Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

ISO 27037:2012 PARA MEJORAR EL ANÁLISIS INFORMÁTICO FORENSE EN LA DIVISIÓN DE INVESTIGACIÓN DE DELITOS DE ALTA TECNOLOGÍA DE LA POLICÍA NACIONAL DEL PERÚ, LIMA 2022

Línea de investigación:
Ingeniería de software, simulación y desarrollo de TICs

Tesis para optar el grado académico de Maestro en Ingeniería de Sistemas con mención en Gestión de Tecnologías de la Información

Autor:

Farfan Chiun, Julio Enrique

Asesora:

Tejada Estrada, Gina Coral

ORCID: 0000-0002-0023-5147

Jurado:

Coveñas Lalupu, José

Petrlik Azabache, Ivan Carlo

Peña Carrillo, Cesar Serapio

Lima - Perú

2024

ISO 27037:2012 PARA MEJORAR EL ANÁLISIS INFORMÁTICO FORENSE EN LA DIVISIÓN DE INVESTIGACIÓN DE DELITOS DE ALTA TECNOLOGÍA DE LA POLICÍA NACIONAL DEL PERÚ, LIMA 2022

INFORME DE ORIGINALIDAD

21%	20%	5%	7%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.ucv.edu.pe Fuente de Internet	6%
2	hdl.handle.net Fuente de Internet	2%
3	repositorio.ulasamericas.edu.pe Fuente de Internet	1%
4	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	1%
5	Submitted to Escuela de Posgrado PNP Trabajo del estudiante	1%
6	repositorio.puce.edu.ec Fuente de Internet	1%
7	repositorio.utp.edu.pe Fuente de Internet	1%
8	ojs.umsa.bo Fuente de Internet	<1%

Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

ISO 27037:2012 PARA MEJORAR EL ANÁLISIS INFORMÁTICO FORENSE EN LA DIVISIÓN DE INVESTIGACIÓN DE DELITOS DE ALTA TECNOLOGÍA DE LA POLICÍA NACIONAL DEL PERÚ, LIMA 2022

Línea de investigación:
Ingeniería de software, simulación y desarrollo de TICs

Tesis para optar el grado académico de:
Maestro en ingeniería de sistemas con mención en
gestión de tecnologías de la información

Autor:
Farfan Chiun, Julio Enrique

Asesor:
Tejada Estrada, Gina Coral
Código ORCID- 0000-0002-0023-5147

Jurado:
Coveñas Lalupu, José
Petrlik Azabache, Ivan Carlo
Peña Carrillo, Cesar Serapio

Lima – Perú
2024

DEDICATORIA

Agradecer en primer lugar a Dios por permitir haber llegado a esta etapa profesional, y a mi familia, en especial a mis padres Julio y Sonia, por todo el apoyo que me han brindado durante todos estos años. Sin su ayuda, no hubiera podido llegar hasta aquí. Agradezco el esfuerzo que han hecho por mí. Siempre estaré eternamente agradecido por toda su dedicación y amor incondicional.

AGRADECIMIENTO

Mi especial reconocimiento para los distinguidos Miembros del Jurado:

Dr. Coveñas Lalupu, José

Dr. Petrlik Azabache, Ivan Carlo

Mg. Peña Carrillo, Cesar Serapio

Por su criterio objetivo en la evaluación de este trabajo de investigación.

Asimismo, mi reconocimiento para mi asesora:

Dra. Tejada Estrada, Gina Coral

Por las sugerencias recibidas para el mejoramiento de este trabajo.

Muchas gracias para todos.

ÍNDICE

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

La presente investigación tiene como objetivo establecer la influencia del ISO 27037:2012 en la mejora del análisis informático forense en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022, esto debido a que, las diversas incidencias informáticas, no se registran adecuadamente en las computadoras y servidores. No se hace uso de plataformas digitales para el almacenamiento, manejo offline y online de la información relevante sobre diversos casos. De esta manera, existe una deficiencia en cuanto al manejo de la información, al tratamiento de ésta y sobre todo la relevancia de cada dato dentro de un proceso legal, la metodología de la presente investigación es experimental y se realizó un análisis pretest y post test. Los resultados obtenidos revelan que la adopción de la norma ISO 27037:2012 ha tenido un efecto notable en la eficiencia y efectividad de las operaciones forenses en la División. En primer lugar, se observó una reducción significativa en las horas empleadas en el proceso de análisis forense, lo que indica una optimización en la gestión del tiempo y recursos. Esta mejora es especialmente valiosa en un entorno en el que la celeridad en la obtención de pruebas es esencial. Además, el promedio de la extracción de datos aumentó de manera significativa, lo que implica que se logró capturar una mayor cantidad de información almacenada en dispositivos móviles. Por último, y no menos importante, se registró un aumento en el número de casos resueltos de manera satisfactoria por parte de los analistas forenses. Esto refleja la influencia positiva de la norma ISO 27037:2012 en la eficacia del proceso de investigación.

Palabras claves: ISO 27037, análisis informático, estudio de tiempos, extracción de datos.

ABSTRACT

The objective of this research is to establish the influence of ISO 27037:2012 on the improvement of Forensic Computer Analysis in the High Technology Crime Investigation Division of the National Police of Peru, Lima 2022, due to the fact that the various computer incidents, are not recorded properly on computers and servers. No use is made of digital platforms for the storage, offline and online management of relevant information about various cases. In this way, there is a deficiency in terms of the management of information, its treatment and, above all, the relevance of each data within a legal process. The methodology of this research is experimental and it carried out a pre-test and post-test analysis. The results obtained reveal that the adoption of the ISO 27037:2012 standard has had a notable effect on the efficiency and effectiveness of forensic operations in the Division. Firstly, a significant reduction was observed in the hours spent in the forensic analysis process, which indicates an optimization in the management of time and resources. This improvement is especially valuable in an environment where speed in obtaining evidence is essential. In addition, the average data extraction rate increased significantly, which implies that a greater amount of information stored on mobile devices was captured. Last but not least, there was an increase in the number of cases resolved satisfactorily by forensic analysts. This reflects the positive influence of ISO 27037:2012 on the effectiveness of the research process.

Keywords: ISO 27037, computer analysis, time study, data extraction.

I. INTRODUCCIÓN

La investigación y persecución sobre delitos en alta tecnología en la actualidad representa un desafío significativo a las policías de todo el mundo. Como resultado del progreso tecnológico, y el aumento de la delincuencia cibernética demandan enfoques innovadores y herramientas efectivas para la investigación y el análisis forense de evidencia digital. En este contexto, la norma ISO 27037:2012 emerge como un recurso fundamental que puede revolucionar la capacidad de la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú para abordar estos de manera más eficiente y precisa.

La norma ISO 27037:2012 establece directrices y principios para la identificación, adquisición, preservación y análisis de evidencia digital con el fin de mejorar la calidad y la eficiencia de los procesos de análisis forense. En este contexto, la norma actúa como un marco de referencia que puede influir en la forma en que se lleva a cabo el análisis informático forense.

El análisis informático forense se refiere al proceso de recolección, preservación, examen y presentación de evidencia digital con el propósito de investigar y prevenir delitos cibernéticos. Esta variable es crucial en la División de Investigación de delitos de alta tecnología, ya que la efectividad de sus operaciones depende en gran medida de la calidad y la integridad de este análisis.

La importancia de esta investigación radica en la creciente amenaza de delitos cibernéticos y la necesidad de mejorar constantemente las capacidades de las instituciones encargadas de combatirlos. La implementación de la norma ISO 27037:2012 podrá representar un avance significativo en la eficiencia y la confiabilidad del análisis informático forense, fortaleciendo así la capacidad de la policía para abordar los delitos de alta tecnología de manera más efectiva.

Esta investigación se llevó a cabo con el propósito de contribuir al avance de las prácticas de análisis informático forense en un contexto específico, como es la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú. La intención es ofrecer una visión más clara sobre cómo la implementación de la norma ISO 27037:2012 puede impactar positivamente en este ámbito.

La tesis que se presenta tiene como objetivo central explorar el impacto y la aplicabilidad de la norma ISO 27037:2012 en el contexto de la investigación de delitos en alta tecnología en Perú. A lo largo de este trabajo, examinaremos en detalle los principios y directrices establecidos por esta norma internacional, su relación con las mejores prácticas en análisis informático forense, y cómo su adopción puede mejorar la capacidad de la policía para recolectar, preservar, analizar y presentar pruebas digitales en procesos judiciales.

Con la creciente dependencia de los dispositivos electrónicos, y las amenazas cibernéticas se multiplican, la necesidad de contar con enfoques avanzados y consistentes en la indagación de infracciones de aceptación *know-how* es más apremiante que nunca. Esta tesis se propone como un aporte significativo en la búsqueda de soluciones que permitan a la Policía Nacional del Perú mantenerse alerta en la disputa hacia la infracción analógica, al tiempo que garantiza la integridad de las pruebas y protección de las libertades fundamentales de los ciudadanos.

Al concluir la lectura de esta tesis, se espera que el lector obtenga una comprensión integral de la relación entre la implementación de la norma ISO 27037:2012 y la mejora del análisis informático forense en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú.

La investigación se llevó a cabo en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima, durante el año 2022. La muestra incluirá datos

recopilados de casos específicos de delitos de alta tecnología, con un enfoque en la implementación de la norma ISO 27037:2012 y su impacto en el proceso de análisis informático forense. La cantidad de datos abarcará un período representativo que permita una evaluación exhaustiva de la influencia de la norma en el análisis forense.

1.1. Planteamiento del problema

Se logra prestar atención a nivel internacional que, detectar, preservar, evaluar y presentar material válido dentro de un procedimiento legal requiere el uso de sofisticadas herramientas científicas y analíticas, que es en lo que consiste el análisis informático forense. Este campo de estudio tiene sus raíces en los primeros días de los sistemas integrados, pero ha progresado en varias direcciones desde entonces. Aunque los equipos digitales y la informática son excelentes ejemplos de la llamada globalización, el sistema jurídico de cada país requiere un enfoque diferente de la informática forense.

Es así como, en el mundo actual de la alta tecnología, muchas tecnologías digitales han hecho la vida más fácil al facilitar una comunicación rápida y sencilla; sin embargo, los mismos medios electrónicos que han contribuido a esta mejora de nuestro nivel de vida también han sido utilizados por los delincuentes. Así, la investigación y el análisis de las pruebas digitales dieron lugar a una nueva disciplina conocida como análisis informático forense. Pero dado que las violaciones de la seguridad afectan a gran cantidad en el mundo, el área de ciencia forense digital acaba de ganar gran protagonismo.

Razón por la cual, Peña y Orellana (2015), sostienen que, debido a la naturaleza omnipresente de las violaciones de seguridad, el análisis forense ha surgido como un subcampo distinto de la seguridad informática. El modo y el lugar en que se utilizan y guardan los medios digitales en los ordenadores evolucionan constantemente junto con los avances tecnológicos.

Por otro lado, se ha podido observar también que, el aumento de la variedad de incidentes relacionados con la seguridad de la información hizo necesario el desarrollo del análisis forense, que implica la aplicación y el perfeccionamiento de una serie de técnicas que permiten reconstruir un activo informático y evaluar su vulnerabilidad para preservar la autenticidad de los datos.

De esta manera, los ciberataques, la pornografía infantil, la extorsión, la filtración de información secreta y otros sucesos ilegales de seguridad son cosas a las que están expuestos algunos sistemas telemáticos; el análisis forense es un intento de mitigar estos peligros. Sobre todo, como parte del plan para hacer cumplir el ISO 27037:2012.

Al respecto, Sullivan (2022) sostiene que, "en cualquier investigación, lo más importante a salvaguardar es el propio elemento tecnológico, ya que contiene pruebas" (p. 36). La informática forense es capaz de descubrir los delitos informáticos, ya que el propio equipo contiene pruebas relevantes para la investigación. Con el fin de salvaguardar la información contenida en los ordenadores, los dispositivos de almacenamiento de archivos digitales, los componentes de comunicación y los teléfonos móviles, la informática forense puede detectar intrusiones. a pesar de cualquier cambio previo que se haya realizado en él.

La Norma ISO 27037:2012 está claramente enfocada sobre los procesos o procedimientos de actuación en el campo pericial, enfocándose en la recogida, la identificación y el manejo de la certeza analógica, sin ingresar a la etapa de estudios de certeza. Ya que, la honradez de los ensayos analógicos debe protegerse en la medida de lo posible a lo largo de la recogida, y deben hacerse copias de seguridad siempre que sea posible.

Dentro de la Norma ISO 27037:2012, según León et al. (2021) se deben utilizar buenas prácticas profesionales para validar y contrastar los procesos seguidos y la documentación elaborada. Todos los pasos dados y sus resultados deben estar documentados y disponibles para

su inspección. Así, las técnicas y procesos utilizados deben ser lo suficientemente repetibles, observables y discutibles como para que los expertos en la materia avalen el trabajo como legítimo. Para ello, el equipo debe estar reconocido, y debe haber sido probado y comparado para garantizar que es adecuado para la tarea en cuestión.

En el ámbito latinoamericano, en el país argentino, Según Presman (2016) la investigación de dispositivos digitales presenta desafíos técnicos universales, pero en el contexto argentino, surgen complicaciones adicionales relacionadas con el funcionamiento de laboratorios forenses y su coordinación con la justicia. Por lo que se destaca la necesidad de un esfuerzo conjunto entre operadores judiciales, jueces, fiscales, secretarios de juzgados, ingenieros y peritos para el éxito de la informática forense. Aunque se percibe un inicio de colaboración, el experto señala problemas estructurales como la falta de presupuesto, recursos y proyectos, así como esfuerzos aislados entre provincias. Estos obstáculos dan lugar a una situación típicamente argentina, donde la sensación de que cada entidad trabaja de manera independiente obstaculiza el avance en el análisis informático forense.

A nivel nacional, la Defensoría de Pueblo indicó que, la falta de un análisis informático forense adecuado ha provocado que los delitos por internet tengan aumento, ya que el aumento alarmante de la explotación sexual en línea de niños y niñas es evidente según las encuestas de Capital Humano y Social Alternativo (CHS Alternativo). Entre 2018 y 2021, los riesgos percibidos por padres y madres aumentaron del 25% al 62%, mientras que la recepción de mensajes de contenido sexual en internet pasó del 5% al 10%. A pesar de la gravedad de estas situaciones, el 33% de los progenitores admite desconocer cómo o dónde realizar denuncias. Este problema resalta la necesidad urgente de concienciación y medidas efectivas para proteger a los menores en línea. (Castillo 2023)

Durante los últimos cinco años, la Policía Nacional ha experimentado un marcado aumento en las denuncias de ciberdelitos, específicamente aquellos contemplados en la Ley de delitos informáticos. Entre 2018 y 2021, se observa una notable cuadruplicación, pasando de 3,031 a 12,827 denuncias. Este incremento se traduce en un aumento significativo de la tasa de ciberdelitos por cada 100 mil habitantes, que ha escalado del 10% al 39%. Este fenómeno destaca la urgente necesidad de mejorar las capacidades de análisis informático forense en la División de investigación de delitos de alta tecnología de la Policía para abordar eficazmente esta creciente problemática. (Castillo, 2023)

En el año 2021, Lima Metropolitana y Lima Provincias fueron los principales lugares donde la Policía Nacional recibió la mayoría de denuncias por delitos informáticos, representando el 53% del total de denuncias. La concentración de denuncias aumenta a 71% cuando se incluye en el cálculo al Callao y tres regiones de la costa norte (La Libertad, Lambayeque y Piura). Por el contrario, Arequipa y Cusco, ambas ubicadas en la región sur de la nación, fueron responsables del 8% de las quejas. Estos hechos, confirmados por el Ministerio Público, revelan una grave situación. De acuerdo a los resultados de la investigación forense, la zona de Lima fue responsable del 53,08% de los delitos cibernéticos clasificados como de alto riesgo en el año 2021. En segundo lugar, se ubican Arequipa (5,71%), La Libertad (5,01%) y Lambayeque (4,27%). Esta situación pone en evidencia la importancia de mejorar las capacidades de la División de investigación de delitos de alta tecnología de la policía para manejar adecuadamente este creciente problema. (Castillo, 2023)

Por otro lado, en el mismo estudio realizado por la Defensoría del Pueblo, indica que la estructura interna de los Depincri–PNP se compone principalmente de secciones de investigación criminal e inteligencia, representando el 100% y 88%, respectivamente. Además, el 22% incorpora una sección de criminalística. Es relevante destacar que un 36% de las

secciones de investigación criminal poseen áreas especializadas según el tipo de delitos, especialmente aquellos relacionados con la vida, el cuerpo, la salud, el patrimonio, la libertad personal, la trata de personas y el tráfico ilícito de drogas. Esta configuración actual plantea un desafío significativo para mejorar el análisis informático forense en la División de investigación de delitos de alta tecnología de la Policía, dado el énfasis en la variedad de delitos y la falta de enfoque específico en la esfera tecnológica.

Asimismo, en tan solo el 9% de las Depincri–PNP, específicamente en Cajamarca, Chiclayo, Cusco, Ilave y Madre de Dios, se ha establecido un área dedicada a la ciberdelincuencia. Este reducido porcentaje se traduce en un personal que varía entre 2 y 14 efectivos. La falta de una presencia más amplia y especializada en el ámbito de la ciberseguridad en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú plantea un desafío significativo para mejorar el análisis informático forense en la institución.

Por otro lado, la supervisión de las unidades de investigación de ciberdelitos en diversas ciudades reveló disparidades en la preparación técnica del personal. En Cajamarca, Chiclayo y Madre de Dios, suboficiales de armas con formación en tecnologías de la información lideran la tarea, mientras que, en Cusco, solo un suboficial posee dicha especialidad. Además, el 16% de las unidades analizadas organizan actividades de capacitación en ciberdelincuencia, abordando aspectos legales, técnicas de investigación y evidencia digital. En Chiclayo, Huancayo y Leoncio Prado, se involucra a especialistas de la Divindat–PNP, mientras que en Tacna y San Juan de Lurigancho II, colaboran con el sistema educativo policial. Estos hallazgos resaltan la necesidad de estandarizar la formación y colaboración interinstitucional para fortalecer la capacidad de análisis informático forense en la División de investigación de delitos de alta tecnología de la Policía. (Castillo, 2023)

1.2. Descripción del problema

Se ha podido observar a través de una observación sistemática que, el análisis informático forense dentro del departamento de la Policía Nacional del Perú especializado en indagación tecnológica, Lima, no se desarrolla adecuadamente. Ya que, mencionada institución no cuenta con un procedimiento sostenible sobre los análisis forenses dentro del manejo de los dispositivos móviles o celulares.

Esto debido a que, las diversas incidencias informáticas, no se registran adecuadamente en las computadoras y servidores. No se hace uso de plataformas digitales para el almacenamiento, manejo offline y online de la información relevante sobre diversos casos. De esta manera, existe una deficiencia en cuanto al manejo de la información, al tratamiento de la misma y sobre todo la relevancia de cada dato dentro de un proceso legal.

Para Raja (2021) “al no tener un manejo definido sobre los procedimientos forenses de análisis de información utilizando métodos modernos de transmisión y almacenamiento, se expone el método de justicia para cualquier atentado informático” (p. 36). Sin estos mecanismos puestos en práctica, los analistas forenses no pueden desarrollar sus análisis respectivos ante un hecho o fenómeno cibernético o informático. Es decir, sin un adecuado proceso de análisis informático forense, se corre el riesgo de dejar a la incertidumbre los procesos legales.

Sin embargo, en la Sección de Investigación sobre Delitos en Tecnología Especializada de la Policía Nacional de Perú, en Lima, existe un desconocimiento sobre el correcto uso metodológico del análisis informático forense, además existe una orfandad cognitiva sobre los procedimientos para este análisis. Esta deficiencia se refleja en los procedimientos incompletos para la revisión del material o evidencia digital.

En la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, se enfrenta a una problemática significativa en el ámbito del análisis informático forense. La falta de un marco normativo sólido y específico para guiar y estandarizar este proceso ha generado ineficiencias y limitaciones en la obtención, preservación y análisis de evidencia digital. La ausencia de directrices claras ha llevado a prácticas heterogéneas y a la falta de uniformidad en los métodos utilizados, lo que impacta directamente en la efectividad de las investigaciones de delitos de alta tecnología.

La carencia de un enfoque estandarizado en el análisis informático forense en la División de investigación de delitos de alta tecnología ha generado una falta de alineación con las normas internacionales, específicamente con la ISO 27037:2012. Esta norma proporciona directrices detalladas para la gestión de evidencia digital, estableciendo procesos y prácticas que garantizan la integridad y autenticidad de la información recolectada. Sin embargo, la falta de implementación efectiva de estas normas en la práctica diaria de la división ha resultado en una desconexión con las mejores prácticas internacionales, limitando la calidad y confiabilidad de las investigaciones.

Estas dificultades son originadas por falta de conocimientos sobre el análisis informático forense dentro de la División de investigación de delitos de alta tecnología en la Policía Nacional del Perú, Lima. Además, otro factor presente dentro de esta problemática, es la falta de una guía actualizada sobre la temática y, además, debido a ciertos desperfectos en los softwares y a la contaminación de la evidencia digital.

La persistencia de la falta de alineación con la ISO 27037:2012 tiene consecuencias graves para la División de investigación de delitos de alta tecnología. En primer lugar, la calidad de las investigaciones se ve comprometida, ya que la ausencia de un enfoque estandarizado dificulta la obtención de pruebas digitalmente válidas. Esto no solo puede

resultar en la pérdida de casos judiciales, sino que también impacta la confianza pública en la capacidad de la policía para abordar delitos de alta tecnología. Además, la falta de cumplimiento con normas internacionales podría tener implicaciones legales y éticas, poniendo en riesgo la validez de las evidencias presentadas en los tribunales y debilitando la credibilidad de la División en el ámbito nacional e internacional. En última instancia, la persistencia del problema puede socavar la efectividad general de la División de investigación de delitos de alta tecnología, debilitando su capacidad para abordar de manera eficiente y eficaz los delitos relacionados con la tecnología.

En suma, estos hechos observados, ha posibilitado el desarrollo del presente estudio científico. Para lo cual, se ha formulado la próxima gran pregunta de la ciencia:

1.3. Formulación del problema

1.3.1. Problema general

¿Cómo influye el ISO 27037:2012 en la mejora del análisis informático forense en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022?

1.3.2. Problemas específicos

a. ¿Cuál es la influencia del ISO 27037:2012 en la mejora de los tiempos de trabajo en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022?
b. ¿Cuál es la influencia del ISO 27037:2012 en la mejora de la extracción de datos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022?

c. ¿Cuál es la influencia del ISO 27037:2012 en la mejora del número de casos resueltos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022?

1.4. Antecedentes

1.4.1. Antecedentes internacionales

Du (2020) realizó un trabajo de investigación titulado: Alleviating the digital forensic Backlog a Methodology for automated digital evience processing. El investigador centró su estudio en desarrollar una metodología para el procesamiento automatizado de pruebas digitales, utilizando una técnica de duplicación de datos con el objetivo de abordar el desafío de analizar grandes volúmenes de información. Según los resultados de su investigación, esta técnica facilita la clasificación automática de las pruebas almacenadas, lo que ayuda a los investigadores a descubrir nuevos datos que no se habían identificado previamente. La técnica de reconstrucción forense implementada por el investigador contribuye a verificar la integridad del sistema de adquisición de datos de duplicados. Además, su sistema elimina la necesidad de procesar datos de forma repetida y determina automáticamente qué archivos son relevantes para la investigación. Los archivos identificados proporcionan pistas valiosas para el resto de la investigación y ayudan en la recopilación de información sobre cómo ocurrió el incidente en el dispositivo.

Cuomo et al. (2022). El informe tiene como propósito abordar diversas situaciones en las que se puede recuperar evidencia digital de dispositivos móviles, manteniendo su relevancia legal. Los autores, basándose en su extensa experiencia en el campo durante la última década y su análisis de casos judiciales reales, han desarrollado una metodología rigurosa para la informática forense móvil, que se detalla en el artículo. Al examinar la muestra a través de pruebas de laboratorio controladas, compararon dos enfoques principales de extracción de

datos digitales de teléfonos móviles (repetibles y no repetibles) para producir evidencia admisible en procedimientos legales. Los resultados mostraron que incluso en extracciones forenses realizadas en períodos muy cortos, se identificó la presencia constante de archivos sujetos a modificaciones. Aunque se descubrieron archivos modificados, la investigación concluye que la estructura de evaluaciones técnicas repetibles puede guiar adecuadamente la recopilación de datos generados por el usuario en dispositivos móviles para fines forenses.

Kigwana et al. (2018). El propósito de este estudio es abordar la carencia de una arquitectura conocida de Preparación Forense Digital (DFR) aplicable a la recopilación de información relevante durante exámenes en línea. Se busca desarrollar una Arquitectura de Preparación Forense Digital para Exámenes en Línea (OEDFRA) y explorar su impacto en DFR. Para alcanzar nuestro objetivo, se seguirá la metodología establecida por la norma ISO/IEC 27043:2015 para principios y procesos de investigación de incidentes. Se propondrá y explicará detalladamente el diseño de la OEDFRA, utilizando metodologías actuales de DFR aplicadas a entornos de exámenes en línea. La muestra de este estudio incluirá instituciones educativas que ofrecen exámenes en línea, donde se implementará la OEDFRA. Se seleccionaron participantes que representen diversas condiciones y contextos para obtener una perspectiva integral de la efectividad de la arquitectura propuesta. Se recopilarán datos de respuesta a incidentes y se evaluará la implementación de la OEDFRA en entornos reales de exámenes en línea. Se analizarán los resultados para determinar la eficacia de la arquitectura en la mejora de la DFR durante tales situaciones. Basándonos en los resultados obtenidos, se elaborarán conclusiones sobre la viabilidad y utilidad de la OEDFRA en la mejora de la Preparación Forense Digital durante exámenes en línea. Además, se discutirán posibles implicaciones y áreas para futuras investigaciones en este campo.

Santillán y Haro (2021) realizaron un trabajo de investigación titulado: Técnicas de seguridad en redes de comunicaciones aplicadas a la custodia de evidencia digital. A medida

que las nuevas tecnologías se expanden en las organizaciones, con una creciente influencia de la transformación digital, surgen desafíos de seguridad que implican la identificación de amenazas y ataques cada vez más sofisticados. La detección de vulnerabilidades y amenazas ha llevado a los profesionales de ciberseguridad a adoptar nuevos métodos y técnicas, respaldados por herramientas que aseguren la aceptación de la evidencia digital a corto y largo plazo. Este proyecto se centra en la implementación de técnicas de seguridad en las redes de comunicación para garantizar una adecuada custodia digital. Para abordar la pregunta de investigación planteada, se ha diseñado un proceso de cuatro etapas: investigación del estado actual de la tecnología, descripción de metodologías y técnicas de seguridad aplicadas en las redes de comunicación, evaluación de las metodologías utilizadas por los actores del sistema judicial y síntesis de las buenas prácticas aplicadas en las técnicas apropiadas para la custodia de la evidencia digital en redes. La parte fundamental de este proyecto se centra en el diagnóstico realizado a los principales actores del Consejo de la Judicatura de la provincia de Chimborazo, revelando la carencia de conocimientos, metodologías, técnicas y recursos necesarios para preservar y admitir la evidencia digital. Esto crea una vulnerabilidad significativa que facilita a los ciberdelincuentes el acceso, alteración, modificación o destrucción de la información.

Coronel (2019) investigó sobre: *Metodología en recolección de evidencia forense generada en la utilización de aplicaciones desplegadas en entornos virtuales*. En referido estudio se pudo concluir que, el número de denuncias y delitos cometidos a través de aplicaciones web también ha aumentado recientemente, destacando el hecho real la necesidad de un manual en el que se detallen las técnicas forenses digitales con fines de la tramitación de pruebas electrónicas procedentes de entornos en línea. Además, se concluyó que, uno de los mayores retos del uso de aplicaciones web es averiguar si se puede o no acceder a ciertos datos debido al lugar en el que se encuentra uno geográficamente. Por ello, realizar una investigación

de escritorio es una posible alternativa para llevar a cabo una auditoría de la información adecuada (lado del cliente). Se podrían haber extraído sugerencias y procedimientos estándar de la metodología y la investigación empírica, pero a menudo están adaptados a un conjunto reducido de páginas web y, por tanto, no pueden utilizarse universalmente.

Roatta et al. (2020) desarrollaron un estudio científico titulado: El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012. En referido estudio se afirma que, las pruebas digitales debidamente procesadas tienen una amplia gama de aplicaciones potenciales. Cada enfoque adopta un enfoque algo diferente en cuanto al objetivo final, que puede ser elevar el nivel de la prueba, un análisis más preciso, la restauración del servicio o la reducción de los costes de recogida de pruebas. Se pudo concluir que, la credibilidad del estudio estriba en gran mesura de la metodología de la investigación y de la experiencia de las personas que han trabajado para construir esa técnica. Este documento proporciona normas para el manejo de las pruebas digitales, normalizando su recogida, procesamiento y almacenamiento. Estos procedimientos se ajustan a la norma ISO/IEC 27037:2012 y tienen por objeto preservar la veracidad de las pruebas utilizando una forma que pueda ser aceptada en los tribunales.

Pomar (2021) realizó un trabajo de investigación titulado: Propuesta de investigación: Modelo de análisis forense digital para el sistema de negociación electrónico de la Bolsa Boliviana de Valores, basado en la Norma ISO/IEC 27037:2012. En referido estudio se concluye que, a la luz de las recomendaciones realizadas en la norma técnica IS0/IEC 27037:2012, este artículo analiza un modelo de análisis forense digital que puede ser entrenado para hacer frente a cualquier tipo de amenaza basada en incidentes de información crítica. Se logró reunir las pruebas suficientes y necesarias que puedan ser utilizadas como evidencia y prueba en los tribunales. Esta especificación detalla cómo debe proceder una organización para localizar, reunir, adquirir y almacenar las pruebas digitales.

Bismark (2021) realizó una investigación científica titulada: *Modelo Para Tratamiento Forense de Incidentes Informáticos en la Nube*. En referida investigación se concluyó que, gracias a la computación en nube, las empresas pueden ahora ofrecer más servicios a más personas, gastando menos en los equipos necesarios y facilitando a esas personas el acceso a Internet. El aumento de la accesibilidad de diversos servicios ha dado lugar al almacenamiento de datos sensibles en la infraestructura de la nube, lo que figura que las filiaciones vitales se guardan en los donados de los despenseros de valores y son vulnerables a la delincuencia. En caso de que se produzca un percance informático, puede ser necesario un proceso legal que incluya los esfuerzos de los administradores legales y los profesionales de la informática. Este artículo analiza el estado del análisis forense en Bolivia, los estándares actuales y los problemas únicos a los que se enfrentan los expertos forenses en la nube.

Antunes et al. (2021). El propósito de este estudio es explorar las suposiciones arraigadas en el delito convencional, utilizando evidencia y artefactos a lo largo de la historia humana. Además, se busca examinar la legislación que respalda la condena de infractores basándose en la prueba de culpabilidad por un delito específico. La metodología empleada se centra en el uso de tecnología digital, especialmente cámaras de circuito cerrado (CCTV), para vincularse con delitos tradicionales. Se abordarán las dificultades asociadas con la baja resolución y la iluminación insuficiente en áreas específicas de los videos de CCTV. Además, se implementarán tecnologías como Adobe Lightroom para realizar alteraciones visuales en el análisis. La muestra en consideración abarca evidencia digital derivada de videos de CCTV. La baja resolución y problemas de iluminación en ciertas áreas de los registros dificultan la evaluación de la calidad de la grabación, lo cual será abordado en el análisis. Los resultados esperados incluyen la validación de suposiciones sobre la actividad criminal a través de la evidencia digital obtenida de los videos de CCTV. Se anticipa que las dificultades relacionadas con la calidad de la grabación serán atenuadas mediante el uso de tecnologías como Adobe

Lightroom. En conclusión, este estudio utiliza el enfoque estático forense, implementando la informática forense y protocolos para el manejo de evidencia digital. Se espera que los resultados obtenidos contribuyan a una comprensión más profunda de la relación entre la tecnología digital y la resolución de crímenes tradicionales.

Rizdqi et al. (2022) desarrollaron un estudio científico titulado: Digital Forensics: Acquisition and Analysis on CCTV Digital Evidence using Static Forensic Method based *on ISO /IEC 27037:2014.* Referido estudio pudo concluir que, las preguntas: qué, dónde, dónde, por qué, quién y cómo son las preguntas estándar utilizadas en la ciencia forense digital. Además, el tipo de delito se está cometiendo, dónde se está cometiendo, cuándo se está cometiendo, por qué se está cometiendo, quién es el sospechoso y quiénes son las víctimas, y cómo se lleva a cabo la estrategia del delito desde la perspectiva de los delincuentes, y cómo, los métodos, los métodos de análisis, los derechos de acceso legales para manejar los indicios desde la perspectiva del investigador. Así mismo, la investigación y el análisis de las pruebas digitales se producen sobre todo en dos etapas: la de preadquisición y la de adquisición del núcleo. La noción de cadena de custodia es esencial en las investigaciones forenses digitales porque garantiza la legitimidad de las pruebas desde el momento en que se descubren y recogen hasta el momento en que se denuncian. La veracidad e integridad de las pruebas puede demostrarse, técnicamente hablando, mediante la determinación de su valor hash. La capacidad de incorporar elementos multimedia en el análisis de las tentativas analógicas es especialmente significativa cuando se trata de pruebas en forma de CCTV.

Ibtesam (2019) en su tesis de doctorado denominado “Métodos y factores que afectan la gestión, asignación y finalización de casos forenses digitales”. Este estudio aborda el creciente número de casos forenses digitales en los departamentos y secciones del DF. Analiza datos de casos de la policía de Dubai para determinar patrones y dificultades que influyen en las horas del personal de investigación. También busca técnicas de asignación y gestión de

casos para prepararse para cuestiones de investigación forense digital. Tres investigaciones sucesivas componen la investigación. La primera investigación cuantifica los datos de la policía de Dubai para analizar el crecimiento de los casos y determinar las causas principales de los retrasos en las investigaciones del DF. La segunda investigación utiliza entrevistas cualitativas con gerentes de DF en todo el mundo para examinar las causas del retraso en la investigación. En tercer lugar, la investigación verifica las entrevistas utilizando un enfoque fenomenológico, concentrándose en la gestión de casos y la implementación de procesos. Los datos secundarios de la base de datos de la policía de Dubai proporcionan una visión cuantitativa de la primera fase. La segunda investigación comprende entrevistas cualitativas con administradores de ciencia forense digital en todo el mundo. La tercera prueba de investigación evalúa la asignación de casos y las opciones de implementación de procesos con participantes elegidos. Las entrevistas cualitativas descubren causas típicas de retrasos en las investigaciones, mientras que los estudios cuantitativos muestran patrones y problemas de crecimiento de los casos forenses digitales. Estas entrevistas evalúan los métodos de implementación del flujo de trabajo y la gestión de casos, lo que demuestra la gama de soluciones utilizadas en todo el mundo. Según el informe, el aumento de la cantidad de datos y la complejidad de los casos retrasan las investigaciones forenses digitales. Además, se destacan los métodos de gestión de casos que abordan estas cuestiones. Las tablas de decisión sugeridas permiten a los administradores del DF elegir técnicas adecuadas en diferentes escenarios, impulsando las operaciones de investigación forense digital en todo el mundo.

Karagiannis y Vergidis (2021) en su estudio titulado “Evidencia digital y análisis forense en la nube: desafíos legales contemporáneos y el poder de eliminación”. Este artículo aborda exhaustivamente las cuestiones prácticas y jurídicas de la investigación de actos delictivos mediante la ocultación de datos esenciales en la nube. La principal contribución fue poner de relieve la complejidad de este problema y abogar por una solución eficaz mediante el

entendimiento y la cooperación internacionales. Se utilizó una metodología descriptiva con un enfoque mixto y un diseño no experimental. El enfoque pretende proporcionar una comprensión clara de las cuestiones prácticas y jurídicas mediante la incorporación de diversas perspectivas y teorías de varios sistemas jurídicos. Debido al creciente uso de Internet, se necesita jurisprudencia sobre la manipulación de juicios en línea. Destaca la necesidad de mitigar la ciberdelincuencia en la nube, considerando el ciberespacio la "última frontera" por explorar y regular a escala mundial. En la actualidad, las autoridades se enfrentan a retos en una zona jurídica ambigua, aplicando doctrinas nacionales en un contexto internacional, promoviendo enfoques colaborativos y normativas globales.

Parvis (2022) en su estudio doctoral denominado “Investigación empírica del proceso de recuperación de pruebas en la investigación forense digital”. El aumento del uso de medios digitales para cometer delitos y la constante expansión de la capacidad de almacenamiento han provocado retrasos en los laboratorios forenses digitales. Esta investigación aborda estas cuestiones. En casos de gran repercusión, los procesos judiciales exigen una investigación exhaustiva de los medios digitales, lo que resulta poco práctico. Se analizaron casos forenses policiales anteriores con cinco etapas forenses para determinar el enfoque. En cada caso se describió el tiempo empleado en cada etapa y las pruebas encontradas. Para determinar los parámetros de recuperación de artefactos probatorios, se utilizaron estadísticas descriptivas convencionales y regresión lineal. Los casos forenses policiales anteriores tenían cinco fases forenses bien definidas. Los datos sobre la duración de cada fase y la recuperación de pruebas proporcionaron una buena base para la investigación empírica. Los análisis estadísticos descriptivos y la regresión lineal produjeron modelos para futuros análisis forenses. La identificación de elementos en la recuperación de artefactos probatorios ayuda a identificar obstáculos y a mejorar los métodos forenses digitales. Esta investigación define cada proceso forense, eliminando la incertidumbre del examen. La información obtenida ayuda a los

examinadores forenses a decidir la profundidad del análisis, reduciendo los retrasos en los laboratorios forenses digitales. Los modelos descritos pueden mejorar las investigaciones forenses digitales en casos criminales de alto perfil y hacer avanzar las técnicas forenses.

Horsman (2021) en su estudio denominado "Estandarización de los procedimientos de examen forense digital: una mirada a Windows 10 en casos que involucran imágenes que representan abuso sexual infantil". El estudio aborda la estandarización operativa de la ciencia forense digital. La estandarización puede aumentar la confiabilidad, la coherencia y el control de calidad en esta industria especializada; por tanto, el objetivo principal es evaluar su necesidad y viabilidad. Los especialistas en forense digital deben crear modelos para establecer métodos operativos basados en el delito, el dispositivo y el sistema operativo. Para respaldar esta idea, se muestra y explora un estándar de ejemplo que especifica los criterios de inspección de dispositivos Windows 10 para fotografías de abuso sexual infantil. La muestra del estudio examina dispositivos con Windows 10 y fotografías de agresión sexual infantil. Podemos demostrar la practicidad de los estándares propuestos usando este ejemplo. Los hallazgos enfatizan la necesidad de una estandarización de la ciencia forense digital y de modelos que tengan en cuenta el tipo de delito, el dispositivo y el sistema operativo. La presentación y el análisis del estándar de ejemplo muestran las necesidades mínimas de inspección del dispositivo en ciertos escenarios. Aunque sea difícil, la estandarización de la ciencia forense digital es necesaria para garantizar la confiabilidad y coherencia profesionales. Para mejorar la calidad operativa y la armonización, las personas en esta industria deben continuar creando e implementando modelos como el proporcionado.

Dong y Zhang (2023) en su trabajo de maestría "Investigación forense digital de sistemas automotrices: requisitos y desafíos". Este proyecto tiene como objetivo resolver los problemas futuros de seguridad de los vehículos, particularmente a medida que la arquitectura y las conexiones de los vehículos se vuelven más complicadas. Los ciberataques y las fallas de

hardware y software (intencionales y accidentales) pueden generar contratiempos. Para establecer la causa de estos accidentes, investigaremos la ciencia forense digital automotriz (ADF). El proceso comprende una evaluación exhaustiva de la literatura automotriz y relacionada. Los procesos forenses, las reglas, los estándares, el cumplimiento de la seguridad y la extracción y verificación de datos son partes clave. El ADF carece de reglas y estándares consistentes; por lo tanto, esta evaluación está sentando una base firme. Además, presentamos un marco completo del ciclo de vida de la ciencia forense digital automotriz. La muestra incluye la industria automotriz y la investigación asociada sobre ciberseguridad, problemas de hardware y software y análisis forense de vehículos. La variedad de fuentes ayuda a explicar los problemas y las soluciones del ADF. Los hallazgos muestran que la ciencia forense digital automotriz carece de estándares y criterios consistentes, lo que dificulta determinar las causas de accidentes relacionados con la tecnología del automóvil. Se definen las técnicas, normas y estándares forenses aplicables al ADF y se enfatiza un enfoque uniforme. Se concluyó que, los ciberataques y los fallos técnicos hacen que la seguridad del coche sea crucial. Para abordar la ausencia de normas y estándares uniformes en la ciencia forense digital automotriz, proponemos un marco para todo el ciclo de vida. Esta estrategia unida puede impulsar la seguridad de los vehículos y la investigación de accidentes.

Guzmán (2023) realizó un trabajo de investigación titulado: Implementación de herramientas para la extracción de evidencia digital. Los progresos tecnológicos han generado una rápida adopción de las Tecnologías de la Información, dando lugar al aumento de los delitos informáticos, como el fraude, el lavado de dinero y el robo de información, entre otros. Ante este escenario, resulta esencial contar con guías metodológicas que capaciten a los agentes policiales para abordar este problema utilizando evidencia sólida respaldada por la legislación vigente. Ecuador no ha quedado al margen de esta realidad, y en este trabajo de integración curricular se indaga sobre la normativa internacional para el manejo de evidencia digital,

destacando la ISO 27037, RFC 3227 y UNE 71505. Asimismo, se explora la existencia de normativa a nivel local. A partir de este análisis, se examinan las metodologías utilizadas en otros países y a nivel local para la extracción de evidencia digital, presentando aquellas que han sido adoptadas internacionalmente o que se proponen con ese propósito. Un elemento crucial a considerar son las herramientas que facilitan la obtención de dichas evidencias, y para ello se ha llevado a cabo un análisis de estas, teniendo en cuenta su costo, así como sus ventajas y desventajas. Con el fin de observar su funcionamiento, se han implementado en un entorno que refleja la realidad actual.

Riggs et al. (2023). Este artículo tiene como objetivo principal proporcionar un resumen detallado de los ciberataques más significativos dirigidos a instalaciones esenciales en las últimas dos décadas. Se busca analizar la naturaleza de estos ataques, sus repercusiones, las vulnerabilidades identificadas, así como identificar a las víctimas y los perpetradores involucrados. Además, se busca destacar estándares y herramientas de ciberseguridad como medidas preventivas. La metodología empleada se centra en la recopilación y análisis exhaustivo de datos relacionados con ciberataques a infraestructuras vitales. Se ha llevado a cabo una revisión de casos relevantes ocurridos desde principios de la década de 2000. La información recopilada se utiliza para categorizar los tipos de ataques, evaluar sus consecuencias y analizar patrones comunes. Se presta especial atención a la identificación de vulnerabilidades explotadas y a la relación entre los ataques y sus impactos en la seguridad cibernética. La muestra utilizada comprende una amplia gama de ciberataques a nivel mundial, dirigidos a servicios esenciales y causantes de interrupciones significativas. Se han considerado casos que afectan a diversas industrias y se ha prestado atención a la exposición masiva de información privada debido a filtraciones de datos. La muestra incluye eventos desde principios de la década de 2000 hasta la fecha actual. Los resultados obtenidos a través del análisis detallado de la muestra revelan patrones consistentes en los ciberataques a infraestructuras

vitales. Se identifican tipos específicos de ataques, se cuantifican las repercusiones financieras y se destacan las vulnerabilidades más comunes. Además, se presentan estándares y herramientas de ciberseguridad como parte de los resultados para abordar estas problemáticas. Basándonos en los resultados obtenidos, se concluye que la amenaza de ciberataques a instalaciones clave es significativa y está en aumento. Se proyecta que, en los próximos cinco años, el número de incidentes aumentará drásticamente a escala global, superando los 1,100 ciberataques importantes. La necesidad de implementar medidas de ciberseguridad más robustas se destaca como crucial para mitigar estas amenazas y proteger la integridad de las infraestructuras esenciales a nivel mundial.

Jahankhani y Ibarra (2019). El rápido crecimiento de la computación en la nube, las tecnologías inteligentes como el Internet de las Cosas Médicas (IoMT) y los avances en inteligencia artificial y aprendizaje automático han generado un aumento significativo en los volúmenes de datos. Esto ha llevado a una mayor complejidad en los desafíos asociados con la seguridad y gestión eficiente de estos datos. Se busca comprender y abordar las implicaciones de este escenario, centrándose en fenómenos como el ransomware como servicio y la organización cada vez más sofisticada de ciberdelincuentes. Se examinaron diversas medidas implementadas por las empresas para reducir el riesgo cibernético, incluyendo revisiones regulares de políticas y cumplimiento, capacitación de empleados, parches de software y la implementación de sistemas de detección y prevención de intrusiones (IDPS). Además, se exploró la tendencia emergente hacia la adopción de innovaciones en software y sistemas, junto con la creciente mentalidad de "datos a pedido". Se puso especial atención en los avances en inteligencia artificial y aprendizaje automático como facilitadores de estas innovaciones. Se analizó un conjunto de datos que abarcó la diversidad de sectores afectados por ciberataques, con un énfasis particular en el sector de la salud. Se consideró información relevante sobre violaciones cibernéticas, sus variaciones en términos de tipo y frecuencia, y cómo estas

afectaron a los clientes y sus datos. Se identificó un aumento notable en la variedad y frecuencia de los ciberataques, destacando que más del 50% de estos incidentes ocurren en el sector de la salud. Se observó que, a pesar de las medidas implementadas por las empresas, persiste la sensación de tener menos control sobre el uso y acceso a los datos. Además, se constató que los avances en inteligencia artificial y aprendizaje automático ofrecen oportunidades significativas para mejorar la seguridad cibernética y la gestión de datos. El estudio destaca la urgencia de abordar los desafíos actuales en la seguridad cibernética, especialmente en el contexto de la creciente sofisticación de ciberdelincuentes. Se concluye que las empresas pueden beneficiarse significativamente de las últimas innovaciones en software y sistemas, así como de la adopción de la mentalidad de "datos a pedido". Sin embargo, persisten preocupaciones sobre el alcance de los efectos de los ciberataques, que pueden tener consecuencias criminales como el robo de identidad y la victimización. La sensación generalizada de tener menos control sobre el uso y acceso a los datos resalta la necesidad de medidas más efectivas para salvaguardar la integridad y la privacidad de la información.

Montasari et al. (2019). El propósito de esta investigación es analizar el papel de las Redes Sociales en Línea (SNS) en las investigaciones forenses digitales (DFIs) y abordar los desafíos comúnmente enfrentados por los examinadores forenses digitales (DFEs) al recolectar pruebas de dichas plataformas. Se llevará a cabo un análisis exhaustivo de la participación social, conversación, intercambio y trabajo en equipo facilitados por las SNS. Además, se examinarán los métodos empleados por los criminales para eludir la detección, contribuyendo al aumento de actividades ilegales. La investigación también se enfocará en los obstáculos que los DFEs encuentran al recopilar pruebas de las SNS. La muestra de estudio abarcará una amplia variedad de Redes Sociales en Línea, considerando la diversidad de plataformas utilizadas a nivel mundial. Se analizarán casos específicos de investigaciones forenses digitales que involucren el uso de SNS. Se presentarán los hallazgos relacionados con la participación

social y criminal en las SNS, así como los desafíos específicos que los DFEs enfrentan al recopilar evidencia de estas plataformas. Se destacarán los procedimientos cruciales para obtener pruebas digitales genuinas y técnicamente sólidas a lo largo de una investigación forense digital.Basándonos en los resultados obtenidos, se extraerán conclusiones sobre el impacto de las SNS en las investigaciones forenses digitales y se proporcionarán recomendaciones para superar los desafíos identificados. Este artículo busca contribuir al conocimiento y la eficacia de los procesos forenses digitales en el contexto de las Redes Sociales en Línea.

1.4.2. Antecedentes nacionales

Pomachagua (2020) investigó sobre: Desarrollo de un sistema de Auditoría de equipos de seguridad de redes. En el que concluyó que, existen posibles brechas de seguridad dentro de la arquitectura de red de una empresa son el tema de esta tesis. Si la red de una empresa es infiltrada, ya sea por un atacante externo o interno, los costes resultantes podrían ser considerables. exposición al riesgo de fuentes externas o internas. Por eso es crucial ser precavido y previsor al establecer las medidas de seguridad. Además, que, cuando el administrador de una organización establece accidentalmente una política de prueba, eso es un ejemplo de violación de la seguridad. Un administrador establece una política de prueba que permite el tráfico a través de TCP/80, pero luego se olvida de eliminarla. Como resultado, un ordenador puede infectarse con un virus similar al Ransomware, que luego puede infectar otras máquinas. Debido a esto, un sistema podría infectarse con un Ransomware, que luego podría extenderse por toda la red interna, dando lugar a un bloqueo generalizado y a una interrupción parcial o total.

Ramos (2021) realizó un estudio científico titulado: ISO 27037:2012 en la mejora del análisis forense en la empresa DG Service, Lima 2021. En mencionado estudio se pudo

concluir que, por encima de los resultados de este trabajo de investigación realizado por la DG de Servicios, se concluyó que el análisis forense se beneficiaría enormemente de la adopción de la norma ISO 27037. Además, se concluyó que, al permitir la captura de más datos de los dispositivos móviles, los indicios sugieren que la aplicación de la norma ISO 27037 ha supuesto avances sustanciales en la evaluación forense, especialmente la realización del índice de responsabilidades, que muestra un descenso de los tiempos dedicados a la investigación.

Velásquez y Davalos (2021) desarrollaron un estudio académico titulado: Informática Forense y su influencia en la Calidad de Servicio en el Centro de Cómputo de la Universidad Tecnológica de los Andes. En el que pudo afirmar que, cuando se habla de informática forense, es fundamental tener en cuenta que este campo se centra principalmente en los problemas de adquisición, conservación, recopilación y presentación de datos para verificar la existencia de un delito informático, evaluar el alcance de los daños causados y localizar a los autores; estos datos también pueden utilizarse como registro histórico para no cometer errores similares dos veces. Además, se concluyó que, este estudio encontró una relación estadísticamente reveladora entre la variable informática y la mejora de calidad del servicio prestado por el laboratorio de informática de la Universidad Tecnológica de los Andes, llevando a los autores a la conclusión que el valor del servicio del laboratorio se ve afectado por la informática forense.

Araníbar (2021) realizó un estudio científico titulado: *La evidencia digital y su influencia en los delitos informáticos en la Corte Superior de Justicia de Arequipa, 2019*. La investigación mencionada, concluyó que, la aceptación del valor admisible del testimonio digital es crucial para la supervivencia de los juicios justos a la luz del dramático aumento de los delitos informáticos causado por la introducción de una nueva inseguridad nacional. En consecuencia, el uso de las pruebas digitales en los casos de delitos informáticos ha experimentado un aumento espectacular debido a los actuales avances tecnológicos. Del mismo

modo, el rápido avance de las nuevas técnicas ha tenido un profundo efecto en la subsistencia diaria de los individuos, lo que ha dado lugar a una mayor dependencia de aplicaciones o productos de software que simplifican la vida, pero que también facilitan a los delincuentes la invasión del espacio personal de las personas, el robo de sus bienes y otros trastornos de sus rutinas y actividades habituales. Este espacio en línea se está convirtiendo en una extensión de nuestra vida cotidiana; protegerlo es una prioridad absoluta. Se concluyó además que, en las circunstancias en las que se trata de admitir las pruebas digitales, es imperativo que sean admisibles para que el valor de corroboración de la información electrónica pueda vincularse a la conclusión satisfactoria de los procedimientos penales que implican delitos informáticos.

Gutiérrez (2022) realizó un estudio de maestría titulado "Extracción de información en teléfonos celulares y su relación con hechos delictivos en la oficina de peritajes del ministerio público - Lima 2020". El principal objetivo de este análisis era determinar si los datos de los teléfonos móviles están relacionados con la delincuencia. Los organismos fiscales, policiales y judiciales solicitan datos a la Oficina de Peritaje en cartas oficiales para ayudar a identificar presuntas actividades ilegales. Un perito informático en análisis forense digital (ADF) debe presentar un informe pericial completo en el que se detallen los resultados para que la autoridad solicitante los evalúe. Este estudio utilizó métodos cuantitativos básicos y una metodología no experimental. La investigación se centró en el análisis sistemático de datos de teléfonos móviles. En la investigación se utilizó una muestra deliberadamente no probabilística de 80 teléfonos móviles que coincidían con 2020 informes periciales. Se investigaron delitos contra la propiedad, asesinato, tráfico de drogas e indemnidad sexual. Se utilizaron informes periciales de 2020 para obtener datos de 80 teléfonos móviles. Estos dispositivos móviles se eligieron con el objetivo profesional de detectar información delictiva, incluidos delitos contra la propiedad, asesinato, tráfico ilegal de drogas e indemnidad sexual. Se encontraron hallazgos significativos al analizar 80 teléfonos móviles en busca de información sobre sucesos

delictivos. En sus informes periciales, los especialistas informáticos de Análisis Forense Digital (ADF) describieron cómo los dispositivos podían haber sido utilizados en delitos contra la propiedad, asesinatos, tráfico de drogas y delitos sexuales. Estos hallazgos aumentan nuestros conocimientos sobre la información de los teléfonos móviles y la delincuencia. Los investigadores lograron vincular los datos de los teléfonos móviles con la delincuencia. El enfoque cuantitativo y el examen de 80 dispositivos ofrecieron una base sólida para comprender el papel de la información digital en la investigación criminal. Se concluyó que la tecnología forense puede ayudar a resolver casos de daños a la propiedad, asesinatos, tráfico de drogas e indemnizaciones sexuales.

Ferreyros (2019) realizó un trabajo de investigación titulado: La auditoría forense como herramienta y de investigación para combatir el fraude y la corrupción financiera publica en el Perú. El propósito principal de la investigación es determinar si la auditoría forense puede desempeñar un papel eficaz como medio preventivo e investigativo para abordar el fraude y la corrupción financiera en el ámbito público en Perú. La investigación se enfoca en comprender las razones y motivaciones detrás de los actos ilícitos, así como en evaluar las dificultades para su detección, centrándose en la contribución de la legislación actual para mitigar la corrupción y el fraude. El enfoque metodológico de la investigación es documental, analítico y descriptivo, con un diseño no experimental y transeccional. La población de estudio comprende trabajadores del sector público, especialmente aquellos en entidades recaudadoras, reguladoras y supervisoras en Lima. Se emplearon técnicas de recolección de datos, como encuestas y cuestionarios, y el procesamiento de datos se realizó mediante tabulación computarizada y análisis de hipótesis y gráficos con el programa SPSS. Los resultados sobresalientes corroboran la naturaleza preventiva e investigativa de la auditoría forense, evidenciada a través de programas, procedimientos, metodologías y técnicas alineadas con conceptos y protocolos legales. Se destacan notables reducciones en los tiempos de trabajo, mejoras en la eficacia de

la extracción de datos y un aumento en la resolución de casos. En conclusión, la auditoría forense emerge como una herramienta de gestión eficaz contra el fraude y la corrupción, respaldada por los hallazgos de la investigación. La inevitable y necesaria expansión de la auditoría forense plantea un desafío para aquellos involucrados en actos corruptos y fraudulentos, quienes ya no cuentan con el tiempo impune que tenían anteriormente.

Ramírez (2022) realizó un trabajo de investigación titulado: Importancia de la evidencia digital en la resolución de casos de la Ley de Delitos Informáticos – Ley N° 30096 y modificatorias con la ley N° 30171 en la división de Alta Tecnología PNP, Lima, 2022. El propósito académico de la investigación presentada consistió en examinar la relación entre la importancia de la evidencia digital y la resolución de casos de delitos informáticos en la División de Alta Tecnología de la Policía Nacional del Perú (Divindat PNP), en Lima, durante el año 2022. Este trabajo se desarrolla en un contexto en el que la tecnología ha experimentado un avance significativo a nivel global, llevando a las personas a modificar sus hábitos y normas de convivencia. Esta evolución tecnológica ha motivado la exposición de información personal a través de dispositivos como teléfonos celulares, tabletas, computadoras, entre otros, así como el uso de plataformas en línea para compartir datos en redes y otros sistemas de comunicación. Los ciberdelincuentes aprovechan este escenario para acceder a sistemas informáticos, apropiarse de datos, obtener beneficios económicos y, como consecuencia, las víctimas se ven obligadas a presentar denuncias por delitos informáticos. Al analizar esta problemática, se ha identificado un vínculo significativo entre la evidencia digital y la resolución de casos de delitos informáticos en la Divindat PNP, en Lima, durante el año 2022. El proyecto de investigación contribuye de manera significativa al ámbito académico al explorar información y archivos relacionados con las variables de evidencia digital y delitos informáticos.

Espinoza (2022) realizó un trabajo de investigación titulado: Análisis de los delitos informáticos el Alor probatorio de la evidencia digital en la Corte Superior de Justicia de Lima.

2021. El propósito académico de la investigación presentada consistió en examinar la relación entre la importancia de la evidencia digital y la resolución de casos de delitos informáticos en la División de Alta Tecnología de la Policía Nacional del Perú (Divindat PNP), en Lima, durante el año 2022. Este trabajo se desarrolla en un contexto en el que la tecnología ha experimentado un avance significativo a nivel global, llevando a las personas a modificar sus hábitos y normas de convivencia. Esta evolución tecnológica ha motivado la exposición de información personal a través de dispositivos como teléfonos celulares, tabletas, computadoras, entre otros, así como el uso de plataformas en línea para compartir datos en redes y otros sistemas de comunicación. Los ciberdelincuentes aprovechan este escenario para acceder a sistemas informáticos, apropiarse de datos, obtener beneficios económicos y, como consecuencia, las víctimas se ven obligadas a presentar denuncias por delitos informáticos. Al analizar esta problemática, se ha identificado un vínculo significativo entre la evidencia digital y la resolución de casos de delitos informáticos en la Divindat PNP, en Lima, durante el año 2022. El proyecto de investigación contribuye de manera significativa al ámbito académico al explorar información y archivos relacionados con las variables de evidencia digital y delitos informáticos. Los datos recopilados se basaron en tesis de grado, fuentes de internet y revistas indexadas, las cuales han proporcionado valiosas contribuciones doctrinales y han estimulado el surgimiento de nuevas líneas de investigación.

Ramos (2019) realizó un trabajo de investigación titulado: Implementación de un software forense para el análisis de la evidencia digital en dispositivos móviles. El propósito principal de la investigación fue implementar software forense para analizar la evidencia digital en dispositivos móviles en la empresa DG Service, Lima, durante el año 2019. A través de esta tesis, se evaluaron los resultados obtenidos en el análisis de la evidencia digital en dispositivos móviles después de la aplicación del software forense. El objetivo era identificar mejoras mediante la medición de indicadores como el tiempo de creación de la imagen forense, el

número de incidencias durante el análisis de la evidencia digital y las vulnerabilidades en dispositivos móviles Android. Esta investigación se enmarca en un enfoque aplicado, con un diseño experimental puro. La población constó de 20 observaciones, y se realizó un muestreo específico para cada indicador. La técnica de recolección de datos empleada fue la observación, utilizando como instrumento la ficha de observación. Los resultados de la investigación indicaron que la implementación de software forense tiene un impacto positivo significativo en el análisis de la evidencia digital en dispositivos móviles. Las mejoras destacadas se reflejaron en los indicadores evaluados. El tiempo de creación de la imagen forense mostró una reducción del 60% en comparación con las horas de trabajo, el número de incidencias durante el análisis de la evidencia digital experimentó una disminución del 68%, y las detecciones de vulnerabilidades en dispositivos móviles Android aumentaron en un 70%.

1.5. Justificación de la investigación

1.5.1. Justificación práctica

Examinar cómo la norma ISO 27037:2012 ha impactado en el desarrollo de la ciencia penal electrónica en la tecnológicamente avanzada División de Investigación Criminal de la Policía Nacional del Perú, Lima 2022 es el foco de este estudio. En este caso, el grupo de investigación está conformado por investigadores correspondiente a la División en Investigación Criminal de tecnología avanzada de la Policía Nacional del Perú, por lo que su éxito en la obtención de este balanceo tiene consecuencias claras y directas. Desde un punto de vista más pragmático, la investigación es importante ya que, en última instancia, dará lugar a una serie de ajustes en esa organización en particular y proporcionará un ejemplo útil para otras secciones de la Policía Nacional del Perú.

1.5.2. Justificación social

Estableciendo la influencia ISO 27037:2012 en la mejora del análisis informático forense en la División de investigación de delitos de alta tecnología correspondiente a la Policía Nacional del Perú, Lima 2022, se propondrá la aplicación o no del análisis informático forense como metodología eficiente para el análisis de los delitos de alta tecnología. Razón por la cual, la sociedad se verá beneficiada, ya que, al tener un mecanismo científico para investigar los delitos cibernéticos, se podrá construir una sociedad más segura y equilibrada.

1.5.3. Justificación metodológica

El equipo está siendo utilizado para aprender cómo la Organización Internacional de Normalización (ISO) 27037:2012 afecta a la calidad de la evaluación legal digital realizada por la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú en Lima en el año 2022. El investigador podrá aplicar instrumentos, métodos, técnicas, modelos y demás constructos metodológicos para el proceso de la investigación científica. Los mismos que servirán a futuras investigaciones en el ámbito de los medios electrónicos y los sistemas telefónicos con fines de análisis informático forense dentro de las diversas divisiones de investigación.

1.5.4. Importancia

La importancia de esta tesis radica en su enfoque crítico y orientado hacia la mejora sustancial de las capacidades de la División de investigación de delitos de alta tecnología de la Policía Nacional, en un momento en que la delincuencia cibernética y la utilización de tecnologías avanzadas para cometer delitos están en constante aumento. La Norma ISO 27037:2012, diseñada específicamente para abordar los desafíos del análisis informático forense en entornos digitales, se convierte en un pilar fundamental en la lucha contra estos delitos. La tesis no solo investiga la implementación de esta norma, sino también su impacto

real en la eficacia y eficiencia de la División, destacando aspectos como la reducción de tiempos de trabajo, la mejora en la extracción de datos y el aumento en la resolución de casos. Los hallazgos y conclusiones de esta investigación pueden contribuir no solo a la mejora de las prácticas forenses en la Policía Nacional sino también a una respuesta más efectiva a la creciente amenaza de la delincuencia en tecnología especializada en Perú y, por extensión, en otros contextos a nivel internacional.

1.6. Limitaciones de la investigación

La presente investigación tiene las siguientes limitaciones:

- **Espacial**

La División de investigación de delitos de alta tecnología de la Policía Nacional del Perú en Lima, el año 2022, llevará a cabo la investigación.

- **Temporal**

Lo mismo cabe decir de los meses de octubre, noviembre y diciembre de 2022, en los que se realizará este estudio.

1.7. Objetivos

1.7.1. Objetivo general

Establecer la influencia del ISO 27037:2012 en la mejora del análisis informático forense en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.

1.7.2. Objetivos específicos

a. Determinar la influencia del ISO 27037:2012 en la mejora de los tiempos de trabajo en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.
b. Determinar la influencia del ISO 27037:2012 en la mejora de la extracción de datos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.
c. Determinar la influencia del ISO 27037:2012 en la mejora del número de casos resueltos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.

1.8. Hipótesis

1.8.1. Hipótesis general

Existe una influencia positiva del ISO 27037:2012 en la mejora del análisis informático forense en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.

1.8.2. Hipótesis específicas

a. El ISO 27037:2012 influye positivamente en la mejora de los tiempos de trabajo en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.
b. El ISO 27037:2012 influye positivamente en la mejora de la extracción de datos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.
c. El ISO 27037:2012 influye positivamente en la mejora del número de casos resueltos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.

II. MARCO TEÓRICO

2.1 Bases teóricas

2.2.1. ISO 27037:2012

Sudyana et al. (2019) indican que el propósito principal de las regulaciones ISO 27000 relativas al análisis forense digital es delinear maneras más efectivas para reunir evidencia digital. Se anticipa que la estandarización de los procedimientos de análisis forense posibilitará la comparación, fusión y cotejo de los datos obtenidos en tales investigaciones, incluso si son llevadas a cabo por distintos individuos u entidades y posiblemente efectuadas en diferentes ámbitos legales.

Se han establecido estándares adicionales en la ciencia forense, como los producidos por el Instituto Nacional de Estándares y Tecnología (NIST) para la ciencia forense. Dicho esto, el estándar más universalmente reconocido es ISO/IEC 27037:2012. Las Unidades de Informática Forense (DFUs, por sus siglas en inglés) enfrentan más que el problema de crear estándares y procedimientos. La capacidad para ocultar información a simple vista solo empeorará las cosas, dando lugar a una esperada explosión de datos. La idea de que las DFUs buscarían activamente programas de ocultación de datos en lugar de programas que revelen o analicen datos presenta un conjunto único de problemas. Las tareas comunes para estas secciones incluyen comparar conjuntos de datos y encontrar o explotar software basado en datos. Los datos ocultos ya son difíciles de descifrar, y la mayoría de las DFUs no pueden decirte si están en una unidad USB, en la nube u otro medio. Aunque las DFUs tienen pocas opciones para obtener estos datos, el RAS Deleted Steganography Applications Scanner se destaca entre los demás. (Justice, 2020)

En este contexto, garantizar la adquisición y preservación de las pruebas de manera que se prevenga la alteración de su autenticidad representa uno de los desafíos más apremiantes en las investigaciones forenses. Las pruebas forenses digitales deben ser salvaguardadas con la

misma diligencia que las pruebas físicas convencionales, mediante procedimientos estructurados que sean admitidos por los tribunales, y la custodia de la cadena debe ser mantenida conjuntamente por el primer encargado y el subsiguiente (identificados como "primeros encargados digitales" y "expertos en pruebas digitales", respectivamente). Aquella calidad de las representaciones forenses es un ejemplo ilustrativo.

En ese sentido, Mohammed (2019) se menciona que, según el autor, "asegurar la adquisición y preservación de las pruebas de manera que se prevenga la alteración de su autenticidad es uno de los retos más apremiantes de las investigaciones forenses" (p. 36). Las pruebas forenses digitales deben ser resguardadas de la misma manera que las pruebas físicas tradicionales, mediante procedimientos estructurados que sean admitidos por los tribunales, y la cadena de custodia debe ser mantenida tanto por el primer interviniente como por el siguiente, quienes son referidos mediante "primeros intervinientes digitales" y "especialistas en pruebas digitales", respectivamente. Este concepto es reflejado por las imágenes forenses de alta calidad.

Siguiendo los métodos analíticos concebidos para mejorar la aceptación de las pruebas en los procedimientos judiciales, los procedimientos delineados en las regulaciones de norma aseguran donde los peritos forenses digitales conserven las pruebas digitales a lo largo de las etapas de recopilación en las investigaciones. La integridad resalta la importancia de manipular las pruebas de manera adecuada para que mantengan su relevancia y puedan ser mostradas a cualquier entidad interesada.

En ese sentido, Boasiako (2018) refiere que “los investigadores forenses pueden evaluar de forma independiente los métodos, técnicas y resultados de la certificación ISO 27037” (p. 38). Si los investigadores documentan meticulosamente sus procedimientos y acciones, las auditorías forenses serán mucho más sencillas. Esto significa que los que llevan a cabo las

investigaciones forenses digitales deben ser capaces de articular el razonamiento detrás de las decisiones que tomaron.

De esta manera, las regulaciones concernientes a la obtención de pruebas digitales comprenden la identificación, el acopio, la obtención y la preservación de datos electrónicos que puedan poseer relevancia legal. Ayuda a las empresas en sus procedimientos internos y en el intercambio de pruebas digitales en todas las jurisdicciones, e instruye a los particulares sobre cómo manejar correctamente las pruebas digitales.

Por lo general, las pautas diseñadas para la adquisición de pruebas digitales siguen las directrices establecidas por la norma ISO/IEC 27037:2012. Esto implica que los procedimientos destinados a obtener evidencia digital en dispositivos móviles están orientados a cumplir con los estándares y principios establecidos por esta norma internacional. El uso de esta norma puede favorecer la aceptación legal de la evidencia, ya que se adhiere a principios reconocidos a nivel internacional en la gestión de pruebas digitales, garantizando su integridad y autenticidad. (Lara et al., 2020)

El primer proceso de recopilación y preservación de evidencia digital prospectiva es el énfasis principal de la norma internacional, que fue producida por la Organización Internacional de Normalización (ISO) en 2012. Al utilizar esta estrategia particular, otros factores como el análisis, La presentación y eliminación de pruebas no se tienen en cuenta. DEFR, que significa "Digital Evidence First Responder", es el término utilizado para describir a las personas que están a cargo del manejo de evidencia digital. Estas personas deben ser capaces de reconocer y gestionar los peligros inherentes a su profesión. Dado que cualquier deterioro podría invalidar la evidencia digital, es crucial preservar la integridad y confiabilidad de la evidencia digital. Cuando se trata de la manipulación de evidencia digital, cumplir con reglas generales se convierte en una necesidad urgente para garantizar la validez de la evidencia durante todo el proceso de la investigación. (Veber y Smutny, 2015)

En el campo de la ciencia forense digital, la norma ISO/IEC 27037:2012 es un estándar internacional que define estándares para la identificación, recopilación, preservación y presentación de evidencia electrónica estableciendo criterios para estas actividades. En el lenguaje que se ha presentado, se dice que el marco de la ciencia forense digital se ve reforzado por la combinación de la estandarización de ISO/IEC 27037:2012 y NIST SP-800-86. El hecho de que este sea el caso muestra que ISO/IEC 27037:2012 es un componente de una estrategia integral que aborda múltiples áreas de la ciencia forense digital. Estos componentes incluyen factores cruciales como el tiempo, la mano de obra, la capacidad de los medios de almacenamiento y la naturaleza de las vulnerabilidades en los sistemas de los dispositivos. (Ramadhan et al., 2022)

"La norma en cuestión desempeña un papel crucial en la resolución de diversas problemáticas asociadas con la administración de evidencia digital. Más específicamente, se centra en proporcionar instrucciones explícitas para la ejecución precisa de la recopilación de datos en situaciones forenses. El objetivo fundamental de este alcance es garantizar la autenticidad, integridad y confiabilidad de la evidencia digital recopilada durante los procesos de investigación forense. Su alcance involucra la definición de ciertas técnicas y métodos.

Este marco legal sirve como referencia vital para profesionales que participan en el proceso de recopilación y mantenimiento de evidencia digital. Establece criterios rigurosos con la intención de preservar la calidad y autenticidad de la información obtenida a lo largo de las investigaciones forenses. Su implementación contribuye a aumentar la solidez y confiabilidad de los hallazgos adquiridos, y proporciona un método organizado y confiable en el ámbito de la evidencia digital, que es un tema complejo. (Stoykova et al., 2022)

2.2.2. Análisis informático forense

Según el Instituto Nacional de Estándares y Tecnología, los cuatro métodos y enfoques empleados en el ámbito de la investigación forense digital han sido concebidos con el propósito de asistir a las organizaciones en la comprensión de la importancia de sus investigaciones. Estos métodos pueden ser ejecutados de diversas maneras, adaptándose a la complejidad inherente al estudio en cuestión. La expansión de la tecnología digital ha provocado un incremento significativo en la variedad de fuentes de datos que pueden ser recopiladas (Yusra et al., 2020). A continuación, se detalla cada una de las etapas implicadas:

- Recopilación de datos: La primera fase en la ejecución de una investigación es la recopilación de datos, que implica la identificación de posibles fuentes de información. Comúnmente, estos datos se obtienen de computadoras portátiles, de escritorio y servidores. Además de las fuentes convencionales, los analistas deben contemplar otras fuentes al examinar las operaciones de una entidad. A modo de ejemplo, podrían obtener detalles sobre las actividades de la organización mediante los registros proporcionados por su proveedor de servicios de Internet.
- Examinación: En la fase de examen, se busca analizar los datos recopilados mediante el empleo de técnicas y herramientas forenses digitales. A través de estos métodos, se extraen las piezas de información esenciales de los datos obtenidos. Asimismo, se identifican y delinean los archivos de datos que albergan información relevante, abarcando detalles ocultos mediante prácticas como la compresión de archivos, el control de acceso y el cifrado.
- Análisis: El análisis se presenta como un procedimiento científico ejecutado en un contexto científico con el objetivo de generar aspectos tales como la identificación de personas, lugares y eventos, así como la comprensión de sus interrelaciones. Este proceso conlleva la examinación de datos provenientes de diversas fuentes. Por

ejemplo, un registro de un Sistema de Detección de Intrusiones (IDS) podría contener información detallada acerca de un usuario específico, mientras que los registros de auditoría podrían proporcionar detalles relacionados con un host en particular. La utilización de herramientas como el software de gestión de eventos de seguridad facilita la correlación y recopilación eficiente de estos datos.

- Informe: El último paso crucial en el proceso de investigación es la creación del informe. En esta etapa, se examinan detenidamente los datos recopilados durante el análisis, y las conclusiones se presentan de manera formal al analista a través de una documentación detallada. Identificar la causa de un evento o proporcionar una explicación precisa puede ser un desafío, pero al recopilar información a partir de los datos, el analista logra comprender más profundamente el evento y adoptar medidas preventivas para evitar su repetición en el futuro.

Teniendo en cuenta ello, existen diversos modelos de investigación en el campo de la Forense Digital. Entre ellos, se encuentran el Modelo de Talleres de Investigación Forense Digital (DFRWS), el Modelo Forense Digital Abstracto (ADFM), el Modelo de Proceso de Investigación Digital Integrado (IDIP) y el Modelo de Proceso de Investigación Digital de Extremo a Extremo (EEDIP). Cada uno de estos modelos ha sido diseñado con el propósito de abordar fases y actividades específicas dentro del ámbito de la investigación forense digital.

El primero modelo, Modelo de investigación DFRWS, sigue un proceso estructurado en fases clave: Identificación, Preservación, Colección, Examen, Análisis y Presentación, con una etapa adicional llamada Decisión. Cada fase utiliza técnicas específicas para detectar eventos, gestionar casos, recopilar datos, garantizar la integridad de la evidencia y presentar resultados de manera clara. La consistencia y estandarización de este enfoque mejoran significativamente la efectividad del proceso forense. (Tahiri, 2016)

Según Babulal et al. (2021) el Modelo Forense Digital Abstracto (ADFM), introducida en el 2002 por Reith, Carr y Gunsh se compone de un conjunto de nueve fases, a las cuales se añaden tres fases adicionales, en comparación al modelo general: la preparación, la estrategia de abordaje y la devolución de la evidencia. Este modelo se inspira en sus predecesores y busca proporcionar un marco integral para la investigación forense digital, abordando diversas etapas del proceso con el objetivo de optimizar la obtención y análisis de evidencia digital. El proceso del Modelo de Abordaje Digital Forense (ADFM) se desglosa en varias fases esenciales para llevar a cabo una investigación efectiva en el ámbito del delito digital.

- En la primera fase, denominada Identificación, se busca reconocer aquellos incidentes que poseen el potencial de constituir delitos digitales. En caso de observarse la participación de dispositivos digitales en la perpetración de un delito, se procede a informar a los investigadores pertinentes.
- La segunda etapa, conocida como Preparación, implica la organización de herramientas, técnicas, órdenes de registro y autorizaciones necesarias para llevar a cabo la investigación. Durante este proceso, se asegura el cumplimiento de todas las formalidades legales requeridas.
- La tercera fase, Estrategia de Abordaje, se enfoca en la formulación de procedimientos y enfoques que se implementarán para maximizar la recopilación de pruebas, minimizando al mismo tiempo el impacto sobre la víctima.
- La fase de Preservación sigue, consistente en el aislamiento, aseguramiento y preservación del estado de las pruebas físicas y digitales para garantizar su integridad.
- La Recogida, como quinta fase, implica registrar la escena física y duplicar las pruebas digitales mediante procedimientos normalizados y aceptados.

- Posteriormente, la fase de Examen se enfoca en una búsqueda sistemática y exhaustiva de pruebas relacionadas con el presunto delito, centrándose en la identificación y localización de posibles evidencias.
- La fase de Análisis deriva en la conclusión del caso examinado.
- Mientras que la Presentación consiste en resumir y explicar dicha conclusión de manera comprensible.
- Finalmente, en la fase de Devolución de Pruebas, los dispositivos físicos y digitales recopilados como evidencia se devuelven al propietario correspondiente. Este ciclo completo de fases del ADFM asegura una investigación forense digital rigurosa y efectiva.

El Modelo de Investigación Forense Digital de Próxima Generación (NGDFIM) es un marco estándar diseñado para abordar los desafíos derivados del rápido avance tecnológico en el campo de la investigación forense digital. Su objetivo principal es facilitar el proceso de investigación para los profesionales al proporcionar una estructura formalizada. Este marco tiene el potencial de generar más evidencia durante la respuesta a incidentes al incorporar la clasificación in situ, en comparación con los métodos de investigación convencionales. NGDFIM también busca reducir el tiempo de análisis, mejorar la eficiencia general del proceso de investigación mediante la clasificación en el sitio y el mapeo de imágenes de memoria. Además, se enfoca en proteger la privacidad del sospechoso al incluir imágenes de contenido personalizado. La aplicación pragmática del marco se destaca como una de sus mayores ventajas, lo que lo hace viable en casos de la vida real. En el futuro, se podría desarrollar un prototipo para implementar este marco, lo que impulsaría aún más su utilidad en la investigación forense digital. (Akash et al., 2021)

Otro modelo importante es el Proceso Integrado de Investigación Digital (IDIP) que representa un modelo típico del procedimiento forense digital. Este modelo consta de diversos

niveles organizados en cinco categorías (Cortés, 2019). A continuación, se presenta una breve explicación de cada una de estas categorías:

En los Niveles de preparación, se asegura que tanto el personal como la infraestructura estén preparados para respaldar una investigación en caso de que ocurra un incidente. Los Niveles de implementación proporcionan un mecanismo para detectar un incidente y confirmarlo de manera efectiva. En los Niveles de investigación física de la escena del crimen, se lleva a cabo la recopilación y análisis de la evidencia física, así como la reconstrucción de las escenas que tuvieron lugar durante el incidente. Los Niveles de investigación de escena digital se centran en el análisis de los dispositivos digitales obtenidos durante las fases de investigación física. Finalmente, en los Niveles de revisión, se examina exhaustivamente toda la investigación, identificando áreas que requieren mejoras. (Cortés, 2019)

El Paradigma Avanzado de Adquisición de Datos (ADAM), tuvo su concepción y elaboración del ADAM en el proceso de investigación de la ciencia del diseño (DSRP) desarrollado por Peffers y otros en 2006. Este proceso consta de seis etapas interrelacionadas. En la primera fase se identifican problemas y motivaciones que llevaron al desarrollo del ADAM, estableciendo necesidades y desafíos. Luego se definen objetivos claros para la solución. La fase de diseño y desarrollo implica la creación del sistema ADAM, aplicando principios y metodologías de diseño. La demostración válida la funcionalidad del ADAM, mostrando su eficacia. La evaluación analiza resultados y recopila comentarios, siendo un proceso iterativo que retroalimenta la fase de diseño y desarrollo. Finalmente, la comunicación comparte resultados y lecciones aprendidas con partes interesadas y la comunidad. El DSRP destaca la importancia de la retroalimentación continua, cerrando el ciclo de manera efectiva. (Adams et al., 2013)

Conforme a Shalaginov et al. (2020) se define el análisis informático forense como el procedimiento de llevar a cabo investigaciones relacionadas con infracciones que involucran

cualquier tipo de equipo informático, incluyendo, pero no limitado a computadoras personales, servidores, laptops, celulares, tablets, webcam, puntos de acceso, dispositivos del Internet de las cosas u otros dispositivos electrónicos. Los forenses digitales también tienen la responsabilidad de investigar ataques que se originan en el ciberespacio. Ejemplos de estos ataques incluyen el malware, el phishing, los ataques, la denegación en servicio descentralizada, violaciones de datos y otros ciberataques que pueden resultar en pérdidas financieras o daño a la reputación. Una investigación utilizando la ciencia forense digital tiene como objetivo principal la preservación, identificación, adquisición y documentación de pruebas digitales que puedan ser utilizadas en procesos judiciales.

En ese contexto, Stelly (2019) argumenta que "una vez realizada y concedida la solicitud, los pasos subsecuentes en el proceso forense comprenden la recopilación de pruebas, su inspección, análisis y comunicación de los resultados" (p. 35). Cuando algún cliente solicitase alguna investigación y se llegue aprobar dicha solicitud, se inician las etapas iniciales. Esto marca el inicio de un nuevo caso en el ámbito de la investigación forense.

Por otro lado, durante la fase conocida como recopilación, se buscan, adquieren y catalogan todos los datos que sean relevantes para la solicitud de estudio. la solicitud de investigación. Para ofrecer una interpretación de los datos, la investigación hace uso de técnicas forenses. En la etapa denominada análisis, se aplican los descubrimientos de la investigación con el fin de intentar desvelar aquellas respuestas a las respectivas interrogantes planteadas en aquella solicitud para generar alguna investigación.

Dentro de esta etapa en la que se crea el informe, se proporciona al solicitante una exposición de los resultados, así como de la metodología empleada. Finalmente, se evalúa con detenimiento el caso y se registra y discuten lo sugerido respecto a las modificaciones en lo político, los procedimientos o las herramientas, fundamentadas en las lecciones adquiridas en

el proceso. Estas adaptaciones en la política, el método o las herramientas se derivan de las enseñanzas obtenidas a lo largo del caso.

En ese sentido, Montasari et al. (2019) afirman que, el procedimiento de preservación, detección, recuperación y guardado de las pruebas en informática que posteriormente podrían ser utilizadas en una actuación judicial se define como análisis forense digital. Un ordenador, un dispositivo móvil, un servidor o una red son ejemplos de medios digitales donde pueden buscarse evidencias en este ámbito de investigación.

Así, el equipo forense dispone de las estrategias y tecnologías más eficaces, lo que le permite resolver casos difíciles relacionados con los medios digitales. El equipo forense puede inspeccionar, analizar, identificar y preservar más eficazmente las pruebas en formato digital que residen en una variedad de medios electrónicos diferentes con la ayuda de la ciencia forense digital.

Según indica Karabiyik et al. (2018) expresan que, "la informática forense es un sinónimo de la informática forense. Este campo de estudio aplica métodos de investigación científica a la indagación de delitos informáticos" (p. 12). Asimismo, se describe como el proceso de identificar, conservar, analizar y valorar las pruebas digitales a través de la adhesión a procedimientos establecidos, así como la posterior presentación de dichas pruebas en los tribunales con el propósito de abordar cuestiones legales relacionadas con actividades delictivas e intrusiones informáticas.

De esta manera, los expertos en informática forense son una parte esencial del proceso de investigación de los casos relacionados con la actividad delictiva en línea. Se centran sobre todo en descifrar datos encriptados, así como en recuperar datos que han sido destruidos o enterrados. Además, los trabajos implican garantizar que la información que se utilizará en el tribunal sea precisa. Los interrogatorios de sospechosos, víctimas y testigos, y víctimas y

testigos pueden implicar la participación de analistas informáticos forenses en varias fases de la investigación. Además, ayudan en la preparación de las pruebas presentadas ante el tribunal.

Por otro lado, para Yeboah y Akwa (2016) la ejecución de la ciencia forense en lo digital no solo demanda la meticulosa recolección e inspección de registros o artefactos digitales, sino también la precisa interpretación y comprensión de las pruebas que se han obtenido" (p. 79). Es de vital importancia que tanto el personal de las fuerzas de seguridad como los peritos forenses digitales cumplan con los estándares exigentes de la profesión, especialmente si se espera que la evidencia forense sea aceptada en un tribunal competente. Este proceso de investigación evalúa la magnitud de los daños en un sistema que ha sido alterado o atacado, recupera información extraviada del sistema que estaría dañado y, en último caso se presenta las pruebas forenses para generar un juicio a los responsables del ciberdelito.

Mientras que, Taubmann (2019) indica que, "el proceso de investigación forense digital actualmente demanda más tiempo que nunca, como resultado directo del incremento tanto en la cantidad de información como en el volumen de las documentaciones que se son utilizados como evidencia" (p. 35). Algunos ejemplos de estas fuentes de datos abarcan los dispositivos vinculados al Internet de las cosas y los sistemas de cómputo en la nube. La duración requerida para cada etapa del proceso forense, que abarca la recolección, el procesar y posterior análisis de las pruebas, ha aumentado.

La inteligencia artificial (IA), que demostró ser una promisoria alternativa para afrontar los desafíos presentes y futuros en esta área, con un elevado potencial para reducir la carga de trabajo manual y para incrementar de manera sustancial la velocidad de los procedimientos. De acuerdo a este autor, una de las soluciones viables radicaría en la utilización de inteligencia artificial con el propósito de optimizar aquel análisis forense digital.

En la actualidad, se enfatiza la relevancia del análisis informático forense en el contexto de la era de Internet y el veloz avance de la tecnología de la información. La tecnología

informática forense ha adquirido un papel destacado como área significativa de investigación, destinada a obtener pruebas relacionadas con delitos informáticos. (Duan y Zhang, 2020)

El proceso de análisis informático forense se lleva a cabo mediante la utilización de herramientas especializadas conocidas como herramientas informáticas forenses (CFT). Estas herramientas tienen como objetivo examinar la evidencia digital presente en escenarios de delitos digitales. El enfoque principal de este estudio radica en evaluar la eficacia de dichas herramientas, centrándose específicamente en su capacidad para extraer evidencia completa y creíble cuando se enfrentan a ataques antiforenses (AF) dirigidos al sistema de archivos. La metodología empleada en este estudio sigue un enfoque de prueba de herramientas forenses de seis etapas, basado en principios de prueba de caja negra. Esto implica que la evaluación se realiza sin un conocimiento detallado del funcionamiento interno de las herramientas en cuestión. Se busca determinar cómo estas herramientas responden y se desempeñan en situaciones prácticas sin un acceso completo a su estructura interna. El análisis revela que algunas de estas herramientas forenses pueden no ser completamente efectivas para identificar ciertos tipos de ataques antiforenses. Esta circunstancia plantea inquietudes en relación con la integridad y confiabilidad de la evidencia digital recopilada cuando se enfrenta a tales ataques. En consecuencia, se sugiere que la capacidad de estas herramientas para lidiar con la complejidad de los ataques antiforenses podría afectar la validez de las pruebas digitales obtenidas durante investigaciones de delitos digitales. (Ahmed et al., 2021)

El análisis forense informático se define como un proceso destinado a descubrir y examinar la información de sistemas mediante el análisis de evidencias digitales. En el contexto de la Cuarta Revolución Industrial, donde la ciberseguridad es crucial debido al aumento de dispositivos conectados y la amenaza de ciberdelincuencia, este análisis se vuelve esencial. Se centra en investigar eventos de seguridad informática utilizando métodos científicos y técnicas especializadas. El proceso consta de seis pasos: diagnóstico del caso, recopilación de pruebas,

copias de archivos, análisis de datos, extracción de información y presentación de resultados. Busca no solo identificar amenazas, sino también proporcionar pruebas digitalmente sólidas para investigaciones y procesos legales en el ámbito de la ciberseguridad. (Villar, 2019)

El análisis informático forense es un proceso en el que expertos, dentro del ámbito de la informática forense y la metodología forense digital, siguen una serie de pasos para obtener y analizar pruebas detalladas. En este proceso, se destaca la importancia de evaluar la eficacia y eficiencia, es decir, considerar el retorno de la inversión en función de las pruebas obtenidas. Aunque los pasos del proceso pueden repetirse, se enfatiza la necesidad de determinar cuándo detenerse, reconociendo que una vez que se obtienen pruebas suficientes, el valor de realizar más análisis disminuye. El análisis informático forense implica la recopilación, identificación y análisis de pruebas digitales con el objetivo de resolver casos relacionados con delitos informáticos, propiedad intelectual u otros asuntos legales. Este proceso se lleva a cabo de manera metódica y eficiente, deteniéndose una vez que se alcanza un nivel adecuado de evidencia. (Carroll et al., 2017)

Por otro lado, el análisis informático forense constituye una disciplina especializada que se enfoca en la aplicación de principios científicos y técnicas específicas para investigar y examinar evidencia digital. Su objetivo principal es respaldar investigaciones criminales al proporcionar pruebas sólidas y confiables en contextos legales. Este campo se dedica a la meticulosa exploración de datos electrónicos con el fin de descubrir, interpretar y documentar información relevante que pueda contribuir a la resolución de casos judiciales. Con un enfoque preciso y fundamentado en la ciencia, el análisis informático forense desempeña un papel crucial al garantizar la integridad y admisibilidad de la evidencia digital en procedimientos legales. (Pilski, 2022)

En el ámbito de la investigación, el análisis forense digital se destaca como crucial, especialmente en la recuperación y examen de datos almacenados en computadoras de

escritorio. El tiempo necesario para estas investigaciones ha ido en aumento, en parte debido al crecimiento en el tamaño de los discos duros. Para abordar este desafío, se introduce una aplicación específica llamada Digital Forensics Compute Cluster (DFORC2). Esta herramienta de código abierto tiene como objetivo reducir el tiempo necesario para realizar investigaciones forenses sólidas en datos de computadoras de escritorio. DFORC2 utiliza la capacidad de procesamiento paralelo de servidores independientes de alto rendimiento o entornos de computación en la nube, lo que sugiere su eficiencia en entornos distribuidos para acelerar el análisis forense digital. (Novak et al., 2018)

2.2.3. Dimensiones del análisis informático forense

2.2.3.1. Tiempos de trabajo. Para Roussev (2019) "según su explicación, el problema es que el área de la ciencia forense digital nunca ha sido capaz de encontrar una solución que logre un equilibrio entre el tiempo promedio que se utilizara y la forma de precisión de precisión que proporciona" (p. 35). Al analizar las diferentes técnicas propuestas para resolver este problema, se ha observado que la mayoría de estos enfoques predicen que una reducción en la cantidad de tiempo invertido invariablemente resultaría en una caída en la precisión, y viceversa. Debido a que cualquier esfuerzo para acelerar las operaciones podría potencialmente perjudicar la precisión de los hallazgos adquiridos, esta paradoja presenta un obstáculo sustancial en el proceso de diseño y optimización de procesos. Es necesario desarrollar enfoques novedosos capaces de superar este aparente conflicto debido a la complejidad subyacente que implica lograr un equilibrio entre eficiencia y precisión. Para encontrar soluciones exitosas, es necesario tener una comprensión profunda de las interrelaciones que existen entre tiempo y precisión, así como la capacidad de idear métodos que cuestionen las normas convencionales que se han establecido.

Adicionalmente, los modelos utilizables no tenían de universalidad, lo cual limitaba su aplicabilidad en un amplio espectro de circunstancias; los modelos que presentaban cierta universalidad aportaban escasa ayuda en el aspecto práctico de la investigación. Esta resultó ser una de las restricciones del estudio. A pesar de que la automatización se perfilaba como la respuesta lógica y paliaba algunas de las dificultades, como la economía de tiempo y esfuerzo, se evidenció su falta de consistencia al evaluar su precisión en varias etapas del proyecto. Por lo tanto, se sugiere optar por un modelo en proceso que incorpore técnica autimatizada con el fin de manejar por lo menos las situaciones informáticas más comunes.

Por otro lado, los límites a la duración de la jornada laboral son como medio para regular las horas de trabajo con el fin de proteger la salud y la seguridad de los empleados. Gradualmente pasaron a primer plano las preocupaciones sobre el tiempo de trabajo, visto como un recurso escaso que debía controlarse para reducir el desempleo y redistribuir los empleos. Una perspectiva más moderna sobre las horas de trabajo se ha desplazado hacia su componente cualitativo, con énfasis en la gestión eficaz del tiempo en respuesta a los cambios en la productividad y las demandas de una economía global interconectada. (Rodríguez, 2017)

Taylor, ampliamente considerado como el pionero de la gestión científica, fue quien utilizó el estudio del tiempo en los años 80 con la intención de establecer de forma precisa y adecuada la duración de un proceso, que es la jornada laboral justa. Este fue el comienzo de la implementación efectiva del estudio del tiempo. A partir de la medición de la sustancia del trabajo y del procedimiento definido, esta investigación incorpora el enfoque de definir un estándar de tiempo permitido para realizar una determinada actividad. Esta evaluación tiene en cuenta el cansancio, la tolerancia, los retrasos personales y los retrasos que no se pueden evitar. (Arteaga et al., 2021)

Cuando se trata de mejorar la eficiencia operativa, el estudio de tiempos es una herramienta importante para toda organización. Una mejor gestión de recursos y menores

costos son resultados directos de examinar y evaluar los procesos para encontrar oportunidades para optimizar la programación de pedidos. Además, este método sienta las bases para garantizar que el almacén esté adecuadamente equipado para hacer frente a las necesidades cambiantes de los clientes. Tomar decisiones fundamentadas para adoptar tácticas que mejoren la productividad y la calidad del servicio se simplifica con datos confiables sobre los tiempos de ejecución de cada trabajo. Al final, el estudio de tiempos demuestra ser un instrumento invaluable para mejorar la eficiencia operativa y la competitividad en el mundo empresarial. (Reyes et al., 2017)

Cuando se trata de maximizar la productividad y lograr los objetivos, la gestión del tiempo es un componente esencial. Este proceso no sólo incluye planificación, sino que también requiere la ejecución deliberada de control sobre la cantidad de tiempo dedicado a determinadas tareas. Quiere trabajar de forma más eficaz e inteligente y puede hacerlo utilizando tácticas que le ayuden a gestionar su tiempo. Este enfoque requiere varios factores críticos, incluida la capacidad de priorizar actividades, establecer plazos razonables y abstenerse de posponer las cosas. La gestión del tiempo no se limita al ámbito laboral; más bien, abarca todos los aspectos de la vida, permitiendo una asignación equitativa y eficiente del tiempo para lograr objetivos tanto personales como profesionales. (Aesides, 2018)

2.2.3.2. Extracción de los datos. Hajar (2020) sostiene que, “la adquisición se realiza con el objetivo de alcanzar los datos que posee una cámara móvil, el cual podría estar encriptados, destruidos o, en general, complicados en desencriptar”. El objetivo de la recogida es recuperar estos datos. En consecuencia, para que un procedimiento de recogida de datos tenga éxito, suele ser necesario utilizar una herramienta de recuperación de datos que sea capaz de romper las contraseñas, burlar las contraseñas o pautas y generar recuperación de los datos eliminados de la memoria que poseen los dispositivos. (Hajar, 2020, p.62)

Debido a ello, la obtención de datos en las investigaciones informáticas agrupa todos los pasos a seguir relacionados a la obtención de evidencia digital, lo que incluye la duplicación y la réplica exacta de cualquier fuente electrónica. También abarca la generación de una réplica idéntica partiendo de dispositivos una variedad de materiales digitales, como puede ser el CD-ROM, discos SSD O HDD, unidades de disco duro móviles, teléfonos inteligentes, unidades USB, decodificadores, servidores y otros dispositivos informáticos que sean capaces de almacenar información electrónica. En este sentido, la recuperación de datos es posiblemente el momento más crítico y, en ciertos casos, la fase más significativa del proceso.

La extracción de datos en informática forense se adentra en el mundo de la delincuencia cibernética, empleando técnicas sofisticadas de minería de datos. Su propósito es analizar extensos conjuntos de información vinculados a crímenes en el ámbito digital, con el fin de desentrañar patrones, motivaciones y otros elementos esenciales para la investigación y prevención de actividades delictivas en entornos virtuales. Este proceso permite revelar detalles cruciales que facilitan la comprensión y resolución de casos, contribuyendo así a la seguridad y protección en el ciberespacio. (Sindhu y Meshram, 2012)

La extracción de datos en informática forense constituye un proceso esencial para obtener información crucial y evidencia digital de diversas fuentes, como sistemas cibernéticos, redes y navegadores web. Su propósito principal es facilitar la investigación y análisis forense, permitiendo a los expertos examinar detalladamente la actividad digital y descubrir posibles pruebas relacionadas con incidentes o delitos. Este procedimiento implica la recolección meticulosa de datos, asegurando su integridad y preservación, con el fin de respaldar de manera sólida la resolución de casos mediante la interpretación experta de la información extraída. La extracción de datos en informática forense se erige como un pilar fundamental para el

esclarecimiento de situaciones legales y la preservación de la integridad digital en entornos cada vez más conectados. (Prashant y Latesh, 2014)

La extracción de datos en informática forense se erige como una fase crucial, llevada a cabo por expertos en ciencia de datos, para enfrentar los desafíos de seguridad asociados con el cibercrimen. Este proceso se destaca por su importancia fundamental en la investigación forense, donde se busca recolectar información relevante y evidencia digital de manera sistemática y meticulosa. Los científicos de datos, al emplear técnicas especializadas, buscan identificar y recuperar datos cruciales que puedan arrojar luz sobre actividades delictivas en entornos cibernéticos. (Jagadeesha et al., 2019)

2.2.3.3. Número de casos resueltos. Según Heeren (2019) "cuando el especialista de la policía elabora un informe completo que documenta sus hallazgos, se dice que el caso está resuelto" (p. 112). Para realizar dicho informe se debe emplear un lenguaje comprensible para las personas que no tienen una orientación técnica. Este es un componente esencial del informe, ya que en él se exponen todos los datos necesarios para comprender lo que provocó la catástrofe informática.

La entrega de un informe que englobe la totalidad de los datos recolectados a lo largo de la investigación, el ciclo de peritos, la custodia de evidencias y, de manera concluyente, as diversas conclusiones que pueda tener el investigador, las cuales se plasman el testimonio para ser presentado ante el tribunal, se considera una investigación finalizada. Todo el material técnico adicional pertinente que se reunió se incluye en el informe de presentación que es el proyecto final.

III. MÉTODO

3.1. Tipo de investigación

Debido a su relevancia, la próxima pesquisa se ejecutará, y se evaluará el impacto de la norma ISO 27037:2012 en el avance de la informática forense dentro de la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú en Lima durante el año 2022. Asimismo, ya que la investigación aplicada, siguiendo el planteamiento del autor en cita, "se distingue por el interés en tener aplicación hacia los diversos conocimientos ante situaciones concretas de la realidad". (Carrasco, 2019, p. 55)

3.2. Población y muestra

La población estará conformada por la cantidad de datos que se observarán. Por lo tanto, la población estará conformada por 60 observaciones según los indicadores estimados. Para Carrasco (2019), la población es "aquella universalidad o comunidad de la cual se parte para escoger la muestra". Se supone que todo estudio tiene como universo objetivo la población . (Carrasco, 2019, p. 42)

Mientras que la muestra estará accedida por 60 observaciones dentro del proceso de análisis forense en función de las tres dimensiones. Estas observaciones se desarrollarán de la misma unidad de análisis en función del pretest y del postest, respectivamente, según la metodología científica.

3.3. Operacionalización de las variables

Tabla 1

Operacionalización de las variables

Variable	Definición	Dimensiones	Definición	Instrumento	Unidad de medida	Fórmulas
Análisis informático forense	**Definición conceptual** La variable análisis informático forense es una variable del tipo cuantitativa de naturaleza continua y con la escala de medición del tipo razón o proporción. De acuerdo con Hernández et al. (2014), refieren que se considera variable a toda característica o propiedad que sea posible medir observar; además, menciona que el enfoque cuantitativo busca recolectar información para aprobar la hipótesis con base en una medición numérica.	Tiempos de trabajo	El tiempo de trabajo se refiere a todas las etapas del proceso forense digital, que incluye la recopilación, el procesamiento y el análisis del material.	Guía de observación	Porcentaje	$x = \frac{horas\ de\ trabajo\ empleado}{horas\ de\ trabajo\ proyectada} x100$
		Extracción de datos	La adquisición tiene por objeto obtener los datos presentes en un dispositivo digital, que pueden estar cifrados, borrados o en general, ser difíciles de localizar.	Guía de observación	Porcentaje	$x = \frac{Datos\ extraidos}{Datos\ Totales} x100$
	Definición operacional El Análisis Informático Forense fue medido por tres indicadores: (a) tiempos de trabajo, siendo la unidad de medida el porcentaje; (b) extracción de datos, teniendo como unidad de medida el porcentaje y (c) casos resueltos; siendo la unidad de medida el porcentaje. Para los tres indicadores se usó como instrumento de recolección de datos a la ficha de observación.	Casos resueltos	Un caso resuelto es la presentación de un informe que implica toda la información del proceso de investigación, la cadena de pruebas, la cadena de custodia y en última instancia, las conclusiones del investigador que se formulan en un dictamen que se presentará.	Guía de observación	Porcentaje	$x = \frac{Nivel\ de\ Actual}{Nivel\ Deseado} x100$

Fuente: Elaboración propia.

3.4. Instrumentos

Según Hernández et al. (2014) "los instrumentos en medición y recogida son recursos que sirven para generar datos cuantitativos y también recibir información sobre las variables de estudio" (p. 36). En ese sentido, en el presente estudio se empleará el siguiente instrumento:

Tabla 2

Técnica e instrumento

TÉCNICAS	DESCRIPCIÓN	INSTRUMENTOS
Observación	La guía de observación, se desarrolla para registrar los datos de un determinado hecho, fenómeno, objeto o sujeto de investigación.	Guía de observación sobre Análisis Informático Forense

Nota. Elaboración Propia.

3.5. Procedimientos

Durante el desarrollo de este estudio, se determinarán tanto las variables que dependen como las que son independientes. Además, en el proceso de adquisición de datos, se aplicará el método de observación. Asimismo, se diseñarán, validarán y garantizarán la fiabilidad de las pautas de observación para la obtención de datos, las cuales tomarán la forma de una pauta de observación.

Después, consultaremos con varios especialistas para determinar si el documento es jurídicamente vinculante o no. Las pruebas realizadas antes y después del experimento deben recopilarse y compararse para comprobar la exactitud de los resultados. Con la ayuda de la versión 26 del SPSS, estos resultados se almacenarán en un archivo. El alfa de Cronbach se utiliza para generar la determinación del porcentaje de fiabilidad, mostrando así lo consistente y fiable que llega a ser un instrumento cuando se prueba con los protocolos adecuados.

3.6. Análisis de datos

El informe de datos preparado para este estudio incluye el uso de herramientas modernas como Microsoft Excel y SPSS de IBM V26 software para estadísticas para examinar los resultados del pretest y el postest. Se utilizarán tablas y figuras para proporcionar datos cualitativos. La información recibida del dispositivo de medición se utilizará para calcular las tendencias centrales y, a continuación, cada indicación podrá entenderse o comprobarse sobre la base de esas cifras.

Esto contribuirá a establecer una comprensión fundamental de todos los datos numéricos al ofrecer una representación gráfica y ordenada de los mismos. Al concluir el estudio, se aplicará el test de Shapiro-Wilk con el propósito de poder saber si los datos que se obtuvieron siguen una distribución normal o no. Además, se analizará la hipótesis empleando la prueba no paramétrica de Wilcoxon en caso de si la distribución no sea normal, y la prueba t de Student cuando los datos sigan una distribución normal.

3.7. Consideraciones éticas

Se respetarán de manera íntegra las directrices éticas de la Universidad Nacional Federico Villarreal, que promueven la honestidad y la preservación de la integridad de la investigación a través de la adecuada transparencia y veracidad de la información. Estas pautas respaldan el cumplimiento de la información con honestidad y transparencia. Es fundamental destacar que el estudio hará uso de codificaciones que se guiarán por las normas establecidas por la APA en su séptima edición. Al tener en cuenta todo lo expuesto en este proyecto, incluida su autenticidad, se prevé la responsabilidad y dedicación a los principios de uso legal y ético, así como el respeto y mantenimiento de la privacidad de los mismos. Además, se cumplirán las normas antiplagio y se verificará la validez de los datos obtenidos con el uso de un software llamado Turnitin.

IV. RESULTADOS

4.1. Modelo Basado en la ISO 27037:2012 para mejorar del análisis informático forense en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú.

Se procede a detallar el procedimiento técnico que realiza el personal especializado de la DIVINDAT – DIRINCRI, para atender los requerimientos de análisis informático forense de los operadores de justicia, a nivel nacional, conforme al siguiente detalle:

1. El procedimiento pericial (análisis informático forense), inicia desde el momento que el operador de justicia (PNP, MP y PJ) se constituye a esta Unidad Policial custodiando la especie incriminada, que debe encontrarse debidamente rotulada, lacrada y con su cadena de custodia para el examen respectivo.
2. Seguidamente, el operador de justicia será atendido por el personal de servicio de la DIVINDAT, quien procederá a la verificación de la documentación remitida conforme al Manual para el recojo de la Evidencia Digital, aprobado con Resolución Ministerial N° 848-2019-IN (documentos que son entregados en el momento de la atención, no se aceptará la subsanación de documentación posteriormente, para evitar trastornos administrativos), los mismos que se detallan a continuación:
    a. Oficio precisando el objetivo del análisis forense de acuerdo al tipo y modalidad del hecho investigado
    b. Copia certificada y/o autenticada del Acta de incautación, recojo, entrega y otros según corresponda, de los dispositivos, materia de estudio.
    c. Copia certificada y/o autenticada del Acta de lacrado de especie con las firmas del RMP, instructor PNP, intervenidos y otros
    d. Contar con la cadena de custodia original.

e. Copia certificada y/o autenticada de la Autorización del usuario para realizar el análisis informático forense o Resolución Judicial de la medida que limita el derecho – levantamiento del secreto de las comunicaciones y/o documentos personales de los dispositivos de almacenamiento (laptops, equipos celulares, tarjetas de memoria, tarjetas sim, USB entre otros), que disponga el análisis informático forense o extracción de información por el personal especializado de la DIVINDAT. (dicha medida deberá ser manera permanente, sin duración o vigencia de la medida para la ejecución de pericias)

3. Luego, de cumplido con lo indicado en el punto 2, el personal de servicio de la DIVINDAT, procede con la verificación de la remisión del soporte digital por parte de la autoridad requirente para ejecutar el estudio de la evidencia digital y grabar posteriormente la información que se recuperará, bajo los siguientes parámetros:
    a. Si la muestra es un (01) disco duro, una (01) laptop o un (01) equipo de cómputo, la autoridad requirente deberá de remitir un (01) disco duro externo de 2TB con conexión USB 3.0 (o superior) para el estudio pericial respectivo, el mismo que será devuelto con la evidencia digital recuperada.
    b. Si la muestra es un (01) celular, un (01) USB o un (01) chip, la autoridad requirente deberá de remitir un (01) USB de 32 GB con conexión USB 3.0 (o superior) para el estudio pericial respectivo, el mismo que será devuelto con la evidencia digital recuperada
    c. De ser una mayor cantidad de muestras, se deberá tener en cuenta la proporción siguiente: Por cada laptop, pc, disco duro; la remisión de un (01) disco duro externo por cada uno de ellos.

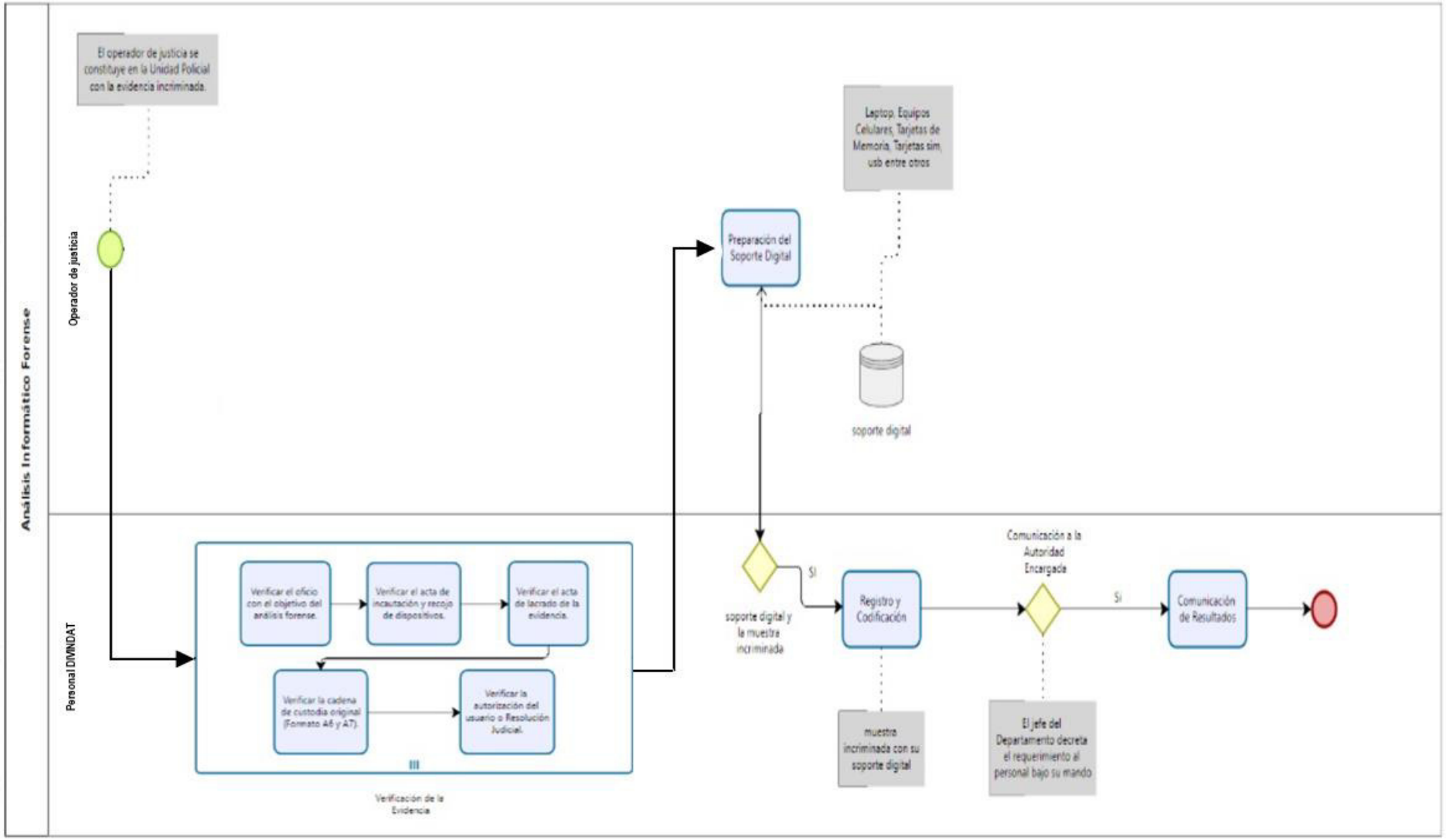
Observación: Es indispensable y obligatorio remitir el soporte digital, al momento de remitir la muestra incriminada a esta unidad policial.

4. Después de cumplirse con la verificación de lo indicado en el punto 3, el personal de servicio de la DIVINDAT, registra y codifica el ingreso de la muestra incriminada con su soporte digital en la plataforma tecnológica de esta Unidad PNP.
5. Seguido a ello, el jefe del Departamento decreta dicho requerimiento al personal bajo su mando, quien a su vez comunica a la autoridad que está a cargo de la investigación el inicio de las diligencias periciales, de acuerdo a lo previsto en el numeral 3 del artículo 177 del Código Procesal Penal.

   Finalmente, luego de haberse culminado con el estudio de la evidencia digital, el personal de esta Unidad comunica a la autoridad requirente que se constituya para realizar el recojo de las muestras y los resultados

Figura 1

Modelo basado en ISO elaboración propia



4.2. Análisis inferencial

4.2.1. Prueba de normalidad

Posteriormente, se describirá los resultados de las pruebas de normalidad de tiempos de trabajo que fueron antes de aplicar la ISO 27037:2012 y posterior a ello.

Tabla 2

Prueba de normalidad

	Kolmogórov-Smirnov			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
pretest 1	,161	60	,001	,890	60	,000
post test 1	,119	60	,034	,948	60	,012
pretest 2	,221	60	,000	,877	60	,000
post test 2	,219	60	,000	,851	60	,000
pretest 3	,396	60	,000	,725	60	,000
post test 3	,373	60	,000	,697	60	,000

a. Corrección de significación de Lilliefors

Los resultados obtenidos en la prueba reflejan que el valor de significancia de la muestra de las dimensiones el pretest 01 es de 0.000 y en el postest 01 es de 0.012; el pretest 2 es de 0.000 y en el postest 2 es de 0.000 y el pretest 3 es de 0.000 y en el postest 3 es de 0.000; los valores han sido menores al error asumido de 0.05 entonces se rechaza la hipótesis nula, deduciendo que las dimensiones no se distribuyen con normalidad.

4.2.2. Contrastación de hipótesis

Prueba de hipótesis 1

Ho: El ISO 27037:2012 no influye positivamente en la mejora de los tiempos de trabajo en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.

Ha: El ISO 27037:2012 influye positivamente en la mejora de los tiempos de trabajo en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.

Considerando el resultado de prueba de normalidad respecto al indicador de extracción de datos evidencia una distribución no normal, se llegó a aplicar la prueba de Wilcoxon.

Tabla 3

Prueba de Wilcoxon para medidas de muestra relacionadas de la dimensión tiempos de trabajo sobre rangos

		N	Rango promedio	Suma de rangos
post test 1 - pretest 1	Rangos negativos	60[a]	30,50	1830,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	60		

a. posttest 1 < pretest 1

b. posttest 1 > pretest 1

c. posttest 1 = pretest 1

Se puede identificar que se analizaron 60 pares encontrándose 60 rangos positivos, un promedio de .00 y una suma total de rangos que es ,00.

Tabla 4

Prueba de Wilcoxon para medidas de muestra relacionadas de la dimensión tiempos de trabajo sobre estadísticos de prueba

	post test 1 - pretest 1
Z	-6,738[b]
Sig. asintótica(bilateral)	,000

b. Se basa en rangos positivos.

Para la contrastación de hipótesis se realizó la prueba de Wilcoxon, donde se visualiza que en la tabla 4 el valor en significancia <fue 0.000 hallándose menor al valor p de 0.05 por lo que se rechaza la hipótesis nula. De igual manera, el valor de Z es de -6,738, la cual está ubicada en la zona de rechazo de la hipótesis nula. Por lo cual se puede concluir que el ISO 27037:2012 influye positivamente en la mejora de los tiempos de trabajo en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.

Prueba de hipótesis 2

Ho: El ISO 27037:2012 no influye positivamente en la mejora de la extracción de datos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.

Ha: El ISO 27037:2012 influye positivamente en la mejora de la extracción de datos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.

Considerando que el resultado de la prueba de normalidad del indicador de extracción de datos muestra una distribución no normal se aplicó la prueba de Wilcoxon.

Tabla 5

Prueba de Wilcoxon para medidas de muestra relacionadas de la dimensión extracción de datos sobre rangos

		N	Rango promedio	Suma de rangos
post test 2 - pre test 2	Rangos negativos	0[a]	,00	,00
	Rangos positivos	60[b]	30,50	1830,00
	Empates	0[c]		
	Total	60		

a. post test 1 < pre test 1

b. post test 1 > pre test 1

c. post test 1 = pre test 1

Se puede identificar que se analizaron 60 pares encontrándose 60 rangos positivos, un promedio de 30,50 y una suma total de rangos que es 1830,00.

Tabla 6

Prueba de Wilcoxon para medidas de muestra relacionadas del indicador de extracción de datos sobre estadísticos de prueba

	post test 1 - pretest 1
Z	-6,737[b]
Sig. asintótica(bilateral)	,000

b. Se basa en rangos positivos.

Para la contrastación de la hipótesis se realizó la prueba de Wilcoxon, donde se visualizó que en la tabla 6 el valor de significancia fue 0.000 hallándose menor al valor p de 0.05 por lo que se rechaza la hipótesis nula. De igual forma, el valor de Z es de -6,737, la cual se ubica en la zona de rechazo de la hipótesis nula. Por lo cual se concluye que el ISO 27037:2012 influye positivamente en la mejora de la extracción de datos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.

Prueba de hipótesis 3

Ho: El ISO 27037:2012 no influye positivamente en la mejora del número de casos resueltos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.

Ha: El ISO 27037:2012 influye positivamente en la mejora del número de casos resueltos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.

Considerando que el resultado de la prueba de normalidad del indicador de extracción de datos muestra una distribución no normal se aplicó la prueba de Wilcoxon.

Tabla 7

Prueba de Wilcoxon para medidas de muestra relacionadas de la dimensión número de casos resueltos sobre rangos

		N	Rango promedio	Suma de rangos
post test 3 - pretest 3	Rangos negativos	0[a]	,00	,00
	Rangos positivos	60[b]	30,50	1830,00
	Empates	0[c]		
	Total	60		

a. post test 3 < pre test 3

b. post test 3 > pre test 3

c. post test 3 = pre test 3

Se puede identificar que se analizaron 60 pares encontrándose 60 rangos positivos, un promedio de 30,50 y una suma total de rangos que es 1830,00.

Tabla 8

Prueba de Wilcoxon para medidas de muestra relacionadas de la dimensión número de casos resueltos sobre estadísticos de prueba

	post test 3 - pretest 3
Z	-6,954[b]
Sig. asintótica(bilateral)	,000

b. Se basa en rangos positivos.

Para la contrastación de la hipótesis se realizó la prueba de Wilcoxon, donde se visualizó que en la tabla 8 el valor de significancia fue 0.000 hallándose menor al valor p de 0.05 por lo que se rechaza la hipótesis nula. De igual forma, el valor de Z es de -6,954, la cual se ubica en la zona de rechazo de la hipótesis nula. Por lo cual se concluye que el ISO 27037:2012 influye positivamente en la mejora del número de casos resueltos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.

4.3.Análisis descriptivo

Descriptivo de la dimensión tiempos de trabajo

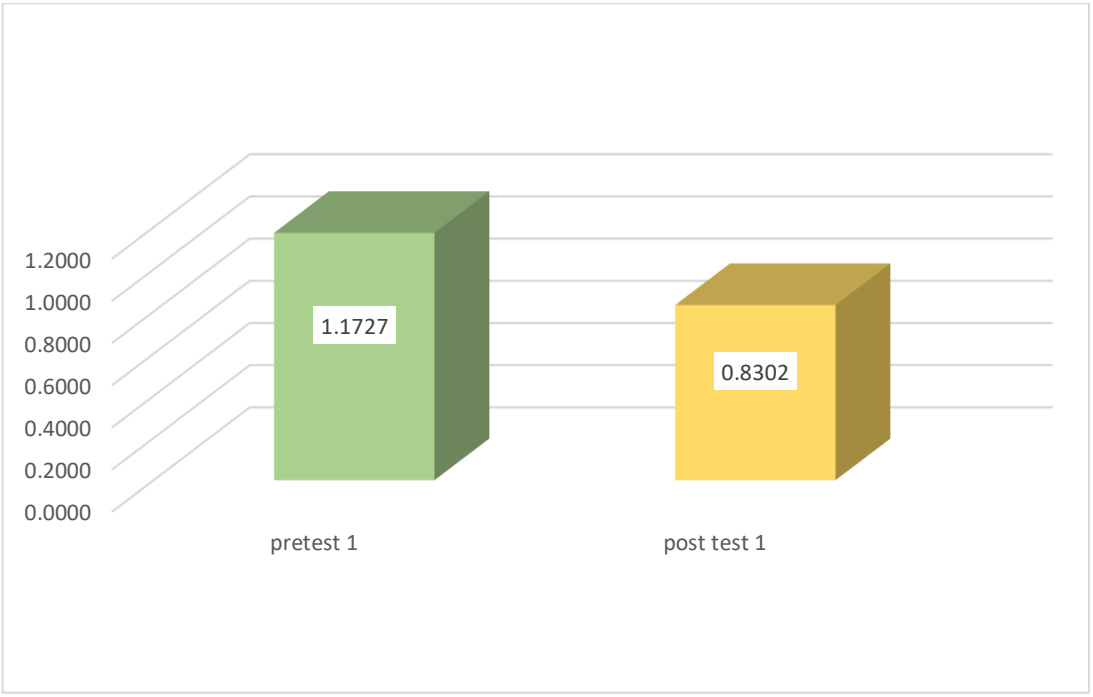
Tabla 9

Análisis descriptivo de los tiempos de trabajo antes y después de aplicar

	N	Mínimo	Máximo	Media	Desv. Desviación
pretest 1	60	,98	1,58	1,1727	,15086
post test 1	60	,67	1,10	,8302	,10301
N válido (por lista)	60				

Figura 2

Grafico descriptivo de la media de tiempos de trabajo



En la tabla 9 se muestra los datos descriptivos del indicador tiempos de trabajo, en el pretest 01 de la muestra la media es 1.1727 veces y el valor del post test 01 es de 0.8302 veces lo que significa que se redujo los tiempos, por lo cual se concluye que existe una mejora significativa después de aplicar el ISO 27037:2012.

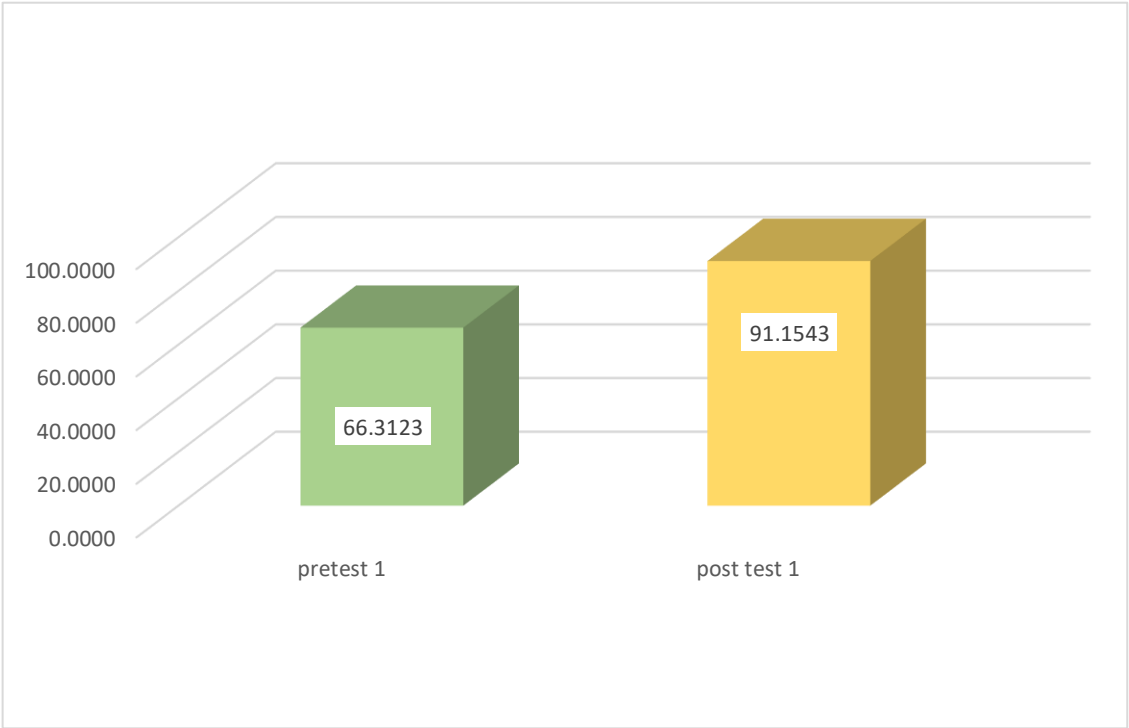
Descriptivo de la dimensión extracción de datos

Tabla 10

Análisis descriptivo de la extracción de datos antes y después de aplicar

	N	Mínimo	Máximo	Media	Desv. Desviación
pre test 2	60	38,92	90,81	66,3123	17,32863
post test 2	60	72,18	99,08	91,1543	7,17699
N válido (por lista)	60				

Figura 3
Grafico descriptivo de la media de extracción de datos



En la tabla 10 se muestra los datos descriptivos del indicador extracción de datos, en el pretest 01 de la muestra la media es 66,3123 datos y el valor del post test 01 es de 91,1543 veces lo que significa que se aumentó la extracción de datos, por lo cual se concluye que existe una mejora significativa después de aplicar el ISO 27037:2012.

Descriptivo de la dimensión números de casos

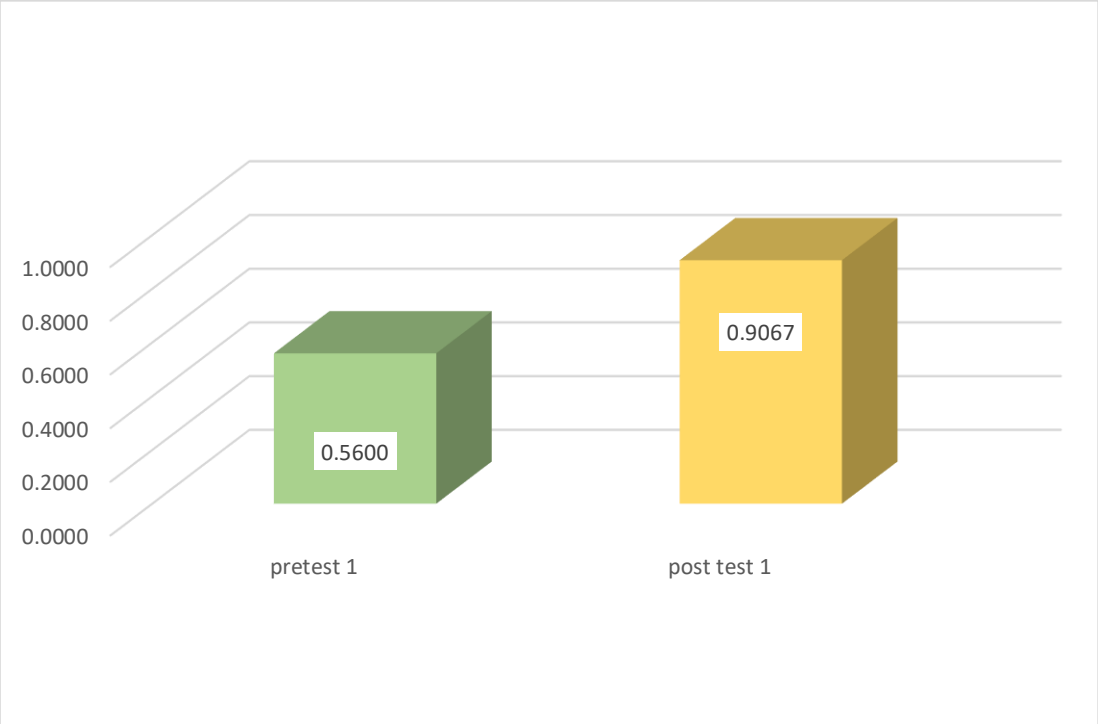
Tabla 11

Análisis descriptivo de los números de casos antes y después de aplicar

	N	Mínimo	Máximo	Media	Desv. Desviación
pre test 3	60	,20	,80	,5600	,12101
post test 3	60	,60	1,00	,9067	,12469
N válido (por lista)	60				

Figura 4

Grafico descriptivo de los números de casos



En la tabla 11 se muestra los datos descriptivos del indicador números de casos, en el pretest 03 de la muestra la media es 0,5600 casos y el valor del post test 03 es de 0,9067 casos lo que significa que se aumentó el número de casos, por lo cual se concluye que existe una mejora significativa después de aplicar el ISO 27037:2012.

V. DISCUSIÓN DE RESULTADOS

Coronel (2019), investigó acerca de la metodología para la obtención de pruebas forenses generadas al momento de utilizar las aplicaciones que fueron desplegadas en entornos web. En dicho estudio, se pudo determinar que el número de denuncias y delitos cometidos a través de aplicaciones web se evidencio un incremento en los años venideros, el cual resalta la necesidad de contar con un manual que detalle las técnicas de investigación forense digital para la gestión de evidencia digital provenientes de entornos virtuales. Asimismo, se llegó a la conclusión de que uno de los principales desafíos al utilizar aplicaciones web es determinar si es factible acceder a ciertos datos en función de la ubicación geográfica. Por esta razón, realizar una investigación de escritorio se presenta como una alternativa viable para llevar a cabo una auditoría de la información adecuada (desde el lado del cliente). A pesar de existentes metodologías y estudios los cuales ofrecen orientación y mejores prácticas, gran parte de ellos se centran en aplicaciones web muy específicas, lo que significa que no pueden generalizarse para abarcar todos los posibles escenarios. En esta investigación, se encuentra que el valor en significancia fue de 0.000, siendo inferior al valor p de 0.05, lo que conduce al rechazo de la hipótesis nula. De igual manera, el valor de Z es de -6.737, lo que lleva a la conclusión de que la norma ISO 27037:2012 tiene un impacto positivo en la mejora de la extracción de datos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú en Lima, en el año 2022.

Pomar (2021) en su trabajo de investigación titulado "Propuesta de investigación: Modelo de análisis forense digital para el sistema de negociación electrónica de la Bolsa Boliviana de Valores, basado en la Norma ISO/IEC 27037:2012", se llega a la conclusión de que, considerando las recomendaciones establecidas en la norma técnica ISO/IEC 27037:2012, se ha analizado un modelo de análisis forense digital que puede ser entrenado para abordar diversas amenazas basadas en incidentes de información crítica. Se logró recopilar pruebas

suficientes y necesarias que puedan utilizarse como evidencia y prueba en los tribunales. Esta especificación proporciona una guía detallada sobre cómo una organización debe proceder para localizar, recopilar, adquirir y almacenar pruebas digitales. En el estudio, se encontró que el valor de significancia fue de 0.000, siendo inferior al valor p de 0.05, lo que lleva la negación la hipótesis nula. De igual manera, el valor de Z es de -6.738, lo que conduce a la conclusión de que la norma ISO 27037:2012 posee un impacto favorable en la mejora de los tiempos de trabajo en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú en Lima en el año 2022.

Rizdqi et al. (2022) en su estudio científico titulado "Digital Forensics: Acquisition and Analysis on CCTV Digital Evidence using Static Forensic Method based on ISO/IEC 27037:2014", se llega a la conclusión de que, en la ciencia forense digital, se utilizan preguntas estándar, como qué, dónde, cuándo, por qué, quién y cómo. Estas preguntas se emplean para comprender el tipo de delito, su ubicación, el momento en que se comete, la motivación detrás del delito, los posibles sospechosos, las víctimas y la estrategia del delincuente, así como los métodos utilizados y los derechos de acceso legales. El proceso de investigación y análisis de pruebas digitales se divide en dos etapas principales: preadquisición y adquisición del núcleo. La cadena de custodia es un concepto fundamental en la investigación forense digital, ya que garantiza la legitimidad de las pruebas desde su descubrimiento y recolección hasta su presentación. La veracidad e integridad de las pruebas se demuestran técnicamente mediante la determinación de su valor hash. La capacidad de incorporar elementos multimedia en el análisis de pruebas digitales es especialmente relevante cuando se trata de pruebas en forma de CCTV. En este estudio, se encontró que el valor de significancia fue de 0.000, siendo inferior al valor p de 0.05, lo que lleva al rechazo de la hipótesis. Asimismo, el valor de Z fue -6.954, lo cual concluye que el estándar ISO 27037:2012 tiene un impacto positivo en la mejora del

número de casos resueltos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú en Lima en el año 2022.

Ramos (2021) el estudio titulado "ISO 27037:2012 en la mejora del análisis forense en la empresa DG Service, Lima 2021" arrojó varias conclusiones relevantes. En primer lugar, se determinó que la adopción de la norma ISO 27037 tendría un impacto significativamente positivo en el análisis forense. En particular, permitiría la captura de más datos de dispositivos móviles, lo que mejoraría la eficiencia del análisis forense. Un aspecto destacado de mejora fue la reducción de las horas dedicadas al análisis forense, lo que implicaba una mayor rapidez en la realización de las operaciones. En el estudio, se encontró el valor de significancia fue de 0.000, lo que es menor que el valor p de 0.05, lo que lleva a la negatividad de la hipótesis nula. Además, el valor de Z fue de -6.738, lo que lleva a la conclusión de que el estándar ISO 27037:2012 influye positivamente en la mejora de los tiempos de trabajo en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú en Lima en 2022.

Velásquez y Davalos (2021) desarrollaron un estudio académico titulado: Informática Forense y su influencia en la Calidad de Servicio en el Centro de Cómputo de la Universidad Tecnológica de los Andes. En el que pudo afirmar que, cuando se habla de informática forense, es fundamental tener en cuenta que este campo se centra principalmente en los problemas de adquisición, conservación, recopilación y presentación de datos para verificar la existencia de un delito informático, evaluar el alcance de los daños causados y localizar a los autores; El estudio identificó que estos datos también pueden servir como un registro histórico que contribuye a prevenir la repetición de errores en el futuro. Además, se llegó a la conclusión de la existencia de una relación significativa entre la variable informática y la calidad del servicio proporcionado por el laboratorio de informática de la Universidad Tecnológica de los Andes. En términos de analizar lo estadístico, se encontró un valor de significancia de 0.000, lo que es menor que el valor p de 0.05. Esto llevó a rechazar la hipótesis nula. Además, el valor de Z fue

de -6.954, lo que llevó a la conclusión de que la norma ISO 27037:2012 influye positivamente en la mejora del número de casos resueltos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú en Lima en 2022.

Araníbar (2021) realizó un estudio científico titulado: La evidencia digital y su influencia en los delitos informáticos en la Corte Superior de Justicia de Arequipa, 2019. La investigación mencionada, concluyó que, la aceptación del valor admisible del testimonio digital es crucial para la supervivencia de los juicios justos a la luz del dramático aumento de los delitos informáticos causado por la introducción de una nueva inseguridad nacional. En consecuencia, el uso de las pruebas digitales en los casos de delitos informáticos ha experimentado un aumento espectacular debido a los actuales avances tecnológicos. Del mismo modo, el rápido avance de las nuevas técnicas ha tenido un profundo efecto en la vida continua de las personas, lo que ha dado lugar a una mayor dependencia de aplicaciones o productos de software que simplifican la vida, pero que también facilitan a los delincuentes la invasión del espacio personal de las personas, el robo de sus bienes y otros trastornos de sus rutinas y actividades habituales. Este espacio en línea se está convirtiendo en una extensión de nuestra vida cotidiana; protegerlo es una prioridad absoluta. Se concluyó además que, en las circunstancias en las que se trata de admitir las pruebas digitales, es imperativo que sean admisibles para que el valor de corroboración de la información electrónica pueda vincularse a la conclusión satisfactoria de los procedimientos penales que implican delitos informáticos. Este estudio revela un valor en significancia de 0.000, que es menor al valor p de 0.05, lo que conduce al rechazo de la hipótesis nula. Asimismo, se obtuvo un valor de Z de -6.954. En consecuencia, se puede concluir que la norma ISO 27037:2012 tiene un impacto positivo en la mejora de la resolución de casos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú en Lima en el año 2022.

VI. CONCLUSIONES

6.1. Según los hallazgos de esta investigación llevada a cabo en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, se puede concluir que la adopción de la norma ISO 27037 conlleva notables mejoras en el campo del análisis informático forense. Estas mejoras son evidentes en dimensiones cruciales, como se refleja en la disminución del tiempo que se emplea durante el estudio de análisis forense, lo que indica una mayor eficiencia temporal. Asimismo, se observa un aumento en la cantidad de datos extraídos, permitiendo una recopilación considerablemente más extensa de información almacenada en dispositivos móviles. Finalmente, se constata una mejora en el indicador relacionado con el número de casos resueltos, lo que se traduce en un aumento de investigaciones concluidas de manera satisfactoria por parte de los analistas forenses.

6.2. Según los resultados obtenidos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú en Lima para el año 2022, se concluye que el ISO 27037:2012 ejerce un impacto positivo en la mejora de los tiempos de trabajo. Esto se sustenta en los resultados pertenecientes a la prueba de hipótesis de Wilcoxon, que arrojaron un valor de significancia de 0.000, siendo inferior al valor p de 0.05, y un valor de Z de -6.738.

6.3. De acuerdo con los hallazgos de la investigación llevada a cabo en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú en Lima en 2022, se concluye que el ISO 27037:2012 genera un efecto favorable en la mejora de la extracción de datos. La conclusión se basa en los resultados de la prueba de hipótesis de

Wilcoxon, donde se obtuvo un valor de significancia de 0.000, lo cual es menor que el valor p de 0.05, y un valor de Z de -6.737.

6.4. Según los resultados de la investigación realizada en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú en Lima en 2022, se concluye que el ISO 27037:2012 tiene un impacto positivo en la mejora del número de casos resueltos. Los hallazgos se sostienen en los resultados que se obtuvieron en la prueba de Wilcoxon, en la que se obtuvo un valor de significancia de 0.000, siendo menor que el valor p de 0.05, y un valor de Z de -6.954. Esto sugiere que la adopción de esta norma contribuye a una mayor eficiencia en la resolución de casos por parte de la División de investigación de delitos de alta tecnología.

VII. RECOMENDACIONES

7.1. Fundamentados en los descubrimientos y resoluciones de este estudio, se sugiere que la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú examine la incorporación y ejecución competente de las regulaciones y guías estipuladas en el ISO 27037:2012 como un componente esencial de su procedimiento de examen de computación forense.

7.2. Explorar la ejecución competente del ISO 27037:2012 como una parte fundamental de sus procedimientos. Esto puede ofrecer una contribución significativa a la mejora de los tiempos de trabajo, mejorando de manera eficiente la forma de gestionar las investigaciones en el dominio de la alta tecnología. La conformidad con este patrón internacional puede asistir en la normalización de operaciones, fomentar la uniformidad y garantizar una mayor rapidez en la obtención de desenlaces, lo que resulta esencial en investigaciones de alta tecnología.

7.3. Es altamente recomendado que la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú adopte y ponga en práctica los conceptos y recomendaciones del ISO 27037:2012 en su fase de obtención de datos. La ejecución de esta norma global puede ejercer un efecto positivo en la optimización de la adquisición de datos, fomentando prácticas normalizadas y efectivas que faciliten la recopilación de evidencia digital con mayor precisión y exhaustividad.

7.4. Se sugiere la implementación de las normativas y pautas del ISO 27037:2012 por parte de División de investigación de delitos de alta tecnología de la Policía Nacional del Perú en sus procedimientos. Esta acción puede influir de manera relevante en el incremento del

número de casos resueltos. La incorporación de prácticas normalizadas y eficaces en el análisis forense de alta tecnología puede agilizar los procesos investigativos, elevar la precisión en la recopilación de pruebas digitales y reforzar la capacidad de la División para resolver casos en un plazo oportuno.

VIII. REFERENCIAS

Adams, R., Hobbs, V. y Mann, G. (2013). The Advanced Data Acquisition Model (Adam): A Process Model for Digital Forensic Practice. *Scientific Journals Journal of Digital Forensics, Security and Law, 8(4), 25*-48. https://commons.erau.edu/cgi/viewcontent.cgi?article=1154&context=jdfsl

Aesides. (2018). Importancia de la gestión del tiempo en el lugar de trabajo. https://www.a3sides.es/blog/importancia-de-la-gestion-del-tiempo-en-el-lugar-de-trabajo/

Ahmed, W., Al, A. y Ahtisham, M. (2021). Can computer forensic tools be trusted in digital investigations? *Scientific Journals Science & Justice, 61(2),* 198-203. https://doi.org/10.1016/j.scijus.2020.10.002

Akash, A., Kapil, K. y Baldev, P. (2021). Next Generation Digital Forensic Investigation Model (NGDFIM) – Enhanced, Time Reducing and Comprehensive Framework. *Scientific Journal of Physics, 1767(1),* e012054. https://iopscience.iop.org/article/10.1088/1742-6596/1767/1/012054/pdf

Antunes, M., Maximiano, M., Gomes, R. y Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *Scientific Journals of Cybersecurity and Privacy, 1(2),* 219-238. https://doi.org/10.3390/jcp1020012

Araníbar, M. (2021). *La evidencia digital y su influencia en los delitos informáticos en la Corte Superior de Justicia de Arequipa, 2019.* (Tesis de grado académico, Universidad Peruana de Las Américas). http://repositorio.ulasamericas.edu.pe/handle/upa/1943

Arteaga, C., Gonzáles, Y., Torres, M. y Valladares, M. (2021). Importancia de un estudio de tiempos y movimientos. Inventio, 16(39), 1–5. https://doi.org/10.30973/inventio/2020.16.39/7

Babulal, S., Roasaheb, G. y Modhe, Y. (2021). A Survey on Digital Forensic Investigation Practitioners Approach and Challenges. *International Journal for Research in Applied Science & Engineering Technology, 9(6).* https://www.ijraset.com/fileserve.php?FID=35544

Baptista, M. (2006). *Aproximaciones a la investigación científica*. España: Siglo XX.

Boasiako, A. (2018), *A Model for digital evidence admissibility assessment*. https://link.springer.com/chapter/10.1007/978-3-319-67208-3_2

Carrasco, S. (2019). *Metodología de la investigación científica*. Ed. San Marcos.

Carroll, O., Brannon, S. y Song, T. (2017). Computer Forensics: Digital Forensic Analysis Methodology. 56 Boletín de abogados de EE. UU. https://www.crime-scene-investigator.net/computer-forensics-digital-forensic-analysis-methodology.html

Castillo, P. (2023). La ciberdelincuencia en el Perú: Estrategias y retos del Estado. Defensoría del Pueblo. https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Cortés, A. (2019). Network Forensics: Concepts and Challenges. Forensic Sci & Criminal Inves, 13(1), 555853. https://juniperpublishers.com/jfsci/JFSCI.MS.ID.555853.php

Cuomo, R., Agostino, D. y Ianurdo, M. (2022). Mobile Forensics: Repeatable and Non-Repeatable Technical Assessments. Sensors, 22(18), e7096. https://doi.org/10.3390/s22187096

Dong, Y. y Zhang, J. (2023). *Digital Forensic Investigation of Automotive Systems: Requirements and Challenges.* [Tesis de maestría, Universidad de Gotemburgo]. Repositorio Institucional Universidad de Gotemburgo. https://odr.chalmers.se/server/api/core/bitstreams/b6fe1760-e2a5-4c32-9d11-b6f230df7b03/content

Du, X. (2020). *Alleviating the digital forensic Backlog a Methodology for automated digital evience processing.* [Tesis de Doctorado]. University College Dublin. Repositorio UCD. https://www.markscanlon.co/papers/PhDThesis-MethodologyAutomatedDigitalEvidenceProcessing.pdf

Duan, R. y Zhang, X. (2020). Research on Computer Forensics Technology Based on Data Recovery. Journal of Physics: Conference Series, 1648, e032025. https://iopscience.iop.org/article/10.1088/1742-6596/1648/3/032025

Espinoza, V. (2022), *Análisis de los delitos informados y el valor probatorio de la evidencia digital en la Corte Superior de Justicia.* [Tesis de Pregrado]. Universidad Cesar Vallejo. Repositorio UCV. https://hdl.handle.net/20.500.12692/90185

Ferreyros, J. (2019). *La auditoría forense como herramienta y de investigación para combatir el fraude y la corrupción financiera publica en el Perú.* [Tesis de Pregrado]. Universidad Inca Garcilaso de la Vega. Repositorio UIGV. http://repositorio.uigv.edu.pe/handle/20.500.11818/4660

Francachs, B. (2021). Modelo para tratamiento forense de incidentes Informáticos en la Nube. *INF-FCPN-PGI Revista PGI*, (8), 22–25. https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/40

Gutiérrez, W. (2022). *Extracción de información en teléfonos celulares y su relación con hechos delictivos en la oficina de peritajes del ministerio público - Lima 2020.* [Tesis de maestría, Universidad Norbert Wiener]. Repositorio Institucional Universidad Norbert Wiener. https://repositorio.uwiener.edu.pe/handle/20.500.13053/7661

Guzmán, A. (2023). *Implementación de herramientas para la extracción de evidencia digital.* [Tesis de Postgrado]. Escuela Politécnica Nacional. Repositorio EPN. https://bibdigital.epn.edu.ec/bitstream/15000/23797/1/CD%2013084.pdf

Hajar, A. (2020). *Analysis of steganographic on digital evidence using general computer forensic investigation model framewor*k. https://www.researchgate.net/publication/346527069work/links/5fc62f2e92851c301299e7a0/analysis-of-steganographic-on-digi- tal-evidence-using-general-computer-forensic-investigation-model-frame- work.pdf

Heeren, H. (2019). *Epistemic problem of pedagogy: some definitions and approximations.* http://repositoriodigital.uct.cl:8080/handle/10925/2506

Horsman, G. (2021). Standardizing digital forensic examination procedures: A look at Windows 10 in cases involving images depicting child sexual abuse. *Scientific Journals Wires Forensic Science, 3(6), e1417*. https://doi.org/10.1002/wfs2.1417

Ibtesam, A. (2019). *Methods and Factors Affecting Digital Forensic Case Management, Allocation and Completion.* [Tesis de doctorado, Universidad Central de Lancashire]. Repositorio Institucional de la Universidad Central de Lancashire. https://clok.uclan.ac.uk/30744/1/30744%20Alawadhi%20Ibtesam%20Final%20e-Thesis%20%28Master%20Copy%29.pdf

Jagadeesha, G., Kotrappa, S. y Veeragangadhara, S. (2019). Digital Forensic Process in Cyber Crime Data Mining, International Journal of Innovative Technology and Exploring Engineering. *Scientific Journals* https://www.ijitee.org/wp-content/uploads/papers/v8i6s/F61320486S19.pdf

Jahankhani, H. y Ibarra, J. (2019). Digital Forensic Investigation for the Internet of Medical Things (IoMT). *Journal of Forensic Legal y Investigative Sciences, 5*. https://www.heraldopenaccess.us/openaccess/digital-forensic-investigation-for-the-internet-of-medical-things-iomt

Justice, M. (2020). The Effectiveness of Digital Forensic Scientific Processes and Methodologies. https://www.linkedin.com/pulse/effectiveness-digital-forensic-scientific-processes-max-justice/

Karabiyik, U., y Akkaya, K. (2018). *Digital forensics for iot and wsns*. https://en.fawproject.com/landingfaw/?gclid=Cj0KCQjw48OaBhDWARIsAMd966B0xk7Byyz1pX2JsRHNrKIFUqKIS2KL04LfHdDZUM4OZed8IqWlw8aAmB6EALw_wcB

Karagiannis C. y Vergidis K. (2021). Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal. *Information, 12*(5), e181. https://doi.org/10.3390/info12050181

Kigwana, I. y Venter, H. (2018). A Digital Forensic Readiness Architecture for Online Examinations. *South African Computer Journal, 30*(1), e466. http://www.scielo.org.za/scielo.php?scriptsci_arttext&pid=S2313783520180100002

Lara, C., Figueroa, Viaña, G. y Corvalán, A. (2020). Evaluación de la Guía de buenas prácticas para la obtención de evidencia digital móvil desde las normas ISO/IEC 27037:2012. La Red. https://elderechoinformatico.com/?p=1208

Mohammed, A. (2019). *Methods and factors affecting digital forensic case management, allocation and completion*. http://clok.uclan.ac.uk/30744/1/30744%20alawadhi%20ibtesam%20fi- nal%20e-thesis%20%28master%20copy%29.pdf

Montasari, R., Hill, R., Carpenter, V. y Montaseri, F. (2019). Digital Forensic Investigation of Social Media, Acquisition and Analysis of Digital Evidence. *International Journal of Strategic Engineering, 2*(1), 1-9. https://www.igi-global.com/article/digital-forensic-investigation-of-social-media-acquisition-and-analysis-of-digital-evidence/219324

Montasari, R., Hill, R., y Carpenter, V. (2019). *The standardised digi- tal forensic investigation process model.* http://nectar.northampton.ac.uk/11862/1/Montasari_etal_Springer_2019_The_Standardised_Digital_Forensic_Investigation_Process_Model_SDFIPM_.pdf

Novak, M., Grier, J. y Gonzales, D. (2018). New Approaches to Digital Evidence Acquisition and Analysis. *National Institute of Justice,* (80), 1-8. https://www.ojp.gov/pdffiles1/nij/250700.pdf

Parvis, K. (2022). *An Empirical Investigation of the Evidence Recovery Process in Digital Forensics.* [Tesis doctoral, Universidad Nova Southeastern]. Repositorio Institucional Universidad Nova Southeastern. https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2177&context=gscis_etd

Pilski, M. (2022). Methods to acquisition digital evidence for computer forensics. *Studia Informatica: systems and information technology, 1*(26), 73-84. https://bibliotekanauki.pl/articles/2175157

Pomachagua, J. (2020), *Desarrollo de un sistema de Auditoría de equipos de seguridad de redes.* [Tesis de posgrado, Pontificia Universidad Católica del Perú]. https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/19072/pomachagua_sotomayor_jorge_desarrollo_sistema_auditor%C3%8DA.pdf?sequence=1&isAllowed=y

Pomar. A. (2021). Modelo de análisis forense digital para el sistema de negociación electrónico de la Bolsa Boliviana de Valores, basado en la Norma ISO/IEC 27037:2012. *INF-FCPN-PGI Revista PGI*, (8), 128–130. Recuperado a partir de https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/68

Prashant, K. y Latesh, M. (2014). Data Generation and Analysis for Digital Forensic Application Using Data Mining. Fourth International Conference on Communication Systems and Network Technologies. http://dx.doi.org/10.1109/CSNT.2014.97

Presman, G. (2016). Desafíos de la Informática Forense. UNL Noticias. https://www.unl.edu.ar/noticias/news/view/desaf%C3%ADos_de_la_inform%C3%A1tica_forense_1

Ramadhan, R., Setiawan, P. y Hariyadi, D. (2022). Digital Forensic Investigation for Non-Volatile MemoryArchitecture by Hybrid Evaluation Based on Revist ISO/IEC27037:2012 and NIST SP800-86 Framework. IT Journal Research and Developmen, 6(2). https://doi.org/10.25299/itjrd.2022.8968

Ramirez, A. (2022). *Importancia de la evidencia digital en la resolución de casos de la Ley de Delitos Informáticos – Ley N° 30096 y modificatorias con la ley N° 30171 en la división de Alta Tecnología PNP, Lima, 2022.* [Tesis de Pregrado]. Universidad Peruana de las Américas. Repositorio UPA. http://repositorio.ulasamericas.edu.pe/handle/upa/1979

Ramos, B. (2019). *Implementación de un software forense para el análisis de la evidencia digital en dispositivos móviles.* [Tesis de Postgrado]. Universidad Tecnológica del Perú. Repositorio UTP. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/5324/B.Ramos_Trabajo_de_Suficiencia_Profesional_Titulo_Profesional_2021.pdf?sequence=1&isAllowed=y

Ramos, B. (2021), *ISO 27037:2012 en la mejora del análisis forense en la empresa DG Service, Lima 2021.* [Tesis de grado, Universidad César Vallejo]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/70930/Ramos_ABD-SD.pdf?sequence=1&isAllowed=y

Reyes, G., Méndez, J., Gonzáles, Y. y Avelino, R. (2017). Importancia de la Aplicación de Estudios de Tiempos y Movimientos para Pequeñas y Medianas Empresas en el Área de Almacén. *Revista Administración y Finanzas, 4(11), 22-41*. https://www.ecorfan.org/bolivia/researchjournals/Administracion_y_Finanzas/vol4num11/Revista_de%20_Administraci%C3%B3n_y_Finanzas_V4_N11_3.pdf

Riggs, H. Imtiaz, P. Aquib, M., Kedari, V. y Sarwat, A. (2023). Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. *Sensor, 23*(8), e4060. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10145335/

Rodríguez, O. (2017). Flexibilidad y distribución del tiempo de trabajo. Especial referencia al caso español. *Revista latinoamericana de derecho social, (25),* 3-35. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-46702017000200003&lng=es&tlng=es.

Roussev, V. (2019). *Forensics knowledge area*. https://www.cybok.org/media/downloads/Forensics_issue_1.0.pdf

Sánchez, H. y. (2006). *Metodología y diseños en la investigación científica*. Visión universitaria.

Santillán, J. y Haro, P. (2021) *Técnicas de seguridad en redes de comunicaciones aplicadas a la custodia de evidencia digital.* [Tesis de Postgrado]. Pontífice Universidad Católica del Ecuador. Repositorio PUCE. https://repositorio.pucesa.edu.ec/bitstream/123456789/3150/1/77312.pdf

Shalaginov, A., Iqbal, A., y Olegård, J. (2020). *Iot digital forensics readi- ness in the edge: a roadmap for acquiring digital evidence from intelligent smart applications.* https://ntnuopen.ntnu.no/ntnuxmlui/bitstream/handle/11250/2729970/_EDGE_2020__IoT_digital_forensics_readiness_in_the_Edge.pdf?sequence=1

Sindhum, K. y Meshram, B. (2012). Digital Forensics and Cyber Crime Datamining. *Journal of Information Security*, 2012(3), 196-201. http://dx.doi.org/10.4236/jis.2012.33024

Stelly, C. (2019). *A domain specific language for digital forensics and incident response analysis*. https://scholarworks.uno.edu/td/2706/

Stoykova, R., Andersen, S. y Stefan, K. (2022). Reliability assessment of digital forensic investigations in the Norwegian police. *Forensic Science International: Digital Investigation*, 40, e301351. https://doi.org/10.1016/j.fsidi.2022.301351

Sudyana, D., Prayudi, Y., Sugiantoro, B. (2019). *Analysis and evaluation digital forensic investigation framework using iso 27037:2012*. https://www.researchgate.net/publication/328281191_Analysis_and_Evaluation_Digital_Forensic_Investigation_Framework_using_ISO_270372012

Tahiri, S. (2016). *Digital forensics models*. Infosec. https://resources.infosecinstitute.com/topics/digital-forensics/digital-forensics-models/

Taubmann, B. (2019). *Improving digital forensics and incident analysis in pro- duction environments by using virtual machine introspection*. https://opus4.kobv.de/opus4-uni-passau/frontdoor/index/index/docId/831 urn:nbn:de:bvb:739-opus4-8319

Veber, J. y Smutny, Z. (2015). Standard ISO 27037:2012 and Collection of Digital Evidence:Experience in the Czech Republic. *14th European Conference on Cyber Warfare & Security*, 2-3. https://www.researchgate.net/publication/283226153_Standard_ISO_270372012_and_Collection_of_Digital_Evidence_Experience_in_the_Czech_Republic

Velásquez, R., y Davalos, F. (2021), *Informática Forense y su influencia en la Calidad de Servicio en el Centro de Cómputo de la Universidad Tecnológica de los Andes.* [Tesis de grado, Universidad Tecnológica de Los Andes]. https://repositorio.utea.edu.pe/handle/utea/288

Villar, H. (2019). Computer forensic analysis protocols review focused on digital evidence recovery in hard disks devices. *Journal of Physics: Conference Series*, 1418, e012008. https://iopscience.iop.org/article/10.1088/1742-6596/1418/1/012008

Yeboah, E. y Akwa, E. (2016). Digital forensic investigations: issues of intangibility, complications and inconsistencies in cyber- crimes. https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/2/5

Yusra, A., Hothefa, S. y Basant, K. (2020). The Use of Machine Learning in Digital Forensics: *Review Paper. Atlantis Press*, (110), 96-113. https://www.atlantis-press.com/proceedings/iciitb-22/125984186

IX. ANEXO

Anexo A. Matriz de Consistencia

PROBLEMA GENERAL	OBJETIVO GENERAL	HIPOTESIS GENERAL	MARCO TEORICO	METODO	TECNICAS E INSTRUMENTOS
¿Cómo influye el ISO 27037:2012 en la mejora del análisis informático forense en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022? **Problemas específicos:** ¿Cuál es la influencia del ISO 27037:2012 en la mejora de los tiempos de trabajo en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022? ¿Cuál es la influencia del ISO 27037:2012 en la mejora de la extracción de datos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022? ¿Cuál es la influencia del ISO 27037:2012 en la mejora del número de casos resueltos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022?	Establecer la influencia del ISO 27037:2012 en la mejora del análisis informático forense en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022. **Objetivos Específicos** Determinar la influencia del ISO 27037:2012 en la mejora de los tiempos de trabajo en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022. Determinar la influencia del ISO 27037:2012 en la mejora de la extracción de datos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022. Determinar la influencia del ISO 27037:2012 en la mejora del número de casos resueltos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.	Existe una influencia positiva del ISO 27037:2012 en la mejora del análisis informático forense en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022. **Hipótesis Específicas** El ISO 27037:2012 influye positivamente en la mejora de los tiempos de trabajo en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022. El ISO 27037:2012 influye positivamente en la mejora de la extracción de datos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022. El ISO 27037:2012 influye positivamente en la mejora del número de casos resueltos en la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú, Lima 2022.	**Fundamentos teóricos** **ISO 27037:2012** Sudyana et al. (2019), refieren que el objetivo principal de las normas ISO 27000 de análisis forense digital es esbozar las formas más eficaces de recopilar pruebas digitales. Se espera que el manejo estandarizado de los pasos del análisis forense permita comparar, combinar y contrastar los datos logrados en dichas investigaciones, a pesar de que puedan ser realizadas por diferentes personas u organizaciones y posiblemente ejecutadas en diferentes jurisdicciones. **Análisis informático forense** Shalaginov et al. (2020), es el proceso de llevar a cabo investigaciones relacionadas con infracciones que involucran cualquier forma de equipo informático, incluidos, entre otros, los ordenadores personales, los servidores, los portátiles, los teléfonos móviles, las tabletas, las cámaras web, los puntos de acceso, los dispositivos del Internet de las cosas o cualquier otro tipo de dispositivo electrónico. También es responsabilidad de los forenses digitales investigar los ataques que se originan en el ciberespacio.	**Métodos** Científico Descriptivo **Tipo** Aplicada **Nivel** Causal **Diseño** Cuasi experimental	**Población** La población estará conformada por la cantidad de datos que se observarán. Por lo tanto, la población estará conformada por 60 observaciones según los indicadores estimados. **Muestra** Mientras que la muestra estará conformada por 60 observaciones dentro del proceso de análisis forense en función de las tres dimensiones. Estas observaciones se desarrollarán de la misma unidad de análisis en función del pretest y del postest, respectivamente, según la metodología científica. **Técnica de muestreo** Se utilizará la técnica de muestreo probabilístico. La misma que según Carrasco (2019), "busca establecer una cantidad muestral en base a un cálculo matemático probabilístico" (p. 92).

Anexo B. Operacionalización de variables

Variable	Definición	Dimensiones	Definición	Instrumento	Unidad de medida	Fórmulas
Análisis informático forense	**Definición conceptual** La variable análisis informático forense es una variable del tipo cuantitativa de naturaleza continua y con la escala de medición del tipo razón o proporción. De acuerdo con Hernández et al. (2014), refieren que se considera variable a toda característica o propiedad que sea posible medir observar; además, menciona que el enfoque cuantitativo busca recolectar información para aprobar la hipótesis con base en una medición numérica.	Tiempos de trabajo	El tiempo de trabajo se refiere a todas las etapas del proceso forense digital, que incluye la recopilación, el procesamiento y el análisis del material.	Guía de observación	Porcentaje	$x = \frac{horas\ de\ trabajo\ empleado}{horas\ de\ trabajo\ proyectada} x100$
		Extracción de datos	La adquisición tiene por objeto obtener los datos presentes en un dispositivo digital, que pueden estar cifrados, borrados o en general, ser difíciles de localizar.	Guía de observación	Porcentaje	$x = \frac{Datos\ extraidos}{Datos\ Totales} x100$
	Definición operacional El Análisis Informático Forense fue medido por tres indicadores: (a) tiempos de trabajo, siendo la unidad de medida el porcentaje; (b) extracción de datos, teniendo como unidad de medida el porcentaje y (c) casos resueltos; siendo la unidad de medida el porcentaje. Para los tres indicadores se usó como instrumento de recolección de datos a la ficha de observación.	Casos resueltos	Un caso resuelto es la presentación de un informe que implica toda la información del proceso de investigación, la cadena de pruebas, la cadena de custodia y en última instancia, las conclusiones del investigador que se formulan en un dictamen que se presentará.	Guía de observación	Porcentaje	$x = \frac{Nivel\ de\ Actual}{Nivel\ Deseado} x100$

Anexo C. Base de datos

	1PreTest	1PostTest	2PreTest	2PostTest	3PreTest	3PostTest
1	1.07	0.78	84.1	94.78	0.2	0.6
2	1.16	0.84	38.92	79.57	0.6	1
3	1.11	0.88	39.97	89.54	0.6	0.8
4	1.11	0.93	82.78	96.6	0.6	1
5	1.15	0.88	90.81	97.7	0.6	1
6	1.22	0.93	41.64	82.94	0.4	0.8
7	1.33	0.67	77.72	97.72	0.6	1
8	1.2	0.73	79.07	97.28	0.4	0.8
9	1.09	0.93	60.59	93.75	0.6	1
10	1.18	0.67	82.16	94.71	0.6	1
11	1.02	0.73	57.95	82.35	0.4	1
12	1.22	0.8	66.46	97.28	0.6	0.8
13	1.58	0.93	52.91	80.64	0.6	1
14	1.07	0.78	84.1	94.78	0.2	0.6
15	1.16	0.84	38.92	79.57	0.6	1
16	1.11	0.91	39.97	89.54	0.6	0.8
17	1.11	0.93	82.78	96.6	0.6	1
18	1.15	0.8	90.81	97.7	0.6	1
19	1.22	0.89	41.64	82.94	0.4	0.8
20	1.33	0.96	77.72	97.72	0.6	1
21	1.2	0.89	79.07	97.28	0.4	0.8
22	1.02	0.93	39.53	79.89	0.6	0.8
23	1.02	0.67	42.32	93.33	0.6	1
24	1.18	0.8	63.41	94.71	0.8	1
25	0.98	0.73	78.41	94.53	0.6	1
26	1.5	1.1	84.1	94.53	0.4	0.8
27	1.4	0.89	63.93	88.61	0.4	1
28	1.05	0.8	72.08	98.66	0.6	0.8
29	1.07	0.8	77.83	89.53	0.6	1
30	1.11	0.91	82.66	92.61	0.6	0.8
31	1.07	0.84	79.09	96.6	0.8	1
32	1.02	0.67	45.51	87.52	0.6	1
33	1.38	0.88	43.02	72.18	0.6	0.8
34	1.33	0.93	76.48	95.79	0.6	1
35	1.02	0.67	39.53	79.89	0.6	0.8

36	1.18	0.73	82.16	94.71	0.6	1
37	1.02	0.73	57.95	82.35	0.4	1
38	1.22	0.8	66.46	97.28	0.6	0.8
39	1.11	0.91	82.66	92.61	0.6	0.8
40	1.07	0.84	79.09	96.6	0.8	1
41	1.02	0.67	45.51	87.52	0.6	1
42	1.02	0.84	42.61	79.89	0.6	0.8
43	1.15	0.75	76.48	99.08	0.6	1
44	1.33	1.02	90.35	94.53	0.4	0.6
45	1.15	0.75	76.48	99.08	0.6	1
46	1.33	1.02	90.35	94.53	0.4	0.6
47	1.58	0.93	52.91	80.64	0.6	1
48	1.07	0.8	77.83	89.53	0.6	1
49	1.09	0.67	60.59	93.75	0.6	1
50	1.4	0.89	63.93	88.61	0.4	1
51	1.05	0.93	72.08	98.66	0.6	0.8
52	1.38	0.8	43.02	72.18	0.6	0.8
53	1.33	0.67	76.48	95.79	0.6	1
54	1.11	0.89	76.48	97.78	0.6	1
55	1.5	0.8	84.1	94.53	0.4	0.8
56	1.02	0.88	42.32	93.33	0.6	1
57	1.18	0.93	63.41	94.71	0.8	1
58	1.11	0.67	76.48	97.78	0.6	1
59	0.98	0.73	78.41	94.53	0.6	1
60	1.02	0.84	42.61	79.89	0.6	0.8