Universidad
Norbert Wiener

Escuela de Posgrado

Extracción de información en teléfonos celulares y su relación con hechos delictivos en la oficina de peritajes del ministerio público - Lima 2020

Tesis para optar el grado académico de Maestro en Ciencia Criminalistica

Presentado por:

Gutiérrez Salvador, Wiliam Rubén

Código ORCID: 0000-0002-2867-6606

Asesor: Dra. Casana Jara, Kelly Milagritos

Código ORCID: 0000-0002-7778-3141

Lima – Perú

2022

Tesis

"EXTRACCIÓN DE INFORMACIÓN DE TELÉFONOS CELULARES Y SU RELACIÓN CON HECHOS DELICTIVOS EN LA OFICINA DE PERITAJES DEL MINISTERIO PÚBLICO - LIMA 2020"

Línea de investigación: Sociedad y Transformación digital

Sub línea: Exámenes de los indicios o evidencia.

ASESOR: Dra. CASANA JARA, KELLY MILAGRITOS
CÓDIGO ORCID: 0000-0002-7778-3141

ÍNDICE

ANEXOS

Índice de tablas

Índice de gráficos

RESUMEN

El propósito de la investigación fue determinar si la información contenida en teléfonos celulares se vincula con hechos delictivos. En este sentido el requerimiento se inicia cuando la autoridad fiscal, policial o judicial envía un oficio a la Oficina de Peritajes, solicitando encontrar o validar un dato que permita esclarecer un posible hecho criminal, siendo este oficio atendido por un Perito informático del área de Análisis Digital Forense (ADF), el cual elabora un Informe Pericial donde describe los hallazgos para ser valorados por la autoridad solicitante.

El tipo de indagación empleado fue cuantitativo, de tipo básica, empleando el diseño no experimental.

La población de estudio fue deliberadamente no probabilística y correspondió a la muestra de estudio de extracción de información de 80 teléfonos celulares correspondientes a informes periciales del año 2020, teniendo como objeto pericial encontrar información de tipo criminal referido a delitos contra el patrimonio, homicidio, tráfico ilícito de drogas y contra la indemnidad sexual.

PALABRA CLAVE: Pericia informática, extracción de teléfono celular, informática forense, informe pericial, Perito informático, hechos delictivos, software forense.

ABSTRACT

The purpose of the investigation was to determine if the information contained in cell phones was linked to criminal acts. In this sense, the request begins when the fiscal, police or judicial authority sends a letter to the Office of Expertise, requesting to find or validate a piece of information that allows clarifying a possible criminal act, this letter being handled by a Computer Expert from the Analysis area. Digital Forensic (ADF), which prepares an Expert Report describing the findings to be assessed by the requesting authority.

The type of inquiry used was quantitative, of the basic type, using the non-experimental design.

The study population was deliberately non-probabilistic and corresponded to the study sample of information extraction from 80 cell phones corresponding to expert reports of the year 2020, with the expert object of finding criminal information referring to crimes against property, homicide, traffic illicit drugs and against sexual indemnity

KEY WORD: Computer expertise, cell phone extraction, computer forensics, expert report, Computer expert, criminal acts, forensic software.

INTRODUCCIÓN

La presente investigación denominada “Extracción de información de teléfonos celulares y su vinculación en hechos delictivos en la OPERIT, 2020” en el departamento de ADF de la oficina de peritajes, sito en la Av. Prolongación Arica N°1832. Breña.

El trabajo de investigación consta de cinco capítulos:

Del capítulo I de la problemática, trata sobre la explicación del problema, relacionado con la extracción de información de teléfonos celulares y su relación con hechos delictivos.

Del capítulo II del ámbito hipotético, antecedentes, fundamento jurídico, fundamento teórico y la declaración del argumento.

Del capítulo III del método, se elaboró el enfoque, tipo de investigación, la muestra que va a analizar, variables, técnica e instrumento de recopilación de datos.

Del capítulo IV de la exposición y controversia del desenlace, se especifica el estudio narrativo y debate de resultados.

Del capítulo V se describen las conclusiones y recomendaciones de la tesis.

CAPÍTULO I: EL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

El auge de los delitos informáticos empleando medios tecnológicos como teléfonos celulares y otros, está fuertemente ligado al crecimiento tecnológico, atrás quedaron los días en que las PC eran la principal fuente de evidencia. Las organizaciones ahora tienen una multitud de fuentes de datos que incluyen Mac, dispositivos móviles y servicios en la nube.

En este contexto la evolución de la tecnología ha venido posibilitando a las personas a cometer delitos informáticos incrementando el porcentaje y diversidad de delitos en el ciberespacio (ONU, 2019).

En España, las personas usan teléfonos celulares no solo para estar comunicados con sus familiares y amigos sino como una herramienta de trabajo y ocio como, por ejemplo: para enviar correos electrónicos, realizar compras por internet, transferir dinero, consultar el clima, el tráfico vehicular, comprar pasajes, ver películas, juegos en línea, redactar documentos, realizar trabajo remoto y otros. (Fernández, 2022)

En una investigación realizada en los Estados Unidos con respecto a los métodos de extracción de datos de teléfonos móviles, se menciona que esta habilidad especial; no es igual que la recuperación de datos de equipos tradicionales. Algunos teléfonos celulares no comparten los mismos sistemas operativos y otros son dispositivos integrados patentados que tienen configuraciones únicas (Saltzman, 2021). La compañía Cellebrite asegura que su nueva herramienta informática CELLEBRITE PREMIUM ayudara a las autoridades policiales, judiciales y fiscales a recabar información de contactos, audios, videos,

imágenes, conversaciones y otros, incluyendo información eliminada de teléfonos celulares bloqueados de alta tecnología tipo Android o IPhone (RT, Agencia de noticias, 2019).

En México, según artículo periodístico de El Diario el Economista (Monroy, 2020), se identificaron 16,470 Tarjetas SIMCARD (Chip telefónico) y 14, 964 equipos celulares ilegales en prisión, siendo estos equipos utilizados mayormente para cometer delitos de extorsión y otros.

Por otro lado, los investigadores de seguridad y forenses han descubierto múltiples casos de ataques de RANSOMWARE, ataques de phishing y malwares en época de covid-19 desde el año pasado. Según una investigación de Barracuda Networks (Endpoint. 2018), los ataques de pishing temáticos de covid-19 han aumentado un 26% en comparación con el año 2018.

En Paraguay, a medida que el mundo se está enfrentando a los desafíos de COVID-19, hay otro tipo de amenaza para las empresas: el riesgo de crímenes cibernéticos en tiempo de covid-19 especialmente, cometidos empleando los teléfonos celulares. Los atacantes se han aprovechado de esta sensación de temor que está rodeando el virus desde el inicio de la pandemia. En una atmósfera de incertidumbre, donde cualquier información aparente sobre una crisis en curso se convierte en un poderoso anzuelo. Esto es algo que los hackers conocen y han estado explotando (ABC Color.2020).

En una entrevista con el jefe de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional, comenta que hubo 3,012 acusaciones de fraude informático, pornografía infantil, robo de identidad y otras actividades ilegales, provenientes en su mayoría de teléfonos móviles (ANDINA,2019).

En el Perú la cantidad de crímenes cometidos a través de medios tecnológicos en la Fiscalía de la Nación se intensifica rápidamente desde el mes de octubre al mes de julio del año 2020 (DIRINCRI-PNP/DIVINDAT-SEC, 2020). Las unidades fiscales contabilizaron 21,687 acusaciones, de los cuales el 40% son del año 2019, sin embargo, en esa misma época se registró el 58% de las mimas y se formularon solo 108 veredictos, produciendo demasiada carga de requerimientos y un sentimiento de liberación e incertidumbre (Ministerio Público – Fiscalía de la Nación, 2020).

En la Oficina de Peritajes del Ministerio Público (OPERIT, 2020), los hechos delictivos han ido aumentando grandemente, recibiendo el año 2019, más de 3 mil celulares, de los cuales aproximadamente más de la tercera parte tienen contraseña o código de patrón o huella digital; dificultando de esta manera la extracción de información.

La pandemia de covid-19 ha hecho que la ciencia forense digital de teléfonos celulares sea más desafiante, particularmente al aumentar la necesidad de realizar adquisiciones remotas desde puntos finales que no están en la red corporativa y porque los ciberdelincuentes están ajustando sus tácticas de manera oportunista. (Revista Digital Magnet Forensics, 2021).

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. Problema general

¿Cómo la extracción de información de teléfonos celulares se relaciona en los hechos delictivos en la OPERIT de Ministerio Público, Lima 2020?

1.2.2. Problemas específicos

1.2.2.1 ¿Qué vinculo tiene la extracción de información de teléfonos celulares con la marca y modelo en los hechos delictivos en la OPERIT, 2020?

1.2.2.2 ¿Qué relación tiene la extracción de información de teléfonos celulares con el software forense en los hechos delictivos en la OPERIT, 2020?

1.2.2.3 ¿Qué relación tiene la extracción de información de teléfonos celulares con la adquisición en los hechos delictivos en la OPERIT, 2020?

1.2.2.4 ¿Qué relación tiene la extracción de información de teléfonos celulares con la evidencia digital en los hechos delictivos en la OPERIT, 2020?

1.3. OBJETIVOS DE LA INVESTIGACIÓN

1.3.1. Objetivo general

Identificar en qué medida la extracción de información de teléfonos celulares se relaciona con los hechos delictivos en la OPERIT del Ministerio Público, 2020".

1.3.2. Objetivos específicos

1.3.2.1 Determinar en qué medida la extracción de información de teléfonos celulares se relaciona con la marca y modelo en los hechos delictivos en la OPERIT, 2020.

1.3.2.2 Identificar de qué manera la extracción de información de teléfonos celulares se relaciona con el software forense en los hechos delictivos en la OPERIT, 2020.

1.3.2.3 Determinar de qué manera la extracción de información de teléfonos celulares se relaciona con la adquisición en los hechos delictivos en la OPERIT, 2020.

1.3.2.4 Determinar de qué manera la extracción de información de teléfonos celulares se relaciona con la evidencia digital en los hechos delictivos en la OPERIT, 2020.

1.4. JUSTIFICACIÓN DE LA INVESTIGACIÓN

1.4.1. Teórica

El argumento teórico se basa en probar o contradecir, si en un teléfono celular, puede existir algún indicio o evidencia digital como una conversación, registro de llamada telefónica, mensaje de texto, archivo de audio u otro elemento que permita establecer un hecho criminal; lo cual permitirá que, al Juez o Fiscal, le dé la valoración pertinente a una prueba digital y con ello demostrar la inocencia o culpabilidad de una persona en un juicio.

Así mismo, los resultados encontrados servirán a las autoridades jurisdiccionales y expertos en Informática Forense de instituciones privadas o públicas, conocer las diferentes técnicas de adquisición de teléfonos celular bloqueados, desbloqueados o dañados que permita encontrar alguna evidencia digital relacionado a un hecho delictivo.

1.4.2. Metodológica

Esta indagación facilitara aclarar por medio de un formulario de recopilación de información las aristas más importantes en la etapa de adquisición de información, empleando diferentes técnicas de desbloqueo y recolección de datos, así como la identificación de archivos digitales relacionados a hechos delictivos

Por otro lado, este trabajo de investigación permitirá a los Policías, Fiscales y Peritos que participan en la etapa de recolección de evidencia digital, valorar la importancia de preservar un teléfono celular para una investigación forense exitosa.

Así mismo, los resultados de este estudio son de necesidad de la Oficina de Peritajes para mejorar las actividades periciales en el área de ADF en la búsqueda de evidencias de hechos delictivos en teléfonos celulares, siendo transcendente la prueba digital, que sirva de elemento de convicción en un juicio.

1.4.2. Práctica

Este trabajo de investigación se justifica, porque permitirá a los Peritos Informáticos aplicar procesos agiles de manejo de evidencia digital en la extracción de información de teléfonos celulares, eligiendo el software más adecuado y empleando métodos óptimos de adquisición con el fin de buscar y encontrar información relevante de un posible hecho delictivo.

Con ello, se pretende capacitar a los Peritos y analistas forenses de la Oficina de Peritajes en materia de Pericia informática a teléfonos celulares; a fin de que ellos puedan apoyar de manera rápida y eficiente en esta labor.

1.5. LIMITACIONES DE LA INVESTIGACIÓN

1.5.1. TEMPORAL

Se realizará durante del año 2020 (01 de enero a 31 de diciembre).

1.5.2. ESPACIAL

Se basó en la información proporcionada por el departamento de Análisis Digital Forense (ADF) de la OPERIT.

1.5.3. POBLACION O UNIDAD DE ANALISIS

Población: Carrasco (2005) "Población es el total de los registros (módulos de evaluación) que forman parte del campo geográfico donde se diseña la actividad de indagación". (p. 236-237).

Se tomo como ejemplo la muestra de extracción de 80 teléfonos celulares con Sistema Operativo Android del área de ADF de la OPERIT.

CAPÍTULO II: MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

Tejo, et al. (2021). En su investigación tuvieron como objetivo “Validar un procedimiento que logre conservar huellas digitales e indicios informáticos en el ámbito hospitalario” basado en el Protocolo de Manchester. Se realizó un estudio observacional de alcance correlacional aplicado a un ciber incidente en el Hospital Oncológico de Barretos, Brasil, acaecido el año 2017. provocado por una versión del virus "Petya", que contagio varios equipos de cómputo, pidiendo US$360,000 en Criptomonedas (dinero digital) por su liberación. El incidente informático elimino cerca de 3000 estudios y ensayos de 350 personas que no tuvieron radioterapia. Debido a ello se contrató a ingenieros informáticos, que se demoraron 6 días en restablecer la atención del hospital, teniendo que reconstruir la historia clínica de algunos pacientes. Concluyéndose que no se logró pagar ningún rescate al delincuente informático.

Mayer, L. (2018). En su investigación tuvo como objetivo “Analizar cómo se relaciona la criminalística con los ciber delitos”. Se realizo un estudio basado en el método descriptivo experimental donde se recopilo información del anuario estadístico del Ministerio del Interior de España (2014) identificándose que los delitos informáticos tienen una prevalencia en víctimas de 26 a 40 años. De ello se obtuvo como resultado que son los hombres más propensos de ser víctima de delitos informáticos con el 59%, en comparación con las mujeres con el 41%. Concluyéndose que los delitos informáticos vienen creciendo exponencialmente, por ejemplo, en el país de Estados Unidos algunas instituciones (menor

de 250 trabajadores) y otras mayores (más de 2,500 trabajadores) centran el 70% de ofensivas de suplantación de identidad.

Romero, M. (2017). En su artículo, analizo sobre "Diagnosticar como el avance de la telefonía celular y las páginas webs se vinculan con el cibercrimen de trata de personas en menores de edad en Colombia, del año 2013 al 2015", se realizó un estudio empleando el método exploratorio descriptivo, con enfoque cuantitativo, tomándose como referencia la base de datos de la Policía Nacional (PONAL). La investigación se realizó a una población formada por 1.705 denuncias del accusatory penal system (SPOA), donde 1510 pertenecen a la fiscalía general de la Nación [FGN] de Colombia, 2016), teniendo como resultado que el 89 % de afectados son niñas y 42 % son niños. Concluyéndose que el teléfono celular es uno de los medios más usados para trasmitir material de pornografía infantil.

Rennó y Brasi. (2022). En su investigación tuvieron como propósito "Analizar como el cyberbullying afecta la vida personal y profesional"; se aplicó un análisis preliminar cuantitativo donde intervinieron 35 personas del Federal Institute of Education, Science and Technology of the South of Minas Gerais. La investigación se realizó mediante el envío de un formulario a través de Google Drive. El instrumento utilizado contó con preguntas de carácter sociodemográfico y preguntas semiestructuradas sobre los fenómenos, uso de internet y ciberacoso. Demostrándose que el 68,6% de las personas ya ha sido víctima de ciberacoso, el 71,4% ya ha sido agresor, el 94,3% ya se ha expuesto en internet, el 57,1% ya ha sido testigo de episodios de ciberacoso y el 5,7% nunca lo fue. Concluyéndose que el ciberacoso promovido a través de redes sociales afecta en cierta medida a las personas en su vida laboral y personal.

Ordoñez, et al, (2019). En su artículo tuvieron como objetivo “Identificar las vulnerabilidades de seguridad en teléfonos celulares”. El estudio está basado en la metodología de Runeson, tomando como muestra los teléfonos celulares de 129 alumnos de siete universidades de Colombia de 16 a 25 años; el examen consistió en verificar la efectividad del programa Android Protect en detectar alguna vulnerabilidad en un celular. Demostrándose que el 19% de los teléfonos fueron detectados por Google Play Protect, el 12% permitió la instalación sin ningún tipo de protección, y el 70% muestra un mensaje solicitando permiso para instalarlo. Concluyéndose que no basta con tener instalado el programa PLAY PROTECT que viene habilitado por defecto en un teléfono ANDROID, sino que es necesario instalar un antivirus para evitar cualquier intrusión de software malicioso que robe nuestra información.

Herrero, (2022). En su investigación tuvo como objetico “Determinar como la dependencia de los teléfonos celulares aumenta el riesgo de ser víctima de los delitos cibernéticos”. Para este estudio se ha empleado datos de la Encuesta Nacional de Ciberseguridad y Confianza en las familias españolas(CCSHNS) realizada por el the National Observatory of elecommunications and the Information Societydesde enero a junio del año 2017 en España, tomando como base a 716 personas de 18 a 75 años; determinándose que el 41 % de los participantes tiene una alta probabilidad de ser víctimas fraude electrónico, mientras que el 11% tienen poca probabilidad de ser víctima de este ciber delito**.** Estos resultados nos permiten confirmar que la adicción al uso de teléfonos celulares afecta negativamente a las personas.

Sanchez et al., (2022). En su investigación tuvo como objetivo “Determinar como el delito de ciberbullying afecta a alumnos de secundaria”. Se realizo una investigación cuantitativa,

de tipo descriptivo; La ciudadanía analizada comprendió a 643 alumnos entre 11 y 19 años de varios colegios de la ciudad de Campeche, México, se aplicó el instrumento de cuestionario de 37 preguntas, donde se pudo identificar que el 59.3% usan teléfono celular, 35.8% usan Laptop, el 35.8% usan Tablet y el 35.1% usan computadora personal para realizar sus estudios. De ello se determinó que el 18% fue asediado en alguna página de internet y el 7.8% afirmo ser agresor en las últimas semanas. Concluyéndose que el ciberbullying afectó alrededor de 1 de cada 5 alumnos de secundaria al menos en alguna ocasión.

De La Cruz, (2017). En su tesis de maestría, estudio el tema sobre "Establecer el grado de conocimiento en informática forense de los Policías de la DIRINCRI (Dirección Nacional de Comunicación y Criminalística) – sede Huaraz/Perú con teléfonos celulares y otros equipos". Se empleo el tipo de investigación aplicada, descriptivo con diseño no experimental transversal, realizándose una encuesta a 45 policías, siendo esta información procesada por el software SPSS v19. Teniendo como resultado que el conocimiento de la informática forense es malo en un 40.0%, 24.4% regular, 24% bueno y el 11.1 pésimo. Concluyéndose que el nivel de conocimiento de los Policías en manejo de evidencia digital no pasa del 20%.

Blossiers, (2018). Su tesis, tuvo como objetivo "Establecer como el ciber delito repercute en los bancos del Perú". Se realizó un estudio de nivel descriptivo con enfoque cuantitativo y diseño fundamental, tomando como fuente la encuesta a 20 jueces penales y 20 fiscales penales de la Corte Superior de Justicia de Lima. teniendo como resultado que el 88% de encuestados cree que los delitos informáticos impactan de gran manera en las entidades bancarias y el 12% no cree que los delitos informáticos impacten en las entidades bancarias;

Además el 68% considera que los delitos informáticos repercuten económicamente en las entidades bancarias y el 32% no cree que haya un impacto económico. Concluyendo que los crímenes cibernéticos producen cambios negativos en las instituciones de por lo menos el 88%.

Herrera (2018). En su investigación, resaltó la importancia de "Determinar la eficiencia de la ley de delitos informáticos en la corte superior de justicia de Huánuco 2017". Se empleó la metodología aplicada, basada en la metodología cuantitativa de tipo descriptiva; tomando como base el análisis a 15 jueces y 15 fiscales, utilizando un cuestionario y fichas textuales empleando el programa IBM SPSS STATISTICS 23. Encontrándose que el 33% de encuestados respondieron que eran muy benignas las penas de delitos informáticos y un 26, 67% dijeron que no eran muy benignas; además 66, 67% afirmaron que no hay ninguna rapidez, por otro lado, el 33, 33% afirmo que si hay rapidez en resolver estos casos. Llegándose al desenlace que la ley de delitos informáticos que se administra en la corte superior de justicia de Huánuco posee un grado bajo de eficiencia, dado a que los fiscales y jueces no poseen formación sobre este tema, motivo por el cual no emiten sanciones sobre delitos informáticos.

Ayma (2020). En su tesis de maestría, tiene como objetivo "Investigar cómo se analizan los crímenes cibernéticos en la fiscalía de Lima Norte – 2019". El método investigación fue hipotético deductivo, teniendo una muestra de 100 personas entre fiscales, abogados y jueces, se emplearon encuestas y cuestionarios para la recolección de datos procesándolo con el programa estadístico SPSS 22. Teniendo estos resultados: i) a la pregunta el Ministerio Público defiende la legalidad ante conductas de ciber delitos, el 33% de entrevistados dijeron que la defiende, el 15% nunca la defiende, el 12% rara vez, el 20%

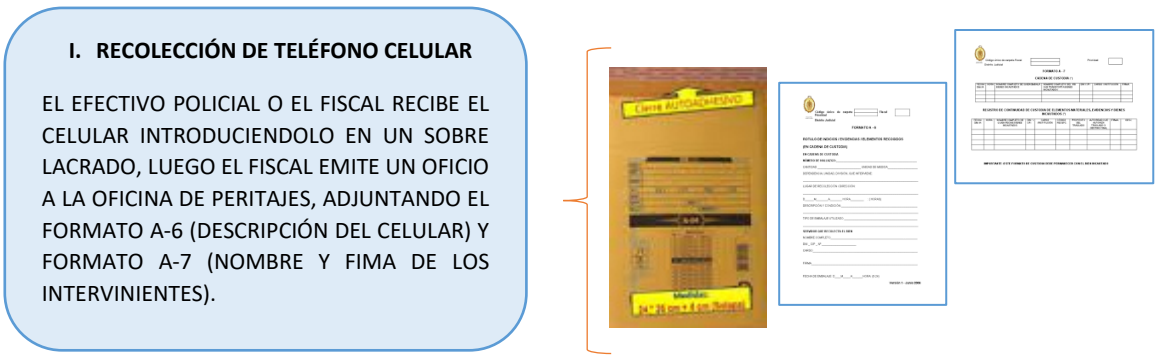
manifestaron en ocasiones, mientras que el 28% dijeron frecuentemente y el 25% informaron que habitualmente. Concluyendo que los delitos informáticos en especial sobre ciberdelincuencia se relacionan con las declaraciones realizadas y los lapsos de tiempos fijados en la etapa de investigación preliminar de la fiscalía de Lima.

2.2. BASES TEÓRICAS

Se relacionan con el Peritaje Informático Forense, que comienza con la identificación de una evidencia digital donde interviene un efectivo policial y/o fiscal en una escena de un hecho o con cuando el fiscal recibe un teléfono celular de un colaborador (testigo). Posteriormente la autoridad jurisdiccional envía un oficio a la Oficina de Peritajes del Ministerio Público, conteniendo el teléfono celular, junto con el acta de lacrado y el formato de cadena de custodia, siendo derivado a un Perito Informático del área de ADF, el cual realiza la adquisición y búsqueda de información relevante según objeto de estudio plasmándolo en un Informe Pericial enmarcado en el artículo 178 “Contenido del informe pericial oficial”.

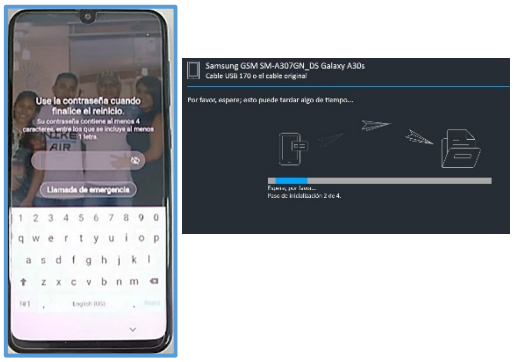
Gráfico 1

Fases de las operaciones periciales en teléfonos celulares en la Oficina de Peritajes.



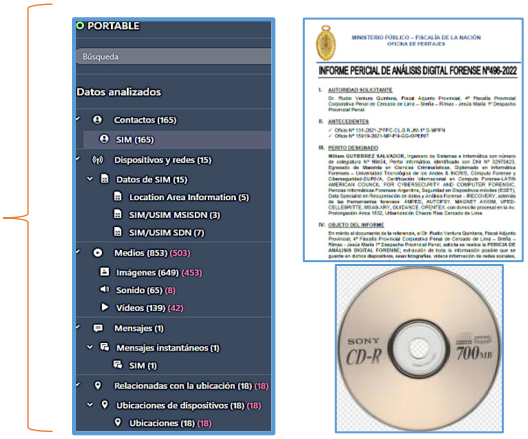
II.EXTRACCÍON DE INFORMACIÓN DE TELÉFONO CELULAR

- EL PERITO DESIGNADO APERTURA DEL SOBRE LACRADO, LUEGO PERENNIZA EL CELULAR (TOMAS FOTOGRÁFICAS)
- VERIFICAR LAS CARACTERISTICAS DEL CELULAR Y CARGAR LA BATERIA MINIMO AL 50 %
- EXTRAER INFORMACIÓN DEL CEULAR CON EL SOFTWARE FORENSE



III.ANÁLISIS DE INFORMACIÓN Y ELABORACIÓN DE INFORME PERICIAL

- BUSCA INFORMACIÓN DE UN HECHO DELICTIVO
- ETIQUETA LOS ELEMENTOS DE INTERES.
- REALIZA CAPTURAS DE PANTALLA DE LAS EVIDENCIAS ENCONTRADAS
- GENERA UN REPORTE DIGITAL COPIANDOLO EN UN DISPOSITIVO DE ALMACENAMIENTO (DVD o PENDRIVE
- EMITE UN IMPRESIÓN DEL INFORME PERICIAL



De la figura 1, para realizar el análisis pericial de un teléfono celular, se empleó la metodología de tratamiento de evidencia digital, la cual indica, las fases de: identificación, preservación, análisis e interpretación de resultados y elaboración de informe pericial, donde se emplea hardware y software forense reconocidos mundialmente como UFED 4PC, XRY y MAGNET AXIOM.

2.2.1 LA EXTRACCIÓN DE INFORMACIÓN PARA LA IDENTIFICACIÓN DE EVIDENCIA DIGITAL

Según la publicación del 30 de enero del 2020 en el blog (wearesocial.com, s.f.). En el mundo existen más de 5.19 billones de celulares, sobrepasando grandemente lo que se tenía el año pasado de 124 millones, siendo este uno de los medios más populares utilizado por los delincuentes para cometer crímenes cibernéticos causando un daño social y económico a personas naturales y empresa. La variedad de marcas y modelos de teléfonos celulares está creando la necesidad de una plataforma forense más consolidada que pueda adquirir de varias fuentes diferentes y analizar los datos en una carpeta fiscal.

1. **METODOLOGIA PARA ANÁLISIS DEL TELÉFONO CELULAR**

   Los teléfonos celulares son usados para comunicarse con familiares y amigos, escuchar música, ver videos, revisar las noticias, hacer transacciones comerciales y otros (Aoki and Downes, 2003); Pero también son usados por criminales para concertar hechos delictivos como rabo extorsión, pornografía infantil o similares. En este contexto es importante tener claro que existen primordialmente 4 fases para el análisis forense del teléfono celular, siendo estas: evaluar, adquirir, analizar y elaborar el informe.

   Así mismo, la ISO 27037:2012; guidelines for identification, collection, acquisition, and preservation of digital evidence (ISO, 2012). Define lo siguiente:

   - Identificación. Involucra el reconocimiento y documentación de evidencia digital; se pone énfasis en la consideración del orden de volatilidad de manera que se proteja la evidencia.

- Recopilación de evidencia. Consiste en remover la evidencia de su origen a laboratorio o sitio seguro. Es importante considerar si el equipo se encuentra encendido o apagado, de manera que se tomen en consideración las actividades a ser ejecutadas y las herramientas a ser usadas.
- Adquisición. Es realizar una imagen (copia) de los dispositivos que mantienen evidencia digital, se establecen las actividades y herramientas de manera que el proceso sea lo menos intrusivo y finalmente se debe mantener la documentación completa.
- Preservación. Involucra la salvaguarda de la potencial evidencia digital, la preservación debe mantenerse durante todo el proceso. Uno de los componentes claves dentro del proceso es la cadena de custodia la cual inicia las actividades de adquisición y/o recopilación.

El proceso de adquisición de evidencias informáticas debe ser legalmente aceptable, basado en métodos científicos para recolectarlos, analizarlos y validarlos, empleando a la Informática Forense (Figueroa et al., 2018).

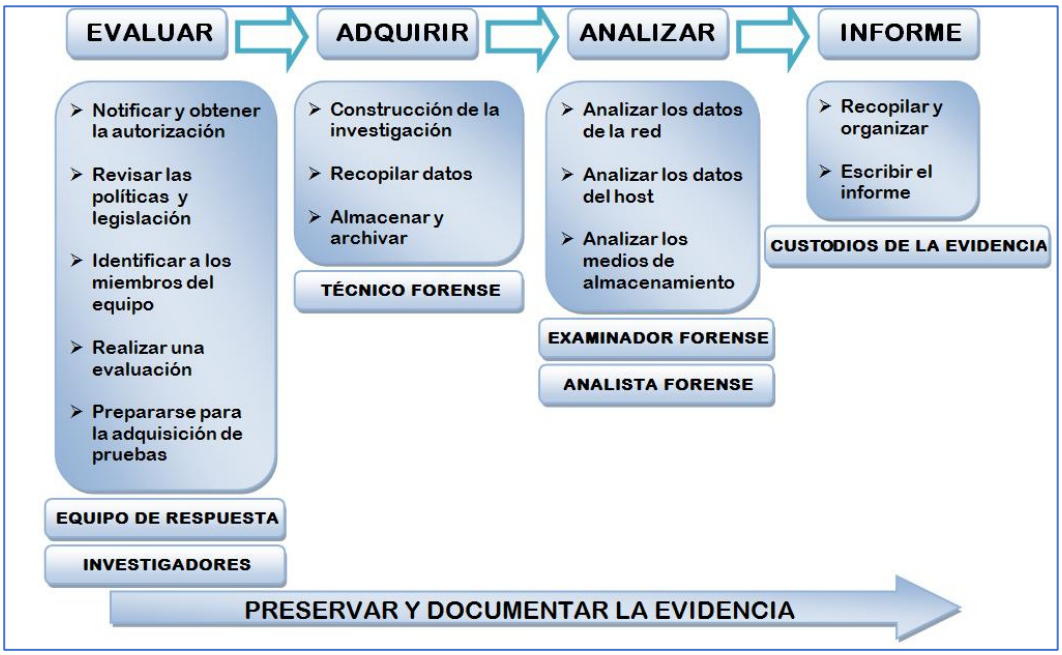
La extracción de información se justifica en sucesos que tiene que ver con delitos contra el patrimonio, informáticos y otros; siendo el fiscal, el encargado de buscar algún indicio almacenado en algún equipo electrónico como un teléfono celular. Es fundamental mencionar que se debe mantener de manera intacta el teléfono celular recepcionando, debiendo estar debidamente lacrado y junto con su formato de cadena de custodia.

Uno de los métodos más empleados en la informática forense, sin tener en cuenta el teléfono celular o sistema operativo, es la que formula Warren G. Kruse II y Jay

G. Heiser, en su apartado “Informática forense: incidente Fundamentos de respuesta”, en el que menciona que un especialista informático forense digital debe saber todos los ciclos del siguiente diagrama en orden lógico.

Gráfico 2

Fases de la informática Forense



Fuente: Kruse II y Heiser, 2007

Es importante que el teléfono celular llegue al Perito informático en buen estado para obtener una adquisición exitosa empleando softwares forenses que permitan extraer la mayor cantidad de información incluyendo elementos eliminados, así como lo hacen en otros laboratorios forenses.

Además de las fases de copia forense y adquisición de teléfonos celulares, es imprescindible perennizar mediante tomas fotográficas y/o grabación de video las características físicas y lógicas del teléfono celular, tarjetas SIMCARD y

memorias MicroSD, describiendo el estado del teléfono, por ejemplo, si estuviera trizado (pantalla rota), con bloqueo de seguridad (PIN, PATRÓN, HUELLA DIGITAL) dañado física o lógicamente para evitar cualquier cuestionamiento de describir información incorrecta que pueda perjudicar al perito en la declaración de un juicio.

Por su parte, la ISO/IEC 27042, provee guías en el análisis y la interpretación de la evidencia digital, de forma que se logre garantizar o abordar cuestiones de continuidad, validez, reproductibilidad y repetitividad (Arévalo Ascanio et al., 2015; Y. Medina- Cárdenas et al., 2019).

2. IDENTIFICACÓN DEL TELÉFONO CELULAR

El término evidencia digital de acuerdo con la ISO/IEC 27037 (2012), se conoce como "información o datos, almacenados o transmitidos de forma binaria que pueden ser tomados en cuenta como evidencia o prueba."

Otra definición que tiene, es que está constituida por los datos e información que se almacena, trasmite o recibe en un dispositivo informático que tiene valor probatorio en el marco de una investigación judicial cuando las circunstancias de un acontecimiento permitan sospechar de la comisión de un delito. En este sentido las investigaciones criminales a menudo se basan en **evidencia digital que reside en teléfonos bloqueados y desbloqueados,** estableciendo y manteniendo un correcto empleo de la cadena de custodia.

La informática forense, también, cuenta con varias definiciones como Peritaje informático, análisis digital forense (ADF), computo forense y otros similares. El

NIST (NIST (National Institute of Standards and Technology) (Kent et al., 2006), define como la aplicación de las fases de identificación, recolección, análisis e interpretación de resultados, preservando en todo momento no contaminar la evidencia digital, es decir conservando su integridad; así mismo (Ochoa Arévalo, 2018) indica que se debe mantener un correcto procedimiento de cadena de custodia evitando su manipulación indebida.

Por su parte, la ISO/IEC 27042, Proporciona orientación sobre el análisis y la interpretación de la evidencia digital, de forma que se asegure garantizar o resolver problemas de continuidad, validez, reproductibilidad y repetitividad (Arévalo Ascanio et al., 2015; Y. Medina- Cárdenas et al., 2019).

Otro concepto es que la evidencia digital, puede ser sujeto a manipulación o eliminación permanente, por lo que es necesario que este objeto sea resguardado y analizado por un profesional experto en Peritaje Informático. Para que esta no sea objeto de desestimación ante un proceso legal. Cuando se recibe un teléfono celular, se identifica la marca y modelo, pudiendo tener estos estados:

- Teléfono celular operativo

  Se dice que está en buen estado de conservación, porque no tiene daño físico o daño lógico, clasificándose a su vez, en:

  - Teléfono celular bloqueado con mecanismo de seguridad

    Presenta pantalla de bloqueo por PIN, PATRON, HUELLA Digital, IRIS u otro.

  - Teléfono celular desbloqueado

No presenta ninguna pantalla de bloqueo, es decir no tiene mecanismo de seguridad.

Gráfico 3

Teléfono celular bloqueado por PIN y teléfono desbloqueado

- Teléfono celular dañado

  Es un equipo que tiene daño físico (pantalla rota, golpes pequeños o pronunciados) o daño lógico (reinicio del teléfono o se queda con la pantalla congelada)

Gráfico 4

Teléfono celular con pantalla trizada (rota) y teléfono con el logotipo congelado

Cadena de custodia: Es el proceso de buscar y asegurar la integridad de la evidencia digital a través de la documentación detallada de la interacción y el proceso al que se somete. (Ferro Veiga, 2015).

Ciberdelincuencia: Es uno de los inconvenientes del uso de Internet. Así como existen diferentes tipos de delincuencia tradicional, existen diferentes formas de ciberdelincuencia. Hay tres categorías principales de delitos contra las personas, la propiedad y el gobierno. Dentro de estas categorías existen múltiples vectores de ataque (Ferro Veiga, 2015).

Evidencia digital: Es un registro digital almacenado en un dispositivo informático o que se transmite a través de una red informática que puede tener un valor probatorio en un juicio. (Cano Martínez, 2015).

3. SELECCIÓN DEL SOFTWARE FORENSE

De los softwares que cuenta la oficina de Peritajes del Ministerio Público, se mencionan a: UFED 4PC, XRY y MAGNET AXIOM.

MAGNET AXIOM: Software de análisis de teléfonos celulares, equipos de cómputo y datos en la nube; permite extraer información de contactos, registros de llamadas, mensajes de texto, multimedia, redes sociales, audio, video e imágenes.

XRY: Software que permite eludir el sistema operativo para volcar todo el sistema y los datos eliminados del celular, además de que también le permite superar los desafíos de seguridad y cifrado en dispositivos bloqueados.

UFED 4PC: Software de análisis forense de teléfonos celulares bloqueados y desbloqueados de gama media y media alta, además de memorias SD, Pendrive, discos duros externos y Tarjetas SIMCARD (Chip telefónico), pudiendo extraer información incluido elementos eliminados, además viene con los programas UFED Physical Analayzer y UFED Reader.

CELLEBRITE PREMIUM: Software de desbloqueo y adquisición de teléfonos celulares de gama alta tipo ANDROID e IOS.

4. MÉTODOS DE ADQUISICIÓN DE TELÉFONOS CELULARES

Hay situaciones en que los programas forenses no pueden extraer toda la información de algunos teléfonos celulares, debido a que el sistema de seguridad es muy fuerte logrando extraer información parcial, no extraer nada o extraer información errónea; por esta razón es imperativo verificar la información extraída con los datos que aparecen en el teléfono celular. En vista de ellos los analistas forenses deben notificar estas ocurrencias anómalas a los fabricantes. [Ayers et al., 2009].

La adquisición de teléfonos celulares es una técnica especializada, y no se asemeja a la recuperación de información de computadoras con Windows MAC0S (APPLE) o Linux. Los teléfonos celulares no comparten todos el mismo sistema operativo o componentes. Muchos son teléfonos propietarios integrados con configuraciones únicas ¿Que implica esto en términos de adquisición de teléfonos celulares? Simplemente, que es muy difícil de realizar.

A continuación, se describen los tipos de adquisición que se pueden realizar a un teléfono celular.

- Adquisición física

  Es la adquisición más completa, inclusiva y forénsicamente correcta. Emplea métodos avanzados para extraer una imagen física bit a bit de la memoria flash de un dispositivo móvil, incluyendo el espacio sin asignar. Se capturan los siguientes datos: usuario, ubicación, sistema de archivos, sistema oculto y archivos eliminados (espacio sin asignar). Es posible que el espacio sin asignar contenga elementos eliminados como SMS, registros de llamadas, entradas de contactos, imágenes y vídeos.

- Adquisición Full File System

  Realiza una adquisición física del archivo, cuando el dispositivo está en modo de gestor de arranque. Con este método de extracción, el sistema operativo se ejecuta. Elude cualquier bloqueo del usuario y es forénsicamente seguro.

- Adquisición Android genérico

  Se divide en 2 técnicas:

  - Extrae la contraseña o código/PIN de usuario que bloquea el dispositivo. La contraseña extraída se puede mostrar en la pantalla o se puede escribir en un lápiz de memoria USB o en un PC para archivarla. La posibilidad de extraer contraseñas depende del fabricante y modelo del dispositivo, el tipo de contraseña habilitada en el dispositivo y la longitud de la contraseña.
  - Deshabilite el bloqueo de usuario (o la contraseña), lo que significa que el dispositivo ya no estará bloqueado. Cada modelo de dispositivo tiene un

proceso ligeramente distinto, dependiendo de la combinación de bloqueo del dispositivo y del modo en que el modelo se conecta con el software.

- Adquisición BFE (Parcial)

  Es la técnica de adquisición de información parcial; es decir solamente de cuentas de usuario y archivos multimedia, no extraer contactos, registros de llamadas, mensajes de texto, de correo electrónico o mensajes de aplicaciones de redes sociales.

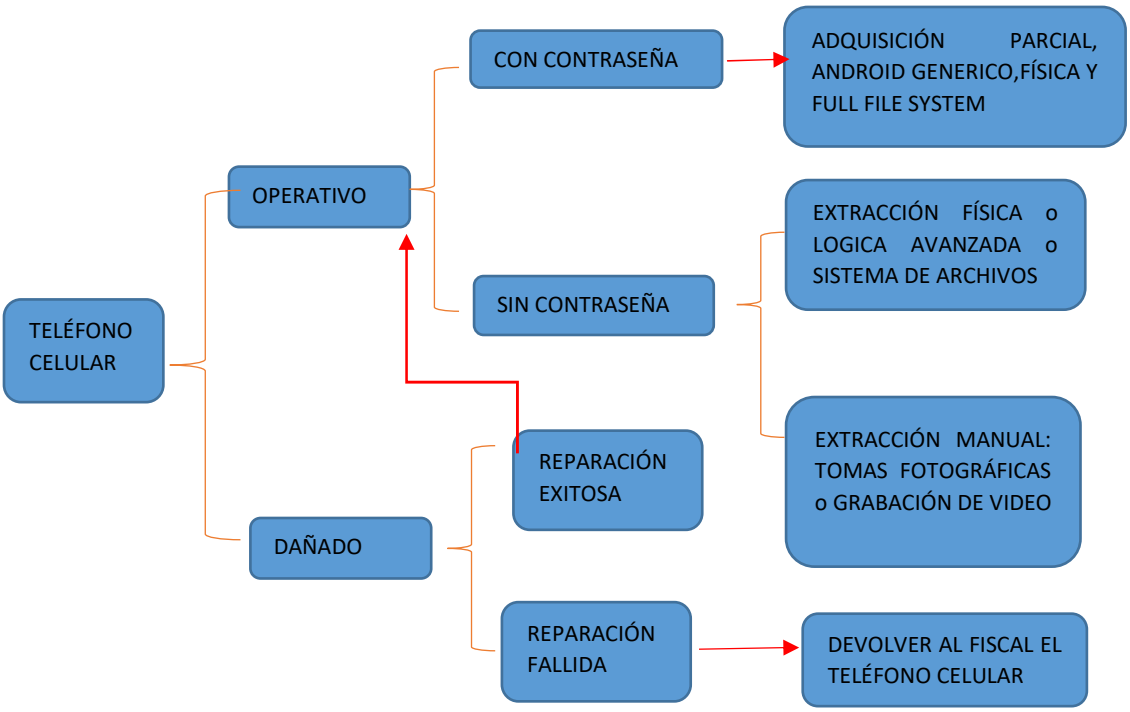
4. LA EXTRACCIÓN O COPIA FORENSE

Hay que definir primeramente lo que significa *visualizar la información contenida en teléfonos celulares*, que es básicamente, manipular un teléfono celular y navegar por las diferentes categorías de contactos, registros de llamadas, mensajes, audio, video e imágenes conociendo la contraseña de acceso para anotar lo relevante en un papel, tomando fotografías o grabaciones en video.

En cambio, *la extracción de información en teléfonos celulares* se enfoca a perennizar, extraer, examinar y presentar la información que se considere relevante según objeto de estudio requerido mediante un oficio fiscal policial o judicial. La cual es realizada por un Perito informático empleando herramientas informáticas forenses.

Gráfico 5

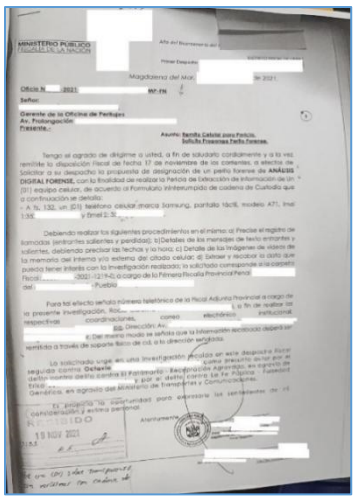
Estado del teléfono y tipo de adquisición en la Oficina de Peritajes



Una vez se tenga el teléfono celular y el Oficio fiscal, ser verificará si este presenta o no algún mecanismo de seguridad (PATRON ó PIN); debiendo elegir el software forense adecuado y el tipo de adquisición a realizar.

Gráfico 6

Oficio fiscal, con el objeto buscar información de delito de contra el patrimonio



Seguidamente se realiza la Perennización (tomas fotográficas y descripción) del teléfono celular, tal como se aprecia en estas imágenes.

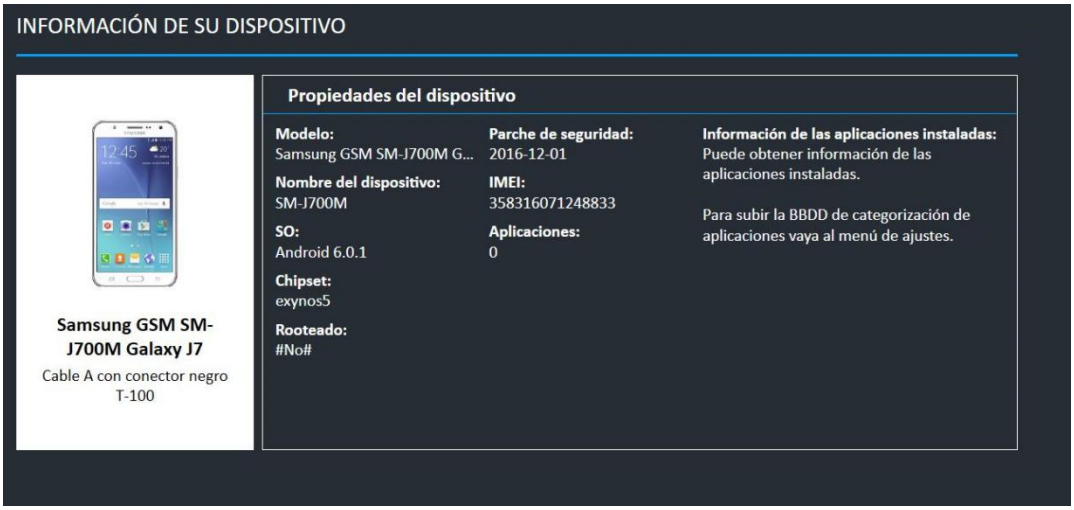
Gráfico 7

Vista frontal y posterior del celular LG y accesorios (tarjeta SIMCARD y memoria MicrosSD)

Luego se conecta el teléfono celular junto con la memoria MicroSD y Chip a la computadora donde se tiene instalado el software forense UFED 4PC y se elige la adquisición física, tal como se aprecia en la siguiente imagen.

Gráfico 8

Captura de pantalla software UFED 4PC, identificando un celular



2.2.2 HECHOS DELICTIVOS

Un delito es un comportamiento que, ya sea por propia voluntad o por imprudencia, resulta contrario a lo establecido por la ley. El delito, por lo tanto, implica una violación de las normas vigentes, lo que hace que merezca un castigo o pena. También lo podemos definir como el acto u hecho, ya sea voluntario o involuntario, que viola una norma o ley.

Tomando como referencia el "Convenio de Ciberdelincuencia del Consejo de Europa", podemos definir los delitos informáticos como: "los actos dirigidos contra

la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos".

2.2.2.1. CONTRA LA INDEMNIDAD SEXUAL

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

2.2.2.2 CONTRA EL PATRIMONIO

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

2.2.2.3 HOMICIDIO

Comete el delito de homicidio, aquel que por voluntad propia o actuando bajo negligencia produce la muerte de otro individuo. Es una conducta reprochable, es decir típica, antijurídica y por regla general culpable, que consiste en atentar contra el bien jurídico de la vida de una persona física.

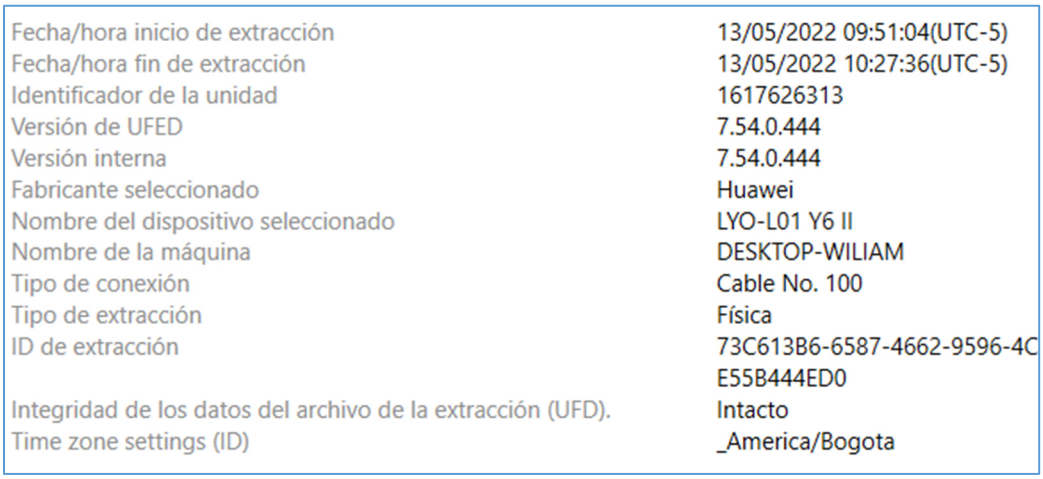
2.2.2.4 TRÁFICO ILÍCITO DE DROGAS

Consiste en fomentar, alentar o facilitar el uso ilegal de una droga a través de su fabricación o comercio, o tener tal sustancia para su comercialización.

Ahora bien, siguiendo la secuencia del ejemplo anterior; una vez obtenido el teléfono celular, se procedió r a realizar la extracción empleando el software forense y el tipo de adquisición, en este caso el programa UFED 4PC, el cual muestra este resumen.

Gráfico 9

Captura de pantalla de Adquisición física con software UFED



Fecha/hora inicio de extracción	13/05/2022 09:51:04(UTC-5)
Fecha/hora fin de extracción	13/05/2022 10:27:36(UTC-5)
Identificador de la unidad	1617626313
Versión de UFED	7.54.0.444
Versión interna	7.54.0.444
Fabricante seleccionado	Huawei
Nombre del dispositivo seleccionado	LYO-L01 Y6 II
Nombre de la máquina	DESKTOP-WILIAM
Tipo de conexión	Cable No. 100
Tipo de extracción	Física
ID de extracción	73C613B6-6587-4662-9596-4C E55B444ED0
Integridad de los datos del archivo de la extracción (UFD).	Intacto
Time zone settings (ID)	_America/Bogota

Fuente: Reporte de software UFED 4PC

Informe Pericial: Consiste en una exposición detallada del análisis efectuado. Deberá describir en profundidad lo siguiente: autoridad solicitante, nombre del Perito, nombre del oficio, objeto de la pericia, descripción de la evidencia (marca, modelo, diseño y otros datos), análisis la evidencia, metodología, fundamento técnico, conclusión y anexos (Delgado, 2007).

2.3. FORMULACIÓN DE HIPÓTESIS

2.3.1. Hipótesis general

Hi: La extracción de información de teléfonos celulares se relaciona en hechos delictivos en la OPERIT del Ministerio Público del año 2020

Ho: La extracción de información de teléfonos celulares no se relaciona en hechos delictivos en la OPERIT del Ministerio Público del año 2020.

2.3.2. Hipótesis específicas

2.3.2.1 Existe correspondencia entre la extracción de información de teléfonos celulares con la marca y modelo en los hechos delictivos en la OPERIT del Ministerio Público.

2.3.2.2 Existe relación entre la extracción de información de teléfonos celulares con el software forense en los hechos delictivos en la OPERIT del Ministerio Público.

2.3.2.3 Existe relación entre la extracción de información de teléfonos celulares con la adquisición en los hechos delictivos en la OPERIT del Ministerio Público.

2.3.2.4 Existe relación entre la extracción de información de teléfonos celulares con la evidencia digital en los hechos delictivos en la OPERIT del Ministerio Público.

CAPÍTULO III: METODOLOGÍA

3.1. MÉTODO DE LA INVESTIGACIÓN

Se empleará el método deductivo, debido a que se sustenta en el razonamiento deductivo que inicia con la teoría para someter a prueba la hipótesis que define si existe relación entre la extracción de información de teléfono celular con los hechos delictivos, sustentado en: Hernández (2014) indica que el enfoque cuantitativo de investigación "Esta aproximación se vale de la lógica o razonamiento deductivo, que comienza con la teoría, y de ésta se derivan expresiones lógicas denominadas "hipótesis" que el investigador somete a prueba."

3.2. ENFOQUE DE LA INVESTIGACIÓN

El enfoque de la presente investigación será cuantitativo, debido a que, del problema concreto, se revisó los antecedentes, los tipos de adquisición, se recolecto datos específicos y se analizó estadísticamente, para interpretar y explicar los resultados basados en los conocimientos existentes, basado en: Creswell (2013) citado por Hernández (2014) "Los análisis cuantitativos se interpretan a la luz de las predicciones iniciales (hipótesis) y de estudios previos (teoría). La interpretación constituye una explicación de cómo los resultados encajan en el conocimiento existente".

3.3. TIPO DE INVESTIGACIÓN

El tipo de investigación será tipo básica, por que busca determinar el impacto de la información extraída de teléfonos celulares y como esta incide en el esclarecimiento de hechos delictivos, que se sustenta en: Creswell (2013) citado por Hernández (2014) donde indica "3)

determinar el impacto de una o más causas (que más adelante denominaremos variables independientes) sobre una o más consecuencias (variables dependientes)".

Según la planificación de la toma de datos será de tipo retrospectivo, debido a que los datos de estudio son recogidos a propósito para la investigación y corresponde al tipo de información extraída en los teléfonos celulares en el año 2020. León y Montero (2003) citado por Hernández (2014) que indica que se conoce como diseño retrospectivo cuando "se reconstruyen las relaciones a partir de las variables dependientes"

3.4. DISEÑO DE LA INVESTIGACIÓN

Será no experimental porque se analiza los datos de la información recolectada en teléfonos celulares, registros de llamadas, mensajes de texto, conversaciones, archivos de audio, video e imágenes y otros, que se sustenta en: The SAGE Glossary of the Social and Behavioral Sciences (2009), citado por Hernández (2014), se detalla que la investigación no experimental podría definirse como la investigación que se realiza sin manipular deliberadamente variables. Es decir, se trata de estudios en los que no hacemos variar en forma intencional las variables independientes para ver su efecto sobre otras variables. Lo que hacemos en la investigación no experimental es observar fenómenos tal como se dan en su contexto natural, para analizarlos.

3.5. POBLACIÓN, MUESTRA Y MUESTREO

3.5.1. Población

El universo o población corresponderá a 400 teléfonos celulares cuyo objeto pericial será encontrar evidencia digital respecto a mensajes de texto, mensajes de multimedia, ficheros tipo video, sonido, imágenes, registros telefónicos y otros que fueron solicitadas

al departamento de ADF de la oficina de peritajes del Ministerio Público en el año 2020 en la ciudad de Lima – Perú, siendo la población finita y la variable principal de estudio es de tipo cuantitativo.

3.5.2. Muestra

Según Sánchez y Reyes (2006), precisa que: el muestreo por conveniencia se caracteriza por un esfuerzo deliberado con la finalidad de obtener una muestra representativa de la población de estudio, teniendo en cuenta que este procedimiento no utiliza fórmulas para obtener el tamaño muestral. En este sentido, se aplicará el muestreo no probabilístico por conveniencia de 80 extracciones de teléfonos celulares.

Criterios de Inclusión:

- Teléfonos celulares bloqueados con patrón, contraseña o Pin.
- Delito: contra el patrimonio, tráfico ilícito de drogas, contra la indemnidad sexual y Homicidio.
- Reos en cárcel.

Criterios de Exclusión: se elegirán los teléfonos de tipo

- Celulares con daño físico.
- Celulares con sistema Operativo Symbian, BlackBerry, Windows Fone.
- Celulares tipo iPhone.

3.6 VARIABLES Y OPERACIONALIZACIÓN

Matriz de operacionalización de variables

Variables	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de Medición	Escala valorativa
Extracción de Información de Teléfono celular	Un teléfono celular contiene información de contactos, mensajes de texto, audios, imágenes, videos y otros que pueden llegar a ser una evidencia digital. (Ho & Li, 2015) Detalla el estándar ISO/IEC 27037:2012 donde se proporciona las pautas para el tratamiento de pruebas electrónicas.	El teléfono celular debe ser reconocido como elemento material en la identificación de evidencia digital	Teléfono celular	- Marca - Modelo - Chipset - IMEI - Serie - Versión Sistema Operativo - Actualización de seguridad de Android - Kernel	Cualitativo nominal	- ZTE V10 - Xiaomi Redmi 4 - Motorola E6 - Motorola G7 - LG G7 - LG K40 - Huawei Y9 - Huawei P20 - Samsung J7 - Samsung A03 - Samsung A21 - Samsung A71
			Software	- Programa de extracción de teléfono celular		- Cellebrite Premium 7.16 - Ufed 4PC 7.38 - XRY 8.2.2. - Magnet Axiom 4.10
			Adquisición	- Tipo de adquisición		- Parcial - Android Genérico - Física - Full File System

Hechos delictivos	Es una serie de conductas que desembocan en actos ilegales. Como, por ejemplo: Delito contra el patrimonio, tráfico ilícito de drogas, pornografía infantil, homicidio; entre otros. En Perú, los delitos se encuentran regulados en el 2° libro (Parte Especial - Delitos) del Código Penal.	Se buscará información relacionada a algún hecho delictivo	Evidencia digital (Registro o archivo digital)	- Registros de llamadas - Contactos - Mensajes de texto - Conversaciones - Archivo audio - Archivo video - Archivo imagen - Cuenta de usuario - Documentos - Geolocalización	Cualitativa nominal	- Delito contra el patrimonio - Delito de tráfico ilícito de drogas - Delito contra la indemnidad sexual - Delito de homicidio

3.7. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

3.7.1. Técnica

Arias (1999), sostiene que "existen diversas formas o métodos de recopilar de información". (p. 25).

Para realizar la presente investigación se empleó la técnica observacional de acuerdo con Mertens (2015) la técnica observacional es muy útil en variables que no pueden ser manipuladas ya sea por su dificultad o por cuestiones éticas.

3.7.2. Descripción

El instrumento que se aplicó fue una lista de cotejo, el mismo consiste en secuencias de acciones que realizan los investigadores para obtener información que les permita lograr un objetivo, o refutar una hipótesis cuando las circunstancias lo ameritan (Arispe Alburqueque et al., 2020).

"Los instrumentos son los medios materiales que se emplean para recoger y almacenar la información" (Arias, 1999, p. 25).

Se producirá documentación para corroborar el instrumento a través de la experiencia de los jueces validadores. Incluyendo conceptos de variables y dimensiones, matriz de operacionalización de variables; la licencia de idoneidad de la herramienta que evalúa el desempeño de la recogida de la información es la recopilación de datos del año 2020 porque servirá para establecer la correspondencia contra la criminalidad.

La recopilación de datos se analizará de la siguiente manera:

- Recopilación a posteriori: Los datos se acopian en el departamento de ADF de la OPERIT, donde se redactan informes de extracción de teléfonos celulares.

- Supervisión inmediata: El investigador empleará la extracción y búsqueda de información con el fin de identificación de evidencia digital de interés criminalístico.

- Relación: Se realizará la relación de las variables: teléfono celular y los hechos delictivos. Los teléfonos celulares se enunciarán en termino de cuantitativo de adquisición parcial, Android genérico, full file system o física.

La información extraída se cuantificará en términos de encontrar evidencia de algún hecho delictivo.

- Tiempos. Tomando en cuenta el número de informes periciales que se integrará a la muestra de estudio para la clasificación y registro de la cantidad de elementos de interés relacionado a un hecho delictivo, el tiempo de ejecución de la investigación será de seis (06) meses.

- Recursos: En relación con los recursos humanos, se tendrá la autorización del Gerente de la Oficina de Peritajes para el acceso a los informes periciales y para la supervisión al coordinador del departamento de ADF, siendo el responsable del estudio el investigador principal para el desarrollo de las coordinaciones y el desarrollo de la investigación.

3.7.3. Validación

Hernández et al (2014) señala que es el "grado en que una herramienta mide realmente la variable que pretende medir". (p. 200).

Hay que mencionar, además, según indica Hernández et al (2014) que "la validez del contenido se refiere al grado en que una herramienta refleja un dominio específico de contenido de lo que se mide". (p. 201).

La corroboración de herramientas fue supervisada por cinco especialistas que tienen especialización, maestría y/o doctorado con trayectoria en labores periciales; los cuales se detalla:

- Mg. Jessica Merino Burgos, Ingeniero de Sistemas e Informática. Perito Judicial independiente de la Corte Superior de Justicia del Santa / Chimbote.
- Dr. Milton Cesar Tullume Ch., Ingeniero Forestal, Perito en materia ambiental. Ministerio Público.
- Mg. Miguel Carrera M. Especialidad Gestión Ambiental. Ministerio Público.
- Mg. Lizbardo Orellano Benancio. Perito del departamento de Análisis Digital Forense. Ministerio Público.
- Mg. Edgar Gómez Enciso, Perito del departamento de Análisis Digital Forense. Ministerio Público.

3.7.4. Confiabilidad

Existen herramientas que no necesitan calcular la confiabilidad como: Listas de cotejo, guías de observación, registros, rubricas.

Así mismo, en los registros de extracciones de celulares, no es necesario realizar la confiabilidad, ya que su uso frecuente ha permitdo que se compruebe sus aciertos, por tanto, ya es una herramienta estandarizada (Guzmán mora, 2006).

3.8. PLAN DE PROCESAMIENTO Y ANÁLISIS DE DATOS

3.8.1. Ficha de recolección de datos

La ficha de recolección de datos permitirá recolectar la información de 80 teléfonos celulares de las pericias del departamento de ADF, registrándose los datos de cada celular en una ficha de recolección datos.

3.8.2. Vaciado de las fichas

Las 80 fichas de recolección de datos se ingresarán en una tabla en Excel de acuerdo con las variables y dimensiones para su proceso en SPSS. Los detalles para el ingreso de las fichas serán:

- Para la variable 1 (extracción de información de teléfonos celulares) con la dimensión teléfono celular y con los indicadores: marca, modelo, chipset, IMEI, serie, versión Sistema Operativo, Actualización de seguridad de Android y Kernel

- Para la variable 1 (extracción de información de teléfonos celulares) con la dimensión software y con los indicadores: Cellebrite Premium 7.16, Ufed 4PC 7.38, XRY 8.2.2, Magnet Axiom 4.10

- Para la variable 1 (extracción de información de teléfonos celulares) con la dimensión adquisición y con los indicadores: Parcial, Android Genérico, Física y Full File System

- Para la variable 2 (hechos delictivos) con la dimensión evidencia digital y con los indicadores: registros de llamadas, contactos, mensajes de texto, conversaciones, archivos de audio, video imágenes, cuentas de usuario, documentos y geolocalización; que tengan

que ven con delitos de: robo contra el patrimonio, indemnidad sexual, tráfico ilícito de drogas y homicidio.

3.8.4. Examen con el SPSS

Para este análisis se empleará el software SPSS para examinar la relación que existe entre la extracción de información de teléfonos celulares con la criminalidad.

3.9. ASPECTOS ÉTICOS

Los aspectos éticos serán muy importantes debido a los temas de confidencialidad en las labores periciales, contándose con la autorización para la recopilación de datos del Gerente de la Oficina de Peritajes, toda vez que se buscaran información relacionada de algún tipo de delito en un teléfono celular, el cual servirá para establecer el grado de culpabilidad de una persona investigada. Asimismo, la presente investigación será analizada por el software Turnitin para identificar el porcentaje de coincidencias y éstas sean por debajo de lo permitido por la Universidad.

CAPÍTULO IV: PRESENTACIÓN Y DISCUSIÓN DE RESULTADOS

4.1. Resultados

Tabla 1

Resultado de recolección de datos 2020

N°	Informe Pericial	Delito encontrado	Teléfono celular	Rango	Software Forense	Rango	Adquisición	Rango
1	2020	Robo contra el patrimonio	Samsung A03	10	UFED 4PC 7.38	4	Física	4
2	2020	Contra la indemnidad sexual	Motorola G7	4	Cellebrite Premium 7.16	3	Full File System	3
3	2020	Robo contra el patrimonio	Samsung A03	10	Cellebrite Premium 7.16	3	Física	4
4	2020	Robo contra el patrimonio	Samsung A03	10	UFED 4PC 7.38	4	Física	4
5	2020	Homicidio	Samsung J7	9	Cellebrite Premium 7.16	3	Física	4
6	2020	Tráfico ilícito de drogas	ZTE V10	1	Magnet Axiom 4.10	1	Física	4
7	2020	Robo contra el patrimonio	Samsung A03	10	UFED 4PC 7.38	4	Física	4
8	2020	Homicidio	Huawei P20	8	Cellebrite Premium 7.16	3	Física	4
9	2020	Robo contra el patrimonio	Samsung A03	10	UFED 4PC 7.38	4	Física	4
10	2020	Robo contra el patrimonio	Samsung A03	10	UFED 4PC 7.38	4	Física	4
11	2020	Homicidio	Huawei P20	8	Cellebrite Premium 7.16	3	Física	4
12	2020	Contra la indemnidad sexual	Motorola G7	4	Cellebrite Premium 7.16	3	Física	4
13	2020	Homicidio	Huawei P20	8	Cellebrite Premium 7.16	3	Física	4
14	2020	Homicidio	Huawei P20	8	Cellebrite Premium 7.16	3	Física	4
15	2020	Robo contra el patrimonio	Samsung A03	10	UFED 4PC 7.38	4	Física	4
16	2020	Robo contra el patrimonio	Samsung A03	10	UFED 4PC 7.38	4	Física	4
17	2020	Homicidio	Huawei P20	8	Cellebrite Premium 7.16	3	Física	4
18	2020	Contra la indemnidad sexual	Motorola G7	4	Cellebrite Premium 7.16	3	Física	4
19	2020	Homicidio	Huawei P20	8	Cellebrite Premium 7.16	3	Física	4
20	2020	Homicidio	Huawei Y9	7	Cellebrite Premium 7.16	3	Física	4
21	2020	Robo contra el patrimonio	Samsung A03	10	UFED 4PC 7.38	4	Física	4
22	2020	Robo contra el patrimonio	Samsung A03	10	UFED 4PC 7.38	4	Física	4

23	2020	Homicidio	Samsung J7	9	Cellebrite Premium 7.16	3	Física	4
24	2020	Homicidio	Samsung J7	9	Cellebrite Premium 7.16	3	Física	4
25	2020	Homicidio	Samsung J7	9	Cellebrite Premium 7.16	3	Física	4
26	2020	Contra la indemnidad sexual	Motorola G7	4	Cellebrite Premium 7.16	3	Física	4
27	2020	Homicidio	Samsung J7	9	Cellebrite Premium 7.16	3	Física	4
28	2020	Homicidio	Samsung J7	9	Cellebrite Premium 7.16	3	Física	4
29	2020	Contra la indemnidad sexual	Motorola G7	4	Cellebrite Premium 7.16	3	Física	4
30	2020	Homicidio	Samsung J7	9	Magnet Axiom 4.10	1	Física	4
31	2020	Robo contra el patrimonio	Samsung A21	11	UFED 4PC 7.38	4	Física	4
32	2020	Homicidio	Samsung J7	9	Cellebrite Premium 7.16	3	Física	4
33	2020	Homicidio	Samsung J7	9	Cellebrite Premium 7.16	3	Física	4
34	2020	Robo contra el patrimonio	Samsung A21	11	UFED 4PC 7.38	4	Física	4
35	2020	Robo contra el patrimonio	Samsung A21	11	UFED 4PC 7.38	4	Física	4
36	2020	Robo contra el patrimonio	Samsung A21	11	UFED 4PC 7.38	4	Física	4
37	2020	Robo contra el patrimonio	Samsung A21	11	UFED 4PC 7.38	4	Física	4
38	2020	Robo contra el patrimonio	Samsung A21	11	UFED 4PC 7.38	4	Física	4
39	2020	Robo contra el patrimonio	Samsung A21	11	UFED 4PC 7.38	4	Física	4
40	2020	Contra la indemnidad sexual	LG K40	6	Cellebrite Premium 7.16	3	Física	4
41	2020	Tráfico ilícito de drogas	Xiaomi Redmi 4	2	Magnet Axiom 4.10	1	Android Genérico	2
42	2020	Robo contra el patrimonio	Samsung A21	11	UFED 4PC 7.38	4	Física	4
43	2020	Contra la indemnidad sexual	LG G7	5	Cellebrite Premium 7.16	3	Full File System	3
44	2020	Contra la indemnidad sexual	LG G7	5	Cellebrite Premium 7.16	3	Full File System	3
45	2020	Robo contra el patrimonio	Samsung A21	11	UFED 4PC 7.38	4	Full File System	3
46	2020	Tráfico ilícito de drogas	Xiaomi Redmi 4	2	Magnet Axiom 4.10	1	Full File System	3
47	2020	Tráfico ilícito de drogas	Motorola E6	3	Magnet Axiom 4.10	1	Full File System	3
48	2020	Robo contra el patrimonio	Samsung A21	11	UFED 4PC 7.38	4	Full File System	3
49	2020	Tráfico ilícito de drogas	Motorola E6	3	Magnet Axiom 4.10	1	Full File System	3
50	2020	Tráfico ilícito de drogas	Motorola E6	3	Magnet Axiom 4.10	1	Full File System	3

51	2020	Tráfico ilícito de drogas	Huawei Y9	7	Magnet Axiom 4.10	1	Full File System	3
52	2020	Robo contra el patrimonio	Samsung A21	11	UFED 4PC 7.38	4	Full File System	3
53	2020	Robo contra el patrimonio	Huawei P20	8	UFED 4PC 7.38	4	Full File System	3
54	2020	Robo contra el patrimonio	Samsung A71	12	UFED 4PC 7.38	4	Full File System	3
55	2020	Contra la indemnidad sexual	LG G7	5	XRY 8.2.2.	2	Full File System	3
56	2020	Tráfico ilícito de drogas	Huawei Y9	7	XRY 8.2.2.	2	Full File System	3
57	2020	Robo contra el patrimonio	Samsung A71	12	UFED 4PC 7.38	4	Full File System	3
58	2020	Robo contra el patrimonio	Samsung A71	12	UFED 4PC 7.38	4	Full File System	3
59	2020	Contra la indemnidad sexual	LG G7	5	XRY 8.2.2.	2	Full File System	3
60	2020	Tráfico ilícito de drogas	Huawei Y9	7	XRY 8.2.2.	2	Full File System	3
61	2020	Robo contra el patrimonio	Samsung A71	12	UFED 4PC 7.38	4	Full File System	3
62	2020	Tráfico ilícito de drogas	Huawei Y9	7	UFED 4PC 7.38	4	Full File System	3
63	2020	Tráfico ilícito de drogas	Huawei Y9	7	XRY 8.2.2.	2	Full File System	3
64	2020	Contra la indemnidad sexual	LG G7	5	XRY 8.2.2.	2	Full File System	3
65	2020	Contra la indemnidad sexual	Huawei Y9	7	XRY 8.2.2.	2	Full File System	3
66	2020	Robo contra el patrimonio	Samsung A71	12	UFED 4PC 7.38	4	Full File System	3
67	2020	Robo contra el patrimonio	Samsung A71	12	UFED 4PC 7.38	4	Full File System	3
68	2020	Robo contra el patrimonio	Samsung A71	12	UFED 4PC 7.38	4	Full File System	3
69	2020	Robo contra el patrimonio	Samsung A71	12	UFED 4PC 7.38	4	Full File System	3
70	2020	Contra la indemnidad sexual	LG K40	6	Cellebrite Premium 7.16	3	Full File System	3
71	2020	Contra la indemnidad sexual	LG K40	6	XRY 8.2.2.	2	Full File System	3
72	2020	Tráfico ilícito de drogas	Huawei Y9	7	UFED 4PC 7.38	4	Full File System	3
73	2020	Robo contra el patrimonio	Samsung A71	12	UFED 4PC 7.38	4	Android Genérico	2
74	2020	Robo contra el patrimonio	Samsung A71	12	UFED 4PC 7.38	4	Android Genérico	2

75	2020	Robo contra el patrimonio	Samsung A71	12	UFED 4PC 7.38	4	Android Genérico	2
76	2020	Contra la indemnidad sexual	LG K40	6	XRY 8.2.2.	2	Full File System	3
77	2020	Robo contra el patrimonio	Samsung A71	12	XRY 8.2.2.	2	Android Genérico	2
78	2020	Contra la indemnidad sexual	LG K40	6	XRY 8.2.2.	2	Parcial	1
79	2020	Contra la indemnidad sexual	LG K40	6	XRY 8.2.2.	2	Parcial	1
80	2020	Robo contra el patrimonio	Samsung A71	12	Cellebrite Premium 7.16	3	Android Genérico	2

4.1.1. Análisis descriptivo de resultados

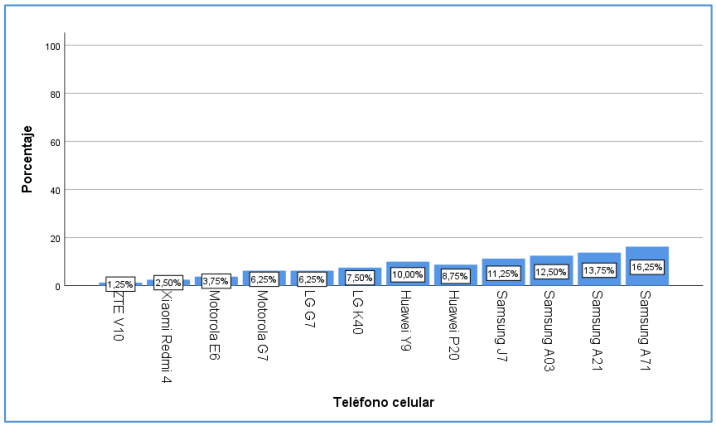
Tabla 2

Teléfonos celulares analizados en sucesos criminales

Teléfono celular	Frecuencia	Porcentaje
ZTE V10	1	1.3
Xiaomi Redmi 4	2	2.5
Motorola E6	3	3.8
Motorola G7	5	6.3
LG G7	5	6.3
LG K40	6	7.5
Huawei Y9	8	10.0
Huawei P20	7	8.8
Samsung J7	9	11.3
Samsung A03	10	12.5
Samsung A21	11	13.8
Samsung A71	13	16.3
Total	80	100.0

Gráfico 10

Teléfonos celulares analizados en sucesos criminales



En la tabla 2 y gráfico 10 se evidencia que el 16.3% de los teléfonos celulares analizados son de marca Samsung A71; el 13.8.% son de marca Samsung A21; el 12.5% son de marca Samsung A03; el 11.3% son de marca Samsung J7; el 10.0% son de marca Huawei Y9; el 8.8% son de marca Huawei P20; el 6.3% son de marca LG G7 y Motorola G7; el 7.5% son de marca LG K40; el 3.8% son de marca Motorola E6; el 2.5% son de marca Xiaomi Redmi 4; el 1.3% son de marca ZTE V10.

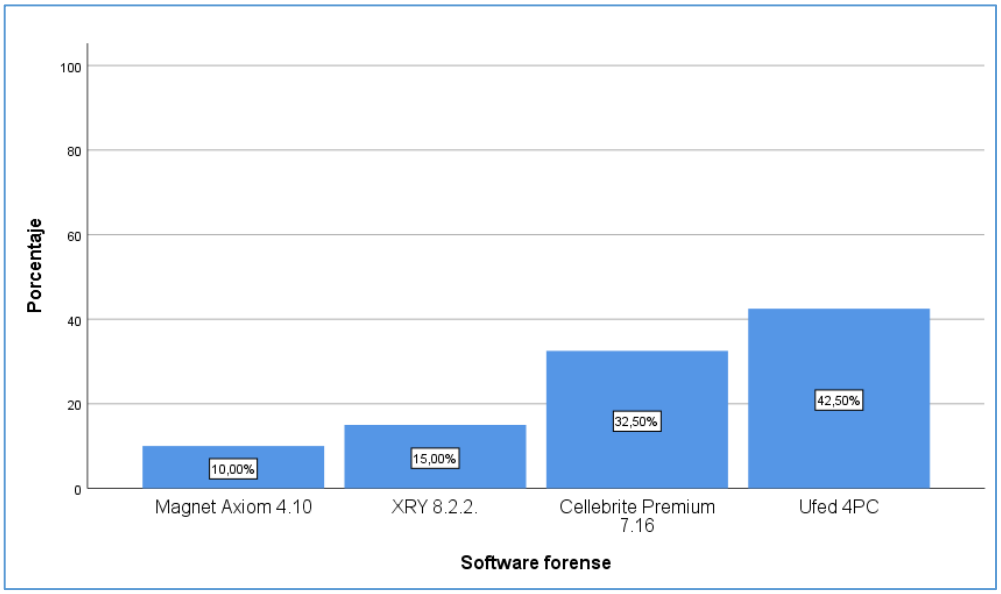
Tabla 3

Software forense empleado en la extracción de teléfono celular

Software forense	Frecuencia	Porcentaje
Magnet Axiom 4.10	8	10.0
XRY 8.2.2.	12	15.0
Cellebrite Premium 7.16	26	32.5
Ufed 4PC 7.38	34	42.5
Total	80	100.0

Gráfico 11

Software forense empleado en la extracción de teléfono celular



En la tabla 3 y figura 11 se muestra que el software más usado en la adquisición de celulares es el Ufed PC 7.38 con un 42.5%; seguido del Cellebrite Premium 7.16 con un 32.5%; en tercer lugar, está el software XRY 8.2.2 poco usado con un 15.0%; por último el software menos usado pero no el menos importante es el Magnet Axiom 4.10 con un 10.0%.

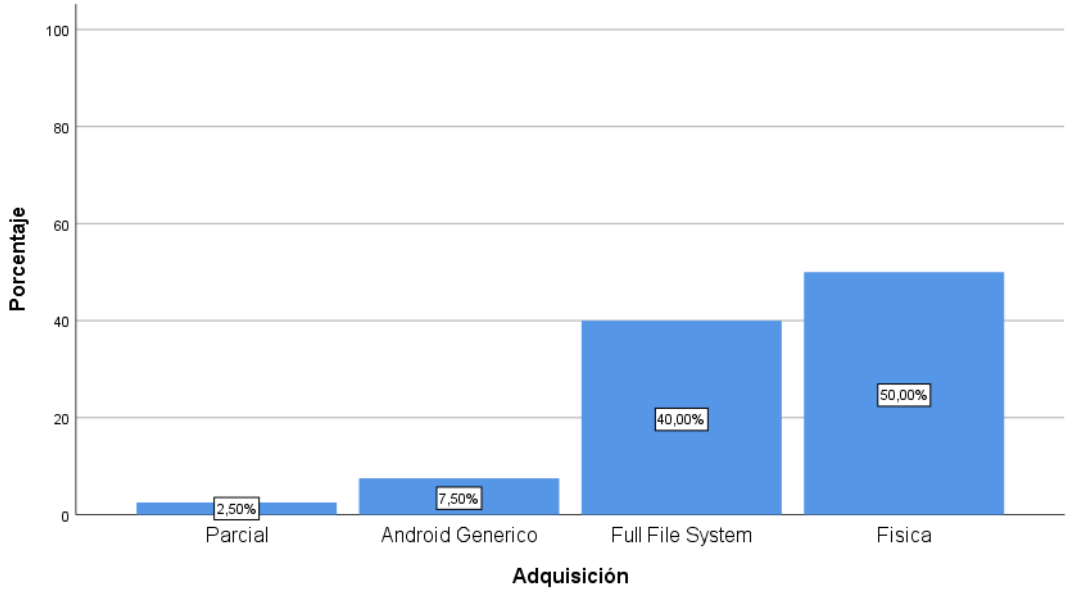
Tabla 4

Adquisición utilizada en la extracción de teléfono celular

Adquisición	Frecuencia	Porcentaje
Parcial	2	2.5
Android Generico	6	7.5
Full File System	32	40.0
Física	40	50.0
Total	80	100.0

Gráfico 12

Adquisición utilizada en la extracción de teléfono celular



En la tabla 4 y figura 12 se advierte que el 50.0% de los teléfonos celulares utilizaron la adquisición física para obtener la mayor cantidad de evidencia digital; 40.0% de los teléfonos celulares utilizaron la adquisición Full File System para obtener la mayor cantidad de evidencia digital; el 7.5% de los teléfonos celulares utilizaron la adquisición Android Genérico para obtener regular cantidad de evidencia digital; 2.5% de los teléfonos celulares utilizaron la adquisición Parcial para obtener poca cantidad de evidencia digital debido a la compleja seguridad del teléfono celular.

Tabla 5

Delitos encontrados según las dimensiones de evidencia digital

		Delito encontrado	
		Media	Desviación estándar
Teléfono celular	ZTE V10	2	
	Xiaomi Redmi 4	2	0
	Motorola E6	2	0
	Motorola G7	1	0
	LG G7	1	0
	LG K40	1	0
	Huawei Y9	2	1
	Huawei P20	4	0
	Samsung J7	4	0
	Samsung A03	3	0
	Samsung A21	3	0
	Samsung A71	3	0
Software forense	Magnet Axiom 4.10	2	1
	XRY 8.2.2.	1	1
	Cellebrite Premium 7.16	3	1
	Ufed 4PC 7.38	3	0
Adquisición	Parcial	1	0
	Android Genérico	3	0
	Full File System	2	1
	Física	3	1

En la tabla 5, se contempla un resumen de los delitos identificados según las dimensiones de la adquisición a los teléfonos celulares.

En el caso de los fabricantes de los celulares, de las marcas ZTE V10, Xiaomi Redmi 4, Motorola E6 y Huawei Y9 se encontraron en promedio 2 hechos delictivos con una desviación estándar de 0 a 1. Asimismo, en las marcas Motorola G7 y LG G7 se identificaron en promedio un (01) hecho delictivo con una desviación estándar de 0; del mismo modo en las marcas Huawei P20 y Samsung J7 se encontraron en promedio cuatro (04) hechos delictivos con una desviación estándar

de 0; por último, en las marcas Samsung A03, Samsung A21, Samsung A71 se encontraron en promedio tres (03) hechos delictivos con una desviación estándar de cero (0).

En cuanto a los softwares forenses, los más usados para extraer información de celulares fueron los programas Cellebrite Premium 7.16, Ufed 4PC 7.38 con un premio de tres (03) con una desviación estándar de 0 y 1; seguido está el software Magnet Axiom con un promedio de dos (02) y una desviación estándar de 1; y por último lugar, pero no menos importante se encontró que el software XRY con un promedio de un (01) hecho delictivo y una desviación estándar de 1

En el caso del tipo de adquisición empleado para obtener información de algún hecho delictivo, se indica que las adquisiciones física y Android Genérico fueron las más utilizadas con un promedio de 3 y una desviación estándar de 0 y 1; así mismo la adquisición Full File System también fue una de las más usadas para obtener la mayor cantidad de información de un teléfono celular con un promedio 2 y una deviación estándar de 1; por último la adquisición parcial aunque no es la que obtiene mayor cantidad de evidencia digital, también sirvió para encontrar información de interés de algún hecho delictivo.

4.1.2. Prueba de Hipótesis

Hipótesis General

- Ho: No existe relación entre la extracción de información de teléfonos celulares con los hechos delictivos en la Oficina de Peritajes del Ministerio Público, Lima, 2020

- H1: Existe relación entre la extracción de información de teléfonos celulares con los hechos delictivos en la Oficina de Peritajes del Ministerio Público, Lima, 2020

Tabla 6

Relación entre los sucesos criminales encontrados y la evidencia digital

			Delito encontrado	Evidencia digital
Rho de Spearman	Delito encontrado	Coeficiente de correlación	1.000	,992**
		Sig. (bilateral)		0.000
		N	80	80
	Evidencia digital	Coeficiente de correlación	,992**	1.000
		Sig. (bilateral)	0.000	
		N	80	80

**. La correlación es significativa en el nivel 0,01 (bilateral).

o

En la tabla 6 se destaca el análisis de correspondencia entre los hechos delictivos encontrados y la evidencia digital.

El coeficiente de vinculación Rho de Spearman es 0.992; esto muestra que la conexión es directa y su grado es muy alto, es decir, a superior cifra de evidencia digitales le pertenece alta cifra de hechos delictivos encontrados. Además, se nota que la cifra de oportunidad p= 0.000. En conclusión, se puede afirmar con un 99% de confianza que existe una relación positiva alta entre la extracción de información de teléfonos celulares con la evidencia digital con hechos delictivos en la OPERIT, 2020.

Hipótesis especifica 1

- Ho: No existe conexión entre la extracción de información de teléfonos celulares con la marca de teléfonos celulares en los hechos delictivos.

- H1: Existe conexión entre la extracción de información de teléfonos celulares con la marca de teléfonos celulares en los hechos delictivos.

Tabla 7

Relación entre los delitos encontrados con los teléfonos celulares

			Delito encontrado	Teléfono celular
Rho de Spearman	Delito encontrado	Coeficiente de correlación	1.000	,562**
		Sig. (bilateral)		0.000
		N	80	80
	Teléfono celular	Coeficiente de correlación	,562**	1.000
		Sig. (bilateral)	0.000	
		N	80	80

**. La correlación es significativa en el nivel 0,01 (bilateral).

En la tabla 7 se atiene el análisis de correspondencia entre los hechos delictivos y las marcas de los teléfonos celulares.

El coeficiente de correlación Rho de Spearman es 0.562; esto indica que la conexión es directa moderada, es decir, a mayor cantidad de hechos delictivos le corresponde mayor cantidad de marcas de teléfonos celulares. También se observa que el valor de probabilidad p= 0.000, En conclusión, se puede afirmar con un 99% de confianza que existe una relación positiva moderada entre la extracción de información de teléfonos celulares con el teléfono celular en hechos delictivos en la OPERIT, 2020.

Hipótesis especifica 2

- Ho: No existe vinculación entre la extracción de información de teléfonos celulares con los softwares forenses con los hechos delictivos.

- H1: Existe vinculación entre la extracción de información de teléfonos celulares con los softwares forenses con los hechos delictivos.

Tabla 8

Relación entre los delitos encontrados con los softwares forenses

			Delito encontrado	Software forense
Rho de Spearman	Delito encontrado	Coeficiente de correlación	1.000	,352**
		Sig. (bilateral)		0.001
		N	80	80
	Software forense	Coeficiente de correlación	,352**	1.000
		Sig. (bilateral)	0.001	
		N	80	80

**. La correlación es significativa en el nivel 0,01 (bilateral).

En la tabla 8 se atiene el análisis de correspondencia entre los hechos delictivos y los softwares forenses en los sucesos criminales.

El coeficiente de correspondencia Rho de Spearman es 0.352; esto demuestra que la relación es directa y su grado bajo, es decir, a mayor cantidad de hechos delictivos le corresponde mayor cantidad softwares forenses empleados. También se observa que el valor de probabilidad p= 0.001, En conclusión, se puede afirmar con un 99% de confianza que existe una relación positiva baja entre la extracción de información de teléfonos celulares con el software forense en hechos delictivos en la OPERIT, 2020.

Hipótesis especifica 3

- Ho: No existe vínculo entre la extracción de información de teléfonos celulares con el método de adquisición en los hechos delictivos.

- H1: Existe vínculo entre la extracción de información de teléfonos celulares con el método de adquisición en los hechos delictivos.

Tabla 9

Correspondencia entre los delitos y los métodos de Adquisición

			Delito encontrado	Adquisición
Rho de Spearman	Delito encontrado	Coeficiente de correlación	1.000	,482**
		Sig. (bilateral)		0.000
		N	80	80
	Adquisición	Coeficiente de correlación	,482**	1.000
		Sig. (bilateral)	0.000	
		N	80	80

**. La correlación es significativa en el nivel 0,01 (bilateral).

En la tabla 9 se observa el análisis de conexión entre los hechos delictivos y los métodos de Adquisición

En los resultados se nota que el coeficiente de correlación Rho de Spearman es 0.482; esto indica que el vínculo es directo moderado, es decir, a mayor cifra de hechos delictivos le corresponde mayor cifra de adquisiciones utilizadas. También se observa que el valor de probabilidad p= 0.000. En conclusión, se puede afirmar con un 99% de confianza que existe una relación positiva moderada entre la extracción de información de teléfonos celulares con la adquisición en hechos delictivos en la OPERIT, 2020.

4.1.3. DISCUCIÓN

De la extracción de información del teléfono celular en los diversos hechos delictivos de tráfico ilícito de drogas, contra el patrimonio, contra la indemnidad sexual y homicidio, suscitados en contra de personas naturales o jurídicas. La fiscalía solicita encontrar evidencia digital relacionada a uno más hechos delictivos en los teléfonos celulares incautados.

Con respecto a la evidencia digital

La evidencia digital está representada como un registro o archivo digital almacenado en un computador, teléfono celular u otro medio tecnológico que contiene alguna conversación, contacto, registro de llamadas telefónicas, mensajes, audio, imágenes, videos u otros de interés relacionado a un hecho delictivo.

Un fundamento teórico que apoya este trabajo de investigación es el de (Mayer, L. (2018)), quien describe en el anuario estadístico del Ministerio del Interior de España (2014) que los hombres son más propensos a ser víctimas de algún tipo de delito, interpretándose que la criminalista esta intimidante ligada a los ciberdelitos; esta situación nos conlleva a manifestar que los delincuentes pueden utilizar algún medio tecnológico llámese computadores, teléfonos celulares u otros medios para cometer sucesos criminales.

Así mismo en la publicación de Tejo, et al. (2021), detalla como un virus informático afecta un Hospital Oncológico, originando la eliminación de muchas historias clínicas, además de pedir un rescate en criptomonedas (dinero digital)

para eliminar el virus. Esta situación nos conlleva a manifestar que los delincuentes pueden utilizar algún medio tecnológico llámese computadores, teléfonos celulares u otros medios para cometer sucesos criminales.

En la publicación “Determinar en qué mediad el avance de los teléfonos celulares y las conversaciones de redes sociales se vinculan con el cibercrimen de trata de personas en menores de edad en Colombia” concluye que el teléfono celular es uno de los medios más usados para trasmitir material de pornografía infantil Romero (2017).

De lo anterior se traduce que el material pornográfico se puede encontrar en un video o imagen de tipo sexual o erótico; además de existir conversaciones o proporciones indecentes a niños o adolescentes que conduzcan a cometer el delito de trata de personas; estos jovencitos a la vez pueden ser reclutados por proxenetas que los esclavizan sexualmente. En este contexto es importante realizar un análisis forense al teléfono celular para buscar evidencias del delito de indemnidad sexual

Con respecto al teléfono celular

Un teléfono celular tiene características de marca, modelo, chipset, sistema operativo, Antivirus, además de poseer un mecanismo de bloqueo por contraseña, PIN o patrón; por lo que al tener diferentes y particulares propiedades, se dificulta extraer toda información.

En el trabajo de investigación “Identificar las vulnerabilidades de seguridad en teléfonos celulares”, realizado por Ordoñez, et al, (2019). Buscó determinar como un programa nocivo puede ser admitido por el programa Google Play Protect (Antivirus de teléfono Android) para instalarse; evidenciándose que fácilmente cualquier aplicación puede, borrar información o ralentizar el teléfono celular o robar información personal de un usuario u otra actividad. Por ello se recomienda tener instalado un programa antivirus en el teléfono celular.

Con respecto al software forense

Un software forense es un programa informático especializado en detectar, desbloquear, extraer y exportar información de un teléfono celular; además de poder reparar algún daño lógico que pueda tener el teléfono celular.

En la publicación de Rennó y Brasi (2022) realizo un estudio de investigación en la “Federal Institute of Education, Science and Technology of the South of Minas Gerais” donde demostró que el cyberbullying afecta de diversas formas la autoestima de las personas. Esta situación nos conlleva a manifestar que los acosadores pueden utilizar algún medio tecnológico como computadores, teléfonos celulares u otros medios para cometer estas agresiones; por lo que es importante utilizar varios programas para forenses para encontrar alguna evidencia digital de tipo cyberbullying.

Con respecto a la adquisición

En el trabajo de investigación “Determinar como la dependencia de los teléfonos celulares aumenta el riesgo de ser víctima de delitos cibernéticos” se describe que las personas que tiene más adicción de los teléfonos celulares son más propensas de sufrir de algún tipo de delito cibernético. Herrero (2022).

Del párrafo anterior, se entiende que es importante realizar la adquisición del teléfono celular más completa posible es decir la adquisición Full File System y Física para buscar información visible y eliminada de aplicaciones nocivas como keylogers, troyanos que roban información de claves de correos, cuentas de bancos y otros originando el delito de robo contra el patrimonio de dinero al dueño del teléfono de celular. Así mismo el analista forense se encarga de buscar en el celular algún rastro como dirección IP o correo electrónico que permita encontrar una pista del delincuente informático.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Primera. Teniendo en cuenta que se debe determinar la relación entre la extracción de información de teléfonos celulares con la evidencia digital. Se concluye que el coeficiente de Rho Spearman es 0.992; entendiéndose que la conexión es directa y su grado es muy alto, es decir, a mayor cifra de evidencias digitales le pertenece alta número de hechos delictivos encontrados. También se nota que la cifra de probabilidad p= 0.000, esto indica que la conexión es significativa al 99%; por lo tanto, existe conexión entre la evidencia digital y los hechos delictivos en la OPERIT del Ministerio Publico, Lima,2019-2020.

Segunda. Teniendo en cuenta que se debe determinar la relación entre los hechos delictivos y las marcas de los teléfonos celulares. Se concluye que el coeficiente de Rho Spearman es 0.562; ello quiere decir que el vínculo es directo, es decir, a mayor cantidad de hechos delictivos le corresponde más número de marcas de teléfonos celulares. Además, se muestra que la cifra de probabilidad p= 0.000, ello quiere decir que la conexión es significativa al 99%; por consiguiente, existe correlación entre los teléfonos celulares y los hechos delictivos en la OPERIT del Ministerio Público, Lima, 2019-2020.

Tercera. Considerando que se debe analizar el grado de correlación de los hechos delictivos y el software forense. Se concluye que el coeficiente de Rho Spearman es 0.352; esto indica que la relación es directa; es decir, a mayor cantidad de hechos delictivos le corresponde mayor cantidad softwares forenses empleados. También se observa que el valor de probabilidad p= 0.001, esto indica que la correlación es significativa al 99%; por lo tanto,

existe relación entre los softwares forenses y los hechos delictivos en la Oficina de Peritajes del Ministerio Público, Lima,2019-2020.

Cuarta. Tomando en cuenta que se debe identificar el nivel de relación entre los hechos delictivos y los métodos de adquisición, se concluye de los resultados que el coeficiente Rho de Spearman es 0.482; es decir, a mayor cantidad de hechos delictivos le corresponde mayor cantidad de adquisiciones realizadas. También se observa que el valor de probabilidad p= 0.000, esto indica que la correlación es significativa al 99%; por lo tanto, existe relación entre las adquisiciones y los hechos delictivos en la Oficina de Peritajes del Ministerio Público, Lima, 2019-2020.

5.2. Recomendaciones

Primera. –De acuerdo con los resultados obtenidos y considerando que se determinó que la extracción de información de teléfonos celulares influye en la identificación de evidencia digital en la búsqueda de hechos delictivos en la OPERIT del Ministerio Público; se propone a los fiscales recolectar los teléfonos celulares donde se presume que contiene evidencia digital y omitir los teléfonos celulares de marcas descontinuadas y así el Perito entregara la información más valiosa para su mejor valoración fiscal.

Segunda. – Teniendo en cuenta los resultados obtenidos y considerando las diferentes marcas, modelos, sistema operativo, chipset y estado del teléfono se recomienda que los teléfonos celulares sean remitidos en buen estado y el menor tiempo posible, de lo contrario alguien puede eliminar información valiosa que impida resolver un hecho criminal.

Tercera. –De acuerdo con los resultados obtenidos y considerando la relación que existe entre el teléfono celulares y el software forense en hechos delictivos en la Oficina de Peritajes

del Ministerio Público. Se recomienda adquirir los mejores softwares forenses y actualizados para poder extraer la mayor cantidad de teléfonos celulares bloqueados o desbloqueados.

Cuarta. –Tomando los resultados hallados y considerando que existe relación entre los hechos delictivos encontrados y los métodos de adquisición, se recomienda a los Peritos informáticos tener una bitácora de los tipos de extracciones compatibles con los teléfonos celulares categorizados por marca y modelo, para que en una próxima lectura de teléfono celular, saber qué tipo de adquisición emplear para que de esta manera se entregue una Pericia informática más rápida y eficiente que sirva la fiscal para su mejor valoración.

REFERENCIAS BIBLIOGRÁFICAS

Anuario Estadístico del Ministerio del Interior (2014). https://ww.interior.gob.es/documents/642317/1203602/Anuario_estadistico_2014_126150729.pdf/112c5a53-cb2d-4b5d-be12-4a3d5b5d057e

Arias, F. (2005). El proyecto de investigación. Caracas: Episteme.

Blossier Mazzini, J. (2008). Los Delitos Informáticos y la Banca Electrónica. Revista Abogados (8).

Cano Pita, G. E. (2018). Las TICs en las empresas: evolución de la tecnología y cambio estructural en las organizaciones. Revista Científica dom. Cien., ISSN: 2477-8818 Vol. 4, núm. 1, pp. 499-510. https://dialnet.unirioja.es/descarga/articulo/6313252.pdf

Cano Martínez, J. (2015). Computación forense - Descubriendo los rastros informáticos 2ª edición. Medellín: Alfaomega.

Carrasco, S. (2005). Metodología de la investigación científica. Lima: San Marcos.

Cyber Crime - Victimology Analysis (2016). https://www.cityoflondon.police.uk/news-and-appeals/Documents/Victimology%20Analysislatest.pdf

Código Penal Peruano (1991). Decreto Legislativo 635 - Código Penal Peruano. Lima, Perú: Diario El Peruano. http://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/001CD7E618605745052583280052F800/%24FILE/COD-PENAL_actualizado_16-09-2018.pdf

Código Procesal Penal (2004). Código Procesal Penal, Decreto Legislativo 957. Perú: El Peruano.

Conedo, A. (2013). La informática forense y los delitos informáticos. Revista Pensamiento Americano, 3(4). 81-88.

Cconislla, R. (2017). Incorporar la modalidad del delito de pedofilia en la Ley Nº 30096 capítulo III de los delitos informáticos (Propuesta legislativa). Puerto Maldonado: Universidad Andina de Cusco.

Delgado, M. L. (junio de 2007). Análisis Forense Digital.

DS 026. (2017). Decreto Supremo Nº 026-2017-IN. Reglamento Ley PNP- Ley 1267. Perú: Diario el Peruano. http://www.gacetajuridica.com.pe/boletin-nvnet/arweb/ DS0262017IN.pdf

Durand (2002) "Los delitos informáticos en el Código Penal Peruano" en revista Peruana de Ciencias Penales. Nº11, Lima.

El comercio (26 de setiembre del 2021). Nueva modalidad vía WhatsApp: delincuentes roban celulares y contactan a amigos y familiares de víctimas para estafar. https://elcomercio.pe/lima/seguridad/nueva-modalidad-via-whatsapp-delincuentes-roban-celulares-y-contactan-a-amigos-y-familiares-de-victimas-para-estafar-pnp-nndc-noticia/

Endpoint. (2018). Barracuda lanza un método para medir la resistencia a los ataques de phishing. https://www.itdigitalsecurity.es/endpoint/2018/04/barracuda-lanza-un-metodo-para-medir-la-resistencia-a-los-ataques-de-phishing

Estadísticas sobre delitos ingresados al Ministerio Público (enero a diciembre de 2015). http://www.fiscaliadechile.cl/Fiscalia/estadisticas/index.do

Figueroa, L.; Lara, C.; Lesca, N.; Viaña, G.; Binda A. (2018). Tratamiento de Evidencias Digitales Forenses en Dispositivos Móviles. XIX Workshop de Investigadores En Ciencias de La Computación, 648–652. https://core.ac.uk/download/pdf/296403001.pdf

Fernández (2002) "Los delitos informáticos", Editorial Juristas, enero.

Ferro Veiga, J. M. (2015). Informática forense, El rastro digital del crimen. España: Amazon

García, C. M. (2017). Los delitos de estafas y sus consecuencias a través de las redes sociales. Babahoyo Ecuador: Universidad Regional Autónoma de los Andes – UNIANDES.

García, J. C. y Peña, D. E. (2017). Cibercriminalidad & postmodernidad: la cibercriminología como respuesta al escenario contemporáneo. https://www.pensamientopenal.com.ar/doctrina/44898-cibercriminalidad-y-posmodernidad-cibercriminologia-respuesta-al-escenario

Hernández R., Fernández, C. y Batista, P. (2014). Metodología de la investigación. México: Mc Graw Hill.

Herrero, Juan, Torres, Andrea, Vivas, Pep, & Urueña, Alberto. (2022). Smartphone addiction, social support, and cybercrime victimization: a discrete survival and growth mixture model. Psychosocial Intervention, 31(1), 59-66. Epub 17 de enero de 2022.https://dx.doi.org/10.5093/pi2022a3

Instituto Nacional de Estadística e Informática (2002). Actualización del impacto de las tecnologías de información y comunicación en el Perú. Lima. https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Inf/Lib5151/Libro.pdf

Instituto Nacional de Estadística e Informática (2020). Victimización en el Perú 2010-2019 https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1730/

López, A. J, López, L. y Jerónimo, G. (2017). Factores que contribuyen a la prevención de los delitos informáticos en el Estado de Tabasco. Revista Gênero & Direito, 6(3). 1-17.

Jorge Monroy, (2020). Identifican 16,470 líneas telefónicas ilegales en prisión. https://www.eleconomista.com.mx/politica/Identifican-16470-lineas-telefonicas-ilegales-en-prision-20201014-0154.html

Loredo, J. A., y Ramírez, A. (2013). Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. Celerinet. 44-51.

Medina-Cárdenas, Y., & Rico-Bautista, D. (2012). Mejores prácticas de gestión para la calidad de los servicios en tecnologías de información. In Gerencia Tecnológica Informática (Vol. 11, Issue 29, pp. 47–58).

Mayer Lux, Laura. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. Ius et Praxis, 24(1), 159-206. https://dx.doi.org/10.4067/S0718-00122018000100159

Ministerio Público. (2012). Observatorio de la Criminalidad. https://www.mpfn.gob.pe/Docs/observatorio/files/boletín_semanal_(34).pdf

Nadjila Tejo Machad, (2021), Protocolo de informática forense ante ciberincidentes en telemedicina para preservar información como primera respuesta. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1900-65862021000100181&lang=en

Navarro Clérigues, J. (2016). Guía actualizada para futuros peritos informáticos. Últimas herramientas de análisis forense digital. Caso práctico. 148.

Ochoa Arévalo, P. A. (2018). El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. Revista Economía y Política, XIV (28), 35–46. https://doi.org/10.25097/rep.n28.2018.03

Ordoñez-Quintero, C.; Ordoñez-Eraso, H.; Ordoñez-Córdoba, J. (2022). Information Management Security Vulnerabilities in Smartphones Used by University Students: A Case Study in the Southwest of Colombia. Revista Facultad de Ingeniería, 31(59), e201. Epub May 04, 2022.

http://www.scielo.org.co/scielo.php?script=sci_abstract&pid=S0121-11292022000100201

Orts, B. & Roig, M. (2001). "Delitos Informáticos y delitos comunes cometidos a través de la informática", Valencia, España. Editorial Tirant Lo Blanch. ISBN: 9788484424406.

Organización de las Naciones Unidad (2019). Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. https://www.unodc.org/documents/Cybercrime/SG_report/V1908185_S.pdf

Policía Nacional del Perú. (2013). Manual de Operaciones Policiales. Lima, Perú.

Policía Nacional del Perú. (2017). Red Social Facebook PNP. Obtenido de Red Social Facebook: PNP: https://www.facebook.com/Policia/photos/línea-whatsapp-para-denuncias-dedelitos-comunes-y-microcomercialización-de-drog/1685362554812372/

Ramírez, D. A., y Castro, E. F. (2018). Análisis de la evidencia digital en Colombia como soporte judicial de delitos informáticos mediante cadena de custodia. Villavicencio: Universidad Nacional Abierta y a Distancia "UNAD".

Rennó y Brasi. (2022). Representações sociais invadidas e maculadas por cyberbullying. https://www.scielo.br/j/bioet/a/b9LMMshjXbBH3tMFMhWhzdr/?lang=pt

Romero, (2017). Tecnología y pornografía infantil en Colombia, 2013-2015: interpretación desde un enfoque victimológico. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082017000100027&lang=es

Rosa Fernández, (2022). Consumo y uso de smartphones en España - Datos estadísticos https://es.statista.com/temas/4086/consumo-y-uso-de-smartphones-en-espana/#dossierKeyfigures

RT Agencia de noticias, (2019). Crean un 'arma' capaz de desbloquear y extraer datos de todos los dispositivos iOS y de los Android de gama alta. https://actualidad.rt.com/actualidad/318246-empresa-israeli-afirma-poder-desbloquear-todos-dispositivos-ios-android

Saltzman, Marc. (2021). ¿Te conviene comprar un iPhone o un Android? https://www.aarp.org/espanol/hogar-familia/tecnologia/info-2019/que-telefono-comprar-iphone-o-android.html

Tello L, E. (2008). Las tecnologías de la información y comunicaciones (TIC) y la brecha digital: su impacto en la sociedad de México. Revista de Universidad y Sociedad del Conocimiento, 3. https://rusc.uoc.edu/rusc/es/index.php/rusc/article/download/v4n2-tello/305-1221-2-PB.pdf

Symantec Intelligence Report (2015). https://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence-report-01-2015-enus.pdf.

Anexo 1: Matriz de Consistencia

Extracción de información de teléfonos celulares y su relación con hechos delictivos en la OPERIT del Ministerio Público 2020

Formulación del problema	Objetivos	Hipótesis	Variables	Diseño Metodológico
Problema general ¿Cómo la extracción de información de teléfonos celulares se relaciona en los hechos delictivos en la OPERIT de Ministerio Público, Lima 2020? **Problemas específicos** 1. ¿Qué vinculo tiene la extracción de información de teléfonos celulares con	**Objetivo General** Identificar en qué medida la extracción de información de teléfonos celulares se relaciona con los hechos delictivos en la OPERIT del Ministerio Público, 2020". **Objetivos específicos** 1. Evaluar en qué medida la extracción de información de teléfonos celulares se relaciona con la marca y modelo en los hechos delictivos en la OPERIT, 2020.	**Hipótesis General** Existe relación entre la extracción de información de teléfonos celulares con los hechos delictivos en la OPERIT del Ministerio Público del año 2020. **hipótesis especificas** 1. Existe correspondencia entre la extracción de información de teléfonos celulares con la marca y modelo en los hechos delictivos en la OPERIT, 2020.	**Variable 1** Extracción de Información de teléfonos celulares. **Variable 2** Hechos delictivos.	**Tipo de investigación:** Básica. **Método:** Deductivo **Diseño de la investigación** No experimental. **Población** 400 teléfonos celulares. **Muestra** 80 teléfonos celulares.

la marca y modelo en los hechos delictivos en la OPERIT, 2020? 2. ¿Qué relación tiene la extracción de información de teléfonos celulares con el software forense en los hechos delictivos en la OPERIT, 2020? 3. ¿Qué relación tiene la extracción de información de teléfonos celulares con la adquisición en los	2. Identificar de qué manera la extracción de información de teléfonos celulares se relaciona con el software forense en los hechos delictivos en la OPERIT, 2020. 3. Determinar de qué manera la extracción de información de teléfonos celulares se relaciona con la adquisición en los hechos delictivos en la OPERIT, 2020. 4. Determinar de qué manera la extracción de información de teléfonos celulares se relaciona con la	2. Existe relación entre la extracción de información de teléfonos celulares con el software forense en los hechos delictivos en la OPERIT, 2020. 3. Existe relación entre la extracción de información de teléfonos celulares con la adquisición en los hechos delictivos en la OPERIT, 2020. 4. Existe relación entre la extracción de información de teléfonos celulares con la evidencia digital en la OPERIT, 2020.		

hechos delictivos en la OPERIT, 2020? 4. ¿Qué relación tiene la extracción de información de teléfonos celulares con la evidencia digital en los hechos delictivos en la OPERIT, 2020?	evidencia digital en los hechos delictivos en la OPERIT, 2020.			

ANEXO 2: INSTRUMENTO

Determinación conceptual de las Variables y Dimensiones

1. Variables

1.1. Extracción de información de teléfonos celulares

Para extraer información de un teléfono celular se debe conocer básicamente la marca y modelo, además del programa de extracción y tipo de adquisición con el fin de obtener la mayor cantidad de información.

1.2. Hechos delictivos

Esta variable comprende la evidencia digital como: mensajes, registros de llamadas, contactos, conversaciones, archivos de audio, video, imágenes y otros relacionares a sucesos criminales como, por ejemplo: Delito contra el patrimonio, tráfico ilícito de drogas, pornografía infantil, homicidio; entre otros.

2. Dimensiones

2.1. Teléfono celular

Un teléfono celular tiene propiedades de marca, modelo, sistema operativo y chipset; siendo estas dos primeras características importantes para el proceso de lectura de teléfono celular por el software forense.

2.2. Software forense

Un software forense es un programa especializado en la detección, desbloqueo y adquisición de información; además de reparar el daño lógico de un teléfono celular. dentro de los mejores softwares tenemos a: Cellebrite Premium, Ufed 4PC, XRY y Magnet Axiom.

2.3. Adquisición

Consiste en utilizar algún método de obtención de información del celular tales como: extracción parcial, Android genérico, full file system o física.

2.4. Evidencia digital

Consiste en encontrar algún contacto, conversación, archivo de imagen, video u otro registro que esté relacionado a algún hecho delictivo que pueda convertirse en evidencia digital.

LISTA DE COTEJO

Número de pericia: …….

Fecha de la pericia. ……..

Marca ……

Modelo del teléfono celular ….

Objeto de la Pericia ….

Alternativas de repuesta: Cifra

N.º	PREGUNTAS	ESTADO
	EXTRACCIÓN DE INFORMACIÓN DE TELÉFONOS CELULARES	
1	¿Cuál es la marca del teléfono celular?	
2	¿Cuál es le modelo del teléfono celular?	
3	¿Cuál es el chipset del teléfono celular?	
4	¿Cuál es el IMEI del teléfono celular?	
5	¿Cuál es la serie del teléfono celular?	
6	¿Cuál es la versión del sistema operativo?	
7	¿Cuál es la actualización de seguridad de Android?	
8	¿Cuál es el kernel del teléfono celular?	

9	¿Cuál es el software forense empleado en el teléfono celular?	
10	¿Cuál es la adquisición empleada en el teléfono celular?	
	HECHOS DELICTIVOS	
1	¿Se encontró registros de llamadas relacionados a un hecho delictivo?	
2	¿Se encontró contactos relacionados a un hecho delictivo?	
3	¿Se encontró mensajes de texto relacionados a un hecho delictivo?	
4	¿Se encontró conversaciones relacionados a un hecho delictivo?	
5	¿Se encontró archivos de audio relacionados a un hecho delictivo?	
6	¿Se encontró archivos de video relacionados a un hecho delictivo?	
7	¿Se encontró archivos de imágenes relacionados a un hecho delictivo?	
8	¿Se encontró cuentas de usuario relacionados a un hecho delictivo?	
9	¿Se encontró documentos relacionados a un hecho delictivo?	
10	¿Se encontró geolocalización relacionados a un hecho delictivo?	

ANEXO 3: VALIDEZ DE LA HERRAMIENTA

Certificado de validez de contenido del instrumento que mide la información de teléfonos celulares y su relación con hechos delictivos en la Oficina de Peritajes del Ministerio Publico 2020

Nº	DETALLES	Pertinencia[1]				Relevancia[2]				Claridad[3]				Sugerencias
		MD	D	A	MA	MD	D	A	MA	MD	D	A	MA	
	DIMENSIÓN: EVIDENCIA DIGITAL													
1	¿Cuántos contactos, registros de llamadas, mensajes y archivos de audio, video, imágenes u otro registro se encontraron relacionado a un delito?				X				X				X	
	DIMENSIÓN: TELEFONO CELULAR													
2	¿Cuál es la marca, modelo, IMEI, serie, Sistema Operativo, chipset del teléfono celular?				X				X				X	
	DIMENSION: SOFTWARE FORENSE													
3	¿Cuál es el software forense empleado en el teléfono celular?				X				X				X	
	DIMENSION: ADQUISICIÓN													
4	¿Cuál es la adquisición empleada en el teléfono celular?				X				X				X	

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia**: El ítem es apropiado para representar al componente o dimensión específica del cor
[3]**Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los Ítems planteados son suficientes para medir la dir

(1) **MD**: Muy en desacuerdo
(2) **D**: En desacuerdo
(3) **D**: En acuerdo
(4) **MA**: Muy en acuerdo

Observaciones: _____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador Mg. Edgar Gómez Enciso. **DNI:** 41784256

Especialidad del validador, Maestro en Sistemas e Informática

Firma del experto
Edgar Gómez Enciso
Maestro en Ciencias con Mención en Gestión Ambiental

Lima, 08 de Julio del 2022

Certificado de validez de contenido del instrumento que mide la información de teléfonos celulares y su relación con hechos delictivos en la Oficina de Peritajes del Ministerio Publico 2020

Nº	DETALLES	Pertinencia[1]				Relevancia[2]				Claridad[3]				Sugerencias
		MD	D	A	MA	MD	D	A	MA	MD	D	A	MA	
	DIMENSIÓN: EVIDENCIA DIGITAL													
1	¿Cuántos contactos, registros de llamadas, mensajes y archivos de audio, video, imágenes u otro registro se encontraron relacionado a un delito?				X				X				X	
	DIMENSIÓN: TELEFONO CELULAR													
2	¿Cuál es la marca, modelo, IMEI, serie, Sistema Operativo, chipset del teléfono celular?				X				X				X	
	DIMENSION: SOFTWARE FORENSE													
3	¿Cuál es el software forense empleado en el teléfono celular?				X				X				X	
	DIMENSION: ADQUISICIÓN													
4	¿Cuál es la adquisición empleada en el teléfono celular?				X				X				X	

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia**: El ítem es apropiado para representar al componente o dimensión específica del cor
[3]**Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dir

(1) **MD**: Muy en desacuerdo
(2) **D**: En desacuerdo
(3) **D**: En acuerdo
(4) **MA**: Muy en acuerdo

Observaciones: _____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador Mg. Miguel Ángel Carrera Muñoz. **DNI:** 43402222

Especialidad del validador, Maestro en Ciencias con Mención en Gestión Ambiental

Firma del experto
Miguel Ángel Carrera Muñoz
Maestro en Ciencias con Mención en Gestión Ambiental

Lima, 08 de Julio del 2022

Certificado de validez de contenido del instrumento que mide la información de teléfonos celulares y su relación con hechos delictivos en la Oficina de Peritajes del Ministerio Publico 2020

Nº	DETALLES	Pertinencia[1]				Relevancia[2]				Claridad[3]				Sugerencias
		MD	D	A	MA	MD	D	A	MA	MD	D	A	MA	
	DIMENSIÓN: EVIDENCIA DIGITAL													
1	¿Cuántos contactos, registros de llamadas, mensajes y archivos de audio, video, imágenes u otro registro se encontraron relacionado a un delito?				X				X				X	
	DIMENSIÓN: TELEFONO CELULAR													
2	¿Cuál es la marca, modelo, IMEI, serie, Sistema Operativo, chipset del teléfono celular?				X				X				X	
	DIMENSION: SOFTWARE FORENSE													
3	¿Cuál es el software forense empleado en el teléfono celular?				X				X				X	
	DIMENSION: ADQUISICIÓN													
4	¿Cuál es la adquisición empleada en el teléfono celular?				X				X				X	

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia**: El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

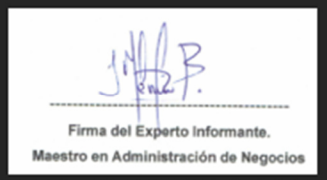
(1) **MD**: Muy en desacuerdo
(2) **D**: En desacuerdo
(3) **D**: En acuerdo
(4) **MA**: Muy en acuerdo

Observaciones: _____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador Mg. JESSICA NATALIA MERINO BURGOS. **DNI:** 32963199

Especialidad del validador, Magister en Contrataciones del estado



Firma del Experto Informante.
JESSICA NATALIA MERINO BURGOS

Lima, 08 de Julio del 2022

Certificado de validez de contenido del instrumento que mide la información de teléfonos celulares y su relación con hechos delictivos en la Oficina de Peritajes del Ministerio Publico 2020

N°	DETALLES	Pertinencia[1]				Relevancia[2]				Claridad[3]				Sugerencias
		MD	D	A	MA	MD	D	A	MA	MD	D	A	MA	
	DIMENSIÓN: EVIDENCIA DIGITAL													
1	¿Cuántos contactos, registros de llamadas, mensajes y archivos de audio, video, imágenes u otro registro se encontraron relacionado a un delito?				X				X				X	
	DIMENSIÓN: TELEFONO CELULAR													
2	¿Cuál es la marca, modelo, IMEI, serie, Sistema Operativo, chipset del teléfono celular?				X				X				X	
	DIMENSION: SOFTWARE FORENSE													
3	¿Cuál es el software forense empleado en el teléfono celular?				X				X				X	
	DIMENSION: ADQUISICIÓN													
4	¿Cuál es la adquisición empleada en el teléfono celular?				X				X				X	

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del cor
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dir

(1) **MD:** Muy en desacuerdo
(2) **D:** En desacuerdo
(3) **D:** En acuerdo
(4) **MA:** Muy en acuerdo

Observaciones: _____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador Mg. Milton Cesar Tullume Chavesta. **DNI:** 07482588

Especialidad del validador, DR. EN MEDIO AMBIENTE Y DESARROLLO SOSTENIBLE

Firma del Experto Informante.
Especialidad

Lima, 08 de Julio del 2022

Certificado de validez de contenido del instrumento que mide la información de teléfonos celulares y su relación con hechos delictivos en la Oficina de Peritajes del Ministerio Publico 2020

N°	DETALLES	Pertinencia[1]				Relevancia[2]				Claridad[3]				Sugerencias
		MD	D	A	MA	MD	D	A	MA	MD	D	A	MA	
	DIMENSIÓN: EVIDENCIA DIGITAL													
1	¿Cuántos contactos, registros de llamadas, mensajes y archivos de audio, video, imágenes u otro registro se encontraron relacionado a un delito?				X				X				X	
	DIMENSIÓN: TELEFONO CELULAR													
2	¿Cuál es la marca, modelo, IMEI, serie, Sistema Operativo, chipset del teléfono celular?				X				X				X	
	DIMENSION: SOFTWARE FORENSE													
3	¿Cuál es el software forense empleado en el teléfono celular?				X				X				X	
	DIMENSION: ADQUISICIÓN													
4	¿Cuál es la adquisición empleada en el teléfono celular?				X				X				X	

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del cor
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dir

(1) **MD:** Muy en desacuerdo
(2) **D:** En desacuerdo
(3) **D:** En acuerdo
(4) **MA:** Muy en acuerdo

Firma del experto
Lizbardo Orellano Benancio
Mg. En Ciencia Criminalística

Observaciones: _____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador Mg. Lizbardo Orellano Benancio **DNI:** 09658864

Especialidad del validador, Mg. En Ciencia Criminalística

Lima, 08 de Julio del 2022

ANEXO 4: Aprobación del Comité de Ética

Universidad Norbert Wiener

COMITÉ INSTITUCIONAL DE ÉTICA PARA LA INVESTIGACIÓN

Lima, 08 de setiembre de 2022

Investigador(a):
Wiliam Rubén Gutiérrez Salvador
Exp. N° 2202-2022

Cordiales saludos, en conformidad con el proyecto presentado al Comité Institucional de Ética para la investigación de la Universidad Privada Norbert Wiener, titulado: "**Extracción de información de teléfonos celulares y su relación con hechos delictivos en la oficina de peritajes del ministerio público - lima 2020**"– versión 1, el cual tiene como investigador principal **Wiliam Rubén Gutiérrez Salvador.**

Al respecto se informa lo siguiente:
El Comité Institucional de Ética para la investigación de la Universidad Privada Norbert Wiener, en sesión virtual ha acordado la **APROBACIÓN DEL PROYECTO** de investigación, para lo cual se indica lo siguiente:

1. La vigencia de esta aprobación es de un año a partir de la emisión de este documento.
2. Toda enmienda o adenda que requiera el Protocolo debe ser presentado al CIEI y no podrá implementarla sin la debida aprobación.
3. Debe presentar 01 informe de avance cumplidos los 6 meses y el informe final debe ser presentado al año de aprobación.
4. Los trámites para su renovación deberán iniciarse 30 días antes de su vencimiento juntamente con el informe de avance correspondiente.

Sin otro particular, quedo de Ud.,

Atentamente

UNIVERSIDAD PRIVADA NORBERT WIENER · Comité Institucional de Ética para la Investigación · Universidad Norbert Wiener

Yenny Marisol Bellido Fuentes
Presidenta del CIEI- UPNW

ANEXO 5: Memorando n°158-2022-mp-fn-gg-operit de autorización para acceso a información estadística de informes periciales

MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN

Decenio de la Igualdad de oportunidades para mujeres y hombres
Año del Fortalecimiento de la Soberanía Nacional
OFICINA DE PERITAJES

Firma Digital

Lima, 15 de Julio del 2022

MEMORANDO N° 000158-2022-MP-FN-GG-OPERIT

A : **WILIAM RUBEN GUTIERREZ SALVADOR**
Analisis Digital Forense - Operit

De : **ANGELICA MARIA BARRERA LAURENTE**
Gerente de Peritajes

Asunto : Solicito autorización para acceso a la información estadística de Informes Periciales del área de Análisis Digital Forense del año 2020.

Referencia : PROVEIDO N° 008570-2022-MP-FN-GG-OPERIT (12JUL2022)

Expediente : GG-OPE20220000294

Por medio de la presente lo saludo cordialmente y en relación al asunto de la referencia, la Oficina de peritajes ha tomado conocimiento del requerimiento educativo del Proyecto de Tesis "INFORMACIÓN DE TELEFONOS CELULARES Y SU RELACIÓN CON HECHOS DELICTIVOS EN LA OFICINA DE PERITAJES DEL MINISTERIO PUBLICO - LIMA 2020" y en ese sentido, otorga la autorización sólo de estadísticas, debiendo mantener en total reserva los datos de nombres de fiscales, numero de oficio, carpeta fiscal, nombre de investigado, números telefónicos o número de serie de los teléfonos celulares y el contenido de información con carácter de reserva contenido en el mismo

Atentamente.

ANGELICA MARIA BARRERA LAURENTE
OFICINA DE PERITAJES

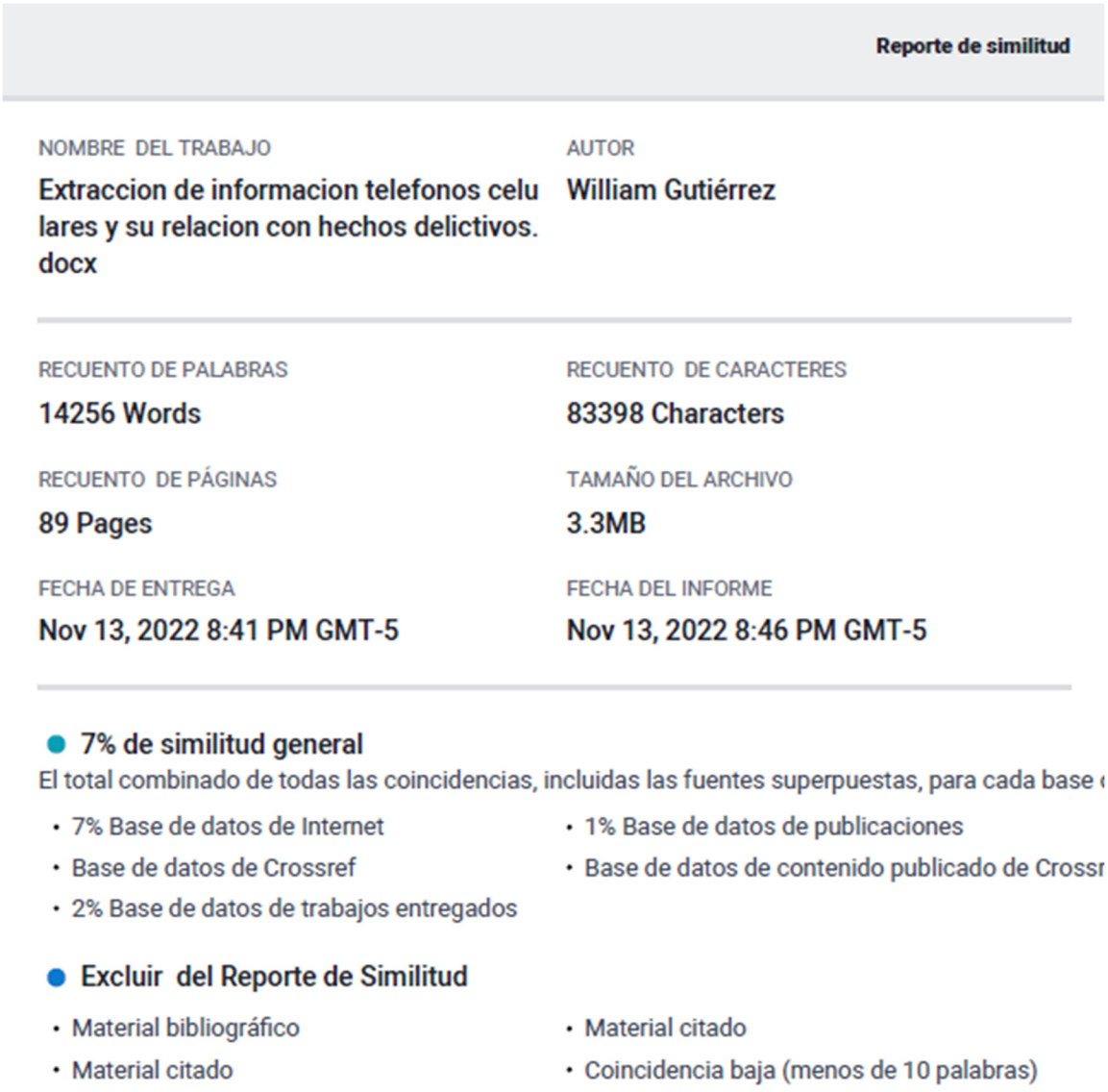
cc:

ABL/loa

OFICINA DE PERITAJES
Av. Prolongación Arica N° 1832 - Cercado de Lima
Teléfono (01) 7110280 - WhatsApp 938353635
peritajesmdp@mpfn.gob.pe

EXPEDIENTE: GG-OPE20220000294
CODUN: 7P2A4
R.33429
ABL/loa

ANEXO 6: Informe del asesor de turnitin



Reporte de similitud

NOMBRE DEL TRABAJO
Extraccion de informacion telefonos celulares y su relacion con hechos delictivos.docx

AUTOR
William Gutiérrez

RECUENTO DE PALABRAS
14256 Words

RECUENTO DE CARACTERES
83398 Characters

RECUENTO DE PÁGINAS
89 Pages

TAMAÑO DEL ARCHIVO
3.3MB

FECHA DE ENTREGA
Nov 13, 2022 8:41 PM GMT-5

FECHA DEL INFORME
Nov 13, 2022 8:46 PM GMT-5

7% de similitud general
El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base

- 7% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossr
- 2% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 10 palabras)