugar indicado, tampoco tiene lo básico que es la norma, que se está construyendo pero lamentablemente el ambiente político influye mucho en este tema	El estado tiene personas capacitadas para enfrentar, pero creo que no están en el lugar indicado. Tampoco tiene lo básico que es la norma, que se está construyendo pero lamentablemente el ambiente político influye mucho en este tema	Convenios
	13. ¿Si conoce Ud. de algún país que actualmente viene enfrentando adecuadamente la lucha contra la ciberdelincuencia desde el ámbito judicial?	Podemos mirar a Colombia que tiene una cuarta Fuerza Armada que es la ciberseguridad, pero la verdad que estaba pensando, en Argentina en Chile tú sabes que en una reunión que tuvimos de Celaes en Miami, se presentó la representante de seguridad del Banco Famérica y hablaba sobre ciberdelitos y ella manifestó que el problema más grande que tenía el banco era el phishing, yo me preguntaba el phishing será problema para un banco tan grande, después seguir escuchando dijo que el phishing que afectaba al banco famerica era el que provenía de Perú el y Cuál era el motivo la calidad del engaño del phishing, entonces los peruanos porque tienen mucha imaginación y el problema de Sudamérica relacionado con ciberdelitos son los hackers peruanos y brasileros. Porque algunos han estudiado en los países de Rusia antigua, terminaron fueron captados por las bandas rusas y ya están de regreso hablan el idioma y aprendieron la tecnología, yo estoy seguro si esas personas practicaran el bien tendrían unas empresas maravillosas y producirían muchos ingresos al país pero sin embargo, se van a lo fácil y te comento algo más en Cybertec de Israel en el 2017 Benjamín Netanyahu habla al empresariado de Israel y les dice hace 5 años yo propuse alcanzar estar entre las cinco primeras economías en ciberseguridad y en el 2017 les decía a todos tus empresarios que esa meta la habían alcanzado y el 20% de la facturación de ciberseguridad global es de Israel, dime tú si no es importante, si no es algo interesante para el país, poder darle la oportunidad los jóvenes orientarlos a estudiar temas de ciberseguridad de ciberdefensa para que puedan también generar empresas que a su vez generan ingresos y desarrollo para el país	Colombia que tiene una cuarta Fuerza Armada que es la ciberseguridad. Es algo interesante para el país, poder darle la oportunidad los jóvenes orientarlos a estudiar temas de ciberseguridad de ciberdefensa para que puedan también generar empresas que a su vez generan ingresos y desarrollo para el país	Modelos

	14. ¿Cree Ud. que organizaciones privadas y/o particulares vienen aplicando soluciones para contrarrestar la ciberdelincuencia?	Si tú quieres identificar algo y darle validez en el internet o de un medio cibernetico lo que hay que usar es certificado digital porque siempre identifica la persona, va apunta a la capa 8 que te estaba diciendo de identificación de personas, pero el certificado lo que te garantiza es que esa persona que genero el documento es quien dice ser y funciona para los teléfonos, laptops o cualquier computadora, lo importante es que tú puedas obtener ese certificado con una entidad en registro que es la que te va a identificar como persona, que tengas una identidad certificadora y que tengas una identidad nacional, son tres niveles ahora el notario digital es eso la entidad certificadora, es el notario y si quieres ir más allá, ahora los sistemas están cambiando para usar tecnología Blockchain de alguna forma también se vuelven como notario básicamente es algo que lo llaman el General electry o sea es el libro contable donde se registra todas las modificaciones o alteraciones de la data y si a eso tú le pones un certificado digital ya lo estás garantizando que la información sea legal.	Si tú quieres identificar algo y darle validez en el internet o de un medio cibernetico lo que hay que usar es certificado digital porque siempre identifica la persona. Lo importante es que tú puedas obtener ese certificado con una entidad en registro que es la que te va a identificar como persona, que tengas una identidad certificadora y que tengas una identidad nacional. El notario digital es eso la entidad certificadora, es el notario y si quieres ir más allá, ahora los sistemas están cambiando para usar tecnología	Soluciones
D. Procedimientos tecnológicos de la evidencia digital	15. ¿Conoce de herramientas tecnológicas o jurídicas eficaces que ayuden a dar la legalidad a las evidencias digitales?	Hay herramientas que están certificadas para poder extraer información del celular y preservarla como evidencia, son herramientas válidas para poder certificar y estas herramientas deben estar acompañadas de personal capacitado con el conocimiento y la certificación necesaria, con los protocolos de cadena de custodia y con la participación de la autoridad tanto de la denuncia y la de la investigación para darle el marco de la legalidad	Hay herramientas que están certificadas para poder extraer información del celular y preservarla como evidencia. Estas herramientas deben estar acompañadas de personal capacitado con el conocimiento y la certificación necesaria, con los protocolos de cadena de custodia y con la participación de la autoridad tanto de la denuncia y la de la investigación para darle el marco de la legalidad	Procesos y Herramientas tecnológicas

Anexo 5. Matriz de Respuestas, triangulación de datos y Triangulación de datos y conclusiones

Respuestas de los Representantes, triangulación de datos, y conclusiones por cada pregunta:

Categoría	Preguntas	RMP	PNP	TIC	Conclusiones
Ciberdelincuencia y Ciberespacio	¿Qué es la ciberdelincuencia y si es una modalidad delictiva considerada en el Código Penal Peruano?	Consiste básicamente en cualquier delito o actividad ilegal cometido con la ayuda de un ordenador o internet contra una persona, sus bienes, negocios o el propio gobierno, y también se le conoce como delito informático. Existe una amplia variedad de cometer un delito informático. Si alguien piensa cometer un delito tradicional requiere de un montón de cosas y el riesgo es también muy alto sin embargo, para cometer un delito informático, la única necesidad está ahí, un ordenador con conexión a internet y las propias habilidades de la persona de tal forma que es capaz de hacerlo	La ciberdelincuencia es una actividad delictiva realizada mediante el uso de las TICs. Actualmente existe la Ley Nro. 30096 y su modificatoria 30171, que sanciona algunas conductas delictivas.	La Ciberdelincuencia es un delito que está focalizado o se desarrolla en el ámbito del internet, generalmente es el canal que utiliza el delincuente para cometer delitos, claro se tipifica el delito cuando existe una norma una ley que así lo define, pero en nuestro país por ejemplo un botmaster no tendría ninguna sanción, en Estados Unidos un botmaster puede ser condenado a 15 años de prisión entonces, que es el ciberdelito son delitos que se realizan principalmente en el canal de Internet pero para ser considerados como delitos tiene que tener una tipificación.	La ciberdelincuencia es una actividad ilícita y se desarrolla en el internet y que en el Perú se tipifica en la Ley 30093 Ley de Delitos informáticos.

		desde la intimidad de su propio hogar			
	¿Qué es el ciberespacio o el territorio donde se desarrolla la ciberdelincuencia?	El Ciberespacio se ha constituido como un nuevo mundo digital o virtual, sin fronteras físicas. Un nuevo mundo que no puede ser ajeno al derecho y a los distintos ordenamientos jurídicos que vertebran nuestro civilizado y moderno mundo. Pero claro, en un mundo donde el espacio físico no existe pero sí el tiempo Inmaterial, carente de materia. No hay fronteras físicas, sin Gobiernos o Estados democráticos o autoritarios, en él conviven ciberciudadanos y ciberorganizaciones y coexisten conductas aceptables y otras no aceptables éticamente por los ciudadanos del otro mundo.	Se podría decir que es espacio virtual, sin límites, donde se puede interactuar con otras personas únicamente a través de una conexión a la red.	El ciberdelito qué va por el internet es global, la razón es muy simple para poder comunicarnos entre nuestras redes locales en nuestro país y con otros países, tenemos que usar la misma tecnología, al usar la misma tecnología usamos equipos de comunicación, medios de enlace, protocolos de comunicación y configuraciones eso hace que todos nosotros nos podamos comunicar. Entonces tu pregunta iba sobre el ciberespacio que es el ámbito en el cual se desarrolla o se transmite información piezas de información usando protocolos, equipos y medios de comunicación estándar.	El Ciberespacio es un espacio virtual donde no hay fronteras y que para poder integrarse debe poseer similares tecnologías.

	¿Qué son delitos transnacionales?	Cuando el delito informático es trasnacional cualquier intento regulatorio Estatal es ineficaz, por ende se patentiza la necesaria aprobación de un tratado internacional que unifique criterios, tanto sustanciales como procesales y establezca las pautas a seguir en tema de cooperación judicial internacional, de lo contrario, será imposible disminuir los altos índices de impunidad registrados en esta materia.	Son aquellos delitos que se comente en dos o más países, por ejemplo un fraude informático que se comete desde Perú a una entidad financiera extranjera.	Las redes están conectadas a nivel global y no tienen un problema de idioma, porque ellos usan su propio mecanismo de entendimiento, los equipos, los medios de comunicación, los protocolos son estándar es lo que permite el sistema de comunicación, entonces tú pregunta era las fronteras, no hay fronteras porque todo es relativo o sea él delito se puede producir aquí o en un país de Sudamérica o en Europa o en Estados Unidos y eso se hacen milisegundos, porque estamos en la misma red. Aquí no hay un tema de países porque si hablamos de territorialidad los conceptos hay que cambiarlos, que sucede antes por ejemplo para proteger el dinero de un banco se hacían grandes bóvedas, se ponían medidas de seguridad electrónicas las llaves y los discos para proteger puertas muy pesadas, paredes de concreto para proteger el dinero pero ahora en el ciberespacio ese dinero que hay en una bóveda de un banco no lo puedes consumir, entonces lo que tratan de hurtar es la información, el activo se convierte de un medio físico papel, barra de oro o un artículo valioso, hoy se convierte en números de cuenta códigos de acceso identidad de las personas etc. y ahí hay una gran vulnerabilidad que nace desde el diseño de la red, porque la red a estado preparada para identificar equipos, medios de comunicación, protocolos y eso en 7 capas que la última era la interface y los programas que te dan acceso al manejo de todas estas anteriores, pero nunca estuvo pensado, la red para identificar a personas, entonces ahora se está trabajando, esta es información ultima que pocas personas la conocen, se está desarrollando últimamente la capa 8 que va a identificar a las personas como parte de la información que circula por internet por eso que es cuando se habla del ciberdelincuente, se habla del ciberespacio, se habla del ámbito jurisdiccional o sea se habla de cosas que no identifican a las personas se está hablando de medios, se está hablando de equipos, se está hablando de otras cosas y no se hablan de la persona, entonces si estamos hablando del ciberdelincuente cómo puedes identificarlo, porque ahora los ataques los hacen robots, piezas de Software que son los que hacen los ataques, sobre qué jurisdicción estamos hablando, cuál es la jurisdicción que estamos protegiendo, entonces todo estado unido es una sola pieza es una sola jurisdicción, porque en el concepto de la red es precisamente global es como decir que yo puedo respirar aire de Perú si voy a otro país No puedo respirar el aire, porque tengo que ser ciudadano ese país para poder respirar ese aire es un derecho, entonces estamos hablando de la vida, entonces el concepto de jurisdicción cambia por eso es que nosotros hemos impulsado, los acuerdos internacionales. Por eso que es importante y siempre lo hemos dicho que Perú se suscriba a la comisión de Budapest y como todavía tenemos representantes que no entienden este tema de la jurisdicción y la necesidad de establecer alianzas e iniciativas globales. La asociación de bancos si lo ha entendido y nosotros nos hemos suscrito “el llamamiento de Paris para la confianza y la seguridad del ciberespacio” iniciativa del presidente francés Emmanuel Macron, que ha invitado a grandes empresas globales, asociaciones y empresas que trabajan en el internet para generar espacios que sean seguros, porque son iniciativas que debemos hacer, si el país no lo entiende así y también sus representantes, las instituciones tienen que volverse globales.	Los delitos transnacionales se desarrollan en el ciberespacio donde no hay control legal y que la lucha se ha centrado más en la identificación de los equipos y no de personas.

Valoración legal de la evidencia digital en el Perú	¿Cuál es bien jurídico protegido en los delitos informáticos?	El bien jurídico que pone en peligro el delito informático es 'la información: (almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos).	La información de manera general es el valor jurídico protegido pero existen otros como la indemnidad sexual, intimidad y el patrimonio.	Es el dato, lo que hay que proteger es el dato, porque la información ya son los datos que ya están procesados Entonces el bien jurídico protegido es el dato.	El bien jurídico en los delitos informáticos es el dato que resulta del procesamiento de la información.
	¿Al ser los delitos informáticos delitos transnacionales, las leyes peruanas que han previsto para que estos no queden impunes?	En los delitos informáticos se necesita trabajar en conjunto con otros países ya que no es un delito solo local, también es transnacional. Actualmente el tratado internacional que rige es el Convenio de Budapest o Convenio sobre ciberdelincuencia, creado para combatir el delito informático y generar la cooperación entre los países al cual aún el Perú no se adherido. El aumento de la criminalidad informática en el Perú y a nivel	Ninguna, ya que el Perú aun no forma parte del Convenio sobre ciberdelincuencia (Convenio de Budapest).	Mira hay un antecedente que te pueden interesar en el 2008, Estonia sufrió el ataque más grande de ciberdelincuencia, cuando se hizo el análisis resulta que fue en el Perú donde se había generado la mayoría de ataques, entonces Estonia fue a las naciones Europeas a solicitar una sanción para Perú, pero justamente haciendo el análisis se demostró que no se podía sancionar a nuestro país porque no había un tema intencional de ataque de un país hacia otro. el presidente Obama en una de sus edictos o pronunciamiento síndico de qué Estados Unidos podría repeler con la fuerza de sus fuerzas armadas un ataque Cibernético identificado en otro país, entonces ahí te doy dos ejemplos y el otro tema es del china con las elecciones de Estados Unidos donde se puede apreciar de que se puede influir desde un país hacia otro, usando las redes sociales, el internet, la información no precisa y técnicas de ingeniería social que son los que más se utiliza para engañar a las personas.	Las leyes peruanas no han previsto la lucha contra la ciberdelincuencia al ser estos trasnacionales y no existe sanciones en el código penal al no tener jurisdicción fuera del país

		mundial trae consigo consecuencias económicas y numerosos fraudes cometidos por organizaciones delictivas que muchas veces no son denunciados o cuyos delitos son cometidos en el exterior sin que muchas veces exista una sanción.			

	¿El Perú se encuentra en condiciones jurídicas de poder sancionar los delitos informáticos?	La legislación existente resulta insuficiente, toda vez que continuamente se renuevan las modalidades delictivas en el ámbito informático, asimismo si se tiene presente que en nuestro país las herramientas existentes para contrarrestar dichos ilícitos no resultan ser suficientes, y que poco es el efecto disuasivo en la proliferación del mismo. Aún falta no solo legislar sobre las nuevas actividades delictivas, sino también difundir y explicar la nueva criminalidad informática en su connotación holística.	No, para que suceda ello tendría que crearse una Fiscalía Especializada.	Considero que no, esté es muy simple, tenemos 3 artículos del año 2000 y la ley delitos informáticos del año 2013, que salió después de 8 años porque nosotros insistimos en la necesidad de que haya una ley, pero eso fue producto del hackeo de una cuenta de la esposa de un funcionario del Estado, eso fue el motivo por el cual se buscó, cuál proyecto había para aprobarlo; cuando nosotros proponemos que Perú se adhiera al a la convención de Budapest, no solamente estamos hablando de una iniciativa que nos pone a nivel Global en el primer mundo, estamos hablando de que el consejo de Europa tiene destinado fondos para qué países como los nuestros, puedan adecuar su legislación y puedan tipificar y sancionar efectivamente los delitos informáticos, nosotros no entendemos que cosa es un delito informático en el Perú no se entiende que es un delito informático, porque no saben en donde nos estamos desarrollando en donde nos desenvolvemos, entonces mal podemos nosotros tipificar y sancionar algo como que te comentaba que en Estados Unidos pueden sancionar a un botmaster 15 años y en el Perú no exista, hemos tenido casos de ciudadanos de otras nacionalidades en Sudamérica con más de 100 tarjetas en un cajero automático y no se le pudo detener por delito informático porque acá ese señor es coleccionista de tarjeta y no es un clonador.	Al ser la ciberdelincuencia un delito sin fronteras el Perú no cuenta con normas jurídicas que sanciones los delitos informáticos en estas condiciones, lo que hasta la fecha se ha logrado en leyes se dieron por insistencias particulares y no por necesidades verdaderas.

	¿Cree Ud. que la normatividad jurídica en el país, ha previsto el tratamiento de la evidencia digital?	Tratamiento especial de la prueba digital en el Código Procesal Penal del 2004 de manera puntual y especifica No existe, no hay regulación actual como prueba digital, sin embargo el Art. 185 del código procesal penal reconoce al contenido de un audio visual o audio grabado como prueba documental, si entre las fuentes de prueba de un hecho ilícito se encontrara un audio, o un video grabación u otro soporte digital o electrónico, simplemente el desahogo probatorio o actuación probatorio se efectúa en observación del artículo 382 del código procesal penal del 2004.	No existe una normativa aborde sobre el tratamiento de la evidencia digital, sin embargo existe un manual de evidencia digital promovido por una ONG, que recoge las buenas prácticas de otros manuales para el manejo de la evidencia digital. En tanto, la PNP ha elaborado un manual para el recojo de la evidencia digital, que se encuentra a la espera de su aprobación.	Considero que eso es importante, pero que no exista en nuestro ordenamiento jurídico es un reflejo simplemente y de nuestra sociedad que nosotros nos gusta ir por el camino corto no respetamos las reglas; en la mañana estaba conversando con un taxista que me traía y hablábamos del callao, en el callao han puesto algo de tecnología con sistema de videocámaras, no es una ciudad inteligente sino que simplemente son cámaras que están conectadas a equipos para poder detectar la velocidad y todo el mundo anda 60 pero apenas cruza la línea que dice callao hacia lima, aumenta su velocidad a 80 o 90, cuál es la diferencia porque en dos cuadras uno puede ver ciudadanos yendo a 60 y a la siguiente cuadra a 80. Porque hay un sector, un territorio donde se cumple con la ley y esta se cumple con una sanción hay una pena en el otro lado no hay una sanción, entonces donde no se regula adecuadamente las cosas la gente hace lo que quiere, en el ciberespacio es exactamente es igual, porque nuestro país a esto el delincuente lo llama paraísos cibernético, es donde no hay la norma, no hay el procedimiento, no hay la pena entonces está libre y ejemplo de estos hay muchos en Argentina había un delincuente denominado el Gordo España, esta persona había cometido una cantidad de delitos terribles en España y le solicita a la Argentina la deportación, para ello argumentan todo y presentan sus leyes y lo demuestra muy bien todo perfecto, pero cuando llega a la Argentina dice no la puedo mandar porque eso aquí no es delito; y yo digo no había cometido el delito en Internet en Argentina. Entonces qué pasó, pasaron dos años o tres y Argentina actualiza su legislación, qué cosa crees que hizo España mando de nuevo el pedido porque ahora si lo consideraba y lo capturaron y lo deportaron y Argentina ya está suscrito el convenio de Budapest.	La evidencia digital en el Perú no cuenta con una normatividad jurídica que determine su tratamiento más aun somos considerado paraíso cibernético por falta de leyes que combatan los ilícitos informáticos en el ciberespacio.

	¿Cuál es el concepto de la evidencia digital en el ámbito jurídico/policial y tecnológico?	La evidencia digital como un tipo de prueba física en donde sus datos pueden ser recolectados, almacenados y analizados con herramientas informáticas forenses y técnicas especiales. Si se la compara con otras formas de evidencia, la prueba digital es única. Si la evidencia fue presentada de manera correcta y su cadena de custodia no fue alterada, puede llegar a ser crucial para resolver cualquier clase de delitos.	Cualquier registro generado por o almacenado en un sistema informático o dispositivo digital que pueda ser utilizado como prueba en un proceso legal.	La evidencia digital es un elemento que debería tener mucha importancia, pero aquí no le dan importancia y te lo digo porque yo he visto manipular evidencias que cualquier abogado podría fácilmente solicitar que no forme parte del proceso, porque esto debe ser formalizado. Por ejemplo la persona que recolecta información o evidencia digital debe tener una certificación, debe tener una profesión, debe tener procedimientos, debe ser una autoridad y debe estar acompañado de la fiscalía; ninguna de esas cosas se dan entonces por eso te digo la evidencia digital en nuestro país lamentablemente no es de interés por falta de conocimiento.	La evidencia digital en nuestro país es tratado como otras evidencias, no se ha establecido legalmente un tratamiento único por sus características, más aun las autoridades manipulan las evidencias contaminándolas y por ende no sirviendo para un proceso judicial.

	¿Qué significa para Ud. La cadena de custodia y si esta se aplica para la evidencia digital?	La Cadena de Custodia es el procedimiento destinado a garantizar la individualización, seguridad y preservación de los elementos materiales y evidencias, recolectados de acuerdo a su naturaleza o incorporados en toda investigación de un hecho punible, destinados a garantizar su autenticidad, para los efectos del proceso.	Procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis, normalmente peritos, y que tiene fin no viciar el manejo que de ellos se haga y así evitar alteraciones, sustituciones, contaminaciones o destrucciones. La cadena de custodia se aplica tanto a la evidencia física así como a la evidencia digital.	La cadena de custodia es importantísimo, fíjate en el momento de recolectar la información también tienes que demostrar que tienes equipo, que has comprado con factura, que tienes software que es legal, que tiene licencia, que tienes el mecanismo utilizando software especializado para la captura de datos, no puede usar cualquier cosa como Encase o herramientas libres, porque para los procesos judiciales la evidencia tiene que ser recolectada de manera autorizada.	La cadena de custodia garantiza la preservación y seguridad de la evidencia digital, si se realiza con personal especializado, equipos certificados y con licencias, una mala práctica de este procedimiento genera que se altere y no se pueda utilizarla para un proceso judicial

	¿Considera Ud. que el personal de la Policía Nacional del Perú está en condiciones de tratar adecuadamente la evidencia digital?	Existe una una insuficiencia de implementación de laboratorios a nivel nacional y existe un centralismo en todo el Perú para las pericias de pruebas digitales y de las tradicionales, para los delitos más comunes se sigue haciendo en Lima. Incluso para los delitos informáticos es más complejo se tiene que remitir a DIVINDAT-PNP de la Av. España y dicha división no existe en el Callao.	Si, la Policía Nacional del Perú, cuenta con personal capacitado que viene laborando en la División de Investigación de Delitos de Alta Tecnología - DIRINCRI.	Sobre los delitos financieros no es DIVINDAT la primera que interviene, tenemos a las Águilas Negras, porque ellos lo que van a hacer es aislar la zona y si están preparados; pero representa al 3 por 1000 de la policía, también ellos cuando van al lugar las evidencias lo derivan a la DIVINDAT. Las Águilas Negras para algunas cosas si está preparado, pero mira los delitos informáticos cambia muy rápido es muy dinámico, entonces no estamos preparados para enfrentarlos; nosotros tenemos otra estrategia, tenemos apoyo de un Cecyt Financiero Europeo y ha sido calificado por dos años consecutivos como el mejor en Europa, entonces eso sí nos da un respaldo para poder enfrentar a una delincuencia internacional que estoy seguro que aquí podríamos hacerlo pero nos tardaríamos demasiado.	El personal de la PNP no se encuentra capacitado y no cuenta con el equipamiento básico para el cumplimiento de sus funciones, la DIVINDAT es la Unidad especializada en la investigación de delitos informáticos y que esta se encuentra en la ciudad de Lima no teniendo alcance efectivo a nivel nacional.

	¿Considera Ud. si el Estado está abordando la lucha de ciberdelincuencia de manera eficaz?	Considero que necesitamos promover la creación e implementación de Fiscalías Especializadas en Cibercrimen a fin de enfrentar adecuadamente los diversos delitos informáticos a fin de llevar a cabo investigaciones eficientes. El Perú requiere de una política de estado sobre el manejo de internet y desarrollar una campaña de educación entre escolares y adolescentes para que sepan proteger su información en la red.	Considero que el Estado tiene mucho por hacer en materia de ciberdelincuencia, modalidad delictiva que viene creciendo debido a que las personas emplean hoy más que ayer tecnología en su vida personal así como laboral, esto conlleva a las posibilidades de ilícitos informáticos.	Si claro definitivamente ahora el estado tiene personas capacitadas para enfrentar, pero creo que no están en el lugar indicado, tampoco tiene lo básico que es la norma, que se está construyendo pero lamentablemente el ambiente político influye mucho en este tema.	El Estado no aborda eficazmente la lucha contra la ciberdelincuencia, es necesario la creación de las fiscalías especializadas, personas capacitas y normatividad legal.

Tratamiento de la evidencia digital en otros países	8. ¿Conoce Ud. el convenio de Budapest?	El Convenio de Budapest es un tratado internacional creado por los países miembros del Consejo de Europa con el fin de hacer frente a los delitos informáticos a través de mecanismos de homologación de normas de derecho penal sustantivo, estandarización de procesos penales y cooperación internacional.	Es un Convenio sobre ciberdelincuencia o llamado Convenio de Budapest, firmado en el 2001 que busca hacer frente a los delitos cometidos a través de la Internet, mediante la cooperación de los países que la integran y el sector privado.	Mira aquí te doy un ejemplo clarísimo en Colombia tuve la oportunidad de conversar con el jefe de la policía de investigaciones de delitos cibernéticos para Europa, entonces les manifesté nuestro interés de tener contacto y poder compartir información y él también se mostró muy interesado por qué era de Perú, le dije tenemos información de ciudadanos búlgaros que han cometido delitos en Perú, como puedo hacer para pasarte esa información, me respondió y me dijo mira no puedo recibirlo porque estás en un país que no ha suscrito la convención de Budapest; yo al principio no lo entendía y luego entendí claramente lo que me estaba diciendo, ellos respetan mucho las normas y los procedimientos y recibir la información que le daba podría contaminar la evidencia o el contaminarse para poder dar testimonios posteriores, hay que tener respeto por los procedimientos y seguir los protocolos y esas cosas no las entendemos; Entonces yo le dije mira yo soy ciudadano europeo también, tengo doble nacionalidad yo como ciudadano comunitario no te puedo pasar la información y me dijo no te la puedo recibir porque estás en un país que no ha suscrito la convención de Budapest. Bueno y qué hacemos y cómo te puedo dar esa información yo quiero colaborar, entonces me dijo si la captura de esos delincuentes ha sido registrada en algún periódico, correcto donde aparezcan los nombres, tú me puedes pasar eso y yo verificar que esa información sea correcta, como es de un medio de prensa y eso poder compartirlo con la comunidad. Entonces mira la dificultad que tenemos nosotros de enfrentar a una delincuencia que es global con las limitaciones de nuestra legislación local.	El Convenio de Budapest es un tratado internacional que busca hacer frente a los delitos cometidos por internet, a través de la cooperación y el Perú al no encontrarse adherido al mismo, pierde beneficios en la lucha contra la ciberdelincuencia.

	13. ¿Si conoce Ud. de algún país que actualmente viene enfrentando adecuadamente la lucha contra la ciberdelincuencia desde el ámbito judicial?	Si considero que Colombia y Argentina en América Latina vienen promulgándose leyes que contribuyen a mejorar y dotar de los instrumentos legales contra la lucha del cibercrimen.	Podría mencionar a España, que cuenta con personal contantemente capacitado y la tecnología adecuada, dentro de la región se encuentran Colombia y Brasil.	Podemos mirar a Colombia que tiene una cuarta Fuerza Armada que es la ciberseguridad, pero la verdad que estaba pensando, en Argentina en Chile tú sabes que en una reunión que tuvimos de Celaes en Miami, se presentó la representante de seguridad del Banco Famérica y hablaba sobre ciberdelitos y ella manifestó que el problema más grande que tenía el banco era el phishing, yo me preguntaba el phishing será problema para un banco tan grande, después seguir escuchando dijo que el phishing que afectaba al banco famerica era el que provenía de Perú el problema más grande del banco famerica en ese momento era el phishing qué provenía de Perú y Cuál era el motivo la calidad del engaño del phishing, entonces los peruanos porque tienen mucha imaginación y el problema de Sudamérica relacionado con ciberdelitos son los hackers peruanos y brasileros. Porque algunos han estudiado en los países de Rusia antigua, terminaron fueron captados por las bandas rusas y ya están de regreso hablan el idioma y aprendieron la tecnología, yo estoy seguro si esas personas practicaran el bien tendrían unas empresas maravillosas y producirían muchos ingresos al país pero sin embargo, se van a lo fácil y te comento algo más en Cybertec de Israel en el 2017 Benjamín Netanyahu habla al empresariado de Israel y les dice hace 5 años yo propuse alcanzar estar entre las cinco primeras economías en ciberseguridad y en el 2017 les decía a todos tus empresarios que esa meta la habían alcanzado y el 20% de la facturación de ciberseguridad global es de Israel, dime tú si no es importante, si no es algo interesante para el país, poder darle la oportunidad los jóvenes orientarlos a estudiar temas de ciberseguridad de ciberdefensa para que puedan también generar empresas que a su vez generan ingresos y desarrollo para el país.	Los países que mejores resultados han obtenido en la lucha contra la ciberdelincuencia son Colombia, Argentina y Brasil y en Europa España.

	14. ¿Cree Ud. que organizaciones privadas y/o particulares vienen aplicando soluciones para contrarrestar la ciberdelincuencia?	Las empresas tecnológicas son un aliado indispensable en la lucha contra la ciberdelincuencia. Es necesario aumentar la participación de los sectores público y privado para abordar inquietudes comunes como mejorar la educación y poner freno al material de abuso en línea.	Las empresas privadas en los últimos años han tomado conciencia de los peligros a los que se encuentra expuesto su información, para ello vienen implementando políticas de seguridad para proteger sus activos.	Si tú quieres identificar algo y darle validez en el internet o de un medio cibernetico lo que hay que usar es certificado digital porque siempre identifica la persona, va apunta a la capa 8 que te estaba diciendo de identificación de personas, pero el certificado lo que te garantiza es que esa persona que genero el documento es quien dice ser y funciona para los teléfonos, laptops o cualquier computadora, lo importante es que tú puedas obtener ese certificado con una entidad en registro que es la que te va a identificar como persona, que tengas una identidad certificadora y que tengas una identidad nacional, son tres niveles ahora el notario digital es eso la entidad certificadora, es el notario y si quieres ir más allá, ahora los sistemas están cambiando para usar tecnología Blockchain de alguna forma también se vuelven como notario básicamente es algo que lo llaman el General electry o sea es el libro contable donde se registra todas las modificaciones o alteraciones de la data y si a eso tú le pones un certificado digital ya lo estás garantizando que la información sea legal	Las entidades privadas son las que mejores resultados han obtenido en la lucha contra la ciberdelincuencia, el sector público en nuestro país no ha desarrollado estrategias de prevención en la lucha contra la ciberdelincuencia.

Procedimientos tecnológicos de la evidencia digital	15. ¿Conoce de herramientas tecnológicas o jurídicas eficaces que ayuden a dar la legalidad a las evidencias digitales?	En materia procesal me documente sobre la utilización del remote forensic como herramientas de investigación. Ella sugiere a los países la adopción de una norma a nivel nacional que prevea estas técnicas de investigación previendo la excepcionalidad de la medida y un uso restrictivo atendiendo a la potencialidad de afectación a la intimidad que significa su uso.	El Triage consiste en realizar una búsqueda rápida empleando criterios sencillos sobre la estructura del disco, evitando profundizar las búsquedas en áreas especiales del disco. La realización de una copia o imagen forense, en la escena de delito mediante una copia bloque a bloque bit a bit del contenido digital almacenado, el que es autenticado mediante una función HASH.	Hay herramientas que están certificadas para poder extraer información del celular y preservarla como evidencia, son herramientas válidas para poder certificar y estas herramientas deben estar acompañadas de personal capacitado con el conocimiento y la certificación necesaria, con los protocolos de cadena de custodia y con la participación de la autoridad tanto de la denuncia y la de la investigación para darle el marco de la legalidad.	Herramientas como remote forensig, el triage, la función hash vienen dando buenos resultados en el tratamiento de la evidencia digital, para ello se requiere que ellas estén validadas y certificadas.

Matriz de triangulación de datos y conclusiones por cada pregunta

Sub categoría	Preguntas	RMP	PNP	TIC	Similitud	Diferencias	Conclusiones
Ciberdelincuencia y Ciberespacio	¿Qué es la ciberdelincuencia y si es una modalidad delictiva considerada en el Código Penal Peruano?	Consiste básicamente en cualquier delito o actividad ilegal cometido con la ayuda de un ordenador o internet contra una persona, sus bienes, negocios o el propio gobierno, y también se le conoce como delito informático. Existe una amplia variedad de cometer un delito informático. Si alguien piensa cometer un delito tradicional requiere de un montón de cosas y el riesgo es también muy alto sin embargo, para cometer un delito informático, la única necesidad está ahí, un ordenador con conexión a internet y las propias habilidades de la persona de tal forma que es capaz de hacerlo desde la intimidad de su propio hogar	La ciberdelincuencia es una actividad delictiva realizada mediante el uso de las TICs. Actualmente existe la Ley Nro. 30096 y su modificatoria 30171, que sanciona algunas conductas delictivas.	La Ciberdelincuencia es un delito que está focalizado o se desarrolla en el ámbito del internet, generalmente es el canal que utiliza el delincuente para cometer delitos, claro se tipifica el delito cuando existe una norma una ley que así lo define, pero en nuestro país por ejemplo un botmaster no tendría ninguna sanción, en Estados Unidos un botmaster puede ser condenado a 15 años de prisión entonces, que es el ciberdelito son delitos que se realizan principalmente en el canal de Internet pero para ser considerados como delitos tiene que tener una tipificación.	Los entrevistados consideran que la ciberdelincuencia es una actividad ilícita se desarrolla en el internet a través de equipos tecnológicos, que si existe varias modalidades y que la Ley 30096 Lay de delitos informáticos sancionas estas malas conductas.	Que la tipificación de los delitos informáticos mediante la Ley 30096 resulta insuficiente	La ciberdelincuencia es una actividad ilícita y se desarrolla en el internet y que en el Perú se tipifica en la Ley 30093 Ley de Delitos informáticos.

	¿Qué es el ciberespacio o el territorio donde se desarrolla la ciberdelincuencia?	El Ciberespacio se ha constituido como un nuevo mundo digital o virtual, sin fronteras físicas. Un nuevo mundo que no puede ser ajeno al derecho y a los distintos ordenamientos jurídicos que vertebran nuestro civilizado y moderno mundo. Pero claro, en un mundo donde el espacio físico no existe pero sí el tiempo Inmaterial, carente de materia. No hay fronteras físicas, sin Gobiernos o Estados democráticos o autoritarios, en él conviven ciberciudadanos y ciberorganizaciones y coexisten conductas aceptables y otras no aceptables éticamente por los ciudadanos del otro mundo.	Se podría decir que es espacio virtual, sin límites, donde se puede interactuar con otras personas únicamente a través de una conexión a la red.	El ciberdelito qué va por el internet es global, la razón es muy simple para poder comunicarnos entre nuestras redes locales en nuestro país y con otros países, tenemos que usar la misma tecnología, al usar la misma tecnología usamos equipos de comunicación, medios de enlace, protocolos de comunicación y configuraciones eso hace que todos nosotros nos podamos comunicar. Entonces tu pregunta iba sobre el ciberespacio que es el ámbito en el cual se desarrolla o se transmite información piezas de información usando protocolos, equipos y medios de comunicación estándar.	Los entrevistados consideran que el Ciberespacio es un espacio global y virtual sin límites físicos, no hay fronteras y en ella se desarrolla conductas ilícitas por ciudadanos.	Para poder integrarse como una sola red, deben tener la misma tecnología, equipos de comunicación y configuraciones. Eso es lo que el ciberdelincuente busca para cometer sus ilícitos	El Ciberespacio es un espacio virtual donde no hay fronteras y que para poder integrarse deben poseer similares tecnologías.

	¿Qué son delitos transnacionales?	Cuando el delito informático es trasnacional cualquier intento regulatorio Estatal es ineficaz, por ende se patentiza la necesaria aprobación de un tratado internacional que unifique criterios, tanto sustanciales como procesales y establezca las pautas a seguir en tema de cooperación judicial internacional, de lo contrario, será imposible disminuir los altos índices de impunidad registrados en esta materia.	Son aquellos delitos que se comente en dos o más países, por ejemplo un fraude informático que se comete desde Perú a una entidad financiera extranjera.	Las redes están conectadas a nivel global y no tienen un problema de idioma, porque ellos usan su propio mecanismo de entendimiento, los equipos, los medios de comunicación, los protocolos son estándar es lo que permite el sistema de comunicación, entonces tú pregunta era las fronteras, no hay fronteras porque todo es relativo o sea él delito se puede producir aquí o en un país de Sudamérica o en Europa o en Estados Unidos y eso se hacen milisegundos, porque estamos en la misma red. Aquí no hay un tema de países porque si hablamos de territorialidad los conceptos hay que cambiarlos, que sucede antes por ejemplo para proteger el dinero de un banco se hacían grandes bóvedas, se ponían medidas de seguridad electrónicas las llaves y los discos para proteger puertas muy pesadas, paredes de concreto para proteger el dinero pero ahora en el ciberespacio ese dinero que hay en una bóveda de un banco no lo puedes consumir, entonces lo que tratan de hurtar es la información, el activo se convierte de un medio físico papel, barra de oro o un artículo valioso, hoy se convierte en números de cuenta códigos de acceso identidad de las personas etc. y ahí hay una gran vulnerabilidad que nace desde el diseño de la red, porque la red a estado preparada para identificar equipos, medios de comunicación, protocolos y eso en 7 capas que la última era la interface y los programas que te dan acceso al manejo de todas estas anteriores, pero nunca estuvo pensado, la red para identificar a personas, entonces ahora se está trabajando, esta es información ultima que pocas personas la conocen, se está desarrollando últimamente la capa 8 que va a identificar a las personas como parte de la información que circula por internet por eso que es cuando se habla del ciberdelincuente, se habla del ciberespacio, se habla del ámbito jurisdiccional o sea se habla de cosas que no identifican a las personas se está hablando de medios, se está hablando de equipos, se está hablando de otras cosas y no se hablan de la persona, entonces si estamos hablando del ciberdelincuente cómo puedes identificarlo, porque ahora los ataques los hacen robots, piezas de Software que son los que hacen los ataques, sobre qué jurisdicción estamos hablando, cuál es la jurisdicción que estamos protegiendo, entonces todo estado unido es una sola pieza es una sola jurisdicción, porque en el concepto de la red es precisamente global es como decir que yo puedo respirar aire de Perú si voy a otro país No puedo respirar el aire, porque tengo que ser ciudadano ese país para poder respirar ese aire es un derecho, entonces estamos hablando de la vida, entonces el concepto de jurisdicción cambia por eso es que nosotros hemos impulsado, los acuerdos internacionales. Por eso que es importante y siempre lo hemos dicho que Perú se suscriba a la comisión de Budapest y como todavía tenemos representantes que no entienden este tema de la jurisdicción y la necesidad de establecer alianzas e iniciativas globales. La asociación de bancos si lo ha entendido y nosotros nos hemos suscrito “el llamamiento de Paris para la confianza y la seguridad del ciberespacio” iniciativa del presidente francés Emmanuel Macron, que ha invitado a grandes empresas globales, asociaciones y empresas que trabajan en el internet para generar espacios que sean seguros, porque son iniciativas que debemos hacer, si el país no lo entiende así y también sus representantes, las instituciones tienen que volverse globales.	Los entrevistados opinan que los delitos transnacionales informáticos se dan al ser el ciberespacio un lugar sin control, que puede involucrar muchos países en un solo hecho ilícito.	Hoy se orienta la lucha hacia los medios tecnológicos ya que estos fueron preparados para identificar equipos y no a personas y generalmente los agraviados son personas y ellos sufren las consecuencias. Así mismo es necesario una norma de carácter internacional para la lucha eficaz.	Los delitos transnacionales se desarrollan en el ciberespacio donde no hay control legal y que la lucha se ha centrado más en la identificación de los equipos y no de personas.

Valoración legal de la evidencia digital en el Perú	¿Cuál es bien jurídico protegido en los delitos informáticos?	El bien jurídico que pone en peligro el delito informático es 'la información: (almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos).	La información de manera general es el valor jurídico protegido pero existen otros como la indemnidad sexual, intimidad y el patrimonio.	Es el dato, lo que hay que proteger es el dato, porque la información ya son los datos que ya están procesados Entonces el bien jurídico protegido es el dato.	La mayoría de entrevistados indica que bien jurídico en los delitos informáticos en la información	El bien jurídico de los delitos informáticos es el dato que es consecuencia del procesamiento de la información	El bien jurídico en los delitos informáticos es el dato que resulta del procesamiento de la información.
	¿Al ser los delitos informáticos delitos transnacionales, las leyes peruanas que han previsto para que estos no queden impunes?	En los delitos informáticos se necesita trabajar en conjunto con otros países ya que no es un delito solo local, también es transnacional. Actualmente el tratado internacional que rige es el Convenio de Budapest o Convenio sobre ciberdelincuencia, creado para combatir el delito informático y generar la cooperación entre los países al cual aún el Perú no se adherido. El aumento de la criminalidad informática en el Perú y a nivel mundial trae consigo consecuencias económicas y numerosos fraudes cometidos por organizaciones delictivas que muchas veces no son denunciados o cuyos delitos son cometidos en el exterior sin que muchas veces exista una sanción.	Ninguna, ya que el Perú aun no forma parte del Convenio sobre ciberdelincuencia (Convenio de Budapest).	Mira hay un antecedente que te pueden interesar en el 2008, Estonia sufrió el ataque más grande de ciberdelincuencia, cuando se hizo el análisis resulta que fue en el Perú donde se había generado la mayoría de ataques, entonces Estonia fue a las naciones Europeas a solicitar una sanción para Perú, pero justamente haciendo el análisis se demostró que no se podía sancionar a nuestro país porque no había un tema intencional de ataque de un país hacia otro. el presidente Obama en una de sus edictos o pronunciamiento síndico de qué Estados Unidos podría repeler con la fuerza de sus fuerzas armadas un ataque Cibernético identificado en otro país, entonces ahí te doy dos ejemplos y el otro tema es del china con las elecciones de Estados Unidos donde se puede apreciar de que se puede influir desde un país hacia otro, usando las redes sociales, el internet, la información no precisa y técnicas de ingeniería social que son los que más se utiliza para engañar a las personas.	Los entrevistados indican que las leyes peruanas en la actualidad no han previsto la lucha de la ciberdelincuencia, considerándose que los delitos informáticos no tienen fronteras. El Perú no se adherido al convenio de Budapest.	La criminalidad informática en el mundo va en aumento en el Perú no se puede denunciar ilícitos que comprometan a otros países así como tampoco existe sanciones en el Código Penal, al no tener una norma de alcance internacional.	Las leyes peruanas no han previsto la lucha contra la ciberdelincuencia al ser estos trasnacionales y no existe sanciones en el código penal al no tener jurisdicción fuera del país

	¿El Perú se encuentra en condiciones jurídicas de poder sancionar los delitos informáticos?	La legislación existente resulta insuficiente, toda vez que continuamente se renuevan las modalidades delictivas en el ámbito informático, asimismo si se tiene presente que en nuestro país las herramientas existentes para contrarrestar dichos ilícitos no resultan ser suficientes, y que poco es el efecto disuasivo en la proliferación del mismo. Aún falta no solo legislar sobre las nuevas actividades delictivas, sino también difundir y explicar la nueva criminalidad informática en su connotación holística.	No, para que suceda ello tendría que crearse una Fiscalía Especializada.	Considero que no, esté es muy simple, tenemos 3 artículos del año 2000 y la ley delitos informáticos del año 2013, que salió después de 8 años porque nosotros insistimos en la necesidad de que haya una ley, pero eso fue producto del hackeo de una cuenta de la esposa de un funcionario del Estado, eso fue el motivo por el cual se buscó, cuál proyecto había para aprobarlo; cuando nosotros proponemos que Perú se adhiera al a la convención de Budapest, no solamente estamos hablando de una iniciativa que nos pone a nivel Global en el primer mundo, estamos hablando de que el consejo de Europa tiene destinado fondos para qué países como los nuestros, puedan adecuar su legislación y puedan tipificar y sancionar efectivamente los delitos informáticos, nosotros no entendemos que cosa es un delito informático en el Perú no se entiende que es un delito informático, porque no saben en donde nos estamos desarrollando en donde nos desenvolvemos, entonces mal podemos nosotros tipificar y sancionar algo como que te comentaba que en Estados Unidos pueden sancionar a un botmaster 15 años y en el Perú no exista, hemos tenido casos de ciudadanos de otras nacionalidades en Sudamérica con más de 100 tarjetas en un cajero automático y no se le pudo detener por delito informático porque acá ese señor es coleccionista de tarjeta y no es un clonador.	El Perú no se encuentra en condiciones jurídicas de sancionar los delitos informáticos de alcance internacional por falta de conocimiento y explicación de esta nueva criminalidad de las autoridades del Estado, así como no tener una política de difusión de su importancia.	Por insistencias particulares a la fecha se logró considerar en el Código Penal sanciones para los ciberdelincuentes.	Al ser la ciberdelincuencia un delito sin fronteras el Perú no cuenta con normas jurídicas que sanciones los delitos informáticos en estas condiciones, lo que hasta la fecha se ha logrado en leyes se dieron por insistencias particulares y no por necesidades verdaderas.

	¿Cree Ud. que la normatividad jurídica en el país, ha previsto el tratamiento de la evidencia digital?	Tratamiento especial de la prueba digital en el Código Procesal Penal del 2004 de manera puntual y especifica No existe, no hay regulación actual como prueba digital, sin embargo el Art. 185 del código procesal penal reconoce al contenido de un audio visual o audio grabado como prueba documental, si entre las fuentes de prueba de un hecho ilícito se encontrara un audio, o un video grabación u otro soporte digital o electrónico, simplemente el desahogo probatorio o actuación probatorio se efectúa en observación del artículo 382 del código procesal penal del 2004.	No existe una normativa aborde sobre el tratamiento de la evidencia digital, sin embargo existe un manual de evidencia digital promovido por una ONG, que recoge las buenas prácticas de otros manuales para el manejo de la evidencia digital. En tanto, la PNP ha elaborado un manual para el recojo de la evidencia digital, que se encuentra a la espera de su aprobación.	Considero que eso es importante, pero que no exista en nuestro ordenamiento jurídico es un reflejo simplemente y de nuestra sociedad que nosotros nos gusta ir por el camino corto no respetamos las reglas; en la mañana estaba conversando con un taxista que me traía y hablábamos del callao, en el callao han puesto algo de tecnología con sistema de videocámaras, no es una ciudad inteligente sino que simplemente son cámaras que están conectadas a equipos para poder detectar la velocidad y todo el mundo anda 60 pero apenas cruza la línea que dice callao hacia lima, aumenta su velocidad a 80 o 90, cuál es la diferencia porque en dos cuadras uno puede ver ciudadanos yendo a 60 y a la siguiente cuadra a 80. Porque hay un sector, un territorio donde se cumple con la ley y esta se cumple con una sanción hay una pena en el otro lado no hay una sanción, entonces donde no se regula adecuadamente las cosas la gente hace lo que quiere, en el ciberespacio es exactamente es igual, porque nuestro país a esto el delincuente lo llama paraísos cibernético, es donde no hay la norma, no hay el procedimiento, no hay la pena entonces está libre y ejemplo de estos hay muchos en Argentina había un delincuente denominado el Gordo España, esta persona había cometido una cantidad de delitos terribles en España y le solicita a la Argentina la deportación, para ello argumentan todo y presentan sus leyes y lo demuestra muy bien todo perfecto, pero cuando llega a la Argentina dice no la puedo mandar porque eso aquí no es delito; y yo digo no había cometido el delito en Internet en Argentina. Entonces qué pasó, pasaron dos años o tres y Argentina actualiza su legislación, qué cosa crees que hizo España mando de nuevo el pedido porque ahora si lo consideraba y lo capturaron y lo deportaron y Argentina ya está suscrito el convenio de Budapest.	Los entrevistados coinciden en afirmar que no existe normatividad jurídica que aborde el tratamiento de la evidencia digital en el Perú.	Que nuestra sociedad no respeta las normas, muchos hacen lo que quieren, el ciberespacio es similar nuestro país es considerado paraíso cibernético.	La evidencia digital en el Perú no cuenta con una normatividad jurídica que determine su tratamiento más aun somos considerados paraíso cibernético por falta de leyes que combatan los ilícitos informáticos en el ciberespacio.

	¿Cuál es el concepto de la evidencia digital en el ámbito jurídico/policial y tecnológico?	La evidencia digital como un tipo de prueba física en donde sus datos pueden ser recolectados, almacenados y analizados con herramientas informáticas forenses y técnicas especiales. Si se la compara con otras formas de evidencia, la prueba digital es única. Si la evidencia fue presentada de manera correcta y su cadena de custodia no fue alterada, puede llegar a ser crucial para resolver cualquier clase de delitos.	Cualquier registro generado por o almacenado en un sistema informático o dispositivo digital que pueda ser utilizado como prueba en un proceso legal.	La evidencia digital es un elemento que debería tener mucha importancia, pero aquí no le dan importancia y te lo digo porque yo he visto manipular evidencias que cualquier abogado podría fácilmente solicitar que no forme parte del proceso, porque esto debe ser formalizado. Por ejemplo la persona que recolecta información o evidencia digital debe tener una certificación, debe tener una profesión, debe tener procedimientos, debe ser una autoridad y debe estar acompañado de la fiscalía; ninguna de esas cosas se dan entonces por eso te digo la evidencia digital en nuestro país lamentablemente no es de interés por falta de conocimiento.	Los entrevistados indican que la evidencia digital es una prueba única, si se le quiere comparar con otras formas de evidencia. Es generada por medios tecnológicos y su tratamiento requiere de una profesión, certificación, legalidad y licencias.	En nuestro país no se le da la importancia. Ya que las mismas autoridades las manipulan contaminándolas y no sirviendo para un proceso legal.	La evidencia digital en nuestro país es tratado como otras evidencias, no se ha establecido legalmente un tratamiento único por sus características, más aun las autoridades manipulan las evidencias contaminándolas y por ende no sirviendo para un proceso judicial.

	¿Qué significa para Ud. La cadena de custodia y si esta se aplica para la evidencia digital?	La Cadena de Custodia es el procedimiento destinado a garantizar la individualización, seguridad y preservación de los elementos materiales y evidencias, recolectados de acuerdo a su naturaleza o incorporados en toda investigación de un hecho punible, destinados a garantizar su autenticidad, para los efectos del proceso.	Procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis, normalmente peritos, y que tiene fin no viciar el manejo que de ellos se haga y así evitar alteraciones, sustituciones, contaminaciones o destrucciones. La cadena de custodia se aplica tanto a la evidencia física así como a la evidencia digital.	La cadena de custodia es importantísimo, fíjate en el momento de recolectar la información también tienes que demostrar que tienes equipo, que has comprado con factura, que tienes software que es legal, que tiene licencia, que tienes el mecanismo utilizando software especializado para la captura de datos, no puede usar cualquier cosa como Encase o herramientas libres, porque para los procesos judiciales la evidencia tiene que ser recolectada de manera autorizada.	Los entrevistados indican que la cadena de custodia es muy importante ya que garantiza la seguridad y preservación de los elementos materiales. Debe ser realizado por personas con conocimiento y con equipos legalmente adquiridos, con licencias.	Que la recolección de la evidencia y su posterior traslado de la evidencia digital, por falta de conocimiento y mal manejo o utilización de herramientas no certificadas conlleva a se alteren y no se puedan utilizar en los procesos judiciales.	La cadena de custodia garantiza la preservación y seguridad de la evidencia digital, si se realiza con personal especializado, equipos certificados y con licencias, una mala práctica de este procedimiento genera que se altere y no se pueda utilizarla para un proceso judicial

	¿Considera Ud. que el personal de la Policía Nacional del Perú está en condiciones de tratar adecuadamente la evidencia digital?	Existe una una insuficiencia de implementación de laboratorios a nivel nacional y existe un centralismo en todo el Perú para las pericias de pruebas digitales y de las tradicionales, para los delitos más comunes se sigue haciendo en Lima. Incluso para los delitos informáticos es más complejo se tiene que remitir a DIVINDAT-PNP de la Av. España y dicha división no existe en el Callao.	Si, la Policía Nacional del Perú, cuenta con personal capacitado que viene laborando en la División de Investigación de Delitos de Alta Tecnología -DIRINCRI.	Sobre los delitos financieros no es DIVINDAT la primera que interviene, tenemos a las Águilas Negras, porque ellos lo que van a hacer es aislar la zona y si están preparados; pero representa al 3 por 1000 de la policía, también ellos cuando van al lugar las evidencias lo derivan a la DIVINDAT. Las Águilas Negras para algunas cosas si está preparado, pero mira los delitos informáticos cambia muy rápido es muy dinámico, entonces no estamos preparados para enfrentarlos; nosotros tenemos otra estrategia, tenemos apoyo de un Cecyt Financiero Europeo y ha sido calificado por dos años consecutivos como el mejor en Europa, entonces eso sí nos da un respaldo para poder enfrentar a una delincuencia internacional que estoy seguro que aquí podríamos hacerlo pero nos tardaríamos demasiado.	Los entrevistados coinciden en indicar que el Personal del Policía Nacional del Perú, no se encuentra capacitado y que no cuenta con el equipamiento necesario para sus investigaciones, que es la DIVINDAT de la DIRINCRI la unidad especializada que investiga los delitos informáticos.	Lamentablemente la Unidad especializada solo funciona en la ciudad de Lima existiendo un centralismo y que no cubre con las exigencias de investigación a nivel nacional. Para contrarrestar la lucha entidades privadas toman sus propias acciones para protegerse	El personal de la PNP no se encuentra capacitado y no cuenta con el equipamiento básico para el cumplimiento de sus funciones, la DIVINDAT es la Unidad especializada en la investigación de delitos informáticos y que esta se encuentra en la ciudad de Lima no teniendo alcance efectivo a nivel nacional.

	¿Considera Ud. si el Estado está abordando la lucha de ciberdelincuencia de manera eficaz?	Considero que necesitamos promover la creación e implementación de Fiscalías Especializadas en Cibercrimen a fin de enfrentar adecuadamente los diversos delitos informáticos a fin de llevar a cabo investigaciones eficientes. El Perú requiere de una política de estado sobre el manejo de internet y desarrollar una campaña de educación entre escolares y adolescentes para que sepan proteger su información en la red.	Considero que el Estado tiene mucho por hacer en materia de ciberdelincuencia, modalidad delictiva que viene creciendo debido a que las personas emplean hoy más que ayer tecnología en su vida personal así como laboral, esto conlleva a las posibilidades de ilícitos informáticos.	Si claro definitivamente ahora el estado tiene personas capacitadas para enfrentar, pero creo que no están en el lugar indicado, tampoco tiene lo básico que es la norma, que se está construyendo pero lamentablemente el ambiente político influye mucho en este tema.	Los entrevistados coinciden que el Estado no aborda la lucha contra la ciberdelincuencia en el país.	Se requiere de Fiscalías especializadas y que si existe personas capacitadas pero que lamentablemente no están en el lugar indicado.	El Estado no aborda eficazmente la lucha contra la ciberdelincuencia, es necesario la creación de las fiscalías especializadas, personas capacitas y normatividad legal.

Tratamiento de la evidencia digital en otros países	8. ¿Conoce Ud. el convenio de Budapest?	El Convenio de Budapest es un tratado internacional creado por los países miembros del Consejo de Europa con el fin de hacer frente a los delitos informáticos a través de mecanismos de homologación de normas de derecho penal sustantivo, estandarización de procesos penales y cooperación internacional.	Es un Convenio sobre ciberdelincuencia o llamado Convenio de Budapest, firmado en el 2001 que busca hacer frente a los delitos cometidos a través de la Internet, mediante la cooperación de los países que la integran y el sector privado.	Mira aquí te doy un ejemplo clarísimo en Colombia tuve la oportunidad de conversar con el jefe de la policía de investigaciones de delitos cibernéticos para Europa, entonces les manifesté nuestro interés de tener contacto y poder compartir información y él también se mostró muy interesado por qué era de Perú, le dije tenemos información de ciudadanos búlgaros que han cometido delitos en Perú, como puedo hacer para pasarte esa información, me respondió y me dijo mira no puedo recibirlo porque estás en un país que no ha suscrito la convención de Budapest; yo al principio no lo entendía y luego entendí claramente lo que me estaba diciendo, ellos respetan mucho las normas y los procedimientos y recibir la información que le daba podría contaminar la evidencia o el contaminarse para poder dar testimonios posteriores, hay que tener respeto por los procedimientos y seguir los protocolos y esas cosas no las entendemos; Entonces yo le dije mira yo soy ciudadano europeo también, tengo doble nacionalidad yo como ciudadano comunitario no te puedo pasar la información y me dijo no te la puedo recibir porque estás en un país que no ha suscrito la convención de Budapest. Bueno y qué hacemos y cómo te puedo dar esa información yo quiero colaborar, entonces me dijo si la captura de esos delincuentes ha sido registrada en algún periódico, correcto donde aparezcan los nombres, tú me puedes pasar eso y yo verificar que esa información sea correcta, como es de un medio de prensa y eso poder compartirlo con la comunidad. Entonces mira la dificultad que tenemos nosotros de enfrentar a una delincuencia que es global con las limitaciones de nuestra legislación local.	Los entrevistados refieren que el Convenio de Budapest es un tratado internacional que hace frente a los delitos cometidos a través del internet, mediante la cooperación internacional	El Perú no es parte de este convenio al no haberse adherido, perdiendo asesoría, legalidad y apoyo para la lucha contra la ciberdelincuencia.	El Convenio de Budapest es un tratado internacional que busca hacer frente a los delitos cometidos por internet, a través de la cooperación y el Perú al no encontrarse adherido al mismo, pierde beneficios en la lucha contra la ciberdelincuencia.

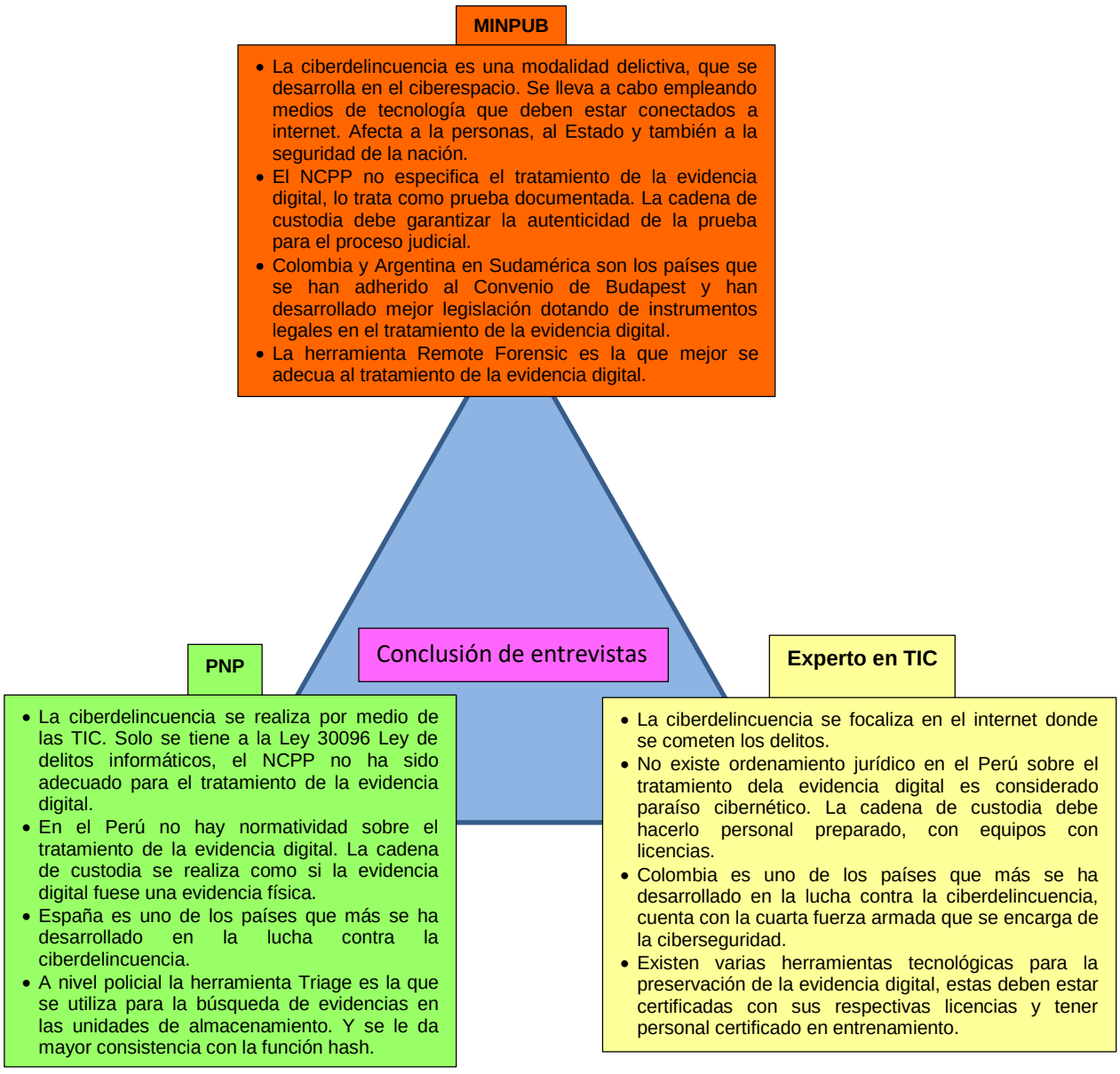
	13. ¿Si conoce Ud. de algún país que actualmente viene enfrentando adecuadamente la lucha contra la ciberdelincuencia desde el ámbito judicial?	Si considero que Colombia y Argentina en América Latina vienen promulgándose leyes que contribuyen a mejorar y dotar de los instrumentos legales contra la lucha del cibercrimen.	Podría mencionar a España, que cuenta con personal contantemente capacitado y la tecnología adecuada, dentro de la región se encuentran Colombia y Brasil.	Podemos mirar a Colombia que tiene una cuarta Fuerza Armada que es la ciberseguridad, pero la verdad que estaba pensando, en Argentina en Chile tú sabes que en una reunión que tuvimos de Celaes en Miami, se presentó la representante de seguridad del Banco Famérica y hablaba sobre ciberdelitos y ella manifestó que el problema más grande que tenía el banco era el phishing, yo me preguntaba el phishing será problema para un banco tan grande, después seguir escuchando dijo que el phishing que afectaba al banco famerica era el que provenía de Perú el problema más grande del banco famerica en ese momento era el phishing qué provenía de Perú y Cuál era el motivo la calidad del engaño del phishing, entonces los peruanos porque tienen mucha imaginación y el problema de Sudamérica relacionado con ciberdelitos son los hackers peruanos y brasileros. Porque algunos han estudiado en los países de Rusia antigua, terminaron fueron captados por las bandas rusas y ya están de regreso hablan el idioma y aprendieron la tecnología, yo estoy seguro si esas personas practicaran el bien tendrían unas empresas maravillosas y producirían muchos ingresos al país pero sin embargo, se van a lo fácil y te comento algo más en Cybertec de Israel en el 2017 Benjamín Netanyahu habla al empresariado de Israel y les dice hace 5 años yo propuse alcanzar estar entre las cinco primeras economías en ciberseguridad y en el 2017 les decía a todos tus empresarios que esa meta la habían alcanzado y el 20% de la facturación de ciberseguridad global es de Israel, dime tú si no es importante, si no es algo interesante para el país, poder darle la oportunidad los jóvenes orientarlos a estudiar temas de ciberseguridad de ciberdefensa para que puedan también generar empresas que a su vez generan ingresos y desarrollo para el país.	Los entrevistados indican que a nivel Latinoamérica los países de Colombia, Argentina y Brasil han desarrollado mejores estrategias en la lucha contra la ciberdelincuencia y en Europa España es uno de los países con mejor preparación.	Las entidades privadas por necesidad propia han implementado mejor su seguridad con tecnología y estrategias de países extranjeros.	Los países que mejores resultados han obtenido en la lucha contra la ciberdelincuencia son Colombia, Argentina y Brasil y en Europa España.

	14. ¿Cree Ud. que organizaciones privadas y/o particulares vienen aplicando soluciones para contrarrestar la ciberdelincuencia?	Las empresas tecnológicas son un aliado indispensable en la lucha contra la ciberdelincuencia. Es necesario aumentar la participación de los sectores público y privado para abordar inquietudes comunes como mejorar la educación y poner freno al material de abuso en línea.	Las empresas privadas en los últimos años han tomado conciencia de los peligros a los que se encuentra expuesto su información, para ello vienen implementando políticas de seguridad para proteger sus activos.	Si tú quieres identificar algo y darle validez en el internet o de un medio cibernetico lo que hay que usar es certificado digital porque siempre identifica la persona, va apunta a la capa 8 que te estaba diciendo de identificación de personas, pero el certificado lo que te garantiza es que esa persona que genero el documento es quien dice ser y funciona para los teléfonos, laptops o cualquier computadora, lo importante es que tú puedas obtener ese certificado con una entidad en registro que es la que te va a identificar como persona, que tengas una identidad certificadora y que tengas una identidad nacional, son tres niveles ahora el notario digital es eso la entidad certificadora, es el notario y si quieres ir más allá, ahora los sistemas están cambiando para usar tecnología Blockchain de alguna forma también se vuelven como notario básicamente es algo que lo llaman el General electry o sea es el libro contable donde se registra todas las modificaciones o alteraciones de la data y si a eso tú le pones un certificado digital ya lo estás garantizando que la información sea legal	Los entrevistados afirman que efectivamente las entidades privadas o particulares son las vienen previendo mejor la lucha contra la ciberdelincuencia.	En el sector público lamentablemente no ha desarrollado estrategias de prevención ante ataques de los ciberdelincuentes.	Las entidades privadas son las que mejores resultados han obtenido en la lucha contra la ciberdelincuencia, el sector público en nuestro país no ha desarrollado estrategias de prevención en la lucha contra la ciberdelincuencia.
Procedimientos tecnológicos de la evidencia digital	15. ¿Conoce de herramientas tecnológicas o jurídicas eficaces que ayuden a dar la legalidad a las evidencias digitales?	En materia procesal me documente sobre la utilización del remote forensic como herramientas de investigación. Ella sugiere a los países la adopción de una norma a nivel nacional que prevea estas técnicas de investigación previendo la excepcionalidad de la medida y un uso restrictivo atendiendo a la potencialidad de afectación a la intimidad que significa su uso.	El Triage consiste en realizar una búsqueda rápida empleando criterios sencillos sobre la estructura del disco, evitando profundizar las búsquedas en áreas especiales del disco. La realización de una copia o imagen forense, en la escena de delito mediante una copia	Hay herramientas que están certificadas para poder extraer información del celular y preservarla como evidencia, son herramientas válidas para poder certificar y estas herramientas deben estar acompañadas de personal capacitado con el conocimiento y la certificación necesaria, con los protocolos de cadena de custodia y con la participación de la autoridad tanto de la denuncia y la de la investigación para darle el marco de la legalidad.	Los entrevistados refieren herramientas tecnológicas como remote forensig, el triage, la función hash.	Es necesario que las herramientas tecnológicas estén validadas y certificadas, con personal capacitado, para que brinden la certificación de sus procesos.	Herramientas como remote forensig, el triage, la función hash vienen dando buenos resultados en el tratamiento de la evidencia digital, para ello se requiere que ellas estén validadas y

			bloque a bloque bit a bit del contenido digital almacenado, el que es autenticado mediante una función HASH.				certificadas.

Anexo 6. Triangulación de entrevistas, análisis documental y observación.

Conclusión de entrevistas



Conclusión de entrevistas

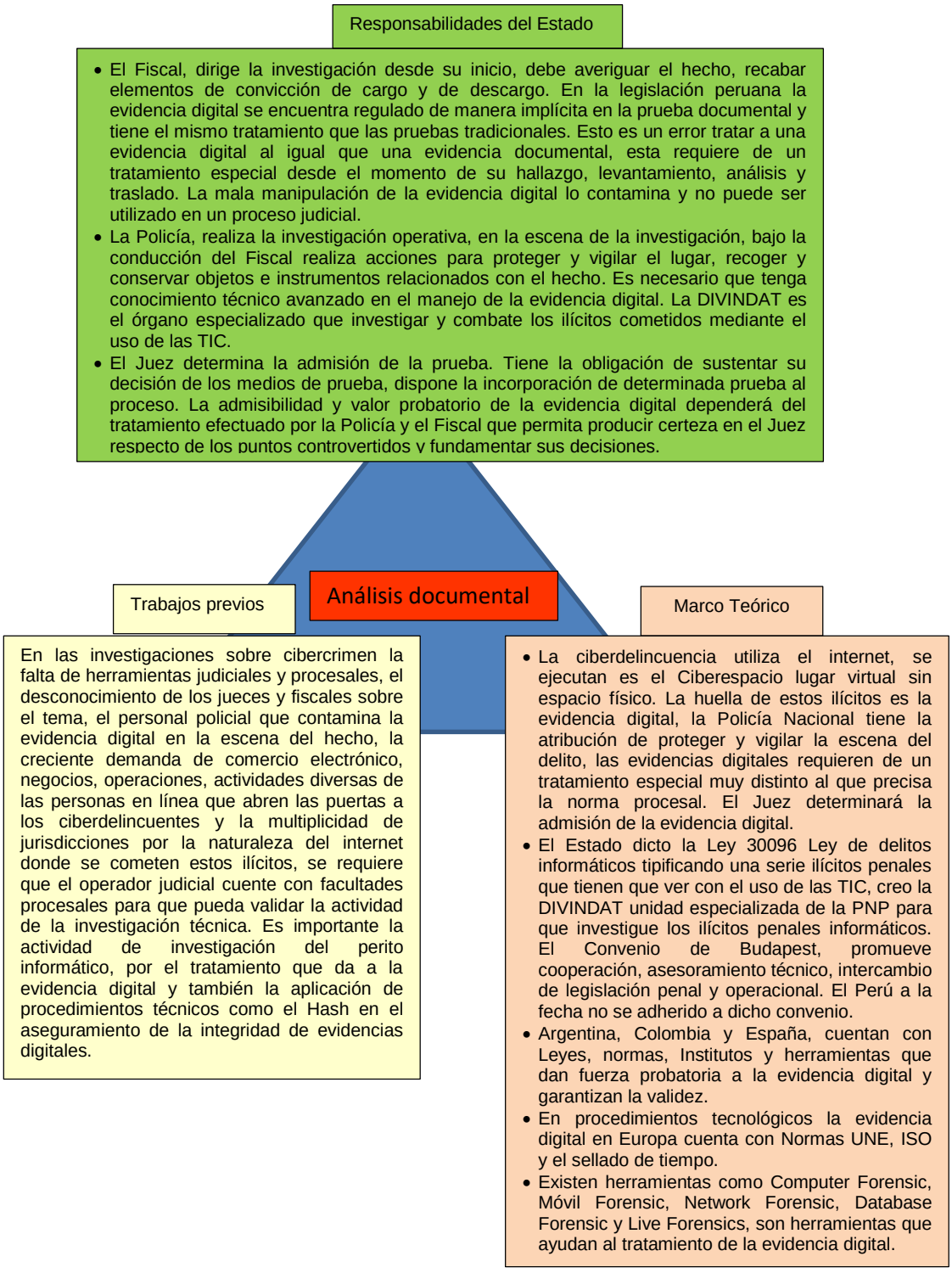
La ciberdelincuencia se desarrolla en el ciberespacio por medio de las Tic conectados a internet.

En el Perú no hay normatividad jurídica sobre el tratamiento de la evidencia digital y la Cadena de Custodia se realiza como si fuese una evidencia física.

España, Colombia y Argentina son los países que mejor se han desarrollado en la lucha contra la ciberdelincuencia, además son parte del Convenio de Budapest.

Existen varias herramientas como el Remote Forensic, Triage para el tratamiento de la evidencia digital, estas deben estar certificadas con licencias y contar con personal capacitado.

Conclusión de análisis documental



Conclusión de análisis documental

Es un error tratar a una evidencia digital como una evidencia documental, esta requiere de un tratamiento especial desde el momento de su hallazgo, levantamiento, análisis y traslado. La mala manipulación de la evidencia digital lo contamina y no puede ser utilizado en un proceso judicial.

El Fiscal, dirige la investigación desde su inicio, debe averiguar el hecho, recabar elementos de convicción de cargo y de descargo. En las investigaciones sobre cibercrimen la falta de herramientas judiciales y procesales, el desconocimiento de los jueces y fiscales sobre el tema, el personal policial que contamina la evidencia digital en la escena del hecho, la creciente demanda de comercio electrónico, negocios, operaciones, actividades diversas de las personas en línea que abren las puertas a los ciberdelincuentes y la multiplicidad de jurisdicciones por la naturaleza del internet donde se cometen estos ilícitos, se requiere que el operador judicial cuente con facultades procesales para que pueda validar la actividad de la investigación técnica.

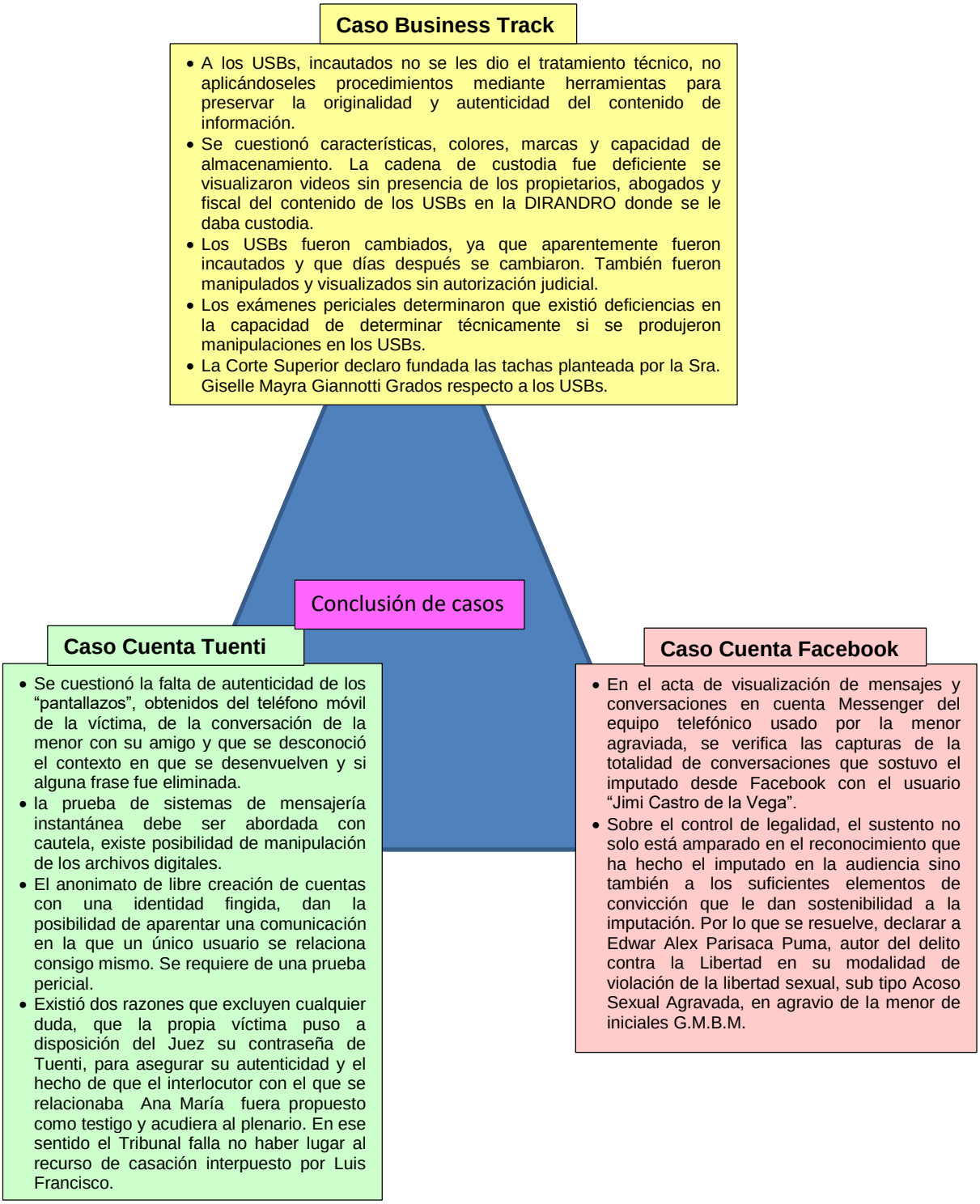
La ciberdelincuencia utiliza el internet, se ejecuta en el Ciberespacio lugar virtual sin espacio físico. La huella de estos ilícitos es la evidencia digital, la Policía Nacional tiene la atribución de proteger y vigilar la escena del delito, las evidencias digitales requieren de un tratamiento especial muy distinto al que precisa la norma procesal. El Juez determinará la admisión de la evidencia digital.

El Estado dicto la Ley 30096 Ley de delitos informáticos tipificando una serie ilícitos penales que tienen que ver con el uso de las TIC, creo la DIVINDAT unidad especializada de la PNP para que investigue los ilícitos penales informáticos. El Convenio de Budapest, promueve cooperación, asesoramiento técnico, intercambio de legislación penal y operacional. El Perú a la fecha no se adherido a dicho convenio.

Argentina, Colombia y España, cuentan con Leyes, normas, Institutos y herramientas que dan fuerza probatoria a la evidencia digital y garantizan la validez. En procedimientos tecnológicos la evidencia digital en Europa cuenta con Normas UNE, ISO y el sellado de tiempo.

Existen herramientas como Hash, Computer Forensic, Móvil Forensic, Network Forensic, Database Forensic y Live Forensics, son herramientas que ayudan al tratamiento de la evidencia digital.

Conclusión de Análisis de Observación.



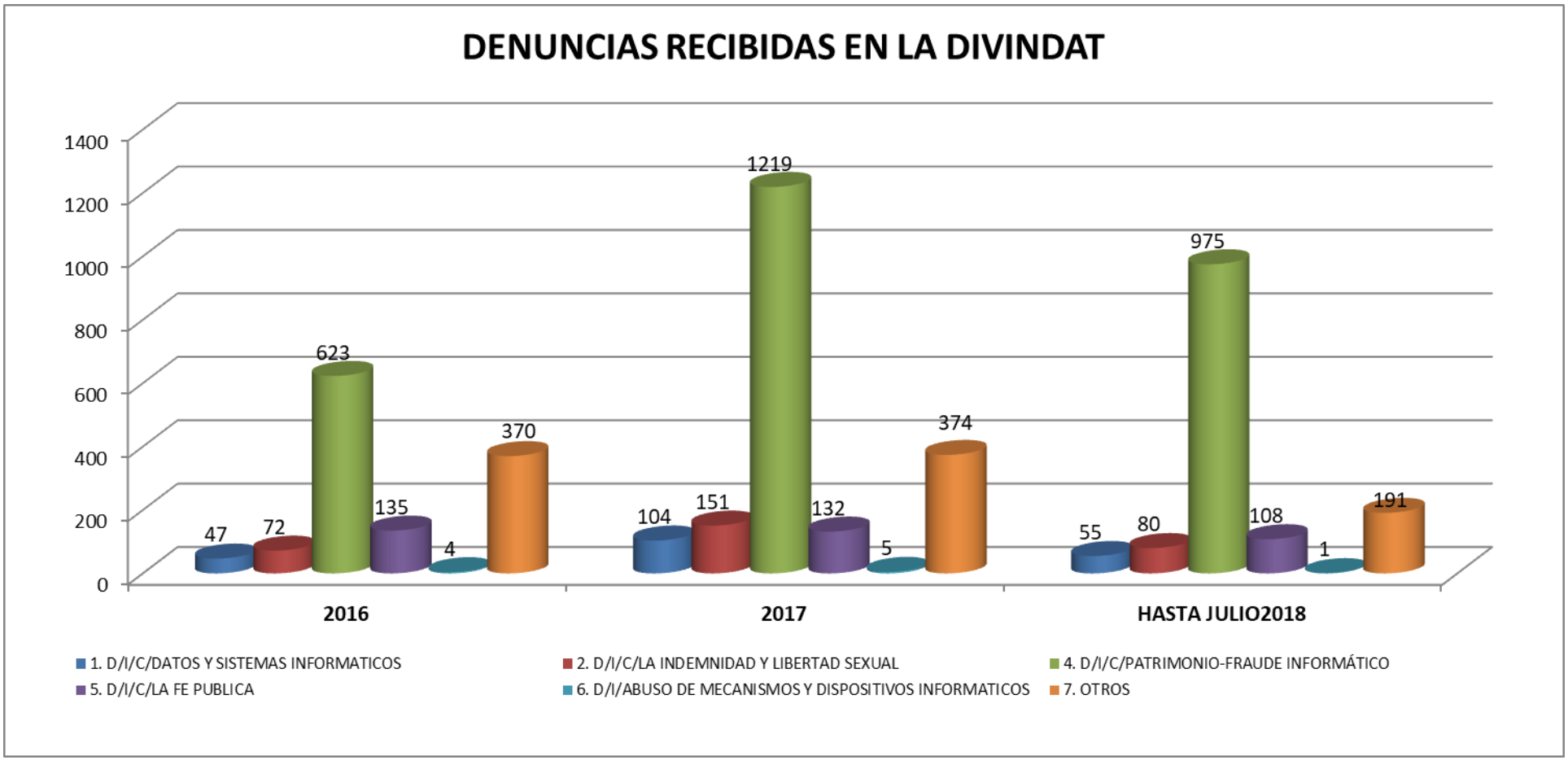
Conclusión de Análisis de observacion

La falta de tratamiento especializado en el recojo de evidencias digitales en la escena del hecho, por parte del personal policial resulta gravitante en la preservación de la originalidad y autenticidad del contenido de información.

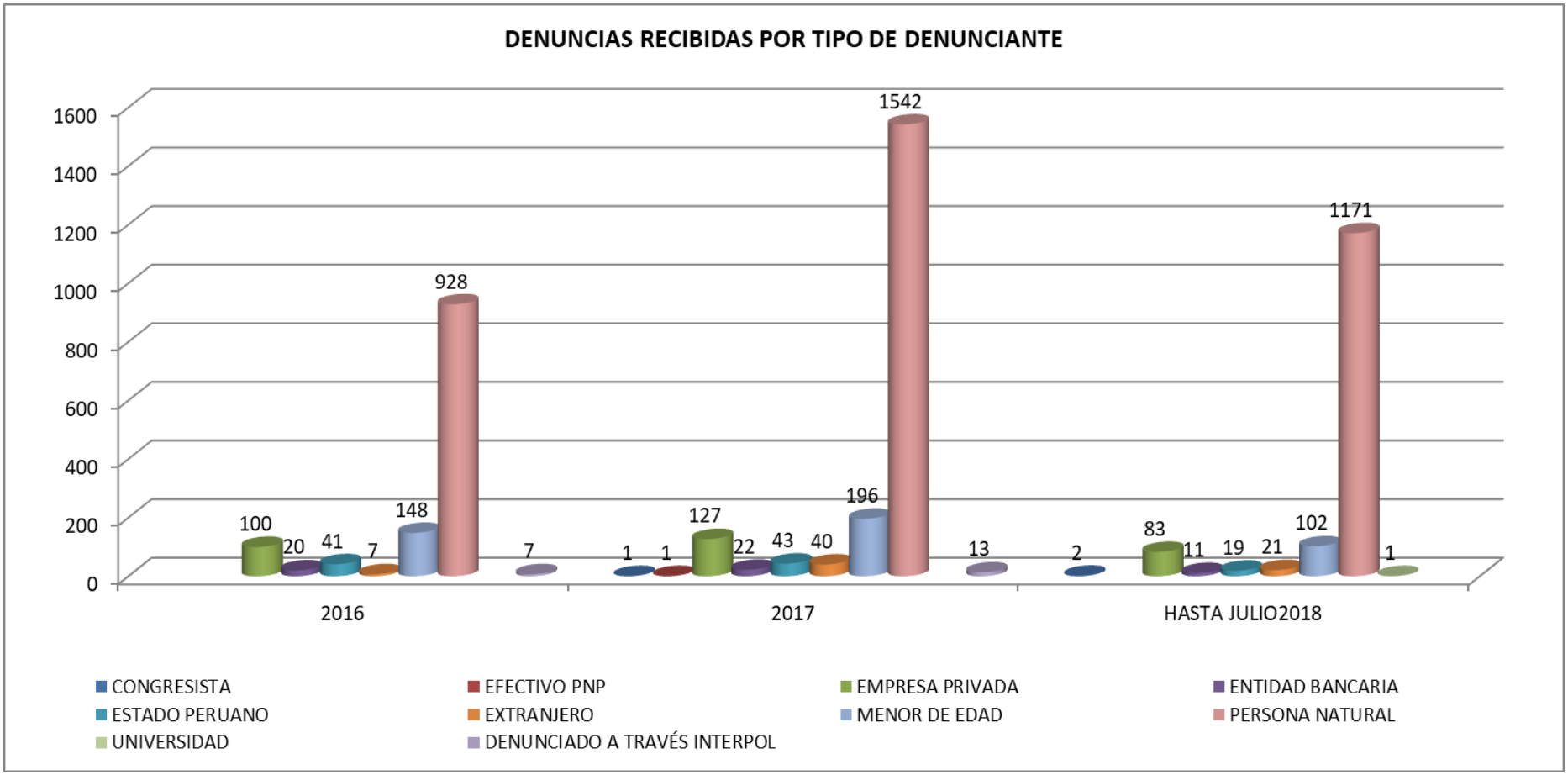
La presentación de evidencias digitales en impresiones de papel de mensajes escritos en redes sociales, no resulta suficiente, en casos de flagrancia es importante incautar el medio tecnológico de donde se hizo la afectación el cual será un elemento de convicción contundente.

Los pantallazos obtenidos de conversaciones en redes sociales de medios tecnológicos deben estar acompañados de elementos que aseguren su autenticidad, ya que existe la posibilidad de manipulación del archivo o la identidad fingida.

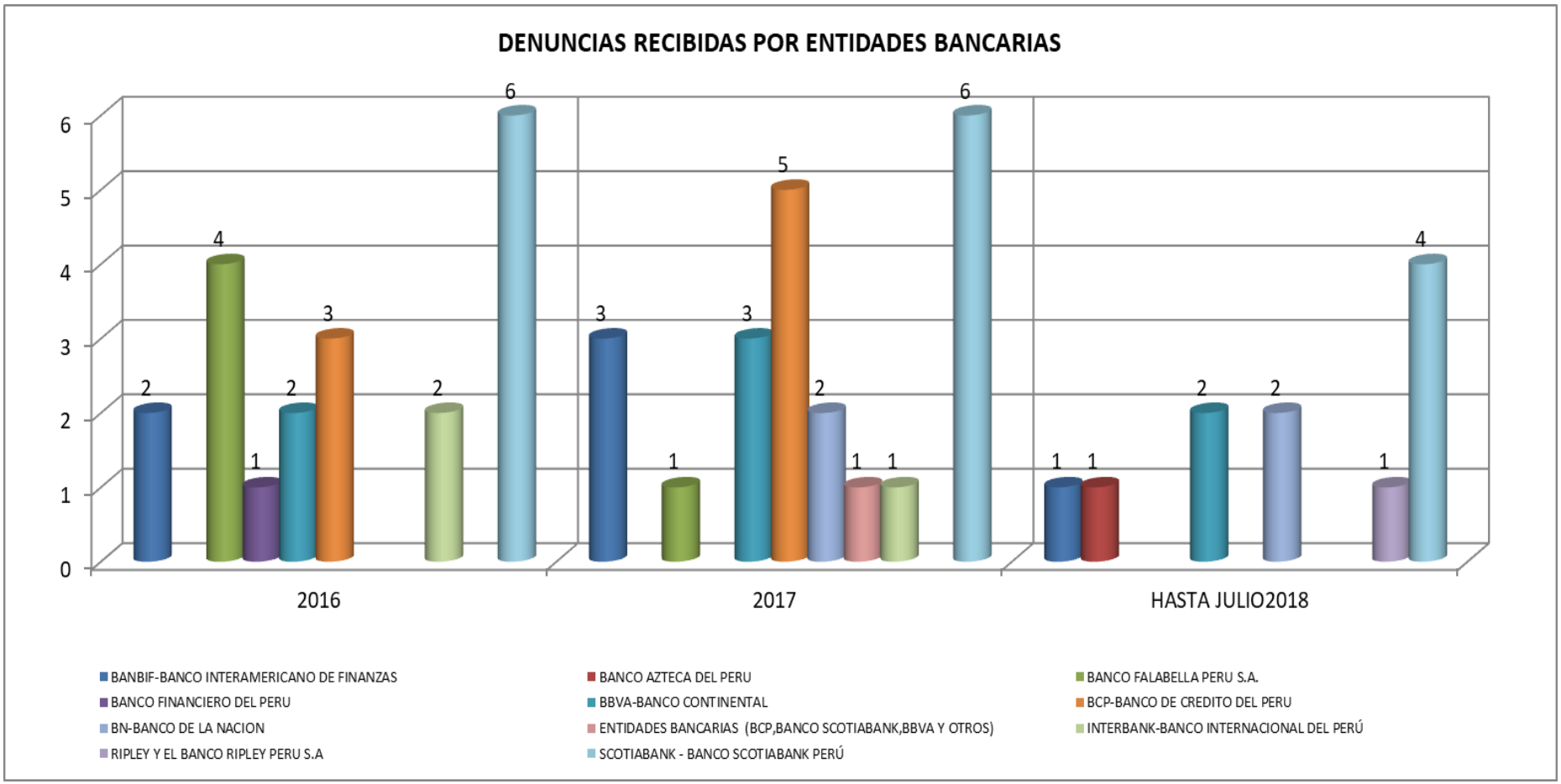
Anexo 7. Estadísticas de incidencia delictiva de Delitos Informáticos



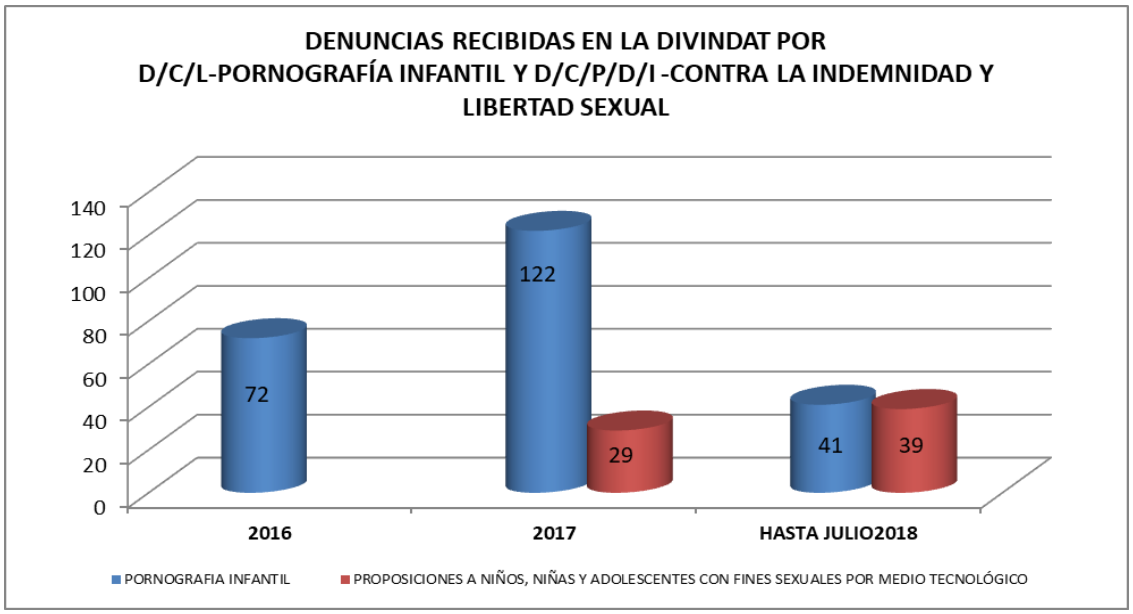
En el gráfico se puede apreciar que son los Delitos Informáticos contra el Patrimonio-Fraude Informático (entre la que se encuentran, transferencia de fondos fraudulentos, clonación de tarjetas, compras fraudulentas por internet, entre otros), la que más se denuncia.



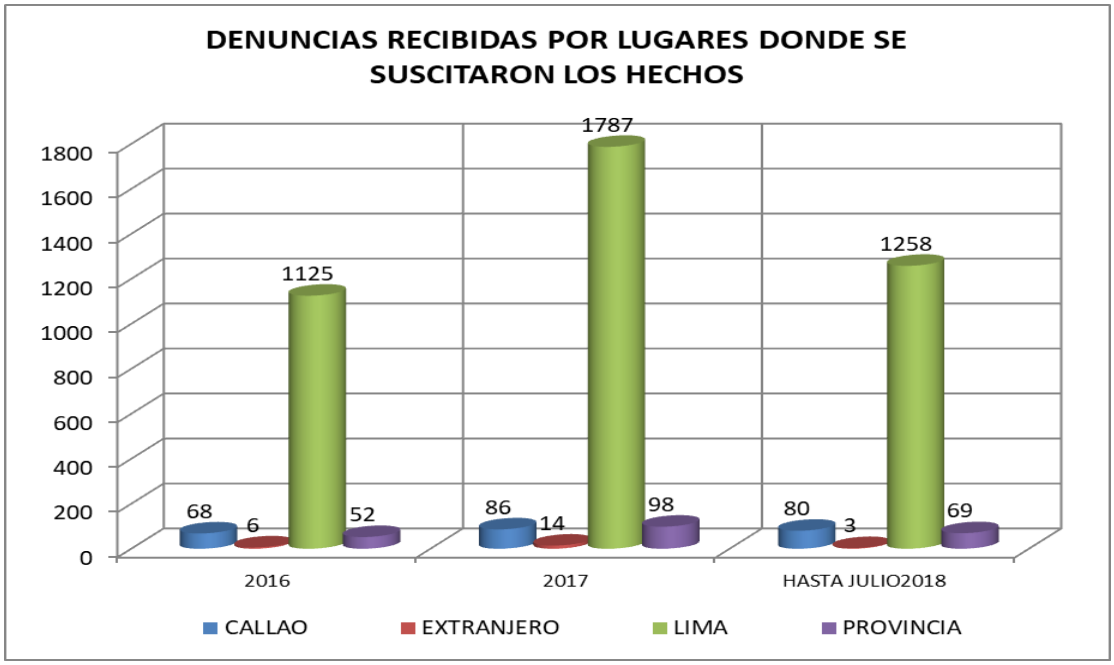
Las personas naturales son las que mayormente denuncian, por ser las principales víctimas de los Delitos cometidos haciendo uso de las TIC, luego una preocupante cifra de menores de edad, y en un tercer lugar las empresas privadas, Las entidades bancarias por un tema de imagen están entre las que menos denuncian algún tipo de ataque a sus sistemas.



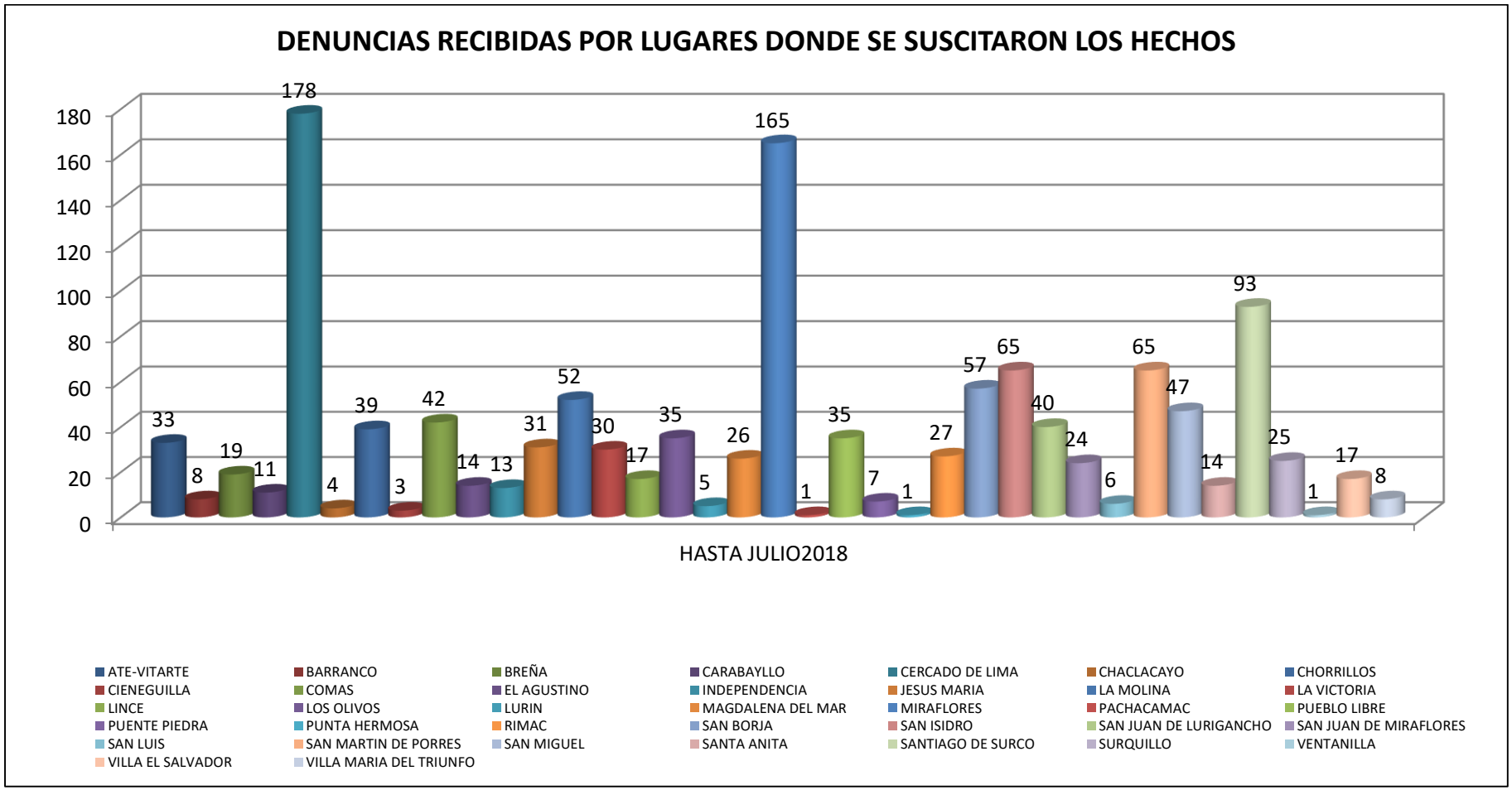
Entre las Entidades Bancarias que más han denunciado en los últimos tres (03) años, tenemos al Scotiabank y al Banco De Crédito, siendo los que menos denunciaron Interbank y Banco Financiero.



Se puede observar que las propuestas a niños, niñas y adolescentes con fines sexuales a través de médios tecnológicos se ha elevado, por ser los menores los que pasan más tiempo haciendo uso de estas tecnologías, sin supervición, y exponiendose a las personas que aprovechandose de ellas los obligan a realizar actividades de connotación sexual, bajo amenaza que en muchas ocasiones termina en una violación.

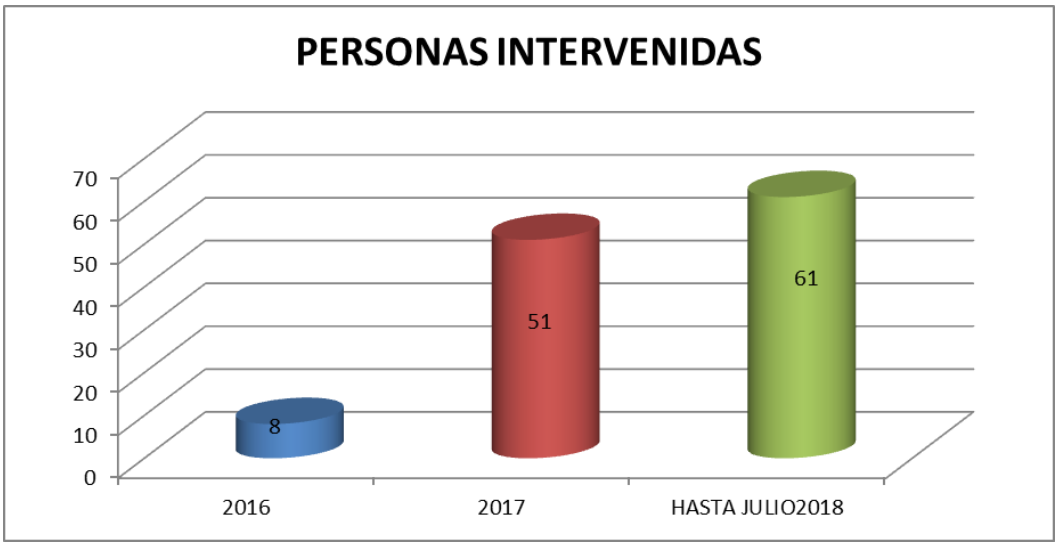


El lugar de mayor incidencia delictiva, en Delitos Informáticos es Lima, seguido del Callao, en ambos casos superan las duncinas del año 2016.

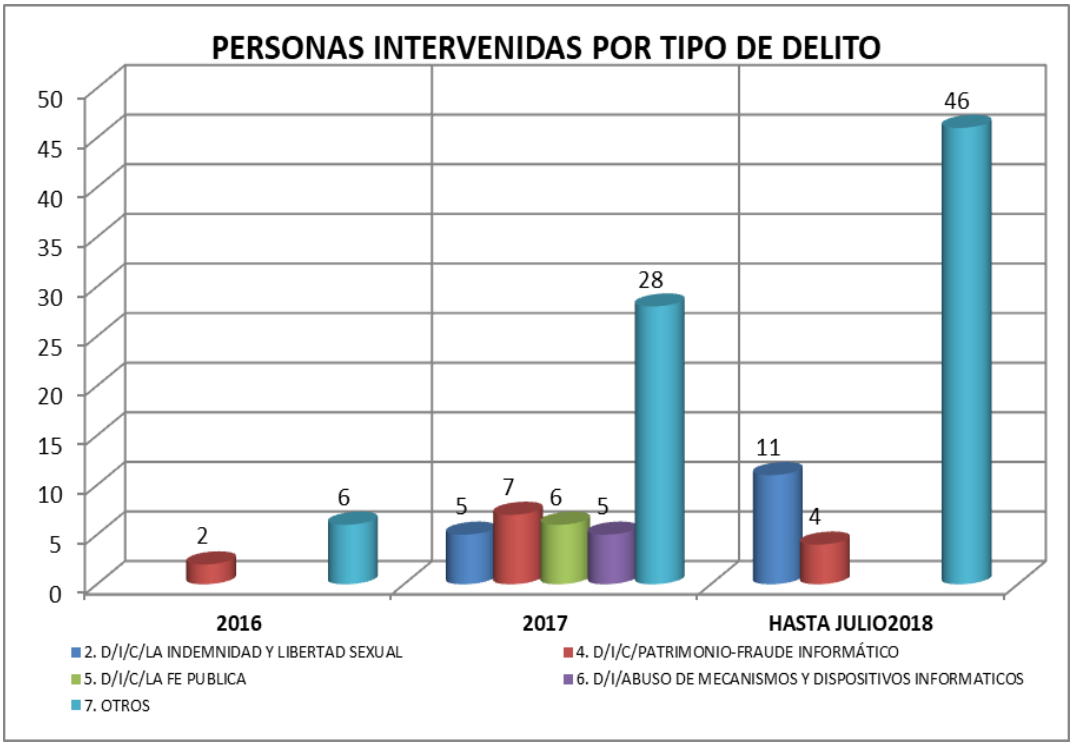


En lo que va del año, los distritos con mayor incidencia en Delitos Informáticos son Lima, seguido de Miraflores y Santiago de Surco, siendo los menos perjudicados Punta Hermosa, Pachacamac y Ventanilla.

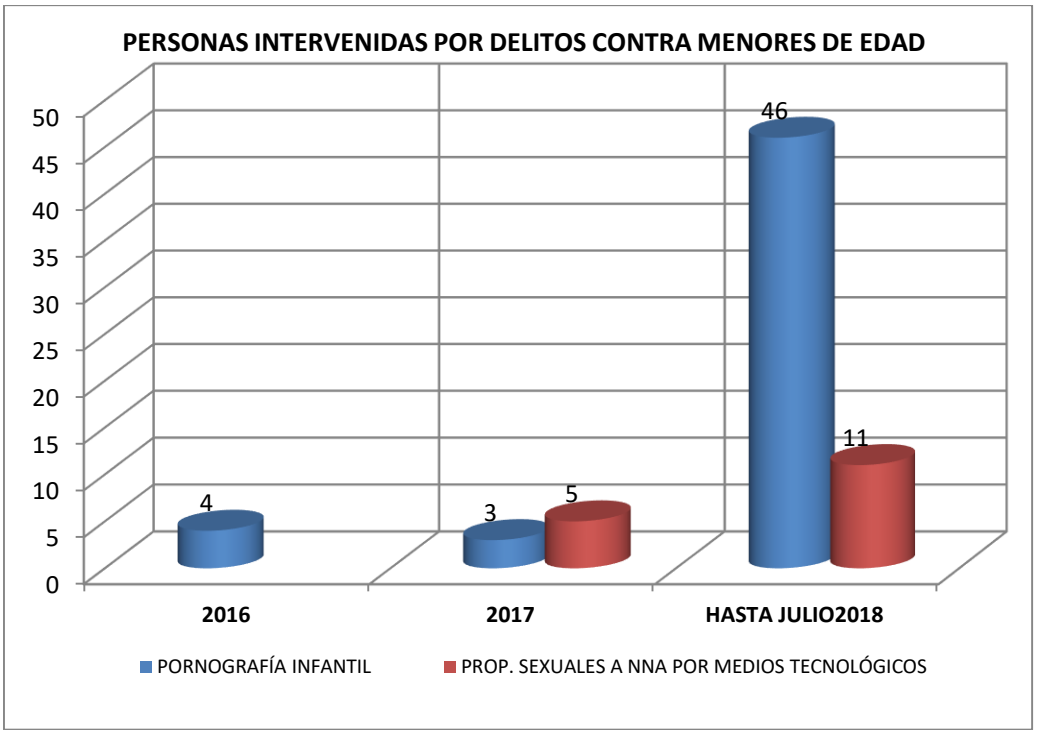
Áreas de intervención desde su sector (prevención, persecución del delito, reinserción, contención de víctimas, entre otros)



En los últimos tres años se ha logrado la intervención y detención de CIENTO VEINTE (120) personas una de ellas menor de edad, por Delitos Informáticos.



Se puede apreciar que el Delito Informático contra la Indemnidad y Libertad Sexual es el que se ha incrementado en los últimos 3 años llegando a duplicar su valor respecto al del año anterior, seguido del Delito Informático Contra el Patrimonio-Fraude Informático.



La cantidad de personas intervenidas por el delito de Pornografía Infantil es el que más se ha incrementado durante el presente año.

ANEXO 8. Caso Business Track. Petro audios

EXP. N ° 99-09 (527-09)

SENTENCIA

Lima, veintitrés de Marzo
Del año dos mil doce.

VISTA; en Audiencia Oral y Pública, el Juzgamiento incoado contra: **ELÍAS MANUEL PONCE FEIJOO, CARLOS ALBERTO TOMASIO DE LAMBARRI, GISELLE MAYRA GIANNOTTI GRADOS, MARTÍN ALBERTO FERNÁNDEZ VIRHUEZ, JESÚS MANUEL OJEDA ANGLES, JESÚS JUAN TIRADO SEGUÍN, ALBERTO OSWALDO SALAS CORTEZ Y PABLO ERIKS MARTELL ESPINOZA,** por el delito Contra la Libertad - Violación del Secreto de las Comunicaciones – **Interceptación Telefónica** en calidad de integrantes de una organización criminal en agravio de Rómulo Augusto León Alegría, Alberto Quimper Herrera, Alberto Fortunato Marcos Ortega, Roberto Enrique Paredes Chirinos, José María Revilla López, Estudio Aurelio García Sayán Abogados S.C.R.Ltda., Remigio H. Morales Bermúdez Pedraglio, Elizabeth Schwarz de Acha de Olcese, Virly del Carmen Torres Curvelo, Rogelio Canches Guzmán, Isabel Paiva Zárate, Genaro Delgado Parker, ONG GRUFIDES, Empresa AMBEV PERU, Agroindustria LAREDO, Estudio Quimper & Abogados Asociados, Estudio Jurídico Enrique Bardales & Asociados, Estudio Linares Abogados S.C.R.Ltda; contra:. **ELÍAS MANUEL PONCE FEIJOO, CARLOS ALBERTO TOMASIO DE LAMBARRI, GISELLE MAYRA GIANNOTTI GRADOS, MARTÍN ALBERTO FERNÁNDEZ VIRHUEZ, JESÚS MANUEL OJEDA ANGLES y JESÚS JUAN TIRADO SEGUÍN** por el delito contra la Libertad - Violación del Secreto de las Comunicaciones – **Interceptación Telefónica** en calidad de integrantes de una organización criminal en agravio del Estudio Jurídico Fernández Concha SCRL (Estudio Fernández – Concha Sociedad Civil de Responsabilidad Limitada), Empresa Trupal S.A., Alexander Martín Kouri Bumachar, Municipalidad Provincial del Callao; y contra. **ELÍAS MANUEL PONCE FEIJOO, CARLOS ALBERTO TOMASIO DE LAMBARRI, GISELLE MAYRA GIANNOTTI GRADOS, MARTÍN ALBERTO FERNÁNDEZ VIRHUEZ y JESÚS MANUEL OJEDA ANGLES** por el delito contra la Libertad – Violación del Secreto de las Comunicaciones – **Violación de Correspondencia** en calidad de integrantes de una organización criminal en agravio de Rómulo Augusto León Alegría, Alberto Alfonso Borea Odría, Francisco Ricardo Soberón Garrido, Alex Ganoza Céspedes, Isaac Alfredo Barnechea García, Aníbal Gonzalo Raúl Quiroga León, Blanca Rosa Rivera Talavera, Carlos Federico Rubina Burgos, César

Antonio Silva Ygnacio, César Augusto Nakasaki Servigón, Cristina Matossian Osorio de Pardo, Carlos Motte Picote, Fernando Tuesta Soldevilla, Fernando Miguel Rospigliosi Capurro, Giovanna Fabiola Vélez Fernández, Guido Rodrigo Lucioni Struque, Gustavo Adolfo Díaz Palacios, Víctor Hiroshi Aritomi Shinto, Jaime Adolfo Crosby Russo, Javier Maximiliano Alfredo Valle Riestra Gonzáles Olaechea, Guillermo Javier Estela Bravo, Jorge Armando Zarate Sousa, José Antonio García Belaunde, José Moisés Asca Montoya, Julio Alberto Ortiz Cerro, Luciana Milagros León Romero, Lucy Esther Calderón Bondani, Luis Juan Alva Castro, Luis Humberto Delgado Aparicio Porta, Alan Gabriel Ludwig García Pérez, Luis Kishimoto Higa, Luis Alberto Silva Santisteban, Marco Antonio Torrey Motta, Mario Díaz Lugo, María Luisa De Cossio De Gonzáles Posada, Mariella Natalia Trujillo Württelle, Martín Carlos Alberto Ugarriza Wetzell, Miguel Aragón Gastón, Miguel Raúl Arbulú Alva, Raúl Enrique Ortecho Castillo, León Gonzálo Rivera Talavera, Víctor Rolando Sousa Huanambal, Ricardo Miguel Pinedo Caldas, Rómulo Diego León Romero, Rosario Urando Prado, Sintia Paniora Alica, Mark Vito Villanella, Rosa Yuri Kobayashi Seki, Aldo Eduardo Bresani Torres, Ana Mariela Edith Guimas Reyna, Luis Bernardo Guillermo Guimas Reyna, Augusto Raymundo Urrutia Prugue, José Gabriel Del Castillo Flores, Blanche Marie Arévalo Fernald, Guillermo Herrera Montesinos, Héctor Jesús Chunga Morales, Bertha Beatriz Somocurcio León, Javier Diez Canseco Montero, Jorge Alfonso Alejandro Del Castillo Gálvez, María Del Pilar Tello Leyva, Carmen Marusia Ruiz Caro Reyes, Miroslav Lauer Holoubek, Pedro Saúl Castillo Carrillo, Remigio H. Morales Bermúdez, Ricardo Letts Colmenares, Sally Bowen, Mariella Aida Balbi Scameo, Baruch Ivcher Bronstein, Eduardo Hochschild Beeck, Empresa Editora Gaceta Jurídica, Estudio Quimper & Abogados Asociados, Estudio Valle Riestra, Instituto Mundo Libre, Revista Caretas – Empresa Editora Multimedia S.A.C., Villarán & Rodrigo S.A.C., EPRODICA – Equipo de Promoción y Desarrollo de Ica, Asociación Civil Foro Democrático, Instituto para una Alternativa Agraria C., Perú Monitor S.A., ONG APRODEH, Sindicato Unico de Telefonía, DEMUS – Estudio para la Defensa y los Derechos de la Mujer, Mitchell Kenneth Trigueros Vela, Jennifer Karoll Miller Arbocco, Dora María Avendaño Arana, Claude Maurice Mulder Bedoya, Ketty Meyling Wong Ayon, Miguel Omar Alberto Reyes Custodio, Humberto Martín Ortiz Pajuelo, Yanina Del Pilar Pando León, Luis Almanzor Sánchez De La Puente, Julio César Del Águila Aguirre, Estudio Jurídico Barturen & Castillo Abogados Sociedad de Responsabilidad Limitada, Heriberto Manuel Benítez Rivas, Juan Francisco Nino Boggio Ubillus, Jorge Arturo Nicolás Lucar De La Portilla, Hugo Ernesto Jiménez Torero, Juan Miguel Servigón Nakano, Flores Tijero & Abogados (Flores Tijero & Asociados SAC), Carlos Fernando Raffo Arce y Javier Diez Canseco Cisneros; contra: **ELÍAS MANUEL PONCE FEIJOO, CARLOS ALBERTO TOMASIO DE LAMBARRI, GISELLE MAYRA GIANNOTTI GRADOS, MARTÍN ALBERTO FERNÁNDEZ VIRHUEZ, JESÚS MANUEL OJEDA ANGLES, JESÚS JUAN TIRADO SEGUÍN, ALBERTO OSWALDO SALAS CORTEZ, PABLO ERIKS MARTELL**

PARTE PRELIMINAR

1.- CONFORMACIÓN DEL TRIBUNAL.-

El Colegiado a cargo del Juzgamiento se encuentra conformado por los señores Jueces Superiores Iván Alberto Sequeiros Vargas, Presidente y Director del Debate, Aissa Rosa Mendoza Retamozo y Antonia Esther Saquicuray Sánchez, quienes se avocaron a la presente causa mediante resolución de fecha 08 de marzo del dos mil once - conforme es de verse de autos de fojas 108877 del tomo 187.

2.- IDENTIFICACIÓN DE LAS PARTES.-

2.1.- Por el Ministerio Público.-

El señor Fiscal Superior doctor Tony Washington García Cano y Fiscal Superior Adjunta doctora Maritza Rosa Alzugaray Cordero de la Segunda Fiscalía Superior Especializada en Criminalidad Organizada.

2.2.- Por las defensas de los acusados.-

1.- Por Elías Manuel Ponce Feijoo, el doctor Edward Hernán Sánchez Rozas identificado con carnet del Colegio de Abogados de Lima número 46296.

2.- Por Carlos Alberto Tomasio De Lambarri, el doctor Carlos Alberto Villafuerte Alva identificado con carnet del Colegio de Abogados de Lima, número 37258.

3.- Por Giselle Mayra Giannotti Grados, la doctora Madelaine Milagros Reyes Gastelú identificada con carnet del Colegio de Abogados de Lima, número 44204; doctor Hugo Manuel Canevaro Fernández identificado con carnet del Colegio de Abogados de Lima, número 18289; José Francisco Urquizo Olaechea, identificado con carnet del Colegio de Abogados de Lima, número 9697.

4.- Por Martín Alberto Fernández Virhuez, el doctor Walter Adán Chinchay Carbajal identificado con Carné del Colegio de Abogados de Lima, número 25994 y el doctor Juan Carlos Siu Romero identificado con carnet del Colegio de Abogados de Lima, número 22081.

5.- Por Jesús Manuel Ojeda Angles, el doctor Vladimir Jorge Cristóbal Gonzáles identificado con carnet del Colegio de Abogados de Lima número 43555.

6.- Por Jesús Juan Tirado Seguin, el doctor Manuel Lizardo Huertas Gonzáles identificado con carnet del Colegio de Abogados de Lima número 31450 y el doctor Jorge Luis Muñoz Quevedo identificado con carnet del Colegio de Abogados de Lima número 45117.

7.- Por Alberto Oswaldo Salas Cortez, la defensora de oficio doctora Judith Rebaza Antúnez identificada con carnet del Colegio de Abogados de Puno 805.

8.- Por Pablo Eriks Martell Espinoza, la defensora de oficio doctora Judith Rebaza Antúnez identificada con carnet del Colegio de Abogados de Puno 805.

2.3.- Por la Parte Civil.-

1.- Procuraduría Pública Anticorrupción, representada por el doctor Eddy Adrián Vizcarra, con carnet del Colegio de Abogados 28523, constituida en Parte Civil por resolución de fecha 13 de julio de 2010 - fojas 103563 del tomo 177. [1]

2.- Rómulo Augusto León Alegría, constituido en Parte Civil por resolución de fecha 09 de febrero del 2009 - fojas 418 del tomo dos.

3.- Alberto Quimper Herrera, constituido en Parte Civil por resolución de fecha 09 de febrero del 2009 – fojas 502 del tomo 2.

4.- Alexander Martín Kouri Bumachar, constituido en Parte Civil por resolución de fecha 24 de marzo del 2010 – fojas 87316 del tomo 142.

5.- Rogelio Antenor Canches Guzmán, constituido en Parte Civil por resolución de fecha 11 de enero de 2010 - fojas 49737 del tomo 78.

6.- Isabel Paiva Zárate, constituida en Parte Civil por resolución de fecha 12 de febrero del 2010 - fojas 70976 del tomo 107.

---

[1] * Mediante resolución de fecha ocho de julio del dos mil diez se tiene por sustituido al Procurador Público del Ministerio de Transportes y Comunicaciones por el Procurador Público Especializado en Delitos de Corrupción – fojas ciento tres mil ciento nueve del tomo ciento setenta y seis.

PARTE PRIMERA

CAPITULO I

ANTECEDENTES

I.- DIFUSION DE LOS PETROAUDIOS.-

El día domingo 05 de octubre del 2008 en el Programa Dominical "Cuarto Poder" de América Televisión se difundió audios en las que se registraba supuestamente conversaciones sostenidas entre Alberto Quimper Herrera – Ejecutivo de PERU- PETRO, entidad estatal a cargo de promover la inversión extranjera en el sector petrolero y Rómulo León Alegría- Ex Ministro Aprista, discutiendo sobre pagos para favorecer a la empresa noruega Discover Petroleum para ganar contratos.

El Presidente de la República Alan García Pérez anunció la destitución de Alberto Quimper Herrera como miembro del Directorio de PERU-PETRO y la suspensión del contrato petrolero adjudicado a la Compañía Discover Petroleum. Asimismo aceptó la renuncia del Ministro de Energía y Minas Juan Valdivia Cano.

A los pocos días el Premier Jorge del Castillo Gálvez, anuncio la renuncia del Gabinete Ministerial, que fue aceptado por el Presidente de la República.

II.- EN LA INVESTIGACION PRELIMINAR.-

1.- La Fiscalía de la Nación mediante Resolución N ° 1419-2008-MP-FN de fecha 20 de octubre del 2008, dispuso que por excepción la Fiscalía Provincial Especializada en Criminalidad Organizada se avoque al conocimiento de la interceptación telefónica difundidos en los medios de comunicación, fojas 01 del anexo 99 y fojas 3077 del anexo J.

2.- El Fiscal Superior Mateo Castañeda Segovia, Coordinador de las Fiscalías Especializadas en Criminalidad Organizada con fecha 31 de octubre 2008, designó a la Tercera Fiscalía Provincial Especializada contra la Criminalidad Organizada, a cargo del doctor Orestes Walter Milla López, para que se encargue de la investigación dispuesta en la resolución de la Fiscalía de la Nación antes citada.

3.- La Tercera Fiscalía Provincial Especializada contra la Criminalidad Organizada a cargo del Fiscal Milla López , mediante resolución de fecha 22 de noviembre del 2008- fojas 3077 del anexo J – designo a la Dirección Nacional Antidrogas de la Policía Nacional del Perú – DIRANDRO para que realicen las indagaciones orientadas a determinar quién o quiénes están dedicados a las actividades de interceptación telefónica y por que razones se realiza esta práctica ilegal; debiendo con dicho conformar un equipo especial.

4.- Colaborador Eficaz, de acuerdo al Acta de fojas 04 del Cuaderno de Colaboración Eficaz, con fecha 22 de diciembre del 2008 , el ciudadano Ismael Medardo Matta Uribe identificado con DNI N ° 43099153, se presento ante la Tercera Fiscalía Especializada en Criminalidad Organizada solicitando acogerse al procedimiento de Colaboración Eficaz, al tener información de la participación de las personas involucradas en actividades ilícitas de interceptaciones telefónicas; por lo que, la Fiscalía mediante resolución de fecha 23 de diciembre del mismo año apertura el procedimiento de verificación de Colaboración Eficaz solicitado por Matta Uribe, a quien se le denominara peticionario con Clave 000917-2008, en mérito de lo dispuesto en el artículo 22 de la Ley N ° 27378, fojas 06 del Cuaderno de Colaboración Eficaz.

5.- La Tercera Fiscalía Provincial Especializada contra la Criminalidad Organizada , mediante resolución de fecha 07 de enero del 2009 solicitó al Juez Penal de Turno de Lima se autorice Medidas Excepcionales de Limitación de Derechos en la investigación seguida contra los que resulten responsables por el presunto delito contra la Libertad – Violación del Secreto de las Comunicaciones – Interceptación Telefónica – a fojas 58 a 68 del anexo 99.-09-09.

6.- Mediante Resolución N ° 01 de fecha 07 de enero del 2009 – fojas 71 a 90 del anexo 99-09-09 - emitida por el señor Juez Penal de Turno, doctor Edwin Elmer Yalico Contreras resolvió: AUTORIZAR: LA DETENCION PRELIMINAR por el término de diez días de *Elías Manuel Ponce Feijoo, Carlos Alberto Tomasio De Lambarri, Giselle Mayra Giannotti Grados, Martín Alberto Fernández Virhuez, Jesús Manuel Ojeda Angles y Jesús Juan Tirado Seguin* y su correspondiente registro personal, incautación de soportes electrónicos, informáticos y/o magnéticos de comunicaciones y telecomunicaciones, documentos públicos o privados, objetos, instrumentos y efectos vinculados al delito materia de la presente investigación que pudieran tener u ocultar al momento de la detención; el DESCERRAJE Y ALLANAMIENTO de inmuebles y ambientes interiores con fines de detención de los ciudadanos en mención; así como el registro domiciliario y de sus distintos ambientes e INCAUTACION de bienes, documentos públicos y privados, equipos informáticos, soportes electrónicos e informáticos y/o magnéticos, equipos de comunicaciones y telecomunicaciones y otros objetos, instrumentos y/o efectos relacionados con

IV.- A NIVEL DE SALA PENAL .

20.- Con fecha 15 de octubre del 2010, la Sala Penal remitió al Despacho del Señor Fiscal Superior los autos para su pronunciamiento, quien emitió Acusación Sustancial el 27 de enero del 2011 – fojas 107958 y siguientes, contra los procesados a excepción de Jesús Juan Tirado Seguin por el delito de Violación del Secreto de las Comunicaciones- Violación de la Correspondencia; en cuyo mérito la Sala Penal emitió auto de Control de Acusación y Auto Superior de Enjuiciamiento el 14 de abril del 2011, declarando No Haber Merito para Pasar a Juicio Oral contra Jesús Juan Tirado Seguin por el delito de Violación del Secreto de las Comunicaciones- Violación de la Correspondencia; y Haber Mérito Para Pasar a Juicio Oral respecto de los extremos de la acusación fiscal, señalándose fecha para el inicio del Juicio Oral el día miércoles 18 de mayo del 2011.

21.- Iniciado el Juicio Oral, la Sala Penal ante los cuestionamientos formulados por algunos de los acusados respecto a la intangibilidad de la cadena de custodia , mediante Resolución de fecha 25 de mayo de 2011.- fojas 109877 del tomo 189, resolvió excluir del debate probatorio aquellas muestras que a criterio del Colegiado no contaban con un margen de seguridad y autenticidad en su recojo o custodia, siendo estos: Bienes de la acusada Giannotti Grados: 02 USB Boston Technologies , precisando que mantienen validez de las actas del deslabrado y las actas de obtención de muestras de imagen, visualización, impresión de archivos y escucha de audios que se consignan en el cuaderno 49, al estar premunidas de las garantías que el debido proceso requiere; tanto más , que los cuestionamientos a dichos USBs están referidos al momento de la entrega de dichas muestras de la custodia policial al Ministerio Público y posteriormente al Poder Judicial, esto es con posterioridad a fecha de incautación , del inicial deslacrado de obtención de muestras que reprodujeron a partir del 08 de enero al 13 de enero del 2009 . Los USB Marca Memorex, debido a las diferencias en la descripción de dichos bienes al momento de su incautación y al momento de su entrega a la autoridad judicial, así como contradicción en cuanto a su contenido. Bienes del acusado Carlos Alberto Tomasio De Lambarri: discos compactos y diskettes que se encontraban contenidos en la Caja 01, debido a que difieren en número.

22.- Con arreglo a lo dispuesto por el inciso 2 del artículo 246 del Código de Procedimiento Penales, el Colegiado dispuso examinar por separado a los acusados, continuando luego con el interrogatorio de agraviados, testigos y peritos; posteriormente se procedió a la oralización de las pruebas instrumentales ofrecidas por las partes procesales, finalmente el Ministerio Público realizó su Requisitoria Oral , los abogados de la defensa sus respectivos Alegatos cuyas conclusiones corren en pliegos por separado, concluyendo con la autodefensas de los acusados conforme aparecen de las

en la parte que escuchó, con referencia de la transcripción no pudo dar fe, que si dijo al Juzgado que no consideraba necesario escuchar más audios debido a que la parte que escuchó le fue más que suficiente porque sabía el contexto, había recordado la totalidad de la conversación y eran temas de carácter personal y también de coyuntura política.

14.7.- Teniendo a la vista los documentos de fojas 21493 – 21506 contenida en el tomo 33 muestra forense MBT-260 reconoció la transcripción escuchada del audio, no pudiendo dar fe de todo su contenido por no haberla oído en su totalidad, no llevando su firma ni su rúbrica, no teniendo la convicción o las pruebas pertinentes para hacer una afirmación en ese sentido, infiriendo que dicha conversación se habría dado en el año 1999 ó 2000.

14.8.- Que no ha sido víctima de extorsión, chantaje o comercialización de los documentos que se le han puesto a la vista y reconocido como suyo.

III.2.- DECLARACION DE TESTIGOS TESTIGOS EN JUICIO ORAL.

1.- Miembros de la Policía Nacional del Perú.

1.- Remigio Hernani Meloni.-

34. En la sesión número cincuenta y siete de Juicio Oral de fecha veinticuatro de octubre de dos mil once que corre a fojas ciento catorce mil seiscientos cincuenta y seis del tomo ciento noventa y siete señaló que se desempeño como Ministro del Interior desde el 14 de octubre de 2008 al 19 de febrero de 2009.

35. Preciso que los casos más importantes tienen que ser de conocimiento del Ministro y esto lo informa el Director General de la Policía Nacional del Perú y en algunas oportunidades a solicitud del Ministro a algún Director de alguna dependencia de la Policía.

36. Refiere que en el periodo que fue Ministro conoció de casos importantes como de narcotráfico, incautaciones, caso de los marcas, homicidios, que era necesario que el Ministro esté informado porque en cualquier momento el Presidente podía pedir información al respecto y no era posible que no se conozca del tema. Precisa que el General Remicio Maguiño como Director General era quien le daba a conocer los casos más resaltantes.

37. Respecto al caso Business Track señala que se entero por medio de la prensa, no conocía detalles sobre el mismo, al parecer el General Hidalgo Medina recibió un documento de un Fiscal para que se haga cargo de investigarlo. Precisa que desconoce porque la investigación

policial del caso Business Track fue derivada a la DIRANDRO, es un hecho totalmente raro.

38. Agrega que la DIRANDRO no era la dependencia policial que debía llevar a cabo estas investigaciones toda vez que la institución policial tiene sus leyes y reglamento, que establecen que hay estamentos, así como la DIRINCRI no puede investigar drogas, la DIRANDRO no puede investigar hechos que se investigan en la DIRINCRI, a no ser que haya algún interés particular.

39. Refiere que después de tomar conocimiento sobre las detenciones que se venían produciendo en virtud del caso Business Track llegó a su despacho en el Ministerio del Interior y llamé al General Remicio Maguiño y le pregunté qué sabía de la detención de estas personas, entre ellos, la señora Giselle Giannotti, detenida en este operativo, el Almirante Ponce y otros señores marinos y él me dijo que no sabía nada; entonces, "llame usted al General Hidalgo Medina", lo llamaron, se apersono y le pregunto, directamente "General, que pasó con este caso, qué me puede informar" y me dijo "yo he hecho una investigación ordenada por el Presidente de la República Alan García Pérez estrictamente reservada y que yo no debo darle cuenta a usted señor Ministro, ni a usted señor Director General, solamente debo darle cuenta directamente al Presidente de la República", "¿está usted seguro de lo que dice?" le pregunté y me respondió "efectivamente estoy seguro", ante esta respuesta yo opté por quedarme callado y ver como se desarrollaban las cosas posteriormente.

40. Precisa que el General Hidalgo Medina por versión propia de él, le daba cuenta del desarrollo de las investigaciones al Presidente de la República, ello lo manifestó en presencia del General Remicio Maguiño.

41. Refiere que al día siguiente se realizó una conferencia de prensa donde se vio a la Fiscal de la Nación conjuntamente con el General Hidalgo Medina dando cuenta a la población del operativo relacionado con BTR, lo cual era sumamente raro, porque la Fiscal de la Nación generalmente no está en las conferencias de prensa y antes de esta el General Remicio Maguiño me pidió permiso para ir y participar de la conferencia y yo le pregunté ¿"General Remicio conoce el tema? A lo que me respondió que "no", entonces le dije porqué va a ir, ya que no puede avalar algo que no conoce y efectivamente él no fue; solamente se presentó la Fiscal de la Nación con el General Hidalgo Medina; y, luego el Presidente de la República habló de "chuponeadores malditos"; entonces, ello evidenciaba que efectivamente el General Hidalgo Medina contaba con la orden y aval del Presidente de la República, además al

finalizar el año 2008, yo quise cambiar de colocación al General Hidalgo Medina y proponerle al Presidente de la República que se le cambie de colocación y vaya a otra dependencia, toda vez que sobre drogas no conocía y el Presidente Alan García ordenó que se queda ratificado como Jefe de la DIRANDRO.

42. Precisa que ha visto en dos oportunidades llegar al General Hidalgo Medina a Palacio de Gobierno sin mi conocimiento, además es ampliamente conocido que él llegaba en varias oportunidades y tan es así que luego fue nombrado Director General y Ministro de Estado.

43. Señala que la investigación del delito de interceptación telefónica le correspondía a la División de Alta Tecnología de la DIRINCRI. Refiere que la investigación no le correspondería a la DIRANDRO y en el caso que se le asigne a esta un caso de investigación criminal es irregular y no dar cuenta a sus Jefes. En el caso del General Hidalgo Medina debió dar cuenta a sus superiores, ha debido manifestar a la Fiscalía que investiga drogas y que no le corresponde investigar interceptación telefónica, ya que le corresponde a la DIRINCRI, devolver el oficio y comunicarle al señor Director General de la Policía Nacional del Perú.

44. La obligación de cada Director es de informarle al Director General de la Policía y este a su vez al Ministro del Interior y si no es así se estaría violando los reglamentos. Precisa que como Ministro del Interior no comunicó a la Inspectoría, el hecho que el General Hidalgo Medina no informe al Director General sobre las investigaciones e intervenciones del caso BTR, debido a que ello lo tenía que realizar el General Mauro Remicio Maguiño como Director General de la Policía Nacional del Perú.

2.- Mauro Walter Remicio Maguiño.-

45. En la sesión número cincuenta y siete de Juicio Oral de fecha veinticuatro de octubre de dos mil once que corre a fojas ciento catorce mil quinientos noventa y ocho del tomo ciento noventa y siete señaló que en enero del año 2009 tenía el Grado de Teniente General y desde el 24 de octubre de 2008 hasta el 31 de mayo de 2009 ejerció el cargo de Director General de la Policía Nacional del Perú.

46. Refiere que como Director General de la Policía tenían que darle cuenta de los principales casos que pudieran ocurrir durante su gestión.

47. Señala que tomo conocimiento de la detención de los procesados en el presente Juicio Oral por intermedio de los medios de comunicación. Que el Director de la DIRANDRO que en ese entonces era el General Miguel

Hidalgo Medina, en ningún momento me hizo conocer con relación a la investigación, ni a las intervenciones.

48. Afirma que luego de producida la detención de los procesados el Ministro del Interior General Hemani Meloni lo llama y pregunta porqué no le había comunicado, a lo que le manifesté que yo tampoco conocía de los hechos; en ese momento llamamos al General Hidalgo Medina y estando en el despacho del Ministro nos señaló que esta investigación las estaba realizando por órdenes del Presidente de la República y que están con el Ministerio Público.

49. Refiere que el General Hidalgo Medina, cuando era Director de Antidrogas le ha debido comunicar todo, desconoce por qué no lo hizo, tendría sus motivos y él solamente los puede responder.

50. Precisa que en la Policía Nacional del Perú tenemos Direcciones Especializadas, es así como la Dirección contra el Terrorismo tiene que ver todo lo relacionado a terrorismo; la Dirección Antidrogas lo relacionado con drogas, la Policía Fiscal que ve contrabandos. Entonces, esto caso por tratarse de un delito común (interceptación telefónica) debería ser investigado por la Dirección de Investigación Criminal por intermedio de la División de Alta Tecnología.

51. Refiere que luego que toma conocimiento de este hecho le pedimos al General Hidalgo Medina que dé cuenta por escrito y si había alguna inconducta tenía que ser investigado por la Inspectoría General de la Policía Nacional del Perú. Para ello el General Hidalgo Medina no informó en forma detallada, sino en forma escueta, al día siguiente. Refiere que con dicho informe se dispuso que él continúe las investigaciones hasta que culmine.

52. Agrega que luego de la detención de los procesados y la investigación el General Hidalgo Medina no informó que bienes se habían incautado a los procesados.

53. Precisa que el ente encargado de investigar y sancionar alguna inconducta del personal es la Inspectoría General de la Policía Nacional del Perú y que en el caso concreto respecto al no informar del General Hidalgo Medina al Director General de la Policía, no dispuso que Inspectoría General le iniciara una investigación.

3.- **Elmer Miguel Hidalgo Medina.-**

54. En la sesión número cincuenta y siete de Juicio Oral de fecha veinticuatro de octubre de dos mil once que corre a fojas ciento catorce

--

mil seiscientos catorce del tomo ciento noventa y siete señaló que es Teniente General de la Policía Nacional del Perú en situación de retiro. Asimismo precisa que se desempeñó como Director Antidrogas durante el año 2007, 2008 hasta los primeros días de abril del año 2009.

55. Refiere que tomó conocimiento sobre la existencia del caso BTR al momento de recepcionar la Resolución Fiscal emitida por la 13° Fiscalía de Crimen Organizado el 22 ó 23 de octubre del 2008 donde dispone que la Dirección Antidrogas por su capacidades, por el nivel profesional de su personal y otros fundamentos ha sido designada para poder investigar un caso de interceptación de las telecomunicaciones con la reserva que el caso amerita.

56. Precisa que en el organigrama de la Policía Nacional los Generales Jefes de las Unidades Especializadas dependen directamente ante el Director General y le informe a mi jefe directo el General Remicio Maguiño de manera personal y con documento sobre esta investigación el mismo día o al día siguiente muy temprano luego de recibir la Resolución Fiscal de que se inicia una investigación.

57. Señala luego que recibida la Resolución Fiscal se me reunió con el Doctor Walter Milla, hicimos una evaluación sobre cuál era el objetivo que perseguía su Fiscalía a través de la resolución y como en todos los casos, le entregue los recursos humanos y logísticos para que pueda cumplir con ese cometido. Se conformaron 02 Sub Grupos; 01 de inteligencia que trabajó directamente con el Fiscal y otro grupo de intervención para la investigación propiamente dicha después de haber intervenido a las personas presuntas involucradas. A nivel cabeza de grupos, el Comandante Farach a cargo del Grupo ORION y el Coronel Morán que estuvo a cargo de la investigación.

58. El primer grupo fue designado recibida la resolución fiscal, hechas las coordinaciones con el señor Fiscal Walter Milla inmediatamente se formó el grupo de inteligencia a cargo del Comandante Farach, inmediatamente se comenzó a trabajar; el otro grupo, si es verdad que teníamos en mente quién iba a comandarlo, que era el Coronel Morán, por guardar el "Compartimentaje" y por la confidencialidad de la investigación y sobre todo cumplir lo que el fiscal textualmente decía en su resolución, guardar la máxima reserva fiscal, se designó al Coronel Morán culminado prácticamente el trabajo del grupo de inteligencia, para que en un "engarce", en algún momento el grupo de inteligencia proporcione la información adecuada e inmediatamente el grupo de intervención intervenga.

59. Señala que el Grupo Operativo empieza su investigación con la información proporcionado por el grupo de inteligencia el día 08 de enero a partir de las 06 de la mañana, empiezan las operaciones teniendo la certeza que la autoridad judicial ha entregado las medidas limitativas para que puedan operar dentro del marco de la Ley.

60. Precisa que participó la noche anterior a la intervención policial de fecha ocho de Enero, en el sentido que se implementó los grupos de intervención debidamente designados por sus Jefes o cabezas de grupo, en este caso el Coronel Moran acompañado de los respectivos Fiscales porque a cada blanco se le había asignado su Fiscal.

61. Refiere que el Grupo ORION o grupo de inteligencia fue designado por mi despacho inmediatamente recibida la resolución fiscal y realizadas las coordinaciones con el Fiscal.

62. Señala que habiendo cumplido con informar al Director General el inicio de la investigación, estaba el deponente esperando la conclusión del trabajo del Coronel Moran para informarle, cosa que se hizo el mismo día 08. Al concluir las investigaciones si le informó, incluso el Director General le curso un documento a raíz del segundo documento el día 08 del presente terminadas las intervenciones de las personas presuntamente involucradas, se le formuló un documento al Director General indicándole que en relación con el primer documento que le envíe, se han intervenido a estas personas y él me lo devuelve con un oficio indicándome hágame un informe, el mismo que se hizo al termino de la investigación.

63. Precisa que tenía oficina en la DIRANDRO en el sétimo piso; la oficina del Coronel Morán en el quinto o sexto piso. El Coronel Moran debería haber dispuesto que los bienes que se incautaron a los intervenidos sean llevados a la Dirección Antidrogas, debe ser uno de los pisos que él tenía a su cargo. La información que me proporcionó el Coronel Moran era que las personas y los bienes incautados están en buen recaudo y con la medida de seguridad. Las medidas de seguridad sobre los bienes incautados era que cada jefe de equipo que detenía a una persona debía adoptar todas las medidas de seguridad de sus bienes incautados para que estos no sufran deterioro.

64. Refiere que no ha tenido contacto con los procesados a excepción del día siguiente de su detención que los visitó personalmente a todos para ver sus condiciones de seguridad y su estado de salud. Refiere que la señora Giannotti estaba en una oficina que se había acondicionado para su detención, era la única dama en este grupo por lo que se consideró que esta dependencia policial era la más apropiada, me acerqué, la

saludé y con el grupo que estaba a cargo de ella indagué sobre su estado de salud, su estado de detención, medida de seguridad y todo estaba correcto.

65. Precisa que no intervino en acto de investigación alguno en el presente caso. Asimismo señala que no conoce quién autorizó que a la señora Giannotti se le trasladara a su casa y que en todo caso el Coronel Morán le hizo conocer que por un asunto humanitario la señora estaba siendo conducida a su domicilio con conocimiento del Fiscal.

66. Niega que el Presidente de la República Alan García Pérez le haya ordenado avocarse a esta investigación. Asimismo desconoce la participación de Jorge Del Castillo Gálvez, Hernán Garrido Lecca, Mateo Castañeda en esta investigación.

67. Señala que se reunió con los Jefes de Equipo, en un momento con el Comandante Farach a cargo del Equipo de Inteligencia y luego con el Coronel Morán, a cargo del Equipo de investigación, éste último organizó sus grupos lo convenientemente posible para cumplir con esa misión, habiéndose formado tantos grupos por cada objetivo por intervenir incluyendo las instalaciones. Asimismo señaló que no se ha reunido con todo el personal que se iba a hacer cargo de las investigaciones, llámese jefes o subalternos.

68. Precisa que cuando se produce la detención de los procesados la Fiscal de la Nación toma la decisión de hacer una conferencia de prensa sobre este caso, lo invitan y procede a dar cuenta al Director General y asisto a esta conferencia.

4.- Carlos Moran Soto ([15]*)

69. En la sesión número sesenta y cinco de Juicio Oral de fecha dieciocho de noviembre de dos mil once que corre a fojas ciento quince mil doscientos setenta y cuatro del tomo ciento noventa y ocho señaló que se desempeña como General de la Policía Nacional del Perú en situación de actividad.

70. Asimismo preciso que en enero del año dos mil nueve se desempeñaba como Coronel Jefe de la División de Investigaciones Especiales de la Dirección Antidrogas, la misma que estuvo a cargo de la investigación del caso Business Track desde el día 08 de Enero del 2009.

---

[15] Testigo que fue citado a Juicio Oral de oficio por el Colegiado luego que la defensa de la procesada Giannotti Orados se desistiera de su declaración.

71. Refiere que el día **07 de enero del 2009** a las 23:30 horas fue convocado por el General Hidalgo Medina Director Antidrogas a una reunión de emergencia en su oficina de la sede DIRANDRO donde me dijo que tenía que concurrir con todo mi personal de Jefes y Oficiales, los convoqué y recibimos la instrucción del General de que íbamos a participar en una intervención policial, pero previamente íbamos a recibir un "Prifin" de un caso que estaba desarrollando el grupo de inteligencia ORION, ninguno de los que concurrimos en esa oportunidad tuvimos conocimiento de qué se trataba hasta después que fuimos notificados.

72. A partir de ese momento tuvimos conocimiento que se trataba de un trabajo de inteligencia que había hecho el grupo ORION al mando del Comandante Farach, nos hizo una explicación detallada de lo que se trataba – investigación que se había iniciado por ellos hace dos meses a mérito de una resolución fiscal emitida por el doctor Walter Milla -, y deducimos que era una organización que se dedicaba a la interceptación telefónica que estaba integrada por miembros de la Marina de Guerra en actividad, retiro y personal civil, a partir de ahí yo armo el grupo de intervención y de investigación.

73. Refiere que en la citada reunión participaron los 07 Oficiales a su mando Jefes de grupos de intervención con su personal, los Fiscales, personal de inteligencia al mando del Comandante Farach, el Fiscal Walter Milla y el General Hidalgo Medina quien fue la persona que dio la orden. Asimismo señala que recibió la instrucción de que se nos encargaba la investigación o intervención, recibió la resolución judicial donde se autoriza la detención preliminar y la información paralela del Grupo ORION. Detalla que procedió a organizar 07 grupos de intervención, los mismos que contaban con un Fiscal que iba a garantizar la legalidad de la intervención.

74. Señala que la **DIRANDRO** es una unidad especializada en investigar delitos de tráfico de drogas, lavado de activos y últimamente está investigando delitos de tráfico de drogas vinculados al terrorismo.

75. Refiere que en el momento de la intervención y en la actualidad la única Unidad capacitada para realizar ese tipo de investigaciones o intervenciones con acciones de inteligencia e investigaciones es la Dirección Antidrogas por la tecnología que posee, por los recurso humanos capacitados y experiencia. Asimismo que la Dirección Antidrogas actualmente y desde el año 2005 tenía ese software "Encase Forensic" para sacar copias espejos de las computadoras o de otros dispositivos de almacenamiento rápido de información, en el año 2005 se practicó esa actividad en el caso de Fernando Zevallos por el tema de

95. Preciso que mientras se estuvo visualizando un disco duro respecto a la información de los USBs surgió la información del Mayor Soller, el Fiscal y el señor Ponce que estaban presentes donde dijeron "es la voz del Presidente de la República", dicha información me la comunica el Mayor a cargo de la visualización. Detalla el deponente que procedió a escuchar el audio conjuntamente con el Mayor y otro personal técnico, sin la presencia del procesado, su defensa, ni el Fiscal. Detalla que de dicho audio se tenía dudas si era la voz o no del Presidente porque era muy parecida, *"el audio era corto donde hablaba con una dama y le lanzaba un piropo y que se iban a encontrar mas tarde"*, al parecer se trataba de un audio del ex Presidente de la CONFIEP Raymundo Morales, pero en ese momento la preocupación era si se trataba de la voz del Presidente de la República o no y se descartó que no era. Precisa que no se puede contaminar la muestra porque se trataba de un espejo. Detalló que luego hablo con Ponce Feijoo.

96. Refiere que no ha recibido llamadas del señor **Del Castillo Gálvez** relacionadas al presente caso y de ninguna persona ajena a la investigación. Señala que las personas de **Alan García, Garrido Lecca y Jorge del Castillo** no han pedido informes respecto a sus investigaciones.

97. Precisa que conversó con el Director de Inteligencia Naval el Almirante **Pedro García Llaque** porque su oficina era la "casa azul" y personal que trabajaba en esa oficina estaba detenido, entonces era obvio tener un acercamiento con él y hacerle las preguntas del caso o que nos proporcione información sobre la conducta de estos efectivos.

98. A la pregunta que se le formuló ¿en algún momento de la conversación que tuvieron, el señor Manuel Elías Ponce Feijoo reconoció que tanto él como el señor Tomasio y la señora Giannotti se dedicaban a la interceptación telefónica? Respondió: *Yo con el señor Ponce nos conocemos y como hombre de inteligencia, dijo eso, pero eso nunca pudo demostrarse por escrito en una manifestación de él, pero, sí, lo dijo.*

99. A la pregunta que se le formuló ¿se lo dijo a usted? Respondió: Sí.
A la pregunta que se le formuló ¿le dijo también que tanto el señor Carlos Tomasio De Lambarri como la señora Giannotti Grados estaban con él en la interceptación de conversaciones electrónicas y de conversación de teléfonos? Respondió: *No, él habló por él mismo.*

100. Precisa que la oficina donde sostuvo una reunión con Ponce Feijoo queda ubicada en el quinto piso, además en dicho piso estaba

Doctor Milla con una resolución complementaria que explicaba que el error consignado en el inmueble se subsana, se le explicó a la señora Giannotti Grados, ésta tomo conocimiento del contenido no leyó todas las páginas de la resolución y cuando vinieron sus abogados, primero una mujer una doctora y después un abogado el Doctor Ruiz leyeron ambos abogados toda la resolución, tomaron conocimiento y se continuo con la diligencia.

187. Precisa que todo el personal se puso de acuerdo para ir de manera conjunta buscando evidencias, en esos momentos nosotros teníamos una noción general por un tema lógico de qué cosa debíamos buscar (documentos, soporte magnético) pero no sabíamos exactamente qué cosa podría ser medio probatorio o no, **recién en el tercer ambiente, en el comedor, donde se encuentra copias de unos correos**, no solamente es que nosotros lo encontramos sino que la Señora tenía una predisposición de colaborar con la investigación, en ese momento en que ella misma abre los cajones mostrando todo de manera transparente encontrando correos, no ocultando nada. Todo lo que se encontraba se le mostraba, se le decía, en algún momento la abogada toma mayor posición activa durante el registro porque en un momento la señora se siente mal y se va a su dormitorio al sentir un estado de malestar.

188. Refiere que iban ambiente por ambiente, abogados, Fiscal, Policía, la señora presente y cuando se iba a incautar algo se separaba, en el **primer ambiente** se encontró recibos, en el **segundo ambiente** fotografías, papeles; y en el **tercer ambiente** unos correos y se le mostraba lo que nos parecía de transcendencia para proceder a lacrar y cerrar esa parte del acta y pasar al otro ambiente.

189. Agrega que no se **visualizó ningún soporte**, si se hubiera realizado se hubiera tenido que plasmar en los documentos, sus abogados se hubieran opuesto si es que no se hubiera hecho; en el **cuarto ambiente**, antes de encontrar los USB y antes que se revisara las computadoras, encontramos en el dormitorio de la señora junto a su televisor y su reproductor una serie de películas caseras, en ese momento su abogada y la Fiscal dan la idea de descartar este material pero el televisor no funcionaba, ante lo cual yo digo que tengo una **laptop** de mi uso personal en la maletera de mi vehículo; cuando uno revisa el audio de esa filmación puede escuchar claramente que voluntariamente la señora propone en ese momento, para no llevar cosas que eran innecesarias en una intervención, demostramos que eran películas caseras, también me dice la señora tráigala para que vean que no es así; salgo de la casa a mi carro y en el camino de regreso al dormitorio aprieto el botón de prender mi laptop, pero al regresar la señora Giannotti Grados ya se sentía muy mal, hay un momento que se suspende la diligencia previamente y llamo a mi unidad para informar que se necesita un médico, por lo cual no se llega a hacer dicha diligencia, no se usó la

laptop, si se hubiera hecho eso se hubiera consignado porque los abogados no van a permitir que nosotros hagamos algo y no consignarlo, en las imágenes se ve que la máquina está prendida pidiendo la clave de acceso y no llegué a meter la clave, no llegué a prender.

190. Se continuó con el registro en ese ambiente quien lo hace son Oficiales femeninas, durante toda esa búsqueda en ese cuarto ambiente, aproximadamente a las dieciocho horas, es donde se encuentra los USB posteriormente se continua con la diligencia no produciendo ninguna novedad; precisa que los CDs encontrados fueron lacrados en el cuarto ambiente, en el ambiente donde se encuentra, pero se hace al final del registro de cada ambiente; en el quinto ambiente, en su "walking closet" se encontró una caja fuerte en cuyo interior se encontró dinero que por indicación de la señora Giannotti Grados se entrega a su abogada, lo que se consigna al final del acta; en este ambiente la señora Giannotti participó activa y normalmente en la diligencia; en el último ambiente, se encuentran las computadoras las que fueron desconectadas y lacradas, nadie manipulo nada, estaban presentes todas las personas, nadie entraba a los ambientes que aun faltaba revisar, una vez que se terminaba de registrar un ambiente, se lacraba, se sellaba, firmaban todos los participantes o algunos de los participantes y se pasaba al siguiente ambiente y eso ya estaba cerrado, lacrado con la firma de los que estábamos realizando esa diligencia.

191. Refiere que la diligencia se llevó sin ninguna fricción, sin ningún malentendido o problema ya sea entre la Policía y la Fiscalía, entre la Policía y los abogados o entre la intervenida y la policía; todo se llevó de la manera más normal, sin ninguna observación, sin ningún problema; había colaboración de parte de la señora, de sus abogados y la diligencia terminó sin ninguna novedad formulándose el Acta que se le pone a la vista y obra de fojas 1138 a 1146 del Anexo C-49, el cual reconoce tanto en su contenido como firma. Refiere que la citada acta fue redactada por el Técnico Añanca quien escribía lo que se le iba dictando.

192. Dice, respecto del lugar donde fue ubicada la intervenida, no fue en la carceleta de la Dirandro, sino que por órdenes del Coronel Moran Soto, fue trasladada a una casa de seguridad, que se trata de uno de los locales donde funciona parte de la Dirección contra drogas, lo que se hizo por seguridad y también por comodidad en vista que se trataba de una señora, la otra razón para que fuera ubicada en ese lugar es para que no se comunicara con los otros intervenidos.

193. En cuanto a la custodia de los bienes incautados precisa, que como no prestaba servicios en el local central de la Dirección Antidrogas, cuando termina la diligencia habilitaron un ambiente del sexto piso, que estaba

199. Indica que el día doce se comienza a hacer dicha diligencia, cuando se encontraba en el USB se ponía, un determinado audio, se ponía en el acta la raíz, el nombre del audio y alguna pequeña transcripción, eso básicamente fue la diligencia, el día trece de enero se continuó con lo mismo, lo que sucede es que ya se contaba con una orden judicial, pero no alteró en nada, porque ya en un primer momento se había acordado que la diligencia se iba a llevar a cabo de manera voluntaria, al haber accedido la titular de los dispositivos incautados.

200. Describe lo que hacía el perito e indica que era bloquear cualquier manera de alterar el dispositivo que se iba a copiar, para que quedara intacto; una vez que obtenía la copia trabajaba sobre la copia del disco espejo, ahí se procedía a visualizar lo que había; posteriormente, al término de la diligencia se entregaba la copia espejo que se iba a seguir trabajando y los otros dispositivos se guardaban a cargo de los oficiales que tenían las llaves; yo tenía la llave externa y se retiraba al otro día cuando iba a haber diligencia, entre las muestras que fueron objeto de toma de imagen se encuentra USBs marca "Boston Technology", los que fueron observados por la intervenida y sus abogados, quienes no formularon cuestionamientos; que reconoce el contenido y firma de las Actas que obran a fojas 1163, 1173, 1203 a 1209, y 1214 al 1223, contenidas en el Anexo C-49.

201. Respecto a la **Elaboración del Atestado**, después de producidas las capturas, cada grupo procedió a trabajar independientemente, cada uno le daba cuenta de los avances al ahora General Carlos Morán Soto, porque él era el Jefe de la División; también estaba el Comandante Marcos Del Aguila Del Aguila, que en esos momentos era el Comandante más antiguo; se coordinaba de manera genérica con él, porque no se sabía en ese momento quién iba a ser el instructor de la investigación, ya faltando tres días aproximadamente se decide que los dos Comandantes con mayor antigüedad en el grado, estuvieran a cargo como el "responsable de la investigación" y el "es conforme"; por ese motivo, el Comandante más antiguo, el Comandante Marcos del Aguila Del Aguila firma el "es conforme" y yo, que seguía al mando, firmo "el Instructor" por eso, unos días antes que se venciera el plazo de la investigación, le pedimos a cada uno de los oficiales superiores que tenían a cargo a cada uno de los detenidos, nos dieran todo el acopio de medios probatorios, todas sus diligencias, para poder plasmar todo eso en un solo documento y suscribirlo los dos.

202. En cuanto al punto sobre **Actas extraviadas** señaló que hay un acta que no se anexó al documento final (Atestado), es un acta de visualización de un CPU de propiedad de la señora Giselle Giannotti; el perito conectó el CPU para hacer la copia y visualizado, igual que los USB y los otros dispositivos, pero, no fue reconocido por el software del equipo que utilizaba; la señora Giselle Giannotti refirió que se encontraba en "Linux", que era por eso que

no lo reconocía; el perito pone eso en el acta "que la señora refiere que está en Linux" lo pone tal como dice ella; esa acta, como todos los documentos, se le entregó al personal a cargo del grupo, para que a su vez la entregue a la persona que estaba centralizando todo para hacer los anexos; en un momento dado se dispuso que cada departamento vea sus propios anexos de cada caso, se devuelven los documentos y parece que en ese interin esa acta no se anexó, no se puso entre los anexos en el Atestado, esa acta no mostraba nada, por eso pasó inadvertida, de repente si se hubiera leído que hubieran encontrado audios de repente uno se hubiera dado cuenta que estaba faltando esto, pero como no nos aportaba nada, no nos dimos cuenta, yo estando fuera de la DIRANDRO, han comenzado a buscar en los archivos y han encontrado los juegos originales del acta, esa que no estaba, y la han mandado con un oficio a la jueza; ese es el único documento y no es que se haya perdido, sino que no se consideró.

203. Sobre los **USBs MARCA "MEMOREX"**, precisa eran de color plomo de plástico, que de las vistas fotográficas que se le pone a la vista y que obran a fojas 190656 del Tomo 189, reconoce como los incautados y entregados los que se ven encima de la tablilla; si en el Acta de entrega a la Fiscalía se describe con tapa de plástico transparente se debe a un error; desconoce lo que ha sucedido después del veintitrés de enero, lo que sé es que los dos USB que visualizamos y los dos USB que no visualizamos, los cuatro no son los que tiene el Poder Judicial, si tenemos en cuenta los **BOSTON TECHNOLOGIES** que nosotros entregamos uno de uno y uno de dos y el Poder Judicial tiene "dos" de "dos" y a nuestro cargo está de "uno" y de "dos", estos **USB** eran amarillos con un borde de metal, en la marca venía la cantidad de GB que tenía, uno era de 1GB y el otro de 2 GB, precisando que adicionalmente tenían en manuscrito una marca que decía uno y dos; estos USBs se lacran el día que se incautan, se guardan lacrados hasta el día doce, el día doce se deslacran y se visualizan, se iba a continuar al día siguiente pero tal como quedaron se guardaron, el día trece se retiran del ambiente de seguridad y se continúa con la visualización, se termina el día trece y tal como quedaron se guardaron y de ahí no se continuó con ninguna diligencia de visualización y así es como se llevan a la fiscalía el día veintitrés; no se volvieron a lacrar porque la Fiscal dispuso que se continuara con la diligencia lo mas que se pueda, pero ese mas que se pueda estaba supeditado a tener el perito el único software que había validado y las demás diligencias que pudieran hacer entonces el día trece se comienza la manifestación de la señora Giannotti que se prolonga hasta el quince.

204. Respecto a los **Teléfonos incautados** cuando se incautan los teléfonos estaban prendidos, no se apagaron con la finalidad de una posible visualización posterior, ya que de repente tenían una clave de acceso y la persona podría no querer colaborar, se lacraron y se quedaron ahí; sabe

incautados; habiéndose encontrado en el cuarto ambiente o dormitorio de la señora Giannotti Grados los USBs, (3 dentro de un sobre blanco y 1 suelto; cree que dos de ellos son amarillo con soporte de metal, uno de 1GB y el otro de 2GB; y, los otros dos de marca Mémorex, de color plomo, creo que cada uno era de dos GB o algo así); así como CDs, respecto de los cuales la señora Giannotti decía que eran películas, que podían comprobar su dicho viéndolas en su DVD, pero como no funcionaba el Comandante Del Castillo trajo su Laptop para visualizarlos, el cual se prendió y permaneció así por espacio de diez a veinte minutos, pero no se llegó a visualizar nada debido a que a la señora Giannotti Grados le bajó la presión, por lo que indicó la Fiscal que se llevarían todos; precisa que el único que manipuló la laptop fue el Comandante Del Castillo; quien optó por llamar a los médicos de la Policía para que auscultaran a la señora Giannotti Grados, quienes llegaron luego de una hora; que como la señora Giannotti dijo que se podía continuar con la diligencia, prosiguieron con el registro conjuntamente con su abogada; en el cuarto de estudio se encontraron los CPUs; habían 3CPU, dos visibles en el escritorio, el tercero en otro lado; los que estaban en stand by, es decir con la pantalla en negro pero la lucecita de encendido prendido, por lo que ordenó que se desenchufe todo, desde la fuente y ahí recién se hizo el registro, nadie manipuló nada; y eso fue en presencia de los dos abogados de la señora Giannotti, la Fiscal y los que estábamos interviniendo, todo lo cual está filmado; el Acta fue firmado, por parte de la Policía, por el Comandante a cargo de la investigación y los Sub Oficiales que la redactaron (Añanca); que al haber la declarante participado en el registro del dormitorio, firmó todo lo que se lacró, lo que se hizo en presencia de los dos abogados para darle seguridad, que en todo lo que se empaquetó se puso la firma de todos los que estábamos ahí presentes; que dicha diligencia concluyó aproximadamente a las once y media de la noche; en que condujeron a la señora Giannotti para los exámenes médicos correspondiente y luego al local donde funciona el Área de Control de Drogas de la DIRANDRO que queda en Rubén Dagnino - Jesús María, donde se acondicionó unos ambientes, lo que imagina se hizo por orden del Director, pero quien le transmitió fue su jefe el General Moran; mientras que todos los bienes incautados fueron trasladados al sexto piso de la DIRANDRO, donde funcionaba las oficinas del grupo de investigaciones especiales cuyo acceso es restringido sólo para los que pertenecen a dicha área y mediante huella digital; debido a que el Grupo del Comandante Del Castillo no laboraba en dicho lugar sino en una casa de seguridad, les asignaron una oficina donde había un gavetero, en el que se guardaron las cosas pequeñas que estaban lacradas, el cual tenía una llave a cargo de la Capitana Portocarrero y ella; los CPU y los otros equipos se pusieron ahí y se cerró la oficina, cuya llave estaba a cargo del Comandante Del Castillo; de tal manera que para acceder a cualquier bien incautado el Comandante Del Castillo abría la puerta y el gavetero lo abría, ya sea la Capitana Portocarrero o ella, siendo

por tanto los tres responsables de la seguridad; los otros sub grupos guardaron los bienes en sus oficinas y cada uno se encargaba del resguardo de lo que había intervenido; posteriormente participó en las Actas de Deslacrados que obran a fojas 1148 y 1156 del anexo C-49, los que puesto a la vista, los reconoce; que cuando se tenía que hacer una diligencia, la Fiscal indicaba qué cosas se iba a deslacrar, lo sacaban del sexto piso y lo llevaban al quinto piso donde había una oficina pequeña que se acondicionó para que los peritos trabajen en el caso de las visualizaciones, diligencia en la que sólo participaban los peritos, los abogados y el Fiscal, era algo reservado, en un lugar cerrado con puerta de metal; que, cuando se terminaba de visualizar el Comandante López los lacraba y procedían a firmar los peritos y el Comandante López, y si estaban presentes los abogados y el Comandante del Castillo, como jefe de grupo, firmaban, y luego se lo entregaban para la custodia; estas diligencias se realizaron en varias fechas, a partir del doce hasta el día diecinueve, precisando que sólo se sacaba lo que se iba a ver y se guardaban en el día, todo en presencia del Fiscal; que participo en la entrega de bienes a la Fiscalía, diligencia que se realizó el veintidós de enero del dos mil nueve, fecha en la cual todos los grupos entregaron los bienes, por lo que se hizo una sola acta de recepción la cual firmaron como a las cinco de la tarde, sin leer, por lo que no se percataron que el encargado de recepcionar, por error ha descrito a los 2 USBs plomos de manera diferente, lo cual habría ocurrido debido a que una sola persona recepcionó los bienes de todos los objetivos. En cuando a los lacrados que hizo la policía de los CPUs, cuyas hojas, obra lacrados a fojas 6011 del Tomo 12, señaló: "Esta no, porque el Comandante López no estaba en la intervención (no tiene su firma) y en los otros dos lacrados sí, porque está su firma; asimismo preguntada, si firmó la hoja estando cortada, dijo: "yo no recuerdo, pero cuando hemos hecho el lacrado se ha cogido un papel y se ha pegado ahí, para poder firmar, no recuerdo"; en cuanto a los USBs que aparece en la vista fotográfica que obran a fojas 109656, dijo que cree que son los "MEMOREX" plomos, los cuales reconoce como los que encontró en la casa de la señora Giannotti Grados, que de la vista fotográfica que obra a fojas 109655, reconoce dos memorias USBs de color plomo con una inscripción que dice "MEMOREX"; los que aparecen al costado, no los ve bien, no lo has ha visto; en cuanto a la capacidad si se ha consignado en el acta es porque lo han visto, que en la diligencia no se ha formulado ninguna observación, la que fue filmada y se tomo fotos por parte del grupo de inteligencia "Orión" hasta aproximadamente las nueve o diez de la noche, que la filmación se hace para darle credibilidad a la investigación; que la participación del personal de dicho grupo fue concretamente el de prestar seguridad (dos de ellos) filmar y tomar fotos (los otros dos).

217. En cuanto a la competencia de la DIRANDRO para investigar, precisa que dicha dirección ha intervenido en investigaciones especiales por delitos

conocimiento y la información tiene que quedarse en la empresa, y cuando una empresa crece y se asocia tiene que establecer políticas claras; por ejemplo, anulamos el Internet, solo para páginas básicas podían acceder de acuerdo a la especialidad.

68.- **Yonhy Lescano Ancieta.-**

601. En la sesión número sesenta y tres de Juicio Oral de fecha once de noviembre de dos mil once que corre a fojas ciento quince mil ciento sesenta y nueve del tomo ciento noventa y siete señaló tener la profesión de abogado y desempeñarse como Congresista de la República desde el año 2001.

602. Señala que formó parte de la Comisión integrada por los Congresistas Walter Menchola, Juan Carlos Eguren, Freddy Otárola, José Vargas, Falla Lamadrid y el deponente, la misma que fuera designada por el Pleno del Congreso de la República para investigar si los USBs incautados en la casa de la señora Giannotti Grados se perdieron o no, se cambiaron o no, ese era el objetivo principal y único de la investigación realizada en el Parlamento; de tal manera que se investigó cómo ingresó la Policía, cómo ingresaron Fiscales, cómo se guardaron las pruebas, cómo se guardaron los USBs, quiénes eran los Fiscales, quiénes eran los miembros de la Policía Nacional.

603. Asimismo el testigo precisó que emitieron un Dictamen en Minoría suscrito con el Congresista Freddy Otárola porque creíamos que había habido algunas irregularidades en la incautación de los bienes.

604. Refiere que el Dictamen en Mayoría no establece los presuntos autores y el Dictamen en Minoría, sí; que de la casa de la señora Giselle Giannotti se incautaron 02 USBs Memorex color plomo entero y, finalmente en la entrega de la Policía a la Fiscalía, se entregaron dos USBs totalmente distintos porque tenían tapa transparente y, de eso sí hay pruebas contundentes porque están las actas de incautación, las tomas fotográficas y eso sí llegó a determinar la Comisión, que se habían cambiado los USBs e, incluso los USBs Boston Technologies, cuando se hace un examen tecnológico a estos otros USBs, se establece que inicialmente uno, tenía supuestamente una capacidad de 01 GB y otro de 02 GB; pero, aparentemente los incautados tenían 02 GB, cada uno; de manera tal que eso suponía que también habían sido cambiados y eso demuestra, dentro de la investigación parlamentaria, que estos USBs están en poder de alguien y que no fueron los originalmente entregados, eso sí determinó la Comisión; y, luego se entregó estos USBs, se pusieron en una bolsa, sin el debido cuidado y el día 12 o 13 del mismo mes que se hizo la incautación, fueron visionados sin autorización judicial, eso está también acreditado en

607. Precisa que en el Dictamen en Minoría decimos que la doctora Martínez no tomó los cuidados necesarios como para verificar la recepción de las pruebas por parte de la Fiscalía y no fue diligente para ver si los bienes incautados eran los que realmente se estaban entregando y ahí encontramos nosotros un cargo respecto a la doctora Martínez que hubo cierto descuido en la recepción de las pruebas.

608. Refiere que se determino contradicciones evidentes y sospechosas en los documentos que el General Miguel Hidalgo Medina presenta, en las que hay contradicciones evidentes y sospechosas, por ejemplo indican los Generales Hernani y ex Ministro del Interior, que no les daban reporte de nada, siendo sus Superiores; y, el General Hidalgo indicó que había entregado documentos, pero entrega documentos sin sellos de recepción y con una serie de contradicciones, por ejemplo, que el día de la incautación los intervenidos habían sido trasladados cerca de las seis de la tarde y la diligencia había terminado a las once de la noche, entonces, hay una contradicción en lo que dicen esos documentos, sin las formalidades de Ley y los hechos que habrían sucedido; cómo intervenidos el día de la incautación, aparecen que se fueron a las carceletas a las seis de la tarde y la diligencia misma terminó a las once de la noche, eso no tiene mucho sentido, yo no creo que haya sido una pérdida de pruebas, sino un ocultamiento de pruebas porque ahí aparecen muchos indicios que la justicia debe indagar e investigar y ahora que se ha formado un grupo de trabajo en el Parlamento para la investigación de actos de corrupción del Gobierno anterior del ex Presidente Alan García, el Parlamento tendrá que ver si este caso que quedó inconcluso, también lo somete a investigación.

609. Señala que no han realizado ningún tipo de indagación sobre otros hechos, que eran los USB que se suponía que ahí se había grabado todas las conversaciones donde se habrían hecho negociados por parte de algunos miembros del Ejecutivo con otras personas, ese era el objetivo de la investigación.

610. Refiere que 02 USBs eran visiblemente cambiados; y los otros 02 mediante el examen técnico, también se llega a determinar que fueron cambiados porque el código Hash, los archivos y todo lo demás no coincidían con los USBs que se habían incautado.

611. En esas fotografías, en esos registros que se tomó al momento de la intervención en la casa de la señora Giselle Giannotti aparecen USBs de un color, luego cuando la Policía le hace entrega a la Fiscalía, aparecen dos USBs de otro color; eso es una clara demostración que se cambiaron los USBs, groseramente, yo creo que cómo van a incurrir en una irregularidad de esta naturaleza, miembros de la Policía Nacional con Fiscales que

intervinieron conjuntamente la casa de la señora Giselle Giannotti, consecuentemente, ese solo hecho involucra la responsabilidad de los miembros de la Policía Nacional y los Fiscales que estuvieron a cargo de la investigación, es una primera evidencia que nosotros hemos establecido; la segunda evidencia, que nosotros pensamos que determina las responsabilidades por los delitos que aparecen en el Dictamen en Minoría, es el registro de llamadas telefónica y ahí el registro de llamadas telefónicas, respecto de los cuales no se ha culminado investigación, determina que la señora Vanessa Aranibar habló casi una hora dentro de la diligencia, es decir, no pudo tener dominio sobre la diligencia que se realizaban y que se estuvo comunicando con personas que no se ha podido indagar quiénes son y qué se conversó y, ella no ha tenido la voluntad de informar al Parlamento esos detalles, ese es un segundo elemento; un tercer elemento por los cuales creemos que hay responsabilidad, malicia y dolo es que al momento del ingreso a la casa de la señora Giannotti, la Policía y los Fiscales le ocultan una resolución dictado por el Juez en el sentido de que el Juez prohibía, mandaba, que no se visualice ningún tipo de USBs que se encontrase, y los señores no comunican esta resolución, no notifican esta resolución, solamente notifican el cambio de domicilio porque se habían equivocado para ingresar al domicilio y hacer allanamiento, se equivocan la dirección y solamente notifican una segunda resolución que modificaba y rectificaba el error en el domicilio; entonces, yo digo por qué los señores siendo peritos en investigaciones que conocían como se hacían incautaciones y conocían sus obligaciones, dejan de notificar una resolución que prohibía la visualización y ellos esconden intencionalmente esa resolución, está en actas que solo notifican la resolución dos y no la uno, de tal manera que eso no puede ser un error.

612. Precisa que han realizado una la evaluación de llamadas telefónicas, las actas de incautación, las tomas fotográficas, las entregas de las pruebas de la policía a la Fiscalía, los documentos presentados por el señor Miguel Hidalgo, el hecho que no se haya entregado toda la filmación sino cuarenta y cinco minutos pero se filmó toda la indagación, que se nos ha ocultado también información.

613. Señala que el Comandante FARACH, el ex Ministro del interior, el ex Director General de la Policía Nacional han señalado que la investigación del presente caso le competía a la DIRINCRI y no a la DIRANDRO y haciendo una interpretación de las normas, pensamos que eso debería ser materia de otro departamento y no de la DIRANDRO, porque la DIRANDRO se dedica a la investigación de drogas y un simple examen de eso nos da la conclusión que no debieron investigar esa materia, sino otro departamento de la Policía Nacional, incluso se dijo que la DIRINCRI tenía un departamento específico para delitos de alta tecnología y a pesar de eso fue la DIRANDRO la que investigó.

614. Refiere que la Comisión de investigación se formó porque había denuncias periodísticas de que se habían cambiado las pruebas conseguidas en la casa de la señora Giannotti y el Congreso vio que había la necesidad de una investigación.

615. Señala que se buscaba investigar si se había cambiado las pruebas porque era importante para la lucha contra la corrupción. Asimismo precisó que sobre los contenidos se hubiera querido indagar más pero los plazos no alcanzó y porque los USBs conforme a las pruebas ya no eran los mismos.

616. Más adelante señaló que el objetivo de la investigación era establecer si había actos de corrupción o no y ese objetivo era verificar si en esa investigación que se había llevado a cabo, se practicaron actos de corrupción o no para hacer desaparecer pruebas; y si usted verifica que un USB incautado es distinto al entregado, es obviamente un acto de corrupción, porque no tendría otra finalidad hacer desaparecer un USB, que tapar algún tipo de información.

617. A la pregunta que se le formuló; ¿cuándo concluyen con una investigación por mayoría y minoría y en la mayoría establecen que no hay responsabilidad y en el de minoría que si, remiten de todas maneras al Ministerio Público? Respondió: *"Una vez discutido en el pleno del Congreso"*.

618. A la pregunta que se formuló ¿no remitieron al Ministerio Público? Respondió: *"No, porque no se remitió al pleno del Congreso, nosotros lo hemos pedido, pero lamentablemente no se ha remitido y como es un documento en alguna comisión, no hay discusión en el pleno del Congreso"*.

69.- Miguel Sagred Gutiérrez Rodríguez.-

619. En la sesión sesenta y cuatro de Juicio Oral de fecha catorce de noviembre de dos mil once que corre a fojas ciento quince mil doscientos veintiséis del tomo ciento noventa y ocho señaló ser periodista de profesión; se dedica al periodismo de investigación y labora en el Diario la República.

620. Refirió también que realizó una investigación relacionado con el caso BTR, el mismo que publicó en un Blog y no en el Diario La República, donde trató de dar a conocer y revelar ciertos indicios que apuntarían que habría injerencia de algunos funcionarios del Gobierno anterior en la investigación; a partir de establecer que había una relación entre el supuesto colaborador eficaz y el hombre de seguridad del señor Jorge Del Castillo.

registrado en el Libro de Matrícula de Acciones; si no es así, no está materializada la transferencia de acciones. Añade que si no se ha registrado, no estaría hecha la transferencia legalmente.

5.- **PRUEBA PERICIAL.-**

DEBATE SOBRE PERICIA GRAFOTECNICA

1032. En posesión de la acusada Giannotti Grados, ha sido hallado un manuscrito que consta en hojas amarillas cuyas grafías ha dicho la acusada que no lo pertenecen, documento sobre el cual el juzgado dispuso la realización de un peritaje grafotécnico que concluyo señalando que dichas grafías le pertenecen a Giannotti Grados, ante lo cual ha presentado un peritaje de parte, que dice lo contrario, razón por la que se produjo en el juicio oral un debate pericial, entre los peritos de parte y los peritos oficiales, cuyo resultado y conclusiones se evaluara al momento de establecer la condición jurídica de la acusada Giannotti Grados en razón que dicho peritaje solo le atañe a ella.

1033. Igualmente la misma acusada Giannotti Grados y también el Ministerio Publico han presentado al concluir los debates de la prueba instrumental, sendos peritajes, en calidad de prueba documental, donde se evalúa si las muestras halladas en la incautación de bienes el día de la intervención policial, referidas a Giannotti Grados, Ponce Feijoo y Tomasio de Lambarri, han sido o no manipuladas luego de haberse puesto el precinto de seguridad denominado EnCase Forensics y haberle otorgado un Código Hash. Las conclusiones de ambos peritajes se transcriben a continuación.

1034. La Defensa de la Procesada Giannotti Grados, presenta como prueba el informe de Pericia de Parte elaborada por el ingeniero Enrique Segundo Suárez Guimarey , el mismo que como versa de sus alcances y objetivos el de determinar su las muestras peritadas han sido o no, objetivo de algún tipo de manipulación, y si así fuera, precisar en qué consisten estas, señalando además las fechas y tipo de manipulación , propiedades y en general, características que permitan a los magistrados de la 2 Sala Penal para procesos con reos en cárcel tener conocimiento cabal del tipo formas de manipulación, de lo que se desprende el análisis de los siguientes dispositivos Memory Card (Tarjeta de Memoria Cámara Canon) , muestras : Giselle Giannotti, USB2 12 enero2009, Giselle Giannotti USB 2 GB -1 12ENE2009, Disco Duro 40GB, del CPU marca DELL OPTIPLEX GX150 (MGG101), Disco Duro 320GB de CPU marca HP modelo DX5150SFF (MGG102), Disco Duro SEAGATE 250 GB del CPU HP Media center negro N° Serie 5QE1L1JH 8 MGG103), IPOD Marca Apple, Modelo A123 con N° de serie 7574118vyxt de 8GB MGG99, USB Memorex de 4GB (MGG93), USB Memorex de 4gb (MGG94), USB Boston Technologies de

2GB (MGG85), USB Boston Technologies de 2GB (MGG96), CDs MGG02, MGG05, MGG06, MGG07, MGG11, MGG12, MGG13, MGG15, MGG17, MGG19, MGG27, MGG31, MGG87 quien ha llegado a las siguientes conclusiones:

1035. Que existe manipulación de los archivos antes de pasar el examen del Software Encase 6.1 en el 34 Juzgado Penal de Lima, asimismo que de los archivos analizados se ha encontrado **diferencias en los segundos de las horas de ultimo acceso (un segundo)**, considerando que al tratase de un atributo mas de los mencionado archivos los harian diferentes, por lo que considera que el Código Hash Debería ser distinto, pero a pesar de dicha diferencia el código Hash es el mismo, por lo que sustenta la existencia de una **colisión de Hash**, con la cual se puede alterar un archivo o muestra y mantener el Código Hash original, caso que se presenta en las siguientes muestras: USB2 12 enero2009, Giselle Giannotti USB 2 GB -1 12ENE2009.

1036. Que de la revisión del acta de obtención de imagen de USB, visualización e impresión de archivos y escucha de audios se observan **diferencias en la cantidad de objetos** entre lo que reporta el software Encase Forensics con lo que se consigna en el acta, esto sucede en las siguientes muestras: Giselle Giannotti, USB2 12 enero2009, Giselle Giannotti USB 2 GB -1 12ENE2009.

1037. **Incongruencias en las fechas de ultima escritura y de creación en las muestras MGG95, MGG96**, asimismo que estas modificaciones han sucedido entre archivo y archivo son de segundos por lo que presume se haya alterado dicha propiedad en cada uno de los archivos o que estos archivos originariamente no hayan estado en ese medio, ni generados en el medio examinado sino copiados o migrados mediante el empleo de otro medio como (USB, CD, portable, etc)

1038. Respecto a la muestra Giannotti USB 2GB 12ENE2009 manifiesta que el **archivo ROLEON 010408.zip no se encuentra** y aparentemente fe sustraído o borrado de la muestra, por lo que se evidencia manipulación y no debería tener el mismo código Hash,

1039. En el Caso de los Discos Duros de 40GB del CPU Marca Dell Optiplex Gx150 (MGG101) indica que la muestra contiene archivos " **lost file**" que tienen fecha de ultima escritura del 8 de enero del dos mil nueve desde las 7:41:10 pm a 7:55:08 pm, infiriendo que **se han borrado los archivos y fueron sobrescritos**.

1040. En el Disco Duro Seagate 250Gb del CPU HP Media Center negro N° Serie 5QE1L1JH (MGG103) se aprecian que en la presente pericia **no se han encontrado dieciocho archivos que aparecen en los reportes de la**

muestra obtenida por el 34 Juzgado Penal de Lima lo que evidencia manipulación de la muestra durante la diligencia de incautación del día 8 de Enero del 2009.

1041. En el caso del Ipod Marca Apple Modelo A123, con N° de serie 7574118VYXT de 8 GB (MGG99) evidencia manipulación al **no aparecer un archivo denominado Playcounts** de fecha de modificación 12 de enero del 2009 **que aparece en el reporte tomado en el juzgado.**

1042. En el caso de los CD´s MGG02, MGG05, MGG06, MGG07, MGG11, MGG12, MGG13, MGG15, MGG17, MGG19, MGG27, MGG31, MGG67 manifiesta que **al no haber código Hash a nivel policial no se puede comparar el código Hash** por lo que no hay certeza que estos sean las mismas que las incautadas el 8 de Enero del 2009, y la recuperación de dicha información **no garantiza un cien por ciento de efectividad.**

1043. Respecto a la Memory Card (Tarjeta de Memoria Canon) manifiesta que el archivo _MG_0012.JPG fue borrado.

1044. Finalmente que en las muestras MGG102 (fue encendida por última vez el 23 de Diciembre del 2008) , MGG93 y MGG94 (No contiene información al ser equipos nuevos)

1045. Así también el mismo perito Enrique Segundo Suárez Guimarey presenta a solicitud de la defensa de **MANUEL PONCE FEIJOO** el análisis de los siguientes bienes: MBT261, MBT218, MBT237, MBT130, MBT235, MBT260, MPF01, MOA19, de con el fin de determinar anomalías, señalando fecha , tipo y propiedades de las mismas, de lo que concluye:

a) Que las muestras en un 99 por ciento las fechas de última modificación son anteriores a la creación del archivo, por lo que se supone que los archivos originariamente no estuvieron en ese medio sino copiados, migrados mediante el empleo de otro medio como USB, CD, etc), esto se presenta en las muestras: MBT 261, MBT 218, MBT 130, MBT 235, MBT 260, MPF01, MOA19.

b) En las muestras MBT 237 (son archivos de sistema).

RESPECTO A LOS FINES Y CONCLUSIONES DE LA PERICIA PRESENTADA POR LA 2 FISCALIA SUPERIOR ESPECIALIZADA EN CRIMEN ORGANIZADO:

1046. Así también la 2 FISCALÍA SUPERIOR ESPECIALIZADA EN CRIMEN ORGANIZADO presenta una pericia elaborada por el Ingeniero Santos Alejandro Camarena Ames con el fin de determinar:

a) La pericia metodológica utilizada en la Primera Etapa y la Segunda Etapa sobre las muestras del caso BTR.
b) Pericia de los dispositivos USB marca Boston Technologies MGG95 y MGG96;
c) Pericia a los dispositivos de almacenamiento Disco Duro MGG101, MGG102, MGG103;
d) Pericia al Disco Duro Laptop Toshiba muestra MBT 260;
e) Pericia a las muestras obtenidas en el ámbito policial (2 memorias USB y una unidad de memoria SD Card) del que se concluye que:

1) Del análisis de las diez muestras , en las muestras MGG103, MGG102, MBT 260 , MGG 102, MBT260 que demuestran fechas de eliminación de archivos anteriores al 8 de Enero del 2009;

2) De las diez muestras analizadas Giselle Giannotti Memory Card 3, Giselle Giannotti USB2GB, Giselle Giannotti USB 2GB-1 , MGG95, MGG96, MGG101, MGG102, MGG103, MOA19, MBT260, solo las muestras denominadas MGG95, MGG96 son las que contienen fecha de creación posteriores al 8 de Enero del 2009, de la lectura de dicho listado se aprecia que las fechas de creación de dichos archivos registran 4 de Mayo del 209 entre las 01:05:59am y 01:37:42 por que las demás muestras analizadas no han sido alteración posterior al 8 de enero del 2009;

3) La generación del Código Hash de la muestra Giselle Gianotti-2GB efectuada el 19 de Enero del 2012, coincide con la obtenida a nivel policial el 12 de Enero del 2009, y la generación del Código Hash de la muestra Giselle Gianotti.-2GB-1 es idéntico al obtenido a nivel policial conforme obra a fojas 69 y 70;

4) El software VRS se encuentra instalado en la muestra MBT260, asimismo se aprecia respecto a este punto un análisis de las capacidades de este software para la grabación profesional Multicanal.

RESPECTO AL PROCEDIMIENTO DE OBTENCIÓN DE MUESTRAS PARA LA PERICIA:

1047. En ambos casos los profesionales realizaron sus pericias con el empleo del Software Encase Forensics Versión 6.0 proporcionado por la Gerencia General del Poder Judicial, software licenciado, diligencia que se realizó en

los ambientes de la Segunda Sala Penal de Reos en Cárcel con la supervisión del Perito Informático Forense Ingeniero Arturo Garro Morey y la presencia de veedores del Poder Judicial, así como de la oficina de prensa de la Corte Suprema realizándose la grabación en video de la diligencia, dichos procesos técnicos obran detallados en las actas que sustentan la presencia e incidencias de las mismas.

ANALISIS DE LAS CONCLUSIONES ARRIBADAS POR AMBOS PERITOS:

1048. Respecto a la precisión presentada por el perito Enrique Segundo Suárez Guimarey en las que aprecia que existe manipulación de los archivos antes de pasar el examen del Software Encase 6.1 en el 34 Juzgado Penal de Lima, asimismo que de los archivos analizados se ha encontrado **diferencias en los segundos de las horas de ultimo acceso de un segundo** en algunas muestras, es de precisar que de lo analizado en el expediente y del informe presentado por el Ingeniero Arturo Garro Morey se puede apreciar que existen diferencias respecto a la versión del software utilizado tanto para la diligencia de toma de muestras (véase fojas 1214 Anexo C49) que arroja en la emisión del código Hash que la versión utilizada para dicha diligencia sería la 4.20 a diferencia de la reciente versión utilizada para esta diligencia 6.0 por lo que la precisión del procedimiento llevado adelante en la pericia realizada tanto por el perito presentado por la Defensa de la procesada Giselle Giannotti y Ponce Feijoo, así como por la Segunda Fiscalía Superior Especializadas, atendiendo al avance de la tecnología y mejora en las versiones hace sostenible la posibilidad de un mejor cálculo y precisión de la hora y fecha de los archivos presentados, asimismo teniendo en consideración el informe final presentado por el perito veedor del Poder Judicial Ingeniero Arturo Garro Morey precisa que el código Hash tomado tanto a las copias espejo mediante el software Encase Forensics Versión 6.0 con los detallados en el expediente resultaron ser idénticos, por lo que se confirma que las copias espejo utilizadas para las pericias de la fiscalía y de la defensa son Bit a Bit idénticas a las copias espejo obtenidas directamente de las muestras originales, por lo que la posibilidad de colisión de hash argumentada por el perito Suarez Guimarey sustentado en el Anexo I de su informe, no prueba la vulnerabilidad en el uso del software Encase Forensics al no haberse demostrado con el uso de dicho software dicha posibilidad real de colisión. Puesto que el Código Hash obtiene de procesar "Bit a Bit" las pistas de un dispositivo (disco duro, CD, USB, etc.) no siendo posible obtener dos Códigos Idénticos para dos dispositivos con contenidos diferentes.

1049. Se concluye que la aseveración presentada por el perito de la Defensa de Giselle Giannotti en su pericia de parte carece de sustento técnico que permita identificar diferencias o manipulación en las muestras analizadas.

pertenencia de dicho archivo al equipo analizado puesto que el mismo perito establece la posibilidad que dichas fechas varían por el uso de medios portátiles que en la actualidad permiten la migración de la información, generando estas variaciones en las fechas de modificación y creación que el mismo sistema permite.

1067. La afirmación del Perito en sus conclusiones no encuentra sustento para determinar la pertenencia o no de dichos archivos sino describe únicamente la posibilidad de uso de medios de almacenamiento, lo que no conduce a establecer manipulaciones indebidas o no en el Encase Forensics ni tampoco intromisiones en el Código Hash.

1068. Podemos concluir en términos definitivos que las apreciaciones que hacen los peritos, necesariamente encuentran explicación lógica y técnica, lo que deriva en considerar que tanto las conclusiones del perito de parte como las conclusiones del perito del Ministerio Publico, tienen deficiencias, puesto que su capacidad de determinar técnicamente y en términos incuestionables si se produjeron manipulaciones o no en los contenidos de los archivos analizados, no es plena, tanto así que la única vertiente segura es que el En Case Forensic que consiste en otorgar un Código Hash a una muestra constituye hasta el momento el único mecanismo seguro para proteger la muestra y si bien es verdad existe la posibilidad de la manipulación de dicho Código Hash, la posibilidad de lograr es virtualmente inexistente, porque las cifras que garantiza el Código son combinaciones de muchas cifras , consecuencia de diversos cálculos y conclusiones lógicas que establece el En Case que sería extremadamente complicado duplicar, en consecuencia aquello que está protegido con un Código Hash y se vuelve a verificar su autenticidad, si el Código coincide tenemos el 99.99% de seguridad que se trata de la misma muestra, de tal manera que su validez probatoria resulta incuestionable. Evidentemente la dialéctica de un debate penal puede conducirnos a cuestionamientos fáciles sin razón técnica o científica, de ahí que la opinión de los técnicos y la información técnica existente es lo que prevalece y todos los técnicos y conocedores de esta materia afirman que no hay mejor seguridad que el Código Hash para garantizar la autenticidad de una muestra de esta naturaleza, por esa razón la copia espejo que ha servido como referencia para hacer los pentajes tiene la misma calidad que el original y no se ha usado dicho original por los riesgos que implica el reiterado uso de una muestra original que puede derivar inclusive en la perdida de la muestra.

1069. Cuando la defensa de Giannotti Grados cuestiona la copia autentica (copia espejo) obtenida con las garantías y seguridades que brinda el En Case Forensic y señala que una copia no es prueba válida, según la jurisprudencia y la doctrina y en todo caso se debe evaluar el original, para lo cual inclusive cita doctrina, evidentemente se está refiriendo a las copias

PARTE TERCERA

DECISION

Por estos fundamentos administrando Justicia a nombre de la Nación y con el criterio de conciencia que la Ley autoriza, los señores Jueces integrantes de la Segunda Sala Penal Especializada para procesos con Reos en Cárcel de la Corte Superior de Justicia de Lima: de conformidad con los artículos 138, e incisos 3; 5; 8; 10 ; 11; 12; 21 del artículo 139, de la Constitución Política del Estado y de los artículos 11, 12, 23, 25, 28, 29, 45,46, 49, 50, 57, 80,83,92, 93, 161, 162 primer párrafo y 317 primer párrafo del Código Penal; en concordancia con los artículos 280, 284 y 285 del Código de Procedimientos Penales , e impartiendo justicia en nombre de la Nación:

RESUELVEN:

1.- **DECLARARON FUNDADAS las TACHAS** planteadas por GISELLE MAYRA GIANNOTTI GRADOS y CARLOS ALBERTO TOMASIO DE LAMBARRI, respecto de los elementos referidos en la parte considerativa respectiva, con excepción de la tacha contra el USB, cassettes y discos duros cuestionados por éste..

2.- **INFUNDADA la TACHA** deducida por la defensa del procesado CARLOS ALBERTO TOMASIO DE LAMBARRI contra la testigo Katherine Roxana Castro Angeles.

3.- **DECLARARON EXTINGUIDA LA ACCION PENAL POR PRESCRIPCION** por el delito contra la Libertad – Violación del Secreto de las Comunicaciones – **Violación de Correspondencia** deducida por la defensa de los procesados ELIAS MANUEL PONCE FEIJOO, GISELLE MAYRA GIANNOTTI GRADOS, CARLOS ALBERTO TOMASIO DE, LAMBARRI, JESUS MANUEL OJEDA ANGLES, MARTIN ALBERTO FERNANDEZ VIRHUEZ, en agravio de Rómulo Augusto León Alegría, Alberto Alfonso Borea Odría, Francisco Ricardo Soberón Garrido, Alex Ganoza Céspedes, Isaac Alfredo Barnechea García, Aníbal Gonzalo Raúl Quiroga León, Blanca Rosa Rivera Talavera, Carlos Federico Rubina Burgos, César Antonio Silva Ygnacio, César Augusto Nakasaki Servigón, Cristina Matossian Osorio de Pardo, Carlos Motte Picote, Fernando

Roj: STS 2047/2015 - ECLI: ES:TS:2015:2047

Id Cendoj: 28079120012015100267
Órgano: Tribunal Supremo. Sala de lo Penal
Sede: Madrid
Sección: 1
Fecha: 19/05/2015
Nº de Recurso: 2387/2014
Nº de Resolución: 300/2015
Procedimiento: PENAL - PROCEDIMIENTO ABREVIADO/SUMARIO
Ponente: MANUEL MARCHENA GOMEZ
Tipo de Resolución: Sentencia

Nº: 2387/2014

***Ponente Excmo. Sr. D.:* Manuel Marchena Gómez**

Fallo:

***Secretaría de Sala:* Ilma. Sra. Dña. Soraoles de la Cuesta y de Quero**

TRIBUNAL SUPREMO

Sala de lo Penal

SENTENCIA Nº:300/2015

Excmos. Sres.:

D. Manuel Marchena Gómez

D. Julián Sánchez Melgar

D. Juan Ramón Berdugo Gómez de la Torre

D. Luciano Varela Castro

D. Perfecto Andrés Ibáñez

En nombre del Rey

La Sala Segunda de lo Penal, del Tribunal Supremo, constituida por los Excmos. Sres. mencionados al margen, en el ejercicio de la potestad jurisdiccional que la Constitución y el pueblo español le otorgan, ha dictado la siguiente

SENTENCIA

En la Villa de Madrid, a diecinueve de Mayo de dos mil quince.

Esta Sala, compuesta como se hace constar, ha visto el **recurso de casación** por infracción de ley, quebrantamiento de forma y vulneración de precepto constitucional, interpuesto por la representación legal de **Luis Francisco** , contra la sentencia dictada por la Audiencia Provincial de Valladolid (Sección Segunda), de fecha 19 de noviembre de 2014 en causa seguida contra Luis Francisco , por un delito de abusos sexuales, los Excmos. Sres. componentes de la Sala Segunda del Tribunal Supremo que al margen se expresan se han constituido para Votación y Fallo bajo la Presidencia del primero de los citados. Ha intervenido el Ministerio Fiscal, el recurrente representado por el procurador don Miguel Ángel Capetillo Vega y como parte recurrida Abilio representado por la procuradora doña Susana Gómez Castaño. Siendo **MagistradoPonente** el Excmo. Sr. D. **Manuel Marchena Gómez** .

I. ANTECEDENTES

Primero.- El Juzgado de instrucción núm. 1 de Valladolid, incoó diligencias previas procedimiento abreviado núm. 3316/2013, contra Luis Francisco y, una vez concluso, lo remitió a la Audiencia Provincial de Valladolid (Sección Segunda), rollo procedimiento abreviado núm. 21/2014 que, con fecha 19 de noviembre de 2014, dictó sentencia nº 346/2014 que contiene los siguientes ***HECHOS PROBADOS:***

" Ana María , nacida el NUM000 de 2000, es hija de Don Abilio y doña Belen , que se separaron de mutuo acuerdo en el año 2005, pasando a residir con la madre tanto Ana María como su hermana Micaela , en la vivienda sita en la CALLE000 nº NUM001 , NUM002 , de la localidad de Villanubla (Valladolid).

Don Luis Francisco , mayor de edad y sin antecedentes penales, inició hace años una relación sentimental con Doña Belen , comenzando a convivir con ésta y sus hijas en el domicilio indicado en el año 2006 ó 2007. Por problemas de convivencia con su madre y con Don Luis Francisco , Micaela en el mes de Octubre de 2012 se marchó a vivir con su padre en la calle CAMINO000 nº NUM003 , NUM004 de la localidad de Villanubla (Valladolid), estando de acuerdo con este cambio su madre, de tal forma que ni siquiera se comunicó al Juzgado que había conocido de la separación matrimonial, llevándose el cambio de residencia de Micaela , que era menor de edad, de forma consensuada entre sus progenitores.

A principios del mes de Abril de 2013, Don Luis Francisco , en fecha que no ha sido exactamente concretada, aprovechando la relación de convivencia con Doña Belen y Ana María , y con la excusa de ayudar a esta última en sus tareas escolares, accedió a la habitación en la que se encontraba Ana María estudiando, mientras su madre estaba en la planta baja de la vivienda, se colocó detrás de Ana María mientras ésta se encontraba sentada delante del ordenador y le tocó el pecho por encima de la ropa, diciéndole Ana María que parase, sin que Don Luis Francisco continuara con estos tocamientos. Este mismo comportamiento lo tuvo Don Luis Francisco con Ana María en otras ocasiones, cuyo número y fecha no ha sido precisado, aunque sucedieron todas ellas entre los meses de Abril y Mayo de 2013.

Un sábado que no ha sido concretado exactamente pero del mes de Abril de 2013, encontrándose Doña Belen trabajando y Don Luis Francisco y Ana María solos en la vivienda, esta última salió a la calle para ver a los niños de las comuniones, percatándose en ese momento de que no había cogido las llaves del domicilio, por lo que ella volvió a casa para recogerlas, abriendo la puerta Don Luis Francisco que, en la planta baja de la vivienda, dijo a Ana María que quería ver su sujetador nuevo, y al negarse ésta a enseñárselo le dijo que si no tenía suficiente confianza con él para mostrárselo, que ella tenía un complejo de tener los pechos demasiado grandes pero que él creía que tenía un pecho muy bonito, intentando levantarle la camiseta y tocarle el pecho, sin conseguir subir la prenda y sin que se haya acreditado que en esa ocasión llegara a tocarle el pecho.

Al menos en dos ocasiones en el mes de Abril de 2013, Don Luis Francisco , con la excusa del auxilio a Ana María en sus tareas, entró en la habitación de ésta, que se encontraba estudiando sentada o tumbada en la cama, y puso la mano a Ana María en los genitales, por encima de la ropa. Ana María le dijo que tenía sueño y que quería dormir y le apartó la mano, marchándose Don Luis Francisco de la habitación.

Esta situación provocó en Ana María una sensación de miedo e intranquilidad, sin que se atreviera a contar estos hechos a su madre, porque no tenía la certeza de que fuera a creerla, y sin que tampoco se lo contara a su padre o a su hermana Micaela , porque no sabía qué reacción podían tener y porque se avergonzaba de lo sucedido.

El día 31 de Mayo de 2013, alrededor de las 20 horas, Ana María estaba manteniendo una conversación a través de Tuenti con su amigo Constancio , al que le contó que el novio de su madre "le tocaba las..." y que la decía que le enseñara su sujetador nuevo, que la había intentado subir la camiseta y que la tocaba, que la había tocado "sus partes", afirmando que "la había tocado las de arriba" y que "la de abajo se la tocó dos veces o así", que el día de las comuniones intentó subir su camiseta, insistiendo Constancio en que se lo contara a su madre.

Tras esta conversación, Ana María continuó sin contar estos hechos ni a sus padres ni a su hermana. En una excursión que hizo con su colegio, en fecha que no se ha concretado pero en cualquier caso entre el 1 y el 19 de Junio de 2013, Ana María y sus compañeros estaban en un bar y a su amiga Sandra le pareció que Ana María estaba triste, por lo que la preguntó que qué le ocurría, marchándose las dos al baño donde Ana María le contó lo que sucedía con el compañero de su madre, contándoselo más tarde, ese mismo día, a sus amigas Lourdes y Ariadna , insistiendo sus amigas en que tenía que contárselo a alguien "por si iba a más", por lo que el día 19 de Junio, Ana María le contó lo que ocurría a una de sus profesoras, Doña Custodia , que a su vez se lo comunicó a la Directora del Instituto, Doña Felicidad . Esta citó a la madre de Ana María y a la Policía Municipal para el día 21 siguiente, narrando de nuevo los hechos Ana María ante su madre, Doña Custodia , Doña Felicidad y los agentes de la Policía Municipal, sin que Doña Belen otorgara credibilidad en ese momento a las manifestaciones de Ana María , sin que tampoco lo haya hecho con posterioridad".

Segundo.- La Audiencia Provincial de Valladolid, Sección Segunda, dictó el siguiente pronunciamiento:

"FALLAMOS: Que debemos CONDENAR Y CONDENAMOS a DON Luis Francisco como autor de un delito continuado de abuso sexual sobre una menor de trece años, con prevalimiento derivado de su situación de superioridad, de los artículos 183.1 y 4. d) y 74.1 del Código Penal , sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, a la pena de CINCO AÑOS Y UN DIA DE PRISIÓN, con la accesoria de inhabilitación especial para el ejercicio del derecho de sufragio pasivo durante la condena, con la pena accesoria de PROHIBICIÓN DE APROXIMACIÓN A Ana María Y A SU DOMICILIO A DISTANCIA INFERIOR A 500 METROS, Y DE COMUNICACIÓN CON ELLA POR CUALQUIER MEDIO O PROCEDIMIENTO, DURANTE UN PERIODO DE SEIS AÑOS Y UN DIA, imponiendo además la MEDIDA DE LIBERTAD VIGILADA, a cumplir una vez que finalice la pena privativa de libertad, de PROHIBICIÓN DE APROXIMACIÓN A Ana María Y A SU DOMICILIO A DISTANCIA INFERIOR A 500 METROS, Y DE COMUNICACIÓN CON ELLA POR CUALQUIER MEDIO O PROCEDIMIENTO DURANTE CINCO AÑOS, ASÍ COMO LA PARTICIPACIÓN EN UN PROGRAMA DE EDUCACIÓN SEXUAL (que podrá compatibilizar con el cumplimiento de la pena privativa de libertad), así como al abono de las costas procesales, incluidas las de la Acusación Particular. En el ámbito de la responsabilidad Civil, Don Luis Francisco deberá indemnizar a Ana María en la cantidad de 3.000 euros, cantidad que devengará el interés previsto en el artículo 576 de la LEC .

Notifíquese la presente Resolución a las partes, haciéndoles saber que no es firme y contra la misma cabe interponer RECURSO DE CASACIÓN ante la Sala Segunda del Tribunal Supremo, que ha de prepararse mediante escrito autorizado por Abogado y Procurador, presentado ante este Tribunal dentro de los CINCO DIAS, siguientes al de la última notificación y que deberá contener los requisitos exigidos en el artículo 855 y siguientes de la Ley de Enjuiciamiento Criminal ".

Tercero.- Notificada la sentencia a las partes, se preparó recurso de casación por el recurrente, que se tuvo por anunciado, remitiéndose a esta Sala Segunda del Tribunal Supremo las certificaciones necesarias para su substanciación y resolución, formándose el correspondiente rollo y formalizándose el recurso.

Cuarto.- La representación legal del recurrente Luis Francisco , basa su recurso en los siguientes **motivos de casación** :

I.- Al amparo del art. 849.2 de la LECrim . II.- Al amparo del art. 850 de la LECrim . III.- Al amparo del art. 852 de la LECrim , por infracción del art. 24 de la CE (derecho a la tutela judicial efectiva y a la presunción de inocencia).

Quinto.- Instruidas las partes del recurso interpuesto, el Ministerio Fiscal, por escrito de fecha 2 de febrero de 2015, evacuado el trámite que se le confirió, y por razones que adujo, interesó la inadmisión de los motivos del recurso que, subsidiariamente, impugnó.

Sexto.- Por providencia de fecha 27 de abril de 2015 se declaró el recurso admitido, quedando **conclusos los autos para señalamiento dela deliberación y fallo** cuando por turno correspondiera.

Séptimo.- Hecho el señalamiento del fallo prevenido, se celebró la deliberación de la mismael día 13 de mayo de 2015.

II. FUNDAMENTOS DE DERECHO

1 .- La sentencia núm. 346/2014, de 19 de noviembre, dictada por la Sección Segunda de la Audiencia Provincial de Valladolid , condenó al acusado Luis Francisco , como autor de un delito continuado de abuso sexual sobre una menor de trece años, a la pena de 5 años y 1 día de prisión, así como a las penas accesorias y medidas de seguridad que se reflejan en los antecedentes fácticos de esta resolución.

Por la representación legal del acusado se interpone recurso de casación. Se formalizan tres motivos, que van a ser objeto de consideración individualizada, sin perjuicio de las remisiones precisas con el fin de evitar las indeseadas reiteraciones.

2 .- La primera de las impugnaciones, al amparo del art. 849.2 de la LECrim denuncia error de hecho en la valoración de la prueba, derivado de documentos que obran en la causa y que demuestran la equivocación del juzgador.

Para avalar el error en que habría incurrido el Tribunal a quo se señalan como documentos las conversaciones a través del Tuenti que se recogen en los folios 178 a 190 y 199 y siguientes de la causa, que demostrarían que las comunicaciones entre la víctima e Constancio no eran diarias, como se menciona en la sentencia. Ello afectaría a la credibilidad de la víctima. También se invocan como documentos demostrativos de la equivocación de los Jueces de instancia el escrito de la acusación particular obrante a los folios 175 y 176, el informe de la perito psicóloga adscrita al Instituto de Medicina Legal, fechado el 16 de septiembre de 2013 y el acta en el que se recoge la exploración de la menor que fue practicado en fase de instrucción.

El motivo es inviable.

De entrada, incurre en la causa de inadmisión -ahora desestimación- prevista en el art. 884.4 de la LECrim , en la medida en que se señalan como documentos lo que no tiene tal carácter a efectos casacionales.

Las conversaciones mantenidas entre Ana María e Constancio , incorporadas a la causa mediante " *pantallazos*" obtenidos a partir del teléfono móvil de la víctima, no son propiamente documentos a efectos casacionales. Se trata de una prueba personal que ha sido documentada *a posteriori* para su incorporación a la causa. Y aquéllas no adquieren de forma sobrevenida el carácter de documento para respaldar una impugnación casacional. Así lo ha declarado de forma reiterada esta Sala en relación, por ejemplo, con las transcripciones de diálogos o conversaciones mantenidas por teléfono, por más que consten en un soporte escrito o incluso sonoro (por todas, SSTS 956/2013 de 17 diciembre ; 1024/2007 , 1157/2000, 18 de julio y 942/2000, 2 de junio).

Como señala el Fiscal en su informe, tampoco tienen tal carácter los escritos de la acusación particular -mencionados por el recurrente en el desarrollo del motivo-. Se trata de actuaciones de carácter procesal, no de verdaderos documentos para habilitar la vía que ofrece el art. 849.2 de la LECrim . Es más, su contenido no sólo no contradice el juicio histórico, sino que lo refuerza. Lo mismo puede decirse del informe pericial psicológico. De hecho, el recurrente -sigue razonando el Fiscal- no se apoya en él para contradecir el factum, sino que lo cuestiona. De ahí que no se atenga al fundamento del motivo, que lo que busca precisamente es añadir o suprimir alguna proclamación fáctica del relato de hechos probados. Y hacerlo mediante el contenido de un dictamen pericial único o de varios coincidentes que hayan sido orillados de forma injustificada por el Tribunal de instancia (cfr. SSTS 458/2014, 9 de junio ; 370/2010, 29 de abril ; 182/2000, 8 de febrero ; 1224/2000, 8 de julio ; 1572/2000, 17 de octubre ; 1729/2003, 24 de diciembre ; 299/2004, 4 de marzo y 417/2004, 29 de marzo , entre otras). Por último, tampoco revisten el carácter de documento las declaraciones de la menor en la fase de instrucción. Su insuficiencia para integrar el concepto casacional de documento ha sido tantas veces proclamada por esta Sala, que resulta ahora innecesario justificar su rechazo con grandes esfuerzos argumentales. Se trata, como es sabido, de pruebas personales que han sido documentadas en la causa, careciendo en casación del significado probatorio que pretende atribuirsele. Su valoración es inseparable de la proximidad del órgano de instancia a la fuente de prueba. De ahí que la tenacidad del recurrente pretendiendo acreditar el supuesto error decisorio del Tribunal *a quo* , resulta manifiestamente estéril (cfr. SSTS 76/2013, 31 de enero ; 546/2007, 12 de junio y 795/2007, 3 de octubre).

Pese a todo, al dar respuesta al tercero de los motivos formalizados por la defensa, la Sala ha valorado las alegaciones del recurrente, no ya desde la perspectiva de la impugnación casacional hecha valer por la vía del art. 849.2 de la LECrim , sino por lo que tienen de afirmación de insuficiencia probatoria y, por tanto, con incidencia en el derecho constitucional a la presunción de inocencia (art. 24.2 CE).

3 .- El segundo de los motivos alega quebrantamiento de forma, al amparo del art. 850.1 de la LECrim .

Aduce la defensa que las declaraciones de los agentes de policía local núms. 8463 y 8856 fueron interesadas en tiempo y forma en el escrito de conclusiones provisionales. Sin embargo, no llegó a practicarse porque el Ministerio Fiscal renunció a su propuesta probatoria. Esa decisión -se razona- no tenía por qué perjudicar a la defensa.

No tiene razón el recurrente.

En principio, la previa declaración de pertinencia y consiguiente admisión de las pruebas interesadas en el escrito de conclusiones provisionales de cualquiera de las partes, no obliga al Tribunal, de forma ineludible, a su práctica en el plenario. La pertinencia inicial de una determinada prueba no es obstáculo para que, a la vista del desarrollo de las sesiones del plenario, su práctica deje de ser útil. No todo lo pertinente confirma su necesariedad cuando ya se ha desarrollado en el plenario -como sucedió en el caso presente- buena parte de la propuesta probatoria de ambas partes. En palabras de esta Sala, expresadas en numerosos precedentes, ni siquiera el hecho de su previa y anticipada declaración de pertinencia, tiene entidad para debilitar la procedencia del rechazo ulterior. A diferencia de la pertinencia, que se mueve en el ámbito de la admisibilidad como facultad del Tribunal, la necesidad de su ejecución se desenvuelve en el terreno de la práctica, de manera que medios probatorios inicialmente admitidos como pertinentes pueden lícitamente no realizarse, por muy diversas circunstancias que eliminen de manera sobrevenida su condición de indispensable y forzosa, como cualidades distintas de la oportunidad y adecuación propias de la idea de pertinencia (cfr. SSTS 46/2012, 1 de febrero ; 746/2010, 27 de julio y 804/2008, 2 de diciembre). Hemos dicho también que este motivo de casación no trata de resolver denegaciones formales de prueba, sino que es preciso que tal denegación haya producido indefensión, de manera que el motivo exige "...demostrar, de un lado, la relación existente entre los hechos que se quisieron y no se pudieron probar por las pruebas inadmitidas, y de otro lado debe argumentar convincentemente que la resolución final del proceso *a quo* podría haberle sido favorable

de haberse aceptado la prueba objeto de controversia" (SSTS 1023/2012, 12 de diciembre ; 104/2002, 29 de enero ; 181/2007, 13 de abril y 421/2007, 24 de mayo).

A las razones que justifican el rechazo del motivo hemos de añadir el hecho de que la defensa -frente a lo que argumenta- no propuso en su escrito de conclusiones la prueba cuya práctica ahora reivindica. La Sala ha examinado su propuesta probatoria (folio 195) y observa que sólo se interesó la declaración testifical de Belen y la del agente de la Guardia Civil núm. NUM005 . El hecho de haber propuesto de forma rutinaria las interesadas por el Ministerio Fiscal "... *aunque fueren renunciadas*" no confiere la disponibilidad de esa propuesta. Implica la anticipada aceptación del desenlace que, sobre su pertinencia y necesidad, pueda adoptar el Tribunal a quo.

El motivo, por tanto, ha de ser desestimado por su falta de fundamento (art. 885.1 LECrim).

4 .- El tercero de los motivos, bajo la cobertura que proporcionan los arts. 5.4 de la LOPJ y 852 de la LECrim , denuncia la infracción de los derechos constitucionales a la tutela judicial efectiva y a la presunción de inocencia (art. 24.1 y 2 CE).

Entiende la defensa que, además de una motivación defectuosa e irracional, la única prueba de cargo sobre la que se ha fundado la condena de Luis Francisco es la declaración de la víctima. Sin embargo, ésta incurrió en visibles contradicciones. Su credibilidad ha sido cuestionada por su propia madre. El dictamen pericial sobre el que se basaron las conclusiones de la psicóloga del Instituto de Medicina Legal, presenta la grieta derivada de la falta de un soporte documental al que pudiera haber tenido acceso la defensa. Además, la lectura por la psicóloga de las declaraciones prestadas por Ana María le predispusieron a su favor, contaminando la obligada imparcialidad a que debe someterse en el desarrollo de su cometido. Por si fuera poco, la mala relación del acusado con la víctima era un hecho notorio, que se puso de manifiesto durante el desarrollo del plenario. Su exigencia y disciplina en los estudios estuvieron en el origen de enfrentamientos. Su realidad fue también adverada por el testigo sargento de la Guardia Civil, quien constató la clara relación de enemistad de Luis Francisco con las dos hijas de Belen , su compañera sentimental.

Los argumentos dirigidos a combatir la apreciación probatoria de la Audiencia también se enriquecen -con cierta descolocación sistemática- con alegaciones que son desarrolladas en el primero de los motivos, al sostener la existencia de un error en la valoración de la prueba del art. 849.2 de la LECrim . Se aduce, por ejemplo, la anomalía que encierra el hecho de que Ana María contara su vivencia a un amigo del sexo opuesto, dos años mayor que ella, "... *en lugar de contárselo, como sería más lógico tratándose de unos hechos tan íntimos, bien a algún miembro de su familia, a una de sus íntimas amigas o a una profesora*". Se reacciona también frente a la incondicional aceptación probatoria del diálogo mantenido entre Ana María y su amigo Constancio , que fue incorporado a la causa mediante pantallazos de la cuenta de Tuenti. Apunta la defensa que "... *se desconoce el contexto en que se desenvuelven y si alguna frase fue eliminada*".

El motivo es inviable.

Sólo un entendimiento preciso del concepto y de la significación funcional del recurso de casación, puede explicar las limitaciones de esta Sala a la hora de valorar una impugnación basada en el quebranto del derecho constitucional a la presunción de inocencia. Estas limitaciones se hacen mucho más visibles en supuestos como el sometido a nuestra consideración. Se trata de una agresión sexual en la que agresor y víctima discrepan abiertamente sobre lo que realmente aconteció y en la que ambas partes ofrecen a la Sala elementos de prueba abiertamente contradictorios. Y es que, por más que con frecuencia se olvide, ningún parecido existe entre la posición procesal de la Audiencia Provincial ante la que se practican las pruebas y la capacidad del Tribunal Supremo para ponderar en términos jurídicos la corrección de la inferencia del órgano decisorio. No nos incumbe ahora realizar una nueva valoración de la prueba. No nos resulta posible, en fin, proceder a un análisis secuencial de todas y cada una de las alegaciones mediante las que la parte recurrente trata de demostrar el error valorativo en que ha podido incurrir el Tribunal a quo. Aun cuando resulte una obviedad recordarlo, nuestra posición como órgano casacional no nos autoriza a optar entre la valoración probatoria que sugiere la parte recurrente y la que ha proclamado la Audiencia Provincial. Nuestro ámbito cognitivo no nos faculta, en fin, a desplazar la conclusión probatoria alcanzada por la Audiencia, ante el mayor atractivo de los argumentos que pudiera encerrar, en su caso, el discurso impugnativo del recurrente. Tampoco podemos neutralizar el razonamiento del órgano decisorio, sustituyéndolo por la hipótesis de exclusión formulada por el recurrente, siempre que, claro es, aquél resulte expresión de un proceso lógico y racional de valoración de la prueba, (SSTS 326/2012, 26 de abril , 80/2012, 10 de febrero , 790/2009, 8 de julio , 593/2009, 8 de junio y 277/2009, 13 de abril). El control casacional del respeto al derecho a la presunción de inocencia ha quedado sobradamente delimitado por la jurisprudencia constitucional y de esta misma Sala (cfr. STS 553/2008, 18 de septiembre). Es en ese exclusivo ámbito en el que hemos de valorar las alegaciones de la defensa.

Conforme a esta idea, la suficiencia del cuadro probatorio ponderado por la Audiencia y la racionalidad del proceso valorativo sobre el que se asienta la proclamación del hecho probado, están fuera de dudas.

La Audiencia ha valorado el testimonio del acusado, quien ha negado en todo momento haber menoscabado la indemnidad sexual de la víctima. Siempre que entró en el cuarto de ésta fue a "... *solicitud de Ana María para que la ayudara con los deberes de Francés, permaneciendo él dos o tres minutos en la habitación, ya que lo que pretendía Ana María era que él hiciera el trabajo por ella, negándose él, negando asimismo que él le hubiera hecho a Ana María comentarios sobre su forma de vestir ni sobre su ropa interior*" (*sic*).

Esta negativa, sin embargo, está en contraste con otros elementos de cargo que son debidamente expuestos y razonados por los Jueces de instancia. De una parte, la conversación mantenida en *Tuenti* entre Ana María y su amigo Constancio, a quien narró de forma espontánea la conducta del acusado. También fue objeto de ponderación el informe psicológico de la perito del Instituto de Medicina Legal, quien descartó que la historia narrada por Ana María tuviera como apoyo su propia fabulación. En el FJ 2º de la sentencia de instancia se abordan, además, las supuestas contradicciones en el testimonio de la menor. Se descarta la existencia de saltos cronológicos que puedan cuestionar la realidad de los hechos y se relativiza la falta de uniformidad en las manifestaciones de Ana María a la hora de fijar el número de veces en el que habría sido objeto de tocamientos por el acusado. Resulta de interés la transcripción literal del razonamiento de los Jueces de instancia: "*... es cierto que Ana María no ha concretado las fechas exactas en las que ocurrieron los hechos, debiendo atenderse especialmente a su edad para valorar su testimonio, siendo obvio que sus referencias no pueden ser las que facilitaría un adulto, ya que una niña de doce años toma como hito elementos distintos a una persona mayor de edad, pero partiendo de esta premisa, no puede estimarse que no existan datos que permitan concretar el periodo de tiempo en el que se desarrollaron los hechos, habiendo mantenido Ana María de modo constante que la primera ocasión en que el acusado la tocó fue tras la Semana Santa de 2013, que ella pasó con su padre, y teniendo en cuenta que el Viernes de Semana Santa fue en 2013 el día 29 de Marzo de 2013, y que la primera vez que Ana María cuenta lo sucedido a alguien es el 31 de Mayo de 2013 (a su amigo Constancio en Tuenti), los hechos se llevan a cabo en esos dos meses de Abril y Mayo de 2013. Esta referencia es suficiente a los efectos de fijar el ámbito temporal en el que se suceden los hechos, sin que la falta de precisión en cuanto a la determinación numérica de los días concretos en los que éstos se llevan a cabo se pueda considerar que genere indefensión alguna al Sr. Luis Francisco* ".

La Sala no constata la existencia de un razonamiento extravagante, ajeno al canon de racionalidad impuesto por nuestro sistema constitucional de valoración probatoria. Tampoco lo detecta en la línea argumental que sirve a los Jueces de instancia para excluir cualquier duda sobre la realidad de los hechos a partir de la determinación numérica de las ocasiones en que se produjeron los abusos: "*... si bien es cierto que no ha habido uniformidad en las manifestaciones de Ana María en relación con el número de veces en las que el acusado la tocó el pecho o los genitales por encima de la ropa, también lo es que sí ha concretado a) que solo una de las ocasiones (era un Sábado y su madre estaba trabajando fuera de casa) ocurrió fuera de su habitación, que fue el día que iba a ver a los niños de las comuniones y se dejó las llaves en casa y al volver a por ella el Sr. Luis Francisco, en la planta baja de la vivienda, le pidió que le enseñara el sujetador e intentó subirle la camiseta, b) el resto de las ocasiones sucedieron en su habitación, dos cuando ella estaba tumbada o sentada en la cama, en las que el Sr. Luis Francisco puso su mano sobre sus genitales por encima de la ropa y al menos otras dos que le tocó el pecho por encima de la ropa cuando estaba sentada, siendo en relación con este último comportamiento donde Ana María apunta a que fueron más ocasiones aparte de estas dos, pero sin aportar datos que permitan concretar las fechas, bien de forma directa, bien por referencia a otros hechos*".

Tampoco apreciamos una falta de valoración de la prueba de descargo. Antes al contrario, existe un razonamiento *ad hoc* de la Audiencia con el fin de atender al núcleo argumental sobre el que se basó la tesis exoneratoria de la defensa, a saber, la existencia de una actuación por rencor para vengar la ruptura del grupo familiar. El contacto de la víctima con su padre biológico y con su hermana estaba garantizado sin necesidad de ninguna denuncia como la que ha dado lugar a la incoación de la presente causa. De hecho, Ana María no tenía obstáculo alguno para el mantenimiento de esa relación familiar, pues ambos domicilios están separados por una distancia que no excede de cien metros. En la misma línea, la Sala hace suyo el argumento de los Jueces de instancia cuando descartan la tesis de la venganza: "*... no se aprecia por tanto que Ana María obtuviera ningún beneficio por inventarse estos hechos, lo que se ve apoyado por el hecho de que Ana María siempre ha mantenido, en relación con la conducta del acusado, una misma versión: que la había tocado el pecho y los genitales por encima de la ropa, lo que revela la ausencia de interés en exagerar la acusación, puesto que podría haber referido tocamientos directos o comportamientos de mayor gravedad, y no lo ha hecho* ".

No podemos, en fin, compartir las críticas de la defensa al sostén probatorio sobre el que se asienta el juicio histórico. El hecho de que la madre de Ana María cuestione la veracidad del testimonio de su propia hija puede obedecer a distintas razones. Una de ellas, por supuesto, podría estar relacionada con el deseo de evitar

una condena de gravedad para la persona con quien comparte la vida. Pero incluso para el caso en que las dudas sobre el testimonio de Ana María fueran reales y ajenas a todo interés no confesado, lo cierto es que su opinión sobre la credibilidad de la denunciante no constituye un presupuesto *sine qua non* para la admisión de los hechos denunciados. Su versión no es sino un elemento más, llamado a integrarse en el cuadro probatorio ofrecido por las partes al órgano decisorio. Y éste ha concluido la autoría a partir de la valoración de todas las propuestas probatorias desarrolladas durante el plenario.

Tampoco podemos aceptar la idea de la parcialidad de la perito del Instituto de Medicina Legal que dictaminó sobre la credibilidad de Ana María . Esa falta de imparcialidad se habría producido por una supuesta contaminación derivada del hecho de que -como razona la defensa- leyó las declaraciones prestadas por Ana María durante la instrucción.

A nuestro juicio, sin embargo, carecería de sentido hacer depender la validez de las conclusiones científicas suscritas por cualquier técnico, del hecho de que, con anterioridad a su elaboración, se hayan consultado los antecedentes precisos para la suscripción del dictamen.

El mismo rechazo resulta obligado frente a las críticas de la defensa por el hecho de que no se pusiera a su disposición el soporte documental y sonoro en el que habría quedado recogida la exploración de la menor. Esa exigencia cobra todo sentido cuando se trata de hacer valer una prueba anticipada ante la ausencia de la testigo en el plenario (cfr. SSTS 925/2012, 8 de noviembre ; 940/2013, 13 de diciembre , entre otras). Pero en el presente caso, Ana María declaró ante el Juez instructor y lo hizo luego en el plenario, sometiéndose al interrogatorio cruzado al que le expusieron las partes. No ha existido, por tanto, atisbo de indefensión.

Por otra parte, el hecho de que un sargento de la Guardia Civil testifique sobre la conflictividad familiar existente en el grupo familiar carece de toda relevancia probatoria. No existe máxima de experiencia alguna que circunscriba los abusos sexuales a las familias que viven en armonía. Del mismo modo, del hecho de que Ana María contase por primera vez su experiencia a un compañero del sexo opuesto por medio del *Tuenti* y no lo hiciera a ningún familiar o profesor, tampoco puede derivarse un argumento exoneratorio. La víctima, como expresa el hecho probado, lo comentó con varias amigas del colegio que, a su vez, trasladaron sus quejas a los profesores. Ninguna anomalía existe en esa forma de transmitir la propia vivencia.

Respecto a la queja sobre la falta de autenticidad del diálogo mantenido por Ana María con Constancio a través del *Tuenti*, la Sala quiere puntualizar una idea básica. Y es que la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido.

Pues bien, en el presente caso, dos razones son las que excluyen cualquier duda. La primera, el hecho de que fuera la propia víctima la que pusiera a disposición del Juez de instrucción su contraseña de *Tuenti* con el fin de que, si esa conversación llegara a ser cuestionada, pudiera asegurarse su autenticidad mediante el correspondiente informe pericial. La segunda, el hecho de que el interlocutor con el que se relacionaba Ana María fuera propuesto como testigo y acudiera al plenario. Allí pudo ser interrogado por las acusaciones y defensas acerca del contexto y los términos en que la víctima - Ana María - y el testigo - Constancio - mantuvieron aquel diálogo. Con toda claridad lo explican los Jueces de instancia en el FJ 2º de la resolución combatida: "*... respecto de la conversación de Tuenti cuya impresión fue aportada por la Acusación Particular, porque las dos personas que la mantuvieron, Ana María y su amigo Constancio , en el plenario han manifestado que efectivamente mantuvieron esa conversación y en esos términos, sin que ninguno de los dos hiciera referencia a que se hubiera producido ninguna manipulación en la impresión de dicha conversación, que consta no solamente aportada por la Acusación Particular en los folios 178 a 190 sino también en las fotografías que del teléfono móvil de la menor adjuntó la Guardia Civil (folios 199 y siguientes), ya que según consta en el oficio, Ana María accedió en su presencia a su cuenta de Tuenti a través de un ordenador, pero el historial solo permitía retroceder hasta el 26 de Octubre de 2013, por lo que únicamente pudieron visualizarlo a través de la aplicación de Tuenti para teléfonos móviles, haciendo los agentes fotografías de las pantallas correspondientes a la conversación, que coinciden exactamente con las hojas impresas que fueron aportadas por la Acusación Particular. Precisamente, en el escrito con el que se adjuntaban estas impresiones, la Acusación Particular facilitó las claves personales de Ana María en Tuenti y solicitaba que, si había alguna duda técnica o probatoria, que se oficiara a "Tuenti España", indicando su dirección, para que se certificara el contenido de*

esa conversación, sin que la Defensa haya hecho petición alguna al respecto. Teniendo en cuenta que tanto Ana María como Constancio han reconocido el contenido de la conversación que se ha facilitado tanto por la Acusación Particular como por la Guardia Civil, no puede estimarse la impugnación de la Defensa, quedando dicha documental dentro del acervo probatorio para su valoración con el conjunto de las restantes pruebas que han sido practicadas" .

En suma, ninguna quiebra de los derechos a la tutela judicial efectiva o el derecho a la presunción de inocencia detecta la Sala. El Tribunal de instancia, con un esfuerzo argumental encomiable, sistematiza los elementos de cargo que militan, con absoluta suficiencia, para respaldar la versión de la víctima y aborda para neutralizar su significado los argumentos de descargo hechos valer por la defensa.

El motivo ha de ser desestimado (art. 885.1 LECrim).

5 .- La desestimación del recurso conlleva la condena en costas, en los términos establecidos en el art. 901 de la LECrim .

III. FALLO

Que **debemos declarar y declaramos NO HABER LUGAR** al recurso de casación, interpuesto por **Luis Francisco** contra la sentencia de fecha 19 de noviembre de 2014, dictada por la Sección Segunda de la Audiencia Provincial de Valladolid , en la causa seguida por el delito de abusos sexuales y condenamos al recurrente al pago de las costas causadas.

Comuníquese esta sentencia a la Audiencia de instancia a los efectos legales oportunos, con devolución de la causa que en su día remitió, interesando acuse de recibo.

Así por esta nuestra sentencia, que se publicará en la Colección Legislativa lo pronunciamos, mandamos y firmamos

D. Manuel Marchena Gómez D. Julián Sánchez Melgar D. Juan Ramón Berdugo Gómez de la Torre D. Luciano Varela Castro D. Perfecto Andrés Ibáñez

PUBLICACION .- Leída y publicada ha sido la anterior sentencia por el Magistrado Ponente Excmo. Sr. D Manuel Marchena Gómez, estando celebrando audiencia pública en el día de su fecha la Sala Segunda del Tribunal Supremo, de lo que como Secretario certifico.

Acuerdo sexual agresor

CORTE SUPERIOR DE JUSTICIA DE MADRE DE DIOS
TERCER JUZGADO DE INVESTIGACIÓN PREPARATORIA DE TAMBOPATA
DE MADRE DE DIOS

Cuaderno N° 01328 -2018-0-2701-JR-PE-02.

ACTA DE REGISTRO DE AUDIENCIA DE PROCESO INMEDIATO

JUEZ: DR. EDGARD LEON QUISPE.

ESPECIALISTA JUDICIAL DE AUDIENCIAS: Norma Vilca Morales.

INICIO:

En la ciudad de Puerto Maldonado, Distrito y Provincia de Tambopata, del Departamento de Madre de Dios, siendo las ***quince horas de la tarde*** del día **LUNES, 01 DE OCTUBRE DEL AÑO 2018**, se constituye el Magistrado **EDGARD LEON QUISPE**, Juez del Tercer Juzgado de Investigación Preparatoria, asistido por la Especialista Judicial de Audiencias NORMA VILCA MORALES, en la sala de audiencias del Tercer Juzgado de Investigación, a efectos de llevar adelante la **AUDIENCIA PROCESO INMEDIATO**, en la investigación seguida en contra de **PARIZACA PUMA, EDWAR ALEX** por la presunta comisión del Delito de **Acoso Sexual Agravado**, en agravio de la menor de iniciales G.M.B.M. de 15 años.

Se deja constancia que la presente audiencia será registrada mediante audio, cuya grabación demostrará el modo como se desarrollará, tal como lo dispone los incisos 1) y 2) del artículo 120° del Código Procesal Penal, pudiendo las partes acceder a la copia de dicho registro; por tanto, solicita procedan oralmente a identificarse para que conste en el registro, y se verifique la presencia de los intervinientes convocados a la audiencia. ------

VERIFICACIÓN DE LAS PARTES INTERVINIENTES:

1. **REPRESENTANTE DEL MINISTERIO PÚBLICO: DR. LUIS ALBERTO DIAZ UGARTE,** Fiscal Adjunto Provincial de la Fiscalía de Tambopata.
   - **Casilla electrónica:** 64409.
2. **DEFENSA PÚBLICA DEL IMPUTADO: DR. OSCAR VIZCARRA RAMOS,** con registro N° 1922 del Colegio de Abogados de Cusco.
   - **Casilla electrónica:** 95190.
   - **Patrocinada:** PARIZACA PUMA, EDWAR ALEX.
3. **IMPUTADO: PARIZACA PUMA, EDWAR ALEX.**
   - **DNI N°: 72158361**
   - **Domicilio:** Cercado de la Joya. (Cuadra y media del colegio la Joya).
   - **Ocupación:** Moto taxista.

DESARROLLO DE AUDIENCIA:

Juez: No habiendo observaciones, le concede el uso de la palabra al señor fiscal, a efectos de que oralice su requerimiento.

Fiscal: Procede a oralizar la **incoación de Proceso Inmediato en flagrancia** en contra de PARIZACA PUMA, EDWAR ALEX, por la presunta comisión del delito Acoso Sexual Acoso, en agravio de la menor de iniciales G.M.B.M., de 15 años de edad; fundamentando conforme lo dispuesto por Ley. Registrado en audio.

Juez: Traslada a la defensa técnica.

Defensa técnica: No tiene observaciones en la incoación de proceso inmediato e indica que su imputado quiere acogerse a la terminación anticipada.

Juez: Procede a emitir la siguiente resolución.

AUTO DE INCOACIÓN DE PROCESO INMEDIATO

CORTE SUPERIOR DE JUSTICIA DE MADRE DE DIOS
TERCER JUZGADO DE INVESTIGACIÓN PREPARATORIA DE TAMBOPATA
DE MADRE DE DIOS

RESOLUCION N° DOS
PUERTO MALDONADO, OCTUBRE, UNO DE
DEL AÑO DOS MIL DIECIOCHO.-

VISTOS y OIDOS: La oralización del proceso Inmediato formulado por el representante del Ministerio Público en contra del investigado, sin mayor observación de la defensa; y.

CONSIDERANDO:
Primero: Se tiene que el Ministerio Publico incoa proceso Inmediato en contra del imputado Parizaca Puma Edwar Alex, por la presunta comisión del delito de Acoso Sexual Agravada, conducta descrita en el artículo 176-BB primer y segundo párrafo con la agravante del tercer párrafo inciso sexto del Código Penal, en agravio de la menor de iniciales G.M.B.M., de 15 años de edad.

Segundo: Como hechos se tiene que el imputado como el nombre de Jimi Castro de la Vega le envía una solicitud de amistad por medio de la red social Facebook a la menor agraviada, es que en fecha 18 de septiembre del año 2018 acepta la solicitud procediendo el imputado a preguntarle si era soltera y si iba a las discotecas, respondiéndole la menor que no lo hacia porque es menor de edad, aclarandole que tiene 15 años, indagando pese a ello si fuma, toma y si puede mandarle una fotos suya, respondiendo la menor que no. El día siguiente el imputado continuó asediando a la menor preguntándole a horas 21:18 "amiga no te gustaria entrar a un grupo de chicas , sexis de servicios discretos", "Dime te gustaria", "ola", "Te pago 50 soles", y a horas 22:35 es más explicito escribiéndole; "Me gustaria follarte si gustas claro", la menor le increpa indicando: "que te pasa" y el imputado insiste escribiendo "Me quitas, Me gustaria tener una noche erótica contigo", por lo que la menor le dice que podria denunciarlo pidiendole el imputado que no lo haga, empero de inmediato persiste "no lo hagas... si servicios discretos", para luego pedirle que mejor lo bloquee y ella le pide "Entonces crt... deja de molestarle vale.", pese a lo cual el dia 22 de septiembre del año 2018 continuo escribiéndole, comentando "Te ves bellisima".

Tercero: El dia 26 de setiembre del 2018 al descubrir la progenitora de la menor estas conversaciones, preguntó al imputado por ese mismo medio si seguia en pie su propuesta, quien le indicó que si, aclarando él nuevamente que seria "todo discreto" y que podrian encontrarse en el cementerio (Av. La joya s/n de esta ciudad), indicándole a la menor que fuera en una moto lineal, que él pagaria el pasaje. Es así que a horas 13:30 aproximadamente la menor concurrió al cementerio, indicándole el imputado por el Facebook que estaba dentro al lado derecho, la menor ingresó y luego vio llegar al imputado aproximársele.

Cuarto: La procenitora de la menor, Carmen Darleni Mariño Gonzales, su prima Kelly Francesca Camacho Mariño y Michael Macias Anmuya vieron desde afuera del cementerio la llegada del imputado en un motokar y cómo es que ingresaba detrás de la menor al cementerio, acercándose, reclamando al imputado, iniciándose una discusión, conglomerándose un grupo de personas. Al notar el tumulto dos policías que se encontraban de franco se aproximaron, siendo informados de lo sucedido, interviniendo al imputado, identificándolo y encontrando entre sus pertenencias el teléfono desde el que conversaba con la menor por las redes sociales.

Quinto.- Elementos de convicción que le dan sustento a esta imputación son las intervención realizada el 28 de septiembre como es el **a)** Acta de intervención practicada al imputado cuando pretendia tener relaciones sexuales con la menor agraviada. **b)** El acta de registro personal del imputado hallándose entre sus pertenencias el teléfono celular desde el que conversaba con la menor por las redes sociales, así como un chaleco amarillo de taxista. **c)** Acta de incautación del teléfono celular marca Samsung de color dorado con IMEI N° 358315088252905. Instrumento del delito. **d)** La declaración referencial de la menor agraviada en la que narra cómo es que sucedieron, los hechos, la incomodidad que se le generaron estas proposiciones, la

CORTE SUPERIOR DE JUSTICIA DE MADRE DE DIOS
TERCER JUZGADO DE INVESTIGACIÓN PREPARATORIA DE TAMBOPATA
DE MADRE DE DIOS

reacción que tuvo por ese motivo de amenazarlo con denunciarlo, así como el temor que siente de que el imputado tome represalias contra ella. **c)** La declaración de Carmen Darleni Mariño Gonzales, progenitora de la menor agraviada, con relación a cómo es que se enteró de los hechos y como es que se logró identificar al imputado. **e)** La ficha de RENIEC de la menor agraviada, nacida el 06 de marzo del 2003. **f)** El acta de visualización de mensales y conversaciones en cuenta messenger del equipo telefónico usado por la menor agraviada, verificándose y extrayéndose las capturas de la totalidad de conversaciones que sostuvo con el imputado. **g)** El Acta de visualización de las conversaciones que sostuvo el imputado desde su equipo telefónico, verificándose como es que en dicho equipo estaba abierta la aplicación de facebook con el usuario "Jimi Castro de La Vega", encontrándose la última conversación que sostuvo con la menor, advirtiéndose que las anteriores fueron borradas.

Sexto: Todos estos elementos de convicción le dan sustento a la conducta que se le atribuye el de Acoso Sexual Agravado conforme al artículo 176- B primer y segundo párrafo con la agravante del inciso sexto del tercer párrafo del Código Penal, no se ha hechos mayor observaciones a esta atribución, corresponde apararse este pedido y dictar una procedencia eventualmente para un juicio inmediato; Fundamentos por los cuáles.

RESUELVE.-

- **DECLARAR FUNDADA** la Incoación del Proceso Inmediato, por el delito en flagrancia en contra de **EDWARD ALEX PARISACA PUMA,** por el delito de **ACOSO SEXUAL AGRAVADO,** en agravio de la menor de iniciales G.M.B.M.

Juez: Notifica la presente resolución, para su pronunciamiento.

Fiscal: No tiene observaciones.

Defensa técnica: No tiene observaciones.

Juez: Señala que el presente delito es posible que pueda calificar para una terminación anticipada por lo que les da un tiempo a fin de que pongan de acuerdo por lo que suspende audio por breve termino (...). Reanudando audio se le concede el uso de la palabra al señor fiscal para que haga conocer a los acuerdos arribados.

Fiscal: Procede dar a conocer los acuerdos arribados, entre el imputado, juntamente con su defensa técnica. Registrado en audio.

Juez: Traslada a la defensa.

Defensa técnica: Indica que son los acuerdos a los cuales han arribado conforme lo ha expuesto el señor fiscal, por lo que solicita se apruebe los acuerdos.

Juez: hace conocer los alcances de una Terminación Anticipada al imputado y realiza las siguientes preguntas: si se encuentra conforme con los hechos que le imputa el Ministerio Publico; si se encuentra de acuerdo con la pena que se ha expuesto en la presente audiencia; si no desea pasar a la siguiente etapa que es de juzgamiento en la que de repente pueda terminar con una pena menor o mayor y si desea terminar en esta etapa.

Imputado: Señalo que: se encuentra conforme en todo los extremos y que no desea pasar a la siguiente etapa.

CORTE SUPERIOR DE JUSTICIA DE MADRE DE DIOS
TERCER JUZGADO DE INVESTIGACIÓN PREPARATORIA DE TAMBOPATA
DE MADRE DE DIOS

Fiscal: Solicita que se realice la confirmatoria de incautación del teléfono celular. Registrado en audio.

Juez: Pregunta, si hay otro caso similar al que se está investigando, habiendo indicado el señor fisca negativamente, el Magistrado indica que no es competente para realizar dicha incautación si no se existe otra denuncia o investigación. Registrado en audio.

Fiscal: Deja constancia que esta es la primera oportunidad para realizar lo pedido. Registrado en audio.

Juez: Indica que solamente se tiene en este caso respecto de una agraviada no de varios agraviado. Detalles registrado en audio; procede a emitir la siguiente resolución.

SENTENCIA DE TERMINACIÓN ANTICIPADA

RESOLUCION N° TRES
PUERTO MALDONADO, OCTUBRE, UNO DE
DEL AÑO DOS MIL DIECIOCHO.-

I. VISTOS y OÍDOS:

En audiencia el requerimiento de proceso inmediato y el pedido de Terminación Anticipada planteado por el representante del Ministerio Público en consenso con la parte imputada debidamente asesorado con abogado defensor.

IDENTIFICACIÓN DEL IMPUTADO:

EDWARD ALEX PARISACA PUMA: Con DNI Nº 72158361; nacido el 26 de julio de 1996; Tambopata, Tambopata, Departamento de Madre de Dios; Con 22 años; Estado civil soltero; Hijo de Leoncio y Ceferina; A quien se le procesa por la comisión del delito Acoso Sexual Agravada, conducta descrita en el artículo 176-B primer y segundo párrafo con la agravante del inciso tercero texto párrafo del Código Penal, en agravio de la menor de iniciales G.M.B.M.

II. CONSIDERANDO:

PRIMERO: ***DE LOS ALCANCES DEL PROCESO ESPECIAL DE TERMINACIÓN ANTICIPADA***

1.1. El artículo 468 del código procesal penal informa que el proceso penal puede terminar anticipadamente si el Ministerio Público y la parte imputada presentan solicitud conjunta sobre la pena reparación civil y demás consecuencias accesorias estás luego de ser debatidas en audiencia pueden ser aceptadas por el Juez siempre que el hecho, la calificación del delito, aplicación de la pena, la reparación civil y otras consecuencias accesorias que resulten legales, razonable y obren suficientes elementos de convicción, esto está previsto ya en el artículo 447 numeral 3 del Código Procesal Penal, modificado por el Decreto Legislativo 1194.

SEGUNDO: ***SOBRE LA IMPUTACIÓN FÁCTICA Y LA CALIFICACIÓN JURÍDICA:***
2.1. Respecto a los hechos están referidos:

CORTE SUPERIOR DE JUSTICIA DE MADRE DE DIOS
TERCER JUZGADO DE INVESTIGACIÓN PREPARATORIA DE TAMBOPATA
DE MADRE DE DIOS

a. Como hechos se tiene que el imputado como el nombre de Jimi Castro de la Vega le envía una solicitud de amistad por medio de la red social Facebook a la menor agraviada, es que en fecha 18 de septiembre del año 2018 acepta la solicitud procediendo el imputado a preguntarle si era soltera y si iba a las discotecas, respondiéndole la menor que no lo hacía porque es menor de edad, aclarándole que tiene 15 años, indagando pese a ello si fuma, toma y si puede mandarle una fotos suya, respondiendo la menor que no. El día siguiente el imputado continuó asediando a la menor preguntándole a horas 21:18 "amiga no te gustaría entrar a un grupo de chicas sexis de servicios discretos", "Dime te gustaría", "cia", "Te pago 50 soles", y a horas 22:35 es más explícito escribiéndole: "Me gustaría follarte si gustas claro", la menor le increpa indicando: "que te pasa" y el imputado insiste escribiendo "Me gustas. Me gustaría tener una noche erótica contigo", por lo que la menor le dice que podría denunciarlo pidiéndole el imputado que no lo haga, empero de inmediato persiste "no lo hagas... si servicios discretos", para luego pedirle que mejor lo bloquee y ella le pide "Entonces crj... deja de molestarle vale.", pese a lo cual el día 22 de septiembre del año 2018 continúo escribiéndole, comentando "Te ves bellísima".

b. El día 28 de setiembre del 2018 al descubrir la progenitora de la menor estas conversaciones, preguntó al imputado por ese mismo medio si seguía en pie su propuesta, quien le indicó que si, aclarando el nuevamente que sería "todo discreto" y que podrían encontrarse en el cementerio (Av. La joya s/n de esta ciudad), indicándole a la menor que fuera en una moto lineal, que él pagaría el pasaje. Es así que a horas 13:30 aproximadamente la menor concurrió al cementerio, indicándole el imputado por el Facebook que estaba dentro al lado derecho, la menor ingresó y luego vio llegar al imputado aproximársele.

c. La progenitora de la menor, Carmen Darleni Mariño Gonzalos, su prima Kelly Francesca Camacho Mariño y Michael Macias Arimuya vieron desde afuera del cementerio la llegada del imputado en un motokar y cómo es que ingresaba detrás de la menor al cementerio, acercándose, reclamando al imputado, iniciándose una discusión, conglomerándose un grupo de personas. Al notar el tumulto dos policías que se encontraban de franco se aproximaron, siendo informados de lo sucedido, interviniendo al imputado, identificándolo y encontrando entre sus pertenencias el teléfono desde el que conversaba con la menor por las redes sociales.

2.2. Respecto a los elementos de convicción:

- Elementos de convicción que le dan sustento a esta imputación son las intervención realizada el 28 de septiembre como es el **a)** Acta de intervención practicada al imputado cuando pretendía tener relaciones sexuales con la menor agraviada. **b)** El acta de registro personal del imputado hallándose entre sus pertenencias el teléfono celular desde el que conversaba con la menor por las redes sociales, así como un chaleco amarillo de taxista. **c)** Acta de incautación del teléfono celular marca Samsung de color dorado con IMEI N° 358215088252905. Instrumento del delito. **d)** La declaración referencial de la menor agraviada en la que narra cómo es que sucedieron, los hechos, la incomodidad que se le generaron estas proposiciones, la reacción que tuvo por ese motivo de amenazarlo con denunciarlo, así como el temor que siente de que el imputado tome represalias contra ella. **e)** La declaración de Carmen Darleni Mariño Gonzales, progenitora de la menor agraviada, con relación a cómo es que se enteró de los hechos y como es que se logró identificar al imputado. **e)** La

ficha de RENIEC de la menor agraviada, nacida el 06 de marzo del 2003. **f)** El acta de visualización de mensajes y conversaciones en cuenta messengar del equipo telefónico usado por la menor agraviada, verificándose y extrayéndose las capturas de la totalidad de conversaciones que sostuvo con el imputado. **g)** El Acta de visualización de las conversaciones que sostuvo el imputado desde su equipo telefónico, verificándose como es que en dicho equipo estaba abierta la aplicación de facebook con el usuario "Jimi Castro de La Vega", encontrándose la última conversación que sostuvo con la menor, advirtiéndose que las anteriores fueron borradas.

2.3. Calificación jurídica:

- La calificación jurídica que le ha dado el Ministerio Público es que los hechos se encuentra conducta descrita en el artículo 176- B primer y segundo párrafo con la agravante del inciso sexto del tercer párrafo del Código Penal.

TERCERO: *SOBRE EL ACUERDO PROVISIONAL:*

a. ***Respecto a los hechos:*** Las partes han explicado que los hechos que merecen esta decisión son los mismos que han sido materia de Incoación de Proceso Inmediato.

b. ***Cómo elementos de convicción:*** Se toma en cuenta que estos ya han sido mencionados y le dan sustento a la imputación qué hace el Ministerio Público.

c. ***En cuanto a la pena:*** Han indicado que el rango punitivos para este tipo de delitos es entre cuatro a ocho de pena privativa de libertad, en este extremo atendiendo a que el imputado no tiene antecedentes penales; Por lo que se fija la pena en un extremo mínimo es decir cuatro año y dos meses, a esa pena acordada se está reduciendo el sexto que permite el artículo 471 del Código Procesal Penal, quedando en definitiva tres años y seis meses de pena privativa de la libertad, cuya efectividad se suspende por el plazo de dos año sujeto a las siguientes reglas de conducta: **a)** Prohibición de acercarse a la menor agraviada ni a sus familiares. **b)** Concurrir al Juzgado y dar cuenta de sus actividades cada dos meses. **c)** No comunicarse con la menor agraviada por ningún medio tecnológico. **d)** Prohibición de ausentarse sin autorización del Juzgado **d)** Deberá pagar el íntegro de la Reparación Civil en la forma en que ha sido acordada, y al cumplimiento de toda las reglas de conducta impuestas todo ello bajo apercibimiento del artículo 59 numeral 3) del Código Penal en caso incumpla estas reglas de conducta.

d. ***Reparación Civil:*** La suma acordada es de cuatrocientos soles, que serán pagados en cuotas de cien soles cada fin de mes comenzando desde el mes de octubre has el mes de enero del año 2019.

CUARTO: *CONTROL DE LEGALIDAD:*

4.1. Sobre los hechos: Tomando en cuenta la imputación fáctica tal y como ha sido postulada por el Ministerio Público la suficiencia de elementos de convicción que le dan respaldo a esta imputación.

CORTE SUPERIOR DE JUSTICIA DE MADRE DE DIOS
TERCER JUZGADO DE INVESTIGACIÓN PREPARATORIA DE TAMBOPATA
DE MADRE DE DIOS

4.2. ***Sobre la suficiencia y elementos de convicción:*** El sustento no sólo está amparado en el reconocimiento que ha hecho el imputado en esta audiencia sino también a los suficientes elementos de convicción que le dan sostenibilidad a la imputación.

4.3. ***Sobre la pena***: Tomamos en cuenta que el marco punitivo que fija el código penal más la reducción que permite el artículo 471 advierte que la pena acordada resulta razonable y proporcionada al delito cometido no se hacen otros análisis toda vez que en esta etapa sólo se emiten juicios de procedibilidad y no se ha actuado prueba alguna.

4.4. ***Sobre la reparación Civil:*** La suma acordada como tal como indicada; tampoco se encuentra afectado de ilegalidad.

QUINTO: *CONCLUSIONES Y APROBACIÓN JUDICIAL DEL ACUERDO:*

5.1. Así entonces se efectúa el análisis del acuerdo de Terminación Anticipada del proceso sustentado en esta audiencia en conformidad con el imputado debidamente asistido por su abogado defensor cabe estimarse el mismo y estarse una sentencia condenatoria, teniendo presente que la pena privativa la libertad sustentada en la forma de suspendida.

5.2. También resulta razonable y proporcional atendiendo a que se ha mencionado que el imputado no tiene antecedentes penales que en atención, forma, naturaleza y modalidad del hecho punible el comportamiento procesal del mismo quién ha reconocido los hechos permite inferir a este despacho que es muy probable que no vuelva a cometer, delito encontrándose en los supuestos que establece el artículo 57 del Código Penal. Por lo que de acuerdo al artículo 467 del Código Procesal Penal; Administrando justicia a nombre del pueblo de quién emana esta potestad.

RESUELVE.-

1. **APROBANDO EL ACUERDO DE TERMINACIÓN ANTICIPADA** del proceso, propuesto por el Ministerio Público y el imputado debidamente asistido con su abogado defensor.
2. **DECLARA** a **EDWARD ALEX PARISACA PUMA,** cuyas calidades personales aparecen en la parte expositiva de esta sentencia como **AUTOR** del delito Contra la Libertad, en su modalidad de Violación de la Libertad Sexual, sub tipo **ACOSO SEXUAL AGRAVADA,** conducta descrita en el artículo 176-B**B** primer y segundo párrafo con la agravante del tercer párrafo inciso sexto del Código Penal, en agravio de la menor de iniciales G.M.B.M.; y como tal se le impone **TRES AÑOS Y SEIS MESES DE PENA PRIVATIVA DE LA LIBERTAD SUSPENDIDA** en su ejecución por el PLAZO DE DOS AÑOS,
3. Sujeta a las siguientes **REGLAS DE CONDUCTA: a) Prohibición de acercarse a la menor agraviada ni a sus familiares. b)** Concurrir al Juzgado y dar cuenta de sus actividades cada dos meses. **c)** No comunicarse con la menor agraviada por ningún medio tecnológico. **d)** Prohibición de ausentarse sin autorización del Juzgado **d)** Deberá pagar el integro de la Reparación Civil en la forma en que ha sido acordada, y al cumplimiento de todas las reglas de conducta impuestas todo ello bajo apercibimiento del artículo 59 numeral 3) del Código Penal en caso incumpla estas reglas de conducta.

CORTE SUPERIOR DE JUSTICIA DE MADRE DE DIOS
TERCER JUZGADO DE INVESTIGACIÓN PREPARATORIA DE TAMBOPATA
DE MADRE DE DIOS

4. Mando que consentida o ejecutoriada sea esta sentencia, se cursen las comunicaciones pertinentes para fines de registro y archivo.

Juez: Notifica la presente resolución, para su pronunciamiento.

Fiscal: Expresa conformidad y solicita se devuelva la carpeta fiscal.

Defensa técnica: Conforme.

Imputada: Conforme.
Juez: Conformes a las partes y autoriza la devolución de la carpeta fiscal.

III.- CONCLUSIÓN:

15:40 HORAS *Siendo las* ***quince horas con cuarenta minutos*** *del mismo día de la fecha, se da por concluida la presente audiencia y por cerrada la grabación del audio, procediendo a firmar el acta señor Juez y la Especialista Judicial de Audiencias encargada de su redacción. De lo que se da fe.*----------

UCV
UNIVERSIDAD
CÉSAR VALLEJO

ESCUELA DE POST GRADO

ENTREVISTA

ADMISIBILIDAD Y VALOR PROBATORIO DE LA EVIDENCIA DIGITAL EN EL SISTEMA JURIDICO PERUANO 2018

ENTREVISTADO: Dr. Angel R. Moron Huaco

ENTIDAD DONDE LABORA: 6TA Fiscalia Superior Penal - Distrito Fiscal Lima Norte.

OBJETIVO GENERAL:

La presente investigación tiene como finalidad describir la admisibilidad y valor probatorio de la evidencia digital en el sistema jurídico peruano 2018.

Firma

ANGEL R. MORON HUACO
Fiscal Adjunto Superior (P)
6ta. Fiscalía Superior Penal
Distrito Fiscal de Lima Norte

UCV
UNIVERSIDAD
CÉSAR VALLEJO

ESCUELA DE POST GRADO

ENTREVISTA

ADMISIBILIDAD Y VALOR PROBATORIO DE LA EVIDENCIA DIGITAL EN EL SISTEMA JURIDICO PERUANO 2018

ENTREVISTADO: S71 PNP ZABARBURU VARGAS, WUILMAN

ENTIDAD DONDE LABORA: DIVISIÓN DE INVESTIGACIÓN DE DELITOS DE ALTA TECNOLOGÍA - DIRINCRI PNP

OBJETIVO GENERAL:

La presente investigación tiene como finalidad describir la admisibilidad y valor probatorio de la evidencia digital en el sistema jurídico peruano 2018.

Firma

CIP. 31209368
Wuilman ZABARBURU VARGAS
SOT / PNP

UNIVERSIDAD CÉSAR VALLEJO

Escuela de Posgrado

"Año del Diálogo y la Reconciliación Nacional"

Lima, 28 de Noviembre de 2018

Carta P. 0787–2018–EPG–UCV–LN

ING. GIOVANNI PICHLING ZOLEZZI
GERENTE DE OPERACIONES DE LA ASOCIACIÓN DE BANCOS DEL PERU
ASOCIACIÓN DE BANCOS DEL PERU

De mi mayor consideración:

Es grato dirigirme a usted, para presentar a **MIGUEL ANGEL OSCO ESCOBEDO** identificado con DNI N.° **43555690** y código de matrícula N.° **6700211295;** estudiante del Programa de **MAESTRÍA EN DERECHO PENAL Y PROCESAR PENAL** quien se encuentra desarrollando el Trabajo de Investigación (Tesis):

LA ADMISIBILIDAD Y EL VALOR PROBATORIO DE LA EVIDENCIA DIGITAL EN EL SISTEMA JURIDICO PERUANO 2018

En ese sentido, solicito a su digna persona otorgar el permiso y brindar las facilidades a nuestro estudiante, a fin de que pueda desarrollar su trabajo de investigación en la institución que usted representa. Los resultados de la presente serán alcanzados a su despacho, luego de finalizar la misma.

Con este motivo, le saluda atentamente,

ESCUELA DE POSGRADO UCV JEFATURA CAMPUS LIMA NORTE

Dr. Carlos Venturo Orbegoso
Jefe de la Escuela de Posgrado
Universidad César Vallejo - Campus Lima Norte

asbanc ASOCIACIÓN DE BANCOS DEL PERU
04 DIC. 2018
RECIBIDO
GERENCIA DE OPERACIONES

RCOA

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

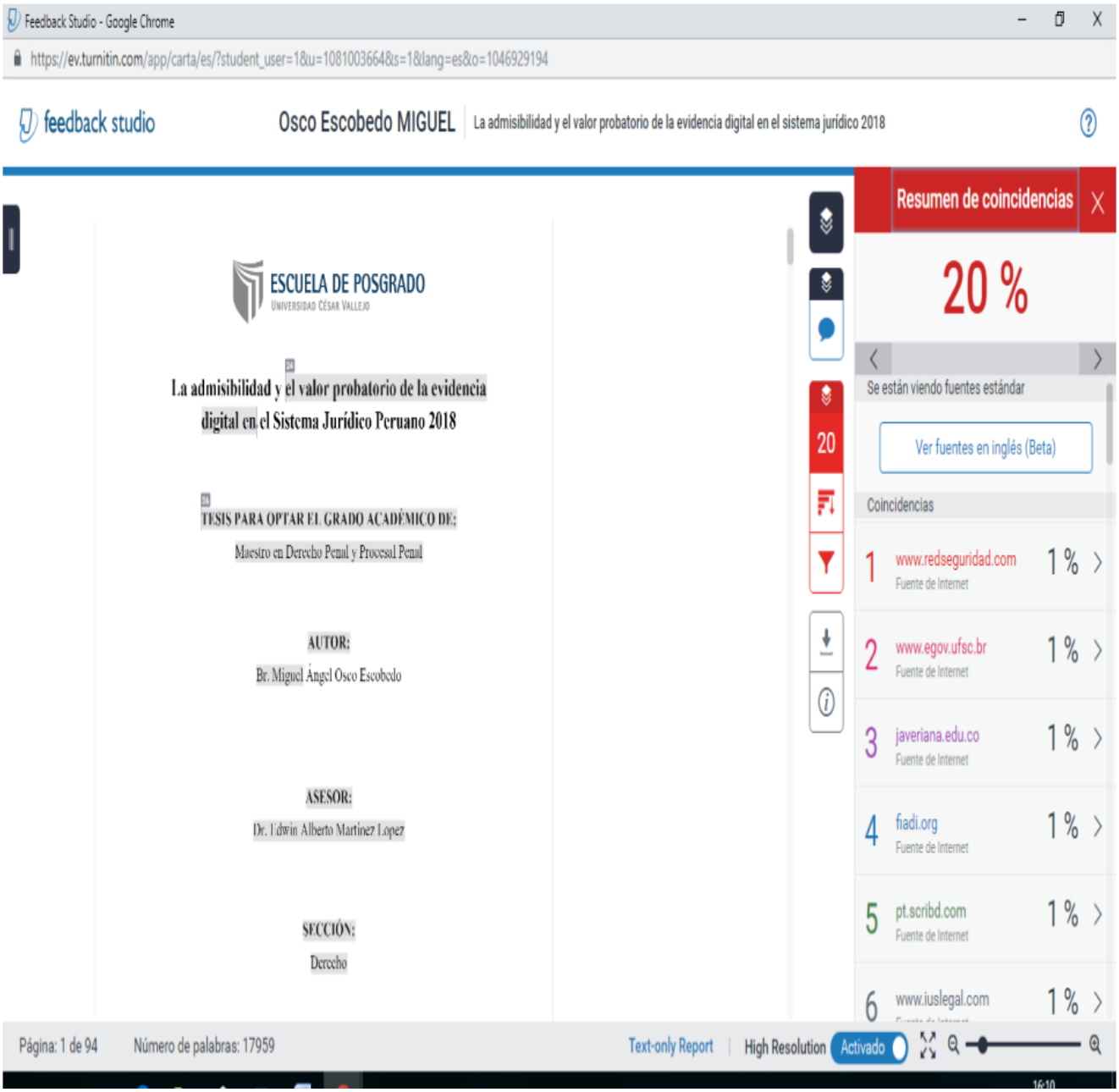
Acta de Aprobación de originalidad de la Tesis

Yo, Edwin Alberto Martínez López, docente de la Escuela de Posgrado de la Universidad César Vallejo filial Lima Norte, revisor de la tesis titulada "La admisibilidad y el valor probatorio de la evidencia digital en el Sistema Jurídico Peruano, 2018" de la estudiante **Miguel Angel Osco Escobedo** y habiendo sido capacitado e instruido en el uso de la herramienta Turnitin, he constatado lo siguiente:

Que el citado trabajo académico tiene un índice de similitud de 20 % verificable en el reporte de originalidad del programa turnitin, grado de coincidencia que cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

Lima, 19 de enero del 2019

Dr. Edwin Alberto Martinez López
Docente de la EPG - UCV


Feedback Studio - Google Chrome
https://ev.turnitin.com/app/carta/es/?student_user=1&u=1081003664&s=1&lang=es&o=1046929194
feedback studio
Osco Escobedo MIGUEL
La admisibilidad y el valor probatorio de la evidencia digital en el sistema jurídico 2018
ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO
La admisibilidad y el valor probatorio de la evidencia digital en el Sistema Jurídico Peruano 2018
TESIS PARA OPTAR EL GRADO ACADÉMICO DE:
Maestro en Derecho Penal y Procesal Penal
AUTOR:
Br. Miguel Ángel Osco Escobedo
ASESOR:
Dr. Edwin Alberto Martínez Lopez
SECCIÓN:
Derecho
Resumen de coincidencias
20 %
Se están viendo fuentes estándar
Ver fuentes en inglés (Beta)
Coincidencias
1 www.redseguridad.com 1 %
Fuente de Internet
2 www.egov.ufsc.br 1 %
Fuente de Internet
3 javeriana.edu.co 1 %
Fuente de Internet
4 fiadi.org 1 %
Fuente de Internet
5 pt.scribd.com 1 %
Fuente de Internet
6 www.iuslegal.com 1 %
Página: 1 de 94
Número de palabras: 17959
Text-only Report
High Resolution
Activado

UNIVERSIDAD CÉSAR VALLEJO

Centro de Recursos para el Aprendizaje y la Investigación (CRAI)
"César Acuña Peralta"

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN ELECTRÓNICA DE LAS TESIS

1. DATOS PERSONALES

Apellidos y Nombres: (solo los datos del que autoriza)
OSCO ESCOBEDO MIGUEL ANGEL
D.N.I. : 43555690
Domicilio : AV. PERU 1292 URB. HUAQUILLAY - HUAS
Teléfono : Fijo : ..... Móvil : 993681922
E-mail : OSCO36@hotmail.com

2. IDENTIFICACIÓN DE LA TESIS

Modalidad:

☐ Tesis de Pregrado
Facultad : .....
Escuela : .....
Carrera : .....
Título : .....

☐ Tesis de Posgrado
☒ Maestría ☐ Doctorado
Grado : MAESTRO
Mención : DERECHO PENAL Y PROCESAL PENAL

3. DATOS DE LA TESIS

Autor (es) Apellidos y Nombres:
OSCO ESCOBEDO MIGUEL ANGEL
.....
.....

Título de la tesis:
LA ADMISIBILIDAD Y EL VALOR PROBATORIO DE LA EVIDENCIA DIGITAL EN EL SISTEMA JUDICIAL PERUANO 2018

Año de publicación : .....

4. AUTORIZACIÓN DE PUBLICACIÓN DE LA TESIS EN VERSIÓN ELECTRÓNICA:

A través del presente documento,
Si autorizo a publicar en texto completo mi tesis. ☒ X
No autorizo a publicar en texto completo mi tesis. ☐

Firma : .....

Fecha : 08/02/2019

UNIVERSIDAD CÉSAR VALLEJO

AUTORIZACIÓN DE LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN

CONSTE POR EL PRESENTE EL VISTO BUENO QUE OTORGA EL ENCARGADO DE INVESTIGACIÓN DE

ESCUELA DE POSGRADO

A LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN QUE PRESENTA:

OSCO ESCOBEDO MIGUEL ANGEL

INFORME TÍTULADO:

LA ADMISIBILIDAD Y EL VALOR PROBATORIO DE LA EVIDENCIA DIGITAL EN EL SISTEMA JURIDICO PERUANO 2018

PARA OBTENER EL TÍTULO O GRADO DE:

MAESTRIA EN DERECHO PENAL Y PROCESAL PENAL

SUSTENTADO EN FECHA: 23 DE ENERO 2019

NOTA O MENCIÓN: APROBADO POR UNANIMIDAD

ESCUELA DE POSGRADO UCV UNIVERSIDAD CÉSAR VALLEJO INVESTIGACIÓN CAMPUS LIMA NORTE

FIRMA DEL ENCARGADO DE INVESTIGACIÓN