UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE INFORMACIÓN

ISO 27037:2012 en la mejora del análisis forense en la empresa DG Service, Lima 2021

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con mención en Tecnologías de Información

AUTOR:

Ramos Anampa, Bruno Dudu (ORCID: 0000-0003-0292-0807)

ASESOR:

Dr. Visurraga Agüero, Joel Martin (ORCID: 0000-0002-0024-668X)

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

LIMA – PERÚ

2021

Dedicatoria

A mis queridos padres por haberme ayudado en gran parte de mi vida; todo lo conseguido no hubiera sido posible sin la ayuda de ellos entre los que incluyó esta investigación. Porque gracias a sus consejos pude siempre encontrar el camino correcto, gracias por estar siempre ahí.

Agradecimiento

El presente trabajo de tesis primeramente me gustaría agradecer a mi familia, a mis amigos y mis maestros por compartir sus conocimientos conmigo. También a la Universidad Cesar Vallejo por darme las facilidades poder estudiar y ser un profesional

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

La investigación tuvo como objetivo general el determinar que el ISO 27037:2012 mejora el análisis forense en la empresa DG Service, Lima 2021.Mediante esta tesis se mide los resultados obtenidos en el análisis forense después de aplicar el ISO 27037:2012, para poder así identificar la mejora mediante los indicadores de tiempos de trabajo, extracción de datos y número de casos resueltos.

El tipo de investigación fue aplicada, con diseño experimental puro, se utilizó una población de 30 observaciones y el muestreo se realizó por cada indicador. La técnica de recolección de datos usada fue la observación y el instrumento para la recolección de datos fue la ficha de observación. En esta investigación se concluyó que la implementación del ISO 27037:2012 mejora significativamente el análisis forense, donde los puntos fuertes de mejora se evidenciaron a través de los indicadores, para el indicador tiempos de trabajo se obtuvo una reducción de 28.39% en relación con las horas de trabajo, en el indicador extracción de datos la captura de información tuvo un incrementó en un 27.25%, y el indicador de número de casos resueltos aumento en un 38.23%.

Palabras clave: ISO 27037:2012, Análisis Forense, Evidencia Digital, Dispositivos Móviles, Imagen Forense

Abstract

The general objective of the research was to determine that ISO 27037:2012 improves forensic analysis in the company DG Service, Lima 2021, by measuring the results obtained in forensic analysis after applying ISO 27037:2012, in order to identify the improvement through the indicators of working time, data extraction and number of cases solved.

The type of research was applied, with a pure experimental design, a population of 30 observations was used and sampling was carried out for each indicator. The data collection technique used was observation and the instrument for data collection was the observation form. In this research it was concluded that the implementation of ISO 27037:2012 significantly improves forensic analysis, where the strong points of improvement were evidenced through the indicators, for the work time indicator there was a reduction of 28.39% in relation to working hours, in the indicator data extraction data capture had an increase of 27.25%, and the indicator number of cases solved increased by 38.23%.

Keywords: ISO 27037, Forensic Analysis, Digital Evidence, Mobile Devices, Forensic Imaging

I. INTRODUCCIÓN

Actualmente vivimos en una era tecnológica en la que varios dispositivos digitales han simplificado la forma que vivimos, ya que gracias a estos podemos comunicarnos de manera fácil y rápida pero estos medios electrónicos no solo han ayudado a mejorar nuestra calidad de vida sino también ha ocasionado que ciertas personas usan estos medios electrónicos para cometer crímenes. Por ello se desarrolló un nuevo campo conocido como análisis forense digital para investigar y examinar las evidencias digitales. Sin embargo, el campo de la investigación forense digital solo ha adquirido una importancia significativa en estos últimos tiempos debido al creciente número de incidentes de seguridad que se han producido afectando a millones de usuarios alrededor del mundo.

Según Eset (2020), en su investigación reporte de seguridad para Latinoamérica, el Perú es uno de los países de la región que más sufre por los ataques informáticos como por ejemplo el phishing donde se usa correos falsos con un tipo de oferta donde se indican que ganaron algún premio para hacer que los usuarios ingresen sus credenciales y los atacantes tengan acceso a su información, otra amenaza es el ransoware que consiste en encriptar datos sensibles y pedir un rescate para desbloquear la información, este ataque afecta generalmente a los bancos, la suplantación de identidad es otro de los incidentes que sufre el Perú, también hacen uso de la ingeniería social para obtener los datos de sus víctimas como es el usuario y contraseña de las cuentas bancarias con el fin de realizar transferencias de dinero de una cuenta a otra, por estos motivos es necesario que las empresas entiendan la importancia del análisis forense digital el cual permite analizar los datos almacenados en los diferentes equipos electrónicos para poder determinar cómo se generó el incidente informático y qué medidas se debe tomar, existen diferentes tipos de análisis forense como por el ejemplo análisis forense para dispositivos móviles, el análisis forense de base datos, análisis forense para servidores, análisis forense para la nube.

Los investigadores forenses digitales a menudo se enfrentan a la cuestión de tener que explicar cómo se recopiló la evidencia digital. Sin embargo, gracias la necesidad de crear metodologías los investigadores han formulado procedimientos y pautas de mejores prácticas cuando se trata de evidencia digital basados en su experiencia en el campo para poder determinar las causas de un incidente informático.

La empresa DG Service no contaba con un adecuado procedimiento de análisis forense para dispositivos móviles, debido a que en un principio las incidencias informáticas solo ocurrían con frecuencia en computadores o servidores, pero actualmente los dispositivos móviles se han vuelto indispensables para la comunicación y el manejo de información en la organización. De igual forma como paso con las computadoras, estos dispositivos electrónicos se han convertido en una necesidad para lograr los objetivos de negocio en la organización. La mayoría de estos dispositivos móviles nos permiten enviar mensajes de texto, correos electrónicos, acceder a internet, almacenar información personal como fotos, videos y realizar videollamadas. Para el autor Raja Ashif (2021), el no tener bien definido un procedimiento de análisis forense para móviles expone a la empresa a cualquier ataque informático que se realiza desde este medio electrónico, debido que la empresa no sabe detectar correctamente como se ha producido el incidente informático. Además, cuando un dispositivo móvil está involucrado en un incidente informático los analistas forenses deben tener en cuenta que este puede contener información personal o sensible, como por ejemplo las claves de los usuarios, información de tarjetas de crédito, su dirección domiciliaria, el lugar donde trabajan por esta razón se debe tener un especial cuidado con el tratamiento de esta información. En DG Service los empleados del área de sistemas no cuentan con un sólido conocimiento sobre el correcto uso de la metodología para el análisis forense en dispositivos móviles, lo cual se ve reflejado al momento de revisar la evidencia digital recolectada, esto puede ser ocasionado ya sea porque no poseen una guía actualizada o también porque usan el software de manera incorrecta lo que provoca la contaminación

de la evidencia digital (la integridad de la información se pierde o sufre modificaciones) y genera demoras o errores en el análisis de la evidencia digital ocasionado incidentes durante la investigación.

Por otra parte, la presente investigación responde a la pregunta formulada como problema general, ¿De qué manera el ISO 27037:2012 mejora el análisis forense en la empresa DG Service, Lima 2021?, En cuanto a los problemas específicos se formularon los siguientes: ¿De qué manera el ISO 27037:2012 mejora los tiempos de trabajo del análisis forense en la empresa DG Service, Lima 2021?, ¿De qué manera del ISO 27037:2012 mejora la extracción de datos del análisis forense en la empresa DG Service, Lima 2021?, ¿De qué manera el ISO 27037:2012 mejora el número de casos resueltos del análisis forense en la empresa DG Service, Lima 2021?.

Los fundamentos que motivaron a realizar esta investigación fueron los siguientes: en la justificación epistemológica del análisis forense el autor Herrera (2019), indica que existen cuatro fases en el proceso del análisis forense digital los cuales son: identificar el tipo de incidente para mantener intacta la cadena de custodia, otra fase es la preservación de la evidencia donde se genera las imágenes forenses a partir de la información digital, la siguiente fase es el análisis de la evidencia donde se conoce como se llevó a cabo el ataque informático y por último la documentación del incidente donde se redacta todos los hallazgos encontrados. Para la justificación teórica del análisis forense los autores Elyas, Ahmad, Maynard y Lonie (2015), aportan información sobre cómo realizar un análisis forense para dispositivos móviles de forma experimental, donde los resultados obtenidos podrán ser utilizados por futuros investigadores al momento de realizar el análisis en dispositivos móviles, aquí se indica cómo asegurar la escena del crimen, como extraer los datos, como establecer una cadena de custodia y llevar a cabo una prueba de integridad a la evidencia digital. En la justificación practica Prasad (2020), menciona que la aplicación del análisis forense digital permite reconocer los incidentes infor-

máticos que pueden presentarse en cualquier dispositivo electrónico, así como obtener información de como ocurrió el incidente, que métodos se usaron para vulnerar la seguridad, que herramientas informáticas son las más adecuadas para realizar el análisis, como se preservo la información manteniendo su autenticidad y como se solucionó el incidente y finalmente en la justificación metodológica los autores Prayudi, Riadi y Subektiningsih (2018), indicaron que el ISO 27037 contribuye a la mejora de la extracción de datos en los dispositivos móviles, también permite la optimización de tiempos de trabajo al momento de analizar la información digital y además aumenta el número de casos resueltos en el análisis forense.

Por otro lado, el objetivo general de esta investigación fue: determinar que el ISO 27037:2012 mejora el análisis forense en la empresa DG Service, Lima 2021, asimismo los objetivos específicos para esta investigación fueron: determinar que el ISO 27037:2012 mejora los tiempos de trabajo del análisis forense en la empresa DG Service, Lima 2021, determinar que el ISO 27037:2012 mejora la extracción de datos del análisis forense en la empresa DG Service, Lima 2021, determinar que el ISO 27037:2012 mejora el número de casos resueltos del análisis forense en la empresa DG Service, Lima 2021.

Con respecto a la hipótesis general se formuló lo siguiente: El ISO 27037 :2012 mejorara significativamente el análisis forense en la empresa DG Service, Lima 2021, siendo sus hipótesis especificas: El ISO 27037:2012 mejorara significativamente los tiempos de trabajo del análisis forense en la empresa DG Service, Lima 2021, El ISO 27037:2012 mejorara significativamente la extracción de datos del análisis forense en la empresa DG Service, Lima 2021 y El ISO 27037:2012 mejorara significativamente el número de casos resueltos del análisis forense en la empresa DG Service, Lima 2021.

II. MARCO TEÓRICO.

En cuanto a los antecedentes nacionales tenemos a Ferreyros (2019), quien basa su tesis de investigación en una auditoría forense que sirve como una herramienta preventiva para combatir el fraude, aquí indica que la mayoría de las organizaciones no realizan una recopilación proactiva de pruebas adecuadas y admisibles antes a un incidente, ya que existe la percepción de que es demasiado caro, sin embargo, si la evidencia está en su lugar y los procesos están bien definidos, el costo y el impacto de una la investigación se minimizará. El estatus legal de los investigadores forenses es muy relevante a la hora de iniciar procedimientos judiciales. Los investigadores deben conocer varios estatutos relacionados con la privacidad al investigar un incidente específico. Si el investigador descubre datos, por ejemplo, imágenes, video, audio, texto, etc. asociados con una actividad delictiva, deben ser conscientes de sus obligaciones legales y sus derechos en la situación, ya que cuando las pruebas no están relacionadas con el incidente, no se pueden adquirir, sin tener la autorización respectiva.

Para Antón (2018), en su investigación da a conocer sobre una propuesta de políticas y procedimientos del cómputo forense el cual mejora la gestión administrativa de la cual se concluye que los analistas forenses deben estar familiarizados con la mayoría de los tipos de imágenes forenses y ser capaces de realizar la extracción de datos. La evidencia encontrada en un disco duro puede ser crítica para determinar una secuencia de eventos u obtener archivos reales que puedan ayudar a determinar la causa raíz. Finalmente, como con cualquier proceso en una disciplina forense, la creatividad por parte de los analistas debe llevarse a cabo de manera sistemática en la que todos los pasos se sigan y se documenten adecuadamente. Esto asegurará que cualquier evidencia obtenida sea sólida y admisible en una corte.

Cajamarca (2016), desarrollo una investigación sobre la implementación de un laboratorio de informática forense donde comento que es necesario tener un

hardware y software especializado para realizar el análisis de las evidencias digitales recolectadas. Además, de conocer las diferentes técnicas de adquisición de imágenes y cuáles son las diferencias de una con respecto a la otra, la cual permitirá a los analistas preparar informes con precisión y testificar sobre sus hallazgos. Uno de los primeros conceptos que debe entenderse es la diferencia entre las imágenes forenses y las copias. Copiar archivos de un disco duro sospechoso u otro medio solo proporciona a los analistas los datos reales asociados con ese archivo. Las imágenes, por otro lado, permiten al analista capturar todo el disco. Esto incluye como el espacio no asignado, acceso a archivos eliminados, los metadatos. A menudo, los términos clonación e imagen se utilizan uno en lugar del otro. Al clonar una unidad, se realiza una copia individual de la unidad. Esto significa que la unidad se puede insertar en un sistema y arrancar. La clonación de una unidad de disco a menudo se utiliza para hacer una copia de seguridad completamente funcional de una unidad crítica. Si bien una unidad clonada contiene todos los archivos necesarios, es complicado trabajar con ella, especialmente con herramientas forenses. Por esta razón se usa una imagen forense.

Asimismo, De La Cruz (2015), planteo una aplicación de metodologías y herramientas de la informática forense para reducir los riesgos de la seguridad informática, donde la evidencia digital que se extrae de una imagen forense debe ser auténtica. Los datos que son extraídos pueden considerarse como auténticos si pueden verificar su integridad, por ello la evidencia digital se verifica mediante un algoritmo hash. Este valor asegurará la autenticidad de la evidencia digital requerida durante las etapas posteriores de la investigación. Los requisitos de integridad se pueden lograr mediante el uso de las características tecnológicas proporcionadas por las herramientas forenses digitales. Entre los algoritmos más usados tenemos al MD5 o SHA-1 para autenticar datos después de generar la imagen forense.

Adicionalmente Yopla y Yopla (2014), presentan una metodología para la captación de pruebas digitales en el análisis forense. Su estudio se basa es sugerir un marco metodológico que pueda aplicarse al cómputo forense de los dispositivos electrónicos. Además, después de generarse las imágenes forenses estas deben

ser capaces de proveer información concisa y clara, la evidencia digital debe ser conservada de manera segura a fin de que la información no sufra algún daño o modificación que pueda dejar inutilizable la evidencia digital. Adicionalmente indica que existen diferentes formatos al realizar la creación de una imagen forense por esta razón se debe tener en cuenta que la aplicación con la cual se analice admita varios formatos diferentes.

En cuanto a los antecedentes internacionales tenemos Du (2020), quien tuvo como objeto de su investigación una metodología para el procesamiento automatizado de pruebas digitales que usa una técnica de deduplicación de datos para hacer frente al reto de analizar datos pesados. Según su estudio su técnica facilita la clasificación de las pruebas almacenadas de forma automatizada la cual ayuda a los investigadores a descubrir nuevos datos que no fueron encontrados anteriormente. Esta técnica de reconstrucción forense facilita la verificación de la integridad del sistema de adquisición de datos deduplicados, Además su sistema elimina el procesamiento repetido de datos y determina automáticamente que archivos son pertinentes para la investigación. Los archivos detectados pueden ofrecer una indicación para el resto de la investigación y ayudar a recopilar información valiosa sobre como ocurrió el incidente en el dispositivo.

Para Heloıse (2019), tuvo como su objeto de investigación la evaluación e identificación de datos auténticos de teléfonos inteligentes y el establecimiento de la autenticidad de dichos datos. Para establecer la autenticidad de los datos del teléfono inteligente, se requiere conocer del comportamiento de las aplicaciones de los teléfonos inteligentes. Para ello es necesario entender el modelo de las aplicaciones de los teléfonos utilizando una arquitectura como referencia. La arquitectura de referencia proporciona la información necesaria para identificar los requisitos que deben cumplir los datos auténticos de los teléfonos inteligentes, lo que llevó al diseño del modelo de evaluación de datos. Los resultados producidos por el modelo de evaluación de datos del teléfono inteligente se utilizan como entrada para esta-

blecer la autenticidad de los datos. Gracias a esto se puede generar una herramienta forense digital que permite detectar con más facilidad los datos auténticos generados.

Para Singh (2019), quien realizo un estudio sobre el análisis forense para detectar un ransomware, indica que la ciencia forense digital consiste en la recuperación e investigación de los datos obtenidos de los dispositivos digitales relacionados con el ataque informático, siendo los dispositivos encriptados un reto importante para la ciencia forense digital debido a la dificultad de recuperar información probatoria potencial para los litigios. Según su investigación, el uso de un mecanismo criptográfico como BitLocker, así como de estándares avanzados de cifrado para proteger la información, plantea un problema importante para un investigador. Si una unidad ha sido cifrada, un investigador necesitaría las claves de descifrado para investigar la unidad. Sin embargo, la mayoría de las veces las claves de descifrado se desconocen y un investigador tendría que utilizar un método de fuerza bruta para descifrar la unidad y realizar una investigación. El sistema operativo Windows, al ser el más utilizado, es un objetivo central para los atacantes que explotan las vulnerabilidades de cada versión del sistema operativo. Por lo tanto, para investigar un ataque de ransomware a menudo es complicado para un investigador forense digital recuperar evidencia digital potencial que pueda ser utilizada en un tribunal. Sin embargo, tras la investigación, se puede encontrar el método de explotación diseccionando el ejecutable del ransomware a un nivel inferior, lo que implica rastrear la ejecución del programa y supervisar los cambios en el comportamiento de cada instancia

Mosbah (2018), se enfocó en técnicas forenses para teléfonos inteligentes, haciendo énfasis en la importancia del análisis forense digital para proporcionar una solución que identifique correctamente al sospechoso, así como la solución que contribuye a un buen nivel de seguridad y como medida de la integridad de las pruebas digitales. Su investigación refleja la importancia del análisis forense digital para los dispositivos en general y para los teléfonos inteligentes en particular, ya que estos dispositivos están ampliamente distribuidos en la vida de las personas y éstas

confían en ellos para realizar sus tareas diarias más que nunca, lo que lleva a los crackers a cometer ciberdelitos. Además, en su investigación propuso un modelo de dos etapas. La primera etapa es el proceso de recogida de datos, que se basa en seguir el proceso forense digital, donde se obtienen los datos necesarios del smartphone y se almacenan un dispositivo de almacenamiento, en segundo lugar, hace uso de una suite forense para poder acceder a los datos y descubrir cómo se originó el incidente informático.

Para Ahmad (2018), tuvo como objeto de estudio la integración del análisis de comportamiento dentro del proceso de análisis forense en donde indica que el nuevo software debe proporcionar a los investigadores profesionales una forma más interactiva, cómoda y eficiente de capturar evidencias mediante herramientas forenses digitales fiables y adecuadas. En el futuro se debe contar con suites especializadas para cada sistema operativo existente, que sean más eficaces y fáciles de usar, porque los sistemas se hacen cada vez más complejos lo cual dificulta poder examinar y analizar la incontable data que puede estar disponible en los medios electrónicos.

Sugiantoro (2018), realizo una investigación de casos comunes sobre el análisis forense en teléfonos inteligentes Android para tratar con la ciberdelincuencia, en su estudio describe en cómo abordar el problema de los casos de delitos con teléfonos inteligentes e intenta realizar un análisis forense exhaustivo a móviles o tabletas que utilicen sistemas operativos Android. Además, este estudio tiene como objetivo evaluar las herramientas forenses que se pueden utilizar para analizar móviles en función de la cantidad de evidencia que puede recopilar desde las herramientas forenses. Además, hace uso de métodos de minería de datos o método de ponderación que se utiliza en el proceso de identificación de casos, donde este método ayudará al investigador a determinar documentos en forma de mensajes que se utilizarán como evidencia y ayudará a los investigadores a encontrar nuevas pistas.

Dimpe y Kogeda (2017), tuvo como objeto de estudio el impacto del uso de herramientas forenses digitales poco fiables, La evolución tecnológica o la proliferación de dispositivos móviles y el aumento de las transacciones de comercio móvil han provocado un aumento de los casos de delitos cibernéticos. Los avances tecnológicos siempre también se han utilizado en beneficio de la criminalidad. Para contrarrestar esto, se desarrollaron una serie de herramientas forenses digitales para ayudar a los investigadores forenses a investigar y detener a los ciberdelincuentes. Algunas de las herramientas se desarrollaron teniendo en cuenta el proceso forense, mientras que otras se diseñaron para satisfacer las necesidades de un grupo de interés en particular, pero carecían de diseños creados con las necesidades de la ciencia forense y como resultado algunas herramientas producen pruebas poco fiables. Los investigadores forenses hacen uso de herramientas (tanto en hardware como software) para investigar el delito cibernético, los resultados producidos por las herramientas se utilizan en el tribunal para emitir juicios y para que la evidencia sea aceptada, debe ser confiable, por lo tanto, Es necesario utilizar una herramienta confiable para producir buenos resultados.

Rochmadi, Riadi y Prayudi (2017), realizaron una investigación sobre técnicas anti forenses en un navegador web portátil privado donde hicieron énfasis sobre los eventos que dificultan el análisis forense en los medios electrónicos: como el ocultamiento de datos, esto es difícil investigar porque los datos no están disponibles y visibles para el investigador. Por lo tanto, los delincuentes emplean diferentes técnicas para ocultar pruebas, como destruir la Información o cambiar la evidencia con el objetivo de hacer que esta sea inutilizable, otra técnica muy usada es el cifrado de datos porque aquí los archivos se encriptan y la única forma de acceder a la información es conociendo la contraseña que por lo general contienen letras, números y caracteres especiales. Por eso el investigador forense tiene que ser consciente que los sospechosos pueden ocultar sus datos utilizando diferentes métodos.

Sadiku, Tembely, Musa (2017), en su investigación sobre el cómputo forense, indicaron que el análisis de las pruebas almacenadas en un medio electrónico es uno de los mayores retos a los que se no enfrentamos como por ejemplo las leyes

pueden restringir la capacidad de los analistas para llevar a cabo investigaciones, ya que las legislaciones nacionales e internacionales pueden obstaculizar la cantidad de información que se puede incautar. Otro de los principales retos de la investigación forense digital es el creciente volumen de datos que hay que analizar. Con la aparición de la big data, la forma de llevar a cabo las investigaciones forenses digitales debe cambiar. Esta big data se consideran conjuntos de datos demasiado grandes y se caracterizan por el volumen, la velocidad, la variedad y la variabilidad de los datos otros retos son la computación en la nube, los metadatos, las técnicas anti forenses, el cifrado, el Internet de las cosas y las redes inalámbricas. Sin embargo, las técnicas anti forenses se están convirtiendo en un formidable obstáculo para la comunidad forense digital. Están diseñadas para obstaculizar o eludir el análisis forense. Porque estos buscan comprometer la disponibilidad o la utilidad de las pruebas durante el análisis.

Según Asha y Singh (2016), indica que la evolución de la informática forense fue debido al aumento de la delincuencia digital por el desarrollo de Internet y la proliferación de la tecnología informática. En esta investigación, se ha identificado muchas categorías de actividades en informática forense. Algunas categorías de investigación son el marco, la fiabilidad, la informática forense en entornos de red o virtualizados, la adquisición y el análisis de datos de pruebas. Esto sumado a que los virus informáticos están desarrollando una inteligencia artificial que les permite interactuar con sus victimas y evadir los controles de seguridad.

Para Hussam, Clarke, Li (2016), el usar una metodología para integrar big data de fuentes heterogéneas y realizar análisis automatizados de datos, es un nuevo desafío clave en la actualidad. Su investigación se centró en el desarrollo de experimentos para evaluar la viabilidad de utilizar solo los metadatos, esto debido a que la información de los medios electrónicos tiene a crecer rápido en poco tiempo, lo cual indica que al realizar el análisis forense a dispositivos de última generación requerirá consumir muchos recursos en términos de hardware y software. Lo cual

se traduce en que el investigador podría tener investigaciones cada vez mas complejas.

Reza (2016), indica que la complejidad de los nuevos dispositivos móviles puede dificultar las investigaciones cuando se realiza el análisis forense sin embargo esto no debe verse como solo un problema sino como una oportunidad para mejorar las herramientas informáticas de tal manera que puedan procesar grandes cantidades de información, incluso agregarles funcionalidades de inteligencia artificial para que estas herramientas puedan detectar mas rápidamente comportamiento inusuales en la información almacenada dentro la evidencia digital.

Sarwar, Shoaib, Shahzad (2016), indica que la concientización sobre los peligros informáticos a los que estamos expuestos está siendo dejado de lado por las compañías, si bien el análisis forense ayuda a establecer controles de seguridad , las capacitaciones sobre seguridad de la información no pueden ser dejados de lado, porque la mayoría de los incidentes informáticos tiene como victima a usuarios que no cumplen con las políticas de seguridad establecidas por la compañía

Para Sathiyanarayanan (2016), tuvo como objeto de estudio el análisis forense en sistemas informáticos abiertos, en sistemas de comunicación y sistemas informáticos integrados. Indicó que las pruebas digitales pueden duplicarse con exactitud y son difíciles de destruir si se hace un correcto almacenamiento de estas, además pueden encontrarse en discos duros, unidades flash, teléfonos, dispositivos móviles, routers, tabletas e instrumentos como el GPS. Para ser admisibles, las pruebas deben cumplir con los requisitos de integridad.

Harbawi, Varol (2016), realizo un estudio sobre el papel del análisis forense en la lucha contra los ciberdelitos, la idea de las ciencias forenses digitales se basa en un entorno electrónico y/o en la escena del crimen del ciberespacio. En este sentido, es probable que se necesiten los conocimientos técnicos para poder analizar la escena. Este análisis tiene como objetivo identificar las piezas del rompecabezas que resuelven el crimen electrónico. Por lo tanto, lo primero que se debe

considerar es que la evidencia esté en la forma digital. Las pruebas digitales pueden definirse como cualquier forma de datos que se hayan movido desde un sistema electrónico; lo que podría ser un documento, un audio, un vídeo, el historial de navegación, las actividades de las redes sociales, los registros, la banca electrónica y las transacciones con tarjetas de crédito.

Jeetendra y Prasad (2016), tiene como objeto de estudio las diferentes herramientas que se pueden aplicar en un análisis forense, como por ejemplo aquellas aplicaciones que pueden extraer los datos desde la imagen forense. Como no existe una herramienta que extraiga toda la información posible, es aconsejable utilizar dos o más herramientas para el examen, el análisis forense de teléfonos móviles implica recabar información sobre registros de llamadas, listas de contactos, registro de navegación web, archivos de configuración, información de ubicación geográfica, correo electrónico, registros de proveedores de servicios, archivos de aplicaciones, etc. La incautación y adquisición del análisis forense para móvil son relativamente diferentes a las del sistema de otros sistemas operativos como Windows. Las herramientas de adquisición forense se pueden clasificar en herramientas de adquisición de hardware y herramientas de adquisición de software. Por ejemplo, la bolsa de Faraday es una herramienta de adquisición de hardware, mientras que la suite forense Santoku Linux son herramientas de software para la adquisición.

Singh y Joshi (2015), indican en su investigación la importancia de la generación de imágenes forenses y sus diferentes tipos además resalta la necesidad de saber que herramientas de adquisición utilizar para no dañar la evidencia digital, por lo cual recomiendan contar con una suite forense como Caine, Kali Linux o Santoku, para recolectar la información se debe comenzar por los datos volátiles , la cual se almacena en la RAM del móvil y luego proseguir con la información interna del móvil, toda esta información debe ser almacenada en un medio electrónico para su posterior procesamiento en un laboratorio forense digital.

Entre tanto en la teoría del análisis forense informático para Kävrestad (2018), la informática forense es un campo joven que se define por su carácter reactivo. Desde sus inicios, la ciencia forense digital ha evolucionado rápidamente sin

que falten fundamentos teóricos. Los profesionales han definido las mejores prácticas y han desarrollado herramientas en función de las necesidades, esas mejores prácticas y herramientas han empezado a ser analizadas por los investigadores durante la última década. Este rápido desarrollo ha dado lugar a muchas preguntas sobre la calidad y solidez de esas mejores prácticas. El objetivo final de los investigadores y profesionales de la ciencia forense digital es que este campo se convierta realmente en una ciencia como la ciencia forense tradicional. La ciencia forense digital está sujeta a los mismos principios legales que la ciencia forense tradicional. Por lo tanto, los investigadores y profesionales deben tener el mismo nivel de rigor y solidez científica para que las pruebas digitales sean admisibles de forma fiable en los tribunales.

Otra teoría es mencionada por Monat y Gannon (2017), que tienen una investigación sobre la aplicación del pensamiento sistémico a la ingeniería y el diseño considera que la unidad fundamental de análisis es "un sistema" formado por muchas partes o estructuras. Desde una perspectiva sistémica donde todo sistema en un determinado nivel está en relación con los suprasistemas y los subsistemas. Los primeros están ordenados jerárquicamente en función de su influencia en el sistema; los segundos deben ser dirigidos y gestionados por el sistema para contribuir a su finalidad. Como el contacto crea participación, un sistema determinado tiende a absorber los suprasistemas y los subsistemas (componentes) para desarrollarse como un sistema completo.

En cuanto a la variable independiente ISO 27037:2012 para Sudyana, Prayudi y Sugiantoro (2019), El objetivo fundamental de las normas ISO 27000 para el análisis forense digital es mostrar métodos y procesos de buenas prácticas para la captura de pruebas digitales. Aunque los investigadores y las organizaciones pueden conservar ciertos métodos, procesos y controles, se espera que una estandarización en el manejo de las de las fases del análisis forense, facilitando la comparación, la combinación y el contraste de los resultados obtenidos de tales investigaciones, incluso si son realizadas por diferentes personas u organizaciones y probablemente ejecutado en otras jurisdicciones deben obtenerse los mismos resultados.

Por ello una de las cuestiones más críticas en las investigaciones forenses es la adquisición y conservación de las pruebas de manera que se garantice su integridad. Al igual que en el caso de las pruebas físicas convencionales, es crucial que el primer interviniente y los subsiguientes (definidos como "Primeros intervinientes en pruebas digitales" y "especialistas en pruebas digitales") mantengan la cadena de custodia de todas las pruebas forenses digitales, garantizando su protección mediante procesos estructurados que sean aceptables para los tribunales. Como por ejemplo la integridad de las imágenes forense.

Para Mohammed (2019), la aplicación del ISO 27037 no debe sustituir a los requisitos legales específicos de ninguna jurisdicción. Por el contrario, puede servir de orientación práctica para cualquier investigación que impliquen posibles pruebas digitales. No se extiende al análisis de las pruebas digitales y no sustituye a los requisitos específicos de cada jurisdicción relativos a cuestiones como la admisibilidad, la ponderación de las pruebas, la pertinencia y otras limitaciones controladas judicialmente sobre el uso de posibles pruebas digitales en los tribunales de justicia. Esta norma internacional puede ayudar a facilitar el intercambio de posibles pruebas digitales entre jurisdicciones. Para mantener la integridad de las pruebas digitales, los usuarios de esta norma internacional deberán adaptar y modificar los procedimientos descritos en esta Norma Internacional de acuerdo con los requisitos legales de la jurisdicción específica en materia de pruebas a la que pertenecen.

Para Proffitt (2019), en su investigación que analizo un modelo para aplicarlo con el ISO 27037, indica que los procesos especificados en las directrices de la norma garantizan que los investigadores forenses digitales mantengan la integridad de las pruebas digitales durante las fases de recogida de las investigaciones, siguiendo metodologías de análisis destinadas a promover la admisibilidad de las pruebas durante los procesos judiciales. La importancia de la integridad subraya que las pruebas deben gestionarse correctamente para que no pierdan valor en consecuencia, sino sean admisibles ante quien solicite información.

Según Boasiako (2018), su modelo aplicado con el ISO 27037 posee procesos, procedimientos y resultados que pueden ser auditados por investigadores forenses independientes para evaluar las actividades realizadas. Las auditorías forenses pueden bajar su complejidad si los procesos y las acciones seguidas por los investigadores están correctamente documentadas. Por ello los investigadores forenses digitales deben ser capaces de explicar porque tomaron ciertos pasos sobre otros cuando realizan sus investigaciones.

Según Veber y Smutny (2015), la adquisición de la evidencia digital proporciona directrices para actividades específicas cuando se manejan de pruebas digitales, por cual en las fases que son la identificación, la recogida, la adquisición y la conservación de posibles pruebas digitales que puedan tener valor probatorio. Esta proporciona orientación a los individuos de cómo llevar a cabo de manera correcta el proceso de manejo de la evidencia digital, además de ayudar a las organizaciones en sus procedimientos disciplinarios y facilitar el intercambio de evidencia digital entre jurisdicciones.

En cuanto para la variable independiente de análisis forense el autor Shalaginov, Asif y Olegård (2020), menciona que es el proceso de investigación de los delitos cometidos mediante cualquier tipo de dispositivo informático, como ordenadores, servidores, portátiles, teléfonos móviles, tabletas, cámaras digitales, dispositivos de red, dispositivos del Internet de las cosas o cualquier tipo de dispositivo electrónico. Los forenses digitales también se encargan de examinar los ataques originados en el ciberespacio, como el ransomware, el phishing, los ataques SQL Injection, los ataques de denegación de servicio distribuidos, la violación de datos y cualquier tipo de ciberataque que cause pérdidas financieras o de reputación. El objetivo final de una investigación forense digital es preservar, identificar, adquirir y documentar las pruebas digitales que se utilizarán en los tribunales.

Para Stelly (2019), El proceso forense tiene cuatro fases que se producen después de que se haya hecho una solicitud y se haya aprobado: recopilación, examen, análisis y el informe. Las actividades previas se producen durante la creación de un caso, cuando un cliente solicita una investigación y ésta se aprueba. En la

fase de recopilación se identifican, recogen e inventarían los datos relacionados con la solicitud de investigación. El examen utiliza herramientas forenses para interpretar los datos. En la fase de análisis se utilizan los resultados del examen para encontrar respuestas a las preguntas formuladas en la solicitud de investigación. En la fase del informe se describen los resultados y la metodología y se entregan al solicitante. Por último, se revisa el caso y se registran y consideran las sugerencias de cambios en la política, el procedimiento o las herramientas basadas en las lecciones aprendidas durante el caso.

Para Montasari, Hill y Carpenter (2019), La ciencia forense digital se define como el proceso de conservación, identificación, extracción y documentación de pruebas informáticas que pueden ser utilizadas por los tribunales. Se trata de una ciencia que busca pruebas en medios digitales como un ordenador, un teléfono móvil, un servidor o una red. Proporciona al equipo forense las mejores técnicas y herramientas para resolver casos complicados relacionados con lo digital. La ciencia forense digital ayuda al equipo forense a analizar, inspeccionar, identificar y preservar las pruebas digitales que residen en diversos tipos de medios electrónicos.

Según Karabiyik Umit y Kemal (2018), La ciencia forense digital es también conocida como ciencia forense informática, una aplicación para determinar un método de examen científico a los ataques informáticos. También se define como "la forma de identificar, preservar, examinar y analizar las pruebas digitales, mediante la validación de los procedimientos, y su representación final de esa evidencia digital en la corte para evidenciar algunas cuestiones legales en relación con el crimen y los ataques informáticos.

Según Obiora (2018), los especialistas en informática forense desempeñan un papel importante en el proceso de investigación de los ciberdelitos. Principalmente, se ocupan de la recuperación de datos que fueron encriptados, borrados u ocultados. Las tareas también incluyen garantizar la integridad de la información que se va a utilizar en los tribunales. En las distintas fases de la investigación, los

analistas informáticos forenses pueden participar en el interrogatorio de sospechosos, víctimas y testigos. También ayudan a preparar las pruebas que se presentarán ante el tribunal.

Según Yeboah-y Akwa (2016), la ciencia forense digital implica recopilar y examinar cuidadosamente pruebas o artefactos electrónicos, así como un análisis e interpretación precisos de las pruebas recopiladas. Este proceso de investigación evalúa el alcance del daño a un sistema comprometido o atacado, así como también recupera la información perdida de dicho sistema comprometido y, en última instancia, presenta la evidencia digital para enjuiciar a los perpetradores de delitos cibernéticos. Se ha vuelto imperativo que los funcionarios encargados de hacer cumplir la ley y los examinadores forenses digitales se adhieran a los altos estándares de la profesión, si las pruebas digitales fueran permitidas en un tribunal de jurisdicción competente.

En cuanto a los indicadores de la variable análisis forense de esta investigación se está considerando los siguientes indicadores los cuales son tiempos de trabajo, extracción de datos, el número de casos resueltos para la variable dependiente análisis forense. para el indicador de tiempos de trabajo según Roussev (2019), lo define como el campo de la ciencia forense digital siempre se ha visto afectado por su incapacidad para desarrollar un compromiso entre el tiempo empleado y la precisión. En la mayoría de las soluciones que se propusieron para resolver este problema, la reducción del tiempo empleado se tradujo en una degradación de la precisión y viceversa. Además, los modelos útiles carecían de generalidad, lo que dificultaba su aplicación en distintos escenarios y los que sí proporcionaban generalidad ofrecían poca o ninguna ayuda en la fase práctica de la investigación. Aunque la automatización se consideraba una solución obvia y resolvía algunos de los problemas, como el tiempo y el esfuerzo, resultó ser incoherente cuando se comprobó su precisión en diferentes fases. Por eso ella recomienda un modelo de proceso que ofrezca su propio método de automatización para afrontar al menos los incidentes informáticos más comunes.

Para Taubmann (2019), El aumento del volumen de datos y de la cantidad de fuentes de datos presentadas como pruebas, como las procedentes de los dispositivos del Internet de las cosas o de los sistemas de computación en la nube, ha hecho que el proceso forense digital sea más largo que antes. El aumento del consumo de tiempo se aplica a todas las etapas del proceso forense digital, que incluye la recopilación, el procesamiento y el análisis del material. Lo cual incrementa los tiempos de trabajo en las investigaciones, unas de las soluciones según este autor serian usar la inteligencia artificial (IA), el cual muestra un gran potencial para responder a los retos actuales y futuros en este campo, reduciendo el esfuerzo manual y aumentando considerablemente la velocidad de los procesos.

Por otra parte, según Rani (2018), Hay muchos retos cuando se trata de los tiempos de trabajo en las pruebas digitales, la gran cantidad de datos que se encuentran en los dispositivos digitales modernos es uno de ellos. En la sociedad actual, se ha convertido en la norma que un individuo posea varios dispositivos digitales con gran capacidad de almacenamiento. Si ese individuo formara parte de un grupo de personas acusadas de un determinado delito, el resultado final sería una gran cantidad de datos, posiblemente en Terabytes. Además, normalmente habría que investigar esos datos en busca de pruebas en un plazo limitado. Los laboratorios forenses digitales que dependen de las herramientas forenses tradicionales suelen carecer de los recursos necesarios para manejar el tamaño de los datos que se encuentran en los dispositivos digitales hoy en día.

Para el indicador de tiempos de trabajo según Varoj y Sonmez (2017), implica esencialmente un proceso secuencial de pasos, captura de los medios, adquisición de los medios; creación de una imagen forense de los medios para su examen, analizar la imagen forense del soporte original. Esto garantiza que los medios originales no se modifican durante el análisis y ayuda a preservar el valor probatorio de las pruebas. Esto debido a que los soportes de gran capacidad que suelen incautarse como pruebas en una investigación, como los discos duros de los ordenadores y las unidades externas, pueden ser de 1 terabyte (TB) o más. Esto equivale a unas 17.000 horas de audio comprimido. En la actualidad, los medios de comunicación

pueden adquirirse forzosamente a una velocidad de aproximadamente 1,5 gigabytes (GB) por minuto. Los soportes adquiridos de forma forense se almacenan en un formato de imagen raw, lo que da lugar a una copia bit a bit de los datos contenidos en el soporte original, sin añadidos ni supresiones, incluso para las partes del soporte que no contienen datos. Esto significa que la adquisición forense de un disco duro de 1 TB tardará aproximadamente 11 horas. Aunque este método captura todos los posibles datos almacenados en un soporte digital, lleva mucho tiempo y crea retrasos.

El indicador de extracción de datos se está considerado en la investigación para la variable dependiente análisis forense es la extracción de datos los siguientes conceptos: para Hajar (2020), la extracción de datos son todas las pruebas físicas y digitales recogidas por personas debidamente formadas en la manipulación de estas. Las pruebas digitales serán recogidas por quienes tengan el debido acceso a los datos pertinentes y sus métodos de adquisición de datos serán documentados y facilitados al investigador, Según Arshad (2018), 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. Por lo tanto, para llevar a cabo un proceso eficaz de adquisición de datos, generalmente se necesita una herramienta forense digital que pueda descifrar contraseñas, evitar el cifrado y recuperar los datos borrados de la memoria de un dispositivo.

Por otra parte Riadi (2017), indica que la adquisición de datos en el ámbito forense digital engloba todos los procedimientos relacionados con la recopilación de pruebas digitales, incluida la clonación y la copia bit a bit de cualquier fuente electrónica además Implica la producción de una imagen forense a partir de dispositivos digitales, como CD-ROM, discos duros, discos duros extraíbles, teléfonos inteligentes, memorias USB, consolas de juegos, servidores y otras tecnologías informáticas que pueden almacenar datos electrónicos, por ello la extracción de datos es tal vez la etapa más crítica e implica un plan exigente, exhaustivo y bien elaborado para la adquisición de pruebas digitales. En el indicador de número de casos resueltos se está considerado en la investigación para la variable dependiente análisis forense

según los siguientes conceptos: Para Scanlon (2017), un caso resuelto es cuando el investigador forense elaborará un informe completo en el que se detallan sus conclusiones. El lenguaje utilizado para redactar el informe debe ser bien entendido por personas no técnicas, es una parte vital donde expone todas las pruebas para entender que causo el incidente informático, según Nye (2017), 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 ante el tribunal. En el informe de presentación final se incluye toda la demás documentación técnica pertinente que se recopiló durante la investigación y que podría ser relevante para llegar a resolver el caso.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo de investigación

La presente investigación fue del tipo aplicada, de acuerdo con Valderrama (2013), esta investigación tiene como finalidad construir, modificar y aplicar un mejor análisis forense a los dispositivos móviles

Diseño de investigación

El diseño de esta investigación fue del tipo experimental, de acuerdo con Hernández (2014), a través de este diseño se manipulará la variable independiente ISO 27037:2012 para examinar su efecto o sus cambios aplicado a la variable dependiente análisis forense en una situación de control. Además, conto con la aleatorización en este caso de dispositivos electrónicos. Se muestra a continuación el siguiente esquema:

RG: O1 → X→ O2

Pretest→ ISO 27037:2012→ Postest

R=Asignación al azar

G=Grupo Experimental (en este caso dispositivos móviles)

X=Tratamiento

O1-O2= mediciones pretest/postest del análisis forense

3.2. Variables y operacionalización

Variable independiente ISO 27037:2012

La variable ISO 27037:2012 viene a ser 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), se considera variable a toda característica o propiedad que sea posible medir observar; además, menciona que el enfoque cuantitativo busca recolectar datos para aprobar la hipótesis con base en una medición numérica.

Definición conceptual de la variable Independiente ISO 27037:2012

El ISO 27037 es una norma que proporciona las directrices para actividades específicas en el manejo de pruebas digitales, que están divididos según esta en la identificación, la recogida, la adquisición y la conservación de posibles pruebas digitales que puedan tener valor probatorio. Indica una serie de pasos para tener en cuenta sobre el manejo de la evidencia digital contenido en un medio electrónico con el fin de evitar que esta se dañe o quede inutilizable.

Definición conceptual del análisis forense

La variable análisis 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), 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.

Definición operacional del análisis forense

El Análisis 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.

Tabla 1

Matriz de operacionalización de la variable dependiente análisis forense

Indicador	Instrumento	U.M.	Formula
Tiempos de trabajo	Guía de Observación	%	$x = \frac{horas\ de\ trabajo\ empleado}{horas\ de\ trabajo\ proyectada} x100$
Extracción de datos	Guía de Observación	%	$x = \frac{Datos\ extraidos}{Datos\ Totales} x100$
Casos resueltos	Guía de Observación	%	$x = \frac{Casos\ resueltos}{Casos\ totaltes} x100$

Nota. Se muestra la operacionalización de la variable análisis forense

3.3. Población, muestra y muestreo

Población

De acuerdo con Hernández et al. (2014) indica que la población es el conjunto de elementos que serán estudiados y en donde se pretende extender los resultados, además la población debe de concordar con ciertas especificaciones. Para este estudio de investigación se consideró como población a la cantidad de datos a observar, es decir, serán 30 observaciones para los tres indicadores.

Tabla 2

Población de la investigación

Población	Cantidad	Indicador
Observaciones	30	Tiempos de trabajo
Observaciones	30	Extracción de datos
Observaciones	30	Número de casos resueltos

Nota. Cantidad de registros por cada indicador

Muestra

Para Hernández *et al.* (2014) define a la muestra como una subclase de la población, este formado por un subconjunto de muestra representativas. En el presente trabajo de investigación se utilizó como tamaño de muestra de 30 observaciones del proceso de análisis forense para los tres indicadores, asimismo, se tomará la cantidad iguales para cada indicador en referencia al pretest y postest

Muestreo

Para este tipo de investigación se usó un muestreo probabilístico, de acuerdo con Hernández et al. (2014), en el muestreo probabilístico permite elegir elementos de la población, se selecciono una muestra de esta para la investigación, considerando que toda la población tiene la misma probabilidad de ser escogida para la muestra, esta se obtiene estableciendo en la población sus propiedades o características y el tamaño de la muestra. La técnica que se uso fue un muestreo aleatorio simple.

3.4. Técnicas e instrumentos de recolección de datos

Técnicas de recolección de datos

De acuerdo con Hernández *et al.* (2014), las técnicas de recolección de datos son las diferentes maneras para conseguir información y de ello depende la validez del estudio a realizar. Para esta investigación se aplicó como técnica de recolección de datos a la guía de observación, donde en esta se registra la información obtenida de los indicadores tiempos de trabajo, extracción de datos y números de casos resueltos.

Instrumentos de recolección de datos

De acuerdo con Hernández et al. (2014), los instrumentos de medición de recolección de datos son los recursos que permiten la recolección de datos cuantitativos y además obtener información. La presente investigación empleó como instrumentos de recolección de datos la guía de observación, mediante esta técnica enfocada a los indicadores de tiempos de trabajo, extracción de datos y número de casos resueltos se pudo recaudar la información requerida para el pretest y el postest. A continuación, se muestra la ficha técnica del instrumento de recolección para esta investigación con los siguientes datos

Tabla 3

Ficha técnica del instrumento

Nombre del instrumento:	Ficha de observaciones de medición del indicador
Autor:	Ramos Anampa Bruno
Año:	2021
Descripción:	
Tipo de Instrumento:	Guía de observación
Objetivo:	Determinar que el ISO 27037:2012 mejora el análisis forense en la empresa DG Service, Lima 2021
Indicadores:	A) Tiempos de trabajo b) Extracción de datos c) Número de casos resueltos
Número de observaciones a recolectar	30
Aplicación:	Directa

Nota. Datos del instrumento

Validez

Hernández et al. (2014) define la validez como el grado en que un instrumento cuantifica la variable que intenta demostrar. La validez de la presente investigación se determinó a través juicio de expertos, compuesto por tres profesionales relacionados con la temática; de acuerdo con Valderrama (2013) menciona que el juicio de expertos está compuesto por un grupo de personas, en donde cada uno de ellos emiten un veredicto del instrumento, valorando la claridad, pertinencia y relevancia; este, con sentido lógico y empleando toda su expertiz.

Tabla 4

Expertos que validaron el instrumento de recolección de datos cuantitativos

DNI	Grado Académico; Apellido y Nombre	Institución donde labora	Calificación
70005373	Mg. Anampa García Jhon Paul	Universidad Tecnológica del Perú	Aplicable
00515158	Mg. Inquilla Quispe Ricardo Carlos	Universidad Nacional de Cañete	Aplicable
10192315	Doctor Visurraga Agüero Joel Martin	Universidad Cesar Vallejo	Aplicable

Nota. Se muestra información de la validación de expertos

3.5. Procedimientos

Para la presente investigación se precisó las variables dependiente e independiente; asimismo, para la recopilación de datos se usó como técnica de observación; además, se construyó el instrumento de recolección de datos siendo en este caso una guía de observación; luego, se emitió la validez del instrumento mediante el juicio de expertos, dónde se recolectó y verificó los resultados obtenidos de la muestra pretest y postest, las cuales se arrojarán en una base de datos usando el

software Microsoft Excel, para que finalmente pueda determinarse el grado de confiabilidad mediante el coeficiente alfa de Cronbach, mostrando la congruencia y coherencia del instrumento medido en esquemas adecuados

Tabla 5

Estadísticas de confiabilidad

Indicador	N° de Elementos	Registros	Alfa de Cronbach Aplicación
Tiempos De Trabajo	2	30	.765
Extracción De Datos	2	30	.703
Número De Casos Resueltos	2	30	.715

Nota. Elaborado con asistencia del software IMB SPSS V25

3.6. Método de análisis de datos

De acuerdo con el análisis de datos de la presente investigación, referente al pretest y postest, se usó herramientas digitales como Microsoft Excel y el software estadístico IBM SPSS V25. En cuanto al análisis descriptivo, se usó tablas y figuras, exponiendo medidas de tendencia central usando la media, se realizará su interpretación o lectura por cada indicador, datos emitidos por el instrumento, lo cual ayudó a fijar de manera visual y estructurada la comprensión sencilla de todos los datos numéricos. Finalmente, para el análisis inferencial de acuerdo con De La Cruz (2017), se comprobará la normalidad de los datos obtenidos mediante la prueba Test de Shapiro Wilk; Además, se usó para la contrastación de la hipótesis la prueba no paramétrica de Wilcoxon para una distribución no normal y la prueba t Student cuando se presente el caso de una distribución normal.

3.7. Aspectos éticos

Para garantizar la integridad en la presente investigación, se cumplió con honestidad los estándares de ética de la Universidad Cesar Vallejo-Resolución de Consejo 0262-2020 UCV, las cuales sostienen la correcta transparencia y veracidad de la información. Es importante mencionar que la investigación empleó codificaciones que estarán regidas bajo las normas APA. Tomando en cuenta la veracidad de todo lo exhibido en este proyecto, se asumió la responsabilidad y el compromiso de las políticas de uso jurídico y ético, respetando y manteniendo la privacidad de estas. Además, para la autenticidad de los datos recolectados y para respetar las políticas anti plagió, se hizo uso del software Turnitin.

IV. Resultados

Análisis Descriptivos

Medidas descriptivas del indicador: tiempos de trabajo

Tabla 6

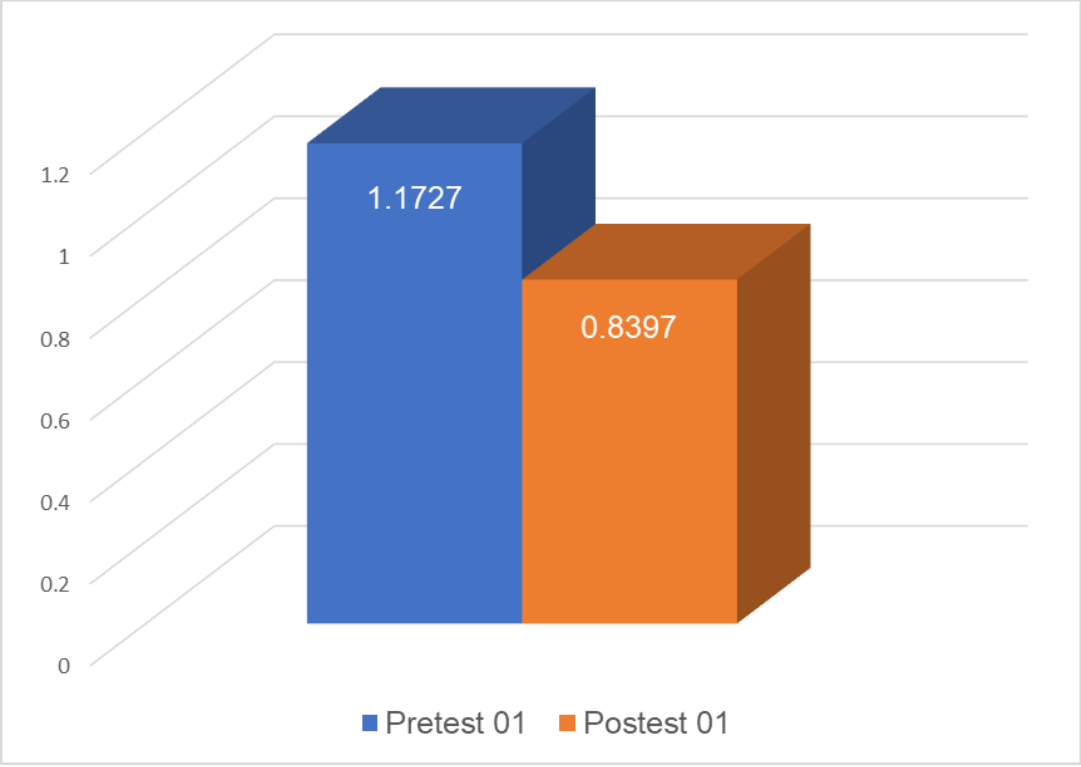
Medidas descriptivas del indicador: tiempos de trabajo antes y después de aplicar el ISO 27037:2012

	N	Mínimo	Máximo	Media	Desv.
Indicador Pretest01	30	.98	1.58	1.1727	.15216
Indicador Postest01	30	.67	1.10	.8397	.10591

Nota: Elaborado con asistencia de IBM SPSS V25

Figura 1

Histograma de la media de tiempos de trabajo



Nota. Elaborado con asistencia de Excel 2019

En la tabla 6 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 postest 01 es de 0.8397 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, Asimismo, es necesario nombrar que la media para ambos casos se ubicó cerca a los rangos mínimos y que la desviación estándar promedio para el pretest 01 es de 0.15216 y para el postest 01 es de 0.10591 relacionado al desvío de la media, mientras tanto en la figura 1 se refleja el comportamiento del indicador tiempos de trabajo antes y después de la aplicación del ISO 27037:2012 en base a los datos obtenidos en la ficha de observaciones, se concluyó que los tiempos de trabajo disminuyo en un 28.39% o se redujo en 0.0333 veces las horas del indicador de tiempos de trabajo

Medidas descriptivas del indicador: extracción de datos

Tabla 7

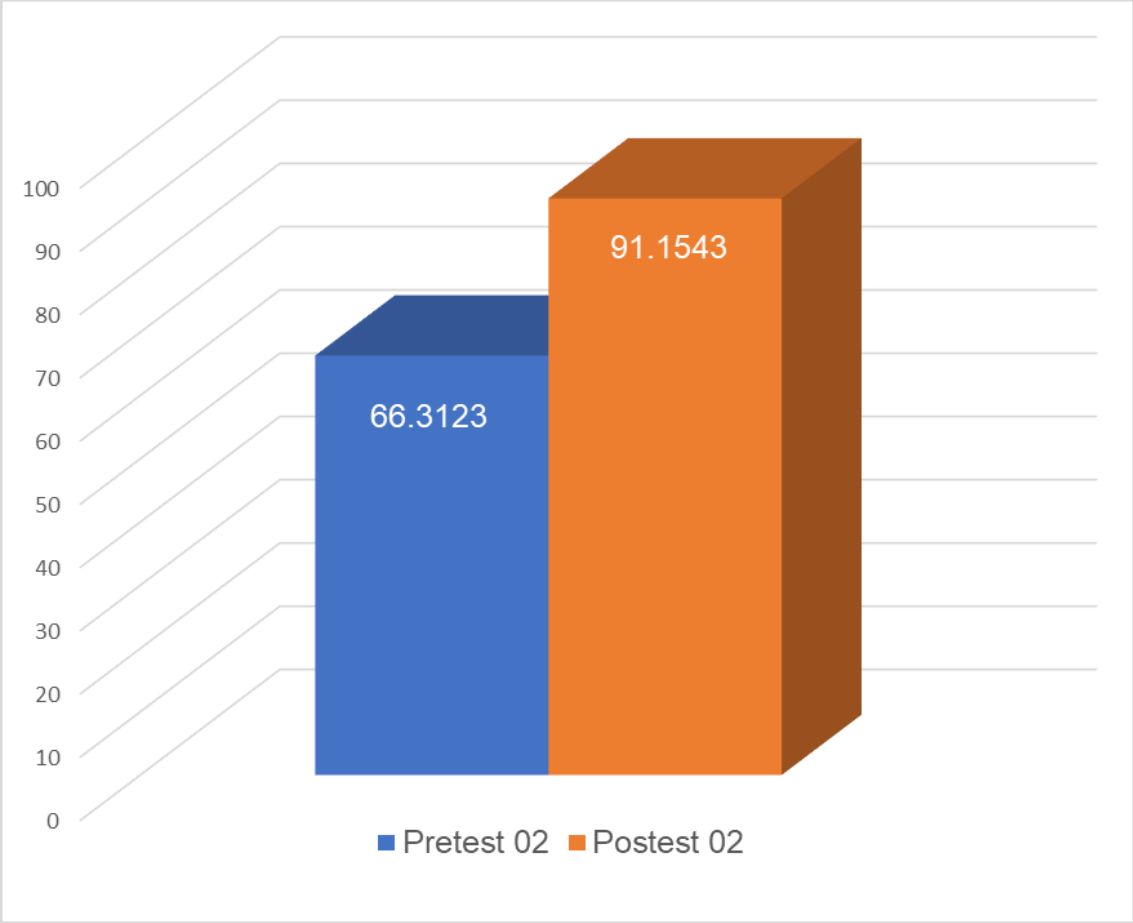
Medidas descriptivas del indicador: extracción de datos antes y después de aplicar el ISO 27037:2012

	N	Mínimo	Máximo	Media	Desv.
Indicador Pretest02	30	38.92	90.81	66.3123	17.47738
Indicador Postest02	30	72.18	99.08	91.1543	7.23859

Nota: Elaborado con asistencia de IBM SPSS V25

Figura 2

Histograma de la media de extracción de datos



Nota. Elaborado con asistencia de Excel 2019

En la tabla 7 se observó que los datos descriptivos del indicador extracción de datos, en el pretest 02 la muestra de la media es de 66.3123 veces y el valor del postest 02 es de 91.1543, lo cual se observó que aumentó la extracción de datos, por lo cual se concluye que existe una mejora significativa después de aplicar el ISO 27037:2012 Asimismo, es necesario mencionar que la media en ambos casos se ubicó cerca a los rangos mínimos y que la desviación estándar promedio para el pretest 02 fue de 17.47738 y para el postest 02 fue de 7.23859 veces relacionado al desvío de la media, En la figura 2 se mostró que el comportamiento del indicador

extracción de datos antes y después de la aplicar el ISO 27037:2012 después de usar la ficha de observaciones, por lo cual, se concluyó que el la extracción de datos mejoró un 27.25 % o aumento un 24.84 veces la extracción de información.

Medidas descriptivas del indicador: número de casos resueltos

Tabla 8

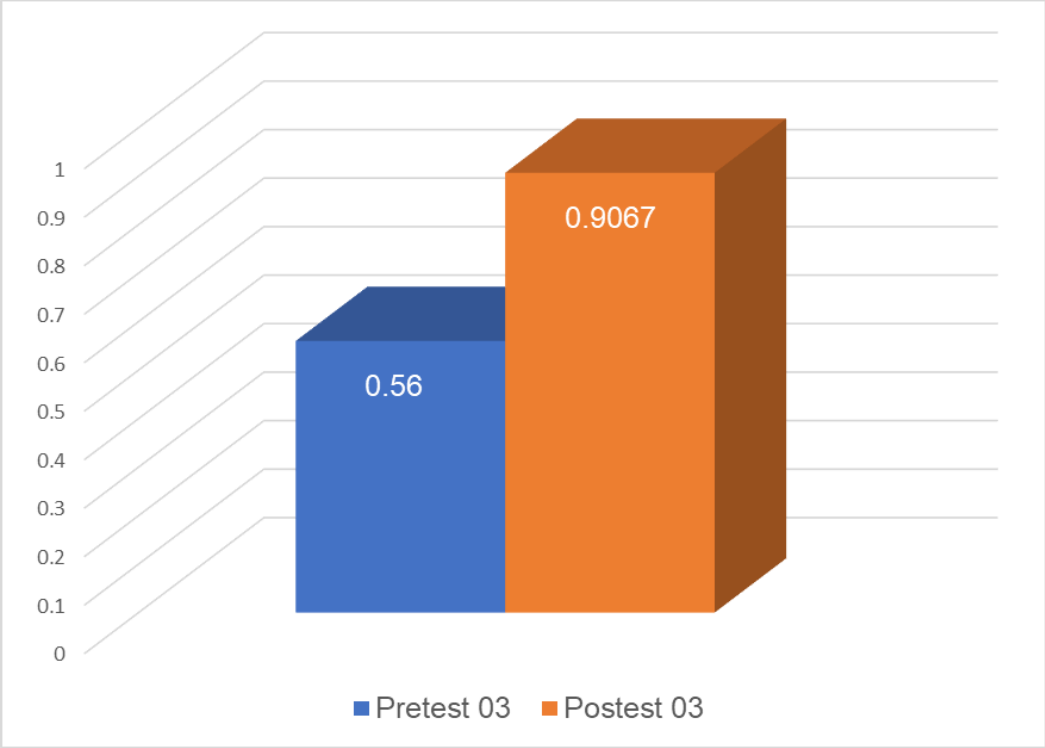
Medidas descriptivas del indicador: número de casos resueltos antes y después de aplicar el ISO 27037:2012

	N	Mínimo	Máximo	Media	Desv.
Indicador Pretest03	30	0.20	0.80	0.5600	0.12205
Indicador Postest03	30	0.60	1.00	0.9067	0.12576

Nota: Elaborado con asistencia de IBM SPSS V25

Figura 3

Histograma de número de casos resueltos



Nota. Elaborado con asistencia de Excel 2019

En la tabla 8 se muestra los datos descriptivos del indicador número de casos resueltos, en el pretest 03 de la muestra la media es 0.5600 veces y el valor del postest 03 fue de 0.9067 por lo cual se concluye, que existe una mejora significativa después de aplicar el ISO 27037:2012, Asimismo, es necesario indicar que la media para ambos casos se ubicó cerca a los rangos mínimos y que la desviación estándar promedio para el pretest 03 fue de 0.12205 y para el postest 03 fue de 0.12576 relacionado al desvío de la media, En la figura 2 se refleja el comportamiento del indicador número de casos resueltos antes y después de aplicar el ISO 27037 en base a los datos obtenidos después de usar la ficha de observaciones, se concluye que el número de casos resueltos aumento en un 38.23% o este mejoro en un 0.3467.

Análisis Inferencial

Prueba de Hipótesis

Según López y Fachelli (2016), Una prueba de hipótesis es una regla que especifica cuando se puede aceptar o rechazar una afirmación sobre una población dependiendo de la evidencia proporcionada por una muestra de datos, una prueba de hipótesis examina dos hipótesis opuestas sobre la población: la hipótesis nula y la hipótesis alternativa. La hipótesis nula es el enunciado que se probará. Por lo general, la hipótesis nula es un enunciado de que "no hay efecto" y la hipótesis alternativa es el enunciado que se desea poder concluir que es verdadero de acuerdo con la evidencia proporcionada por los datos de la muestra recogida.

Prueba de hipótesis específica 1: indicador tiempos de trabajo

Formulación de la hipótesis estadística:

H_0: El ISO 27037:2012 no mejora significativamente los tiempos de trabajo del análisis forense en la empresa DG Service, Lima 2021.

H_1: El ISO 27037:2012 mejora significativamente los tiempos de trabajo del análisis forense en la empresa DG Service, Lima 2021.

Considerando que el resultado de la prueba de normalidad del indicador tiempos de trabajo muestra una distribución normal (ver Anexo 7), se aplicó la prueba de t student.

Tabla 9

Prueba de t de Student para el indicador tiempos de trabajo antes y después del ISO 27037:2012

		95% de intervalo de confianza de la diferencia						
		Media	Desv. Error	Inferior	Superior	t	gl	Sig
Par 1	pretest01 postest01	.33300	.02087	.29031	.37569	15.954	29	.001

Nota: Elaborado con asistencia de IBM SPSS V25

.

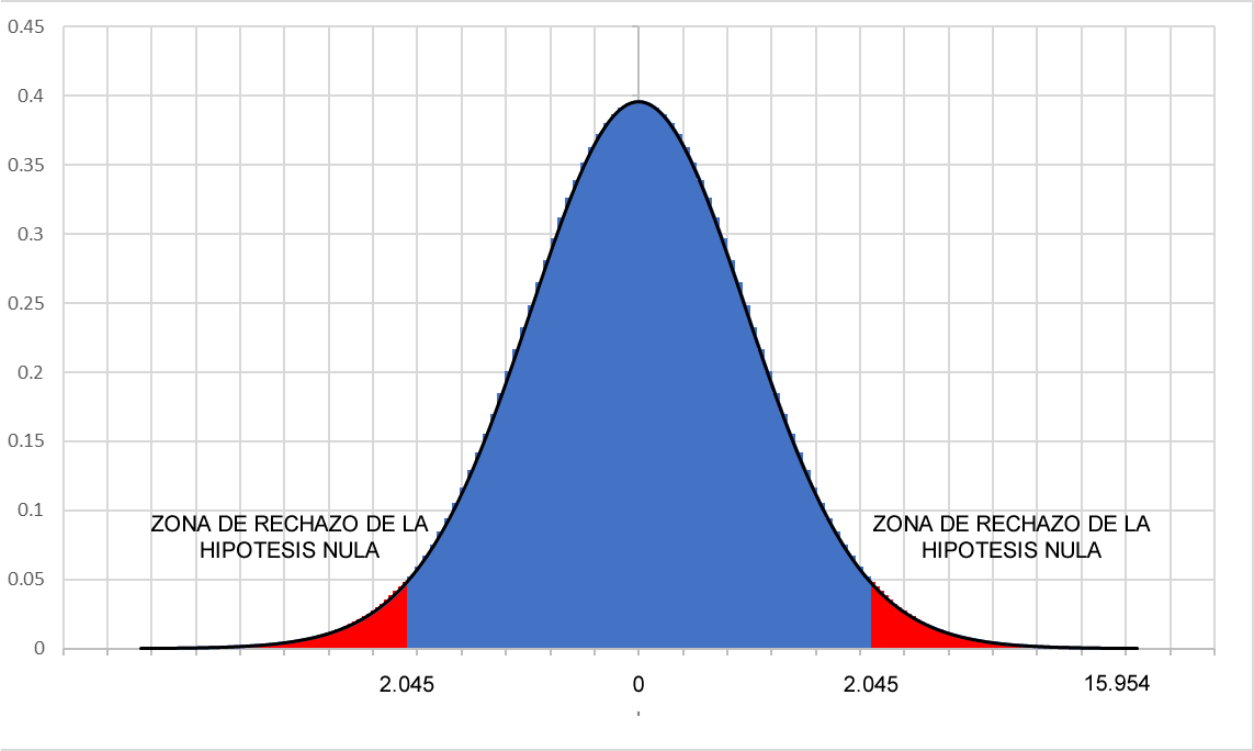
Contrastación de hipótesis

Para la contrastación de la hipótesis se realizó la prueba de t Student, se visualiza en la tabla 12 que el valor estadístico de t de Student de 15.954 se ubica en la zona de rechazo de la hipótesis nula, como se muestra en la figura 4. De igual forma, presenta un valor de significancia de 0.001 hallándose menor al valor p de 0.05, por lo cual se rechaza la hipótesis nula. Por lo tanto, se concluye que el ISO 27037:2012 mejora significativamente los tiempos de trabajo del análisis forense en la empresa DG Service, Lima 2021.

En la figura 4 se observó que la representación gráfica de la prueba t de Student para el indicador tiempos de trabajo presento 29 grados de libertad y un nivel de significancia de 0,05, por lo cual obtiene un valor t critico igual a ± 2.045. Siendo el valor t obtenido mayor al valor critico (+2.045), se concluyó que esta se ubicó en la zona de rechazo.

Figura 4

Representación gráfica de distribución del t de Student



Nota. Elaborado con asistencia de Excel 2019

Prueba de hipótesis específica 2: indicador de extracción de datos

Formulación de la hipótesis estadística:

H_o: El ISO 27037:2012 no mejora significativamente la extracción de datos del análisis forense en la empresa DG Service, Lima 2021.

H_1: El ISO 27037:2012 mejora significativamente la extracción de datos del análisis forense en la empresa DG Service, Lima 2021.

Considerando que el resultado de la prueba de normalidad del indicador de extracción de datos muestra una distribución no normal (ver Anexo 7), se aplicó la prueba de Wilcoxon.

Tabla 10

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

		Rangos		
		N	Rango promedio	Suma de rangos
postest02 - pretest02	Rangos negativos	0[a]	,00	,00
	Rangos positivos	30[b]	15,50	465,00
	Empates	0[c]		
	Total	30		

a. postest02 < pretest02

b. postest02 > pretest02

c. postest02 = pretest02

Nota: Elaborado con asistencia de IBM SPSS V25

En la tabla 10 vemos que se analizaron 30 pares encontrándose 30 rangos positivos, un promedio de 15.50 y una suma total de rangos que es 465.

Tabla 11

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

	Estadístico de prueba	
	Z	Sig. Asint
pretest02-postest02	-4.782	0.001

Nota: Elaborado con asistencia de IBM SPSS V25

Contrastación de hipótesis

Para la contrastación de la hipótesis se realizó la prueba de Wilcoxon, se visualizó que en la tabla 11 que el valor de significancia fue de 0.001 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 -4.782, la cual se ubica en la zona de rechazo de la hipótesis nula. Por lo cual se concluye que El ISO 27037:2012 mejora significativamente la extracción de datos del análisis forense en la empresa DG Service, Lima 2021.

Prueba de hipótesis específica 3: indicador de número de casos resueltos

Formulación de la hipótesis estadística:

H_o: El ISO 27037:2012 no mejora significativamente el número de casos resueltos del análisis forense en la empresa DG Service, Lima 2021.

H_1: El ISO 27037:2012 mejora significativamente el número de casos resueltos del análisis forense en la empresa DG Service, Lima 2021.

Considerando que el resultado de la prueba de normalidad del indicador de número de casos resueltos muestra una distribución no normal (ver Anexo 7), se aplicó la prueba de Wilcoxon.

Tabla 12

Prueba de Wilcoxon para medidas de muestra relacionadas del indicador números de casos resueltos sobre rangos

Rangos				
		N	Rango promedio	Suma de rangos
postest03 - pretest03	Rangos negativos	0[a]	,00	,00
	Rangos positivos	30[b]	15,50	465,00
	Empates	0[c]		
	Total	30		

a. postest03 < pretest03
b. postest03 > pretest03
c. postest03 = pretest03

Nota: Elaborado con asistencia de IBM SPSS V25

En la tabla 12 vemos que se analizaron 30 pares encontrándose 30 rangos positivos, un promedio de 15.50 y una suma total de rangos que es 465.

Tabla 13

Prueba de Wilcoxon para medidas de muestra relacionadas del indicador números de casos resueltos sobre estadísticos de prueba

Estadísticos de prueba		
	Z	Sig. Asint.
pretest03-postest03	-4.932	0.001

Nota: Elaborado con asistencia de IBM SPSS V25

Contrastación de hipótesis

Para la contrastación de la hipótesis se realizó la prueba de Wilcoxon, donde se visualizó que en la tabla 13 el valor de significancia fue 0.001 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 -4.932, la cual se ubica en la zona de rechazo de la hipótesis nula. Por lo cual se concluye que el ISO 27037:2012 mejora significativamente el número de casos resueltos del análisis en la empresa DG Service, Lima 2021.

V. Discusión

De acuerdo con los resultados obtenidos en esta investigación se obtuvo cambios en los indicadores pertenecientes a la variable dependiente del análisis forense, cuando se aplicó de la variable independiente ISO 27037:2012 en la empresa DG Service., Lima-2021.

Respecto al indicador tiempos de trabajo

En el análisis descriptivo se visualizó una disminución de horas en el indicador de tiempos de trabajo en las 30 observaciones realizadas de las muestras recogidas en el postest donde se observa una mejoría en un 28.39%, es decir que se realiza el análisis forense de dispositivos móviles en un menor tiempo con la implementación del ISO 27037:2012, siendo su diferencia numérica entre medias de 0.0333, lo que significa que en promedio se requiere menos horas hombre aplicando el ISO 27037:2012 cuando se realiza el análisis forense.

En el análisis inferencial referente a la prueba de normalidad se tuvo los siguientes resultados: para el pretest fue de 0.005 , para el postest fue de 0.345, y como ambos son mayores al valor p que es 0.05 se determina que presento una distribución del tipo normal. En consecuencia, para la contrastación de la hipótesis se utilizó la prueba paramétrica t Student, obteniendo un valor de 15.954 y se obtuvo que el valor de la significancia es de 0.001, el cual es menor que el valor p de 0.05, por lo tanto, la hipótesis nula fue rechazada, en consecuencia, se concluye que aplicar el ISO 27037:2012 mejora significativamente los tiempos de trabajo del análisis forense en la empresa DG Service., Lima-2021.

Los resultados contrastan con los siguientes antecedentes como el del autor Du (2020), que indica su técnica de deduplicación de datos con el ISO 27037 permite un ahorro sustancial de tiempo al momento de procesar los datos digitales de los medios electrónicos. Además de tener la ventaja de poder ordenar la información

según su tipo, tamaño o fecha de modificación. Gracias a esto permite sintetizar más el análisis forense porque puede procesar grandes cantidades de información lo cual ayuda a optimizar las horas de otra.

Por otra parte, Jalal Mosbah (2018), indica que el ISO 27037 es ideal para el análisis forense digital en dispositivos móviles porque esta metodología se puede adaptar con facilidad a las nuevas tecnologías que se pueden presentar en los dispositivos móviles. Además, que al adaptar la metodología se puede dar un tratamiento correcto a la evidencia digital en las diferentes fases del análisis forense evitando realizar tareas repetitivas que generan pérdidas de tiempo.

Finalmente, Yopla y Yopla (2014), indica que la mejor manera de llevar a cabo un análisis forense sin contratiempos o demoras es aplicar el ISO 27037 porque nos sugiere los pasos que se debe tomar en cada fase además que hace énfasis en como se debe dar el tratamiento a la evidencia digital cuando esta es analizada por el investigador puesto que es aquí donde se presentan la mayor cantidad de incidentes que pueden generar perdidas de tiempo porque si omite algunos pasos de la metodología del ISO 27037 se deberá hacer uso de otra copia de la imagen forense para volver a comenzar desde la fase de análisis.

Respecto al indicador de: extracción de datos, en el análisis descriptivo se realizó una toma de 30 observaciones, para el pretest y postest del indicador, en la cual se detectó una mejoría en un 27.25% al momento de comparar ambas muestras, es decir, la extracción de datos aumento con la aplicación del ISO 27037:2012, con una diferencia numérica en la media de 24.84, lo que significa que hubo un aumento en la adquisición de datos en el análisis forense cuando se aplica el ISO 27037:2012.

En el análisis inferencial referente a la prueba de normalidad se tuvo los siguientes resultados: para el pretest fue de 0.005 , para el postest fue de 0.001 y como ambos son menores al valor p que es 0.05, se concluye que la distribución

que se presento fue del tipo no normal. En consecuencia, para la contrastación de la hipótesis se uzo la prueba no paramétrica de Wilcoxon y se comprobó que el valor de la significancia es de 0.001, el cual es menor que el valor p de 0.05, por lo tanto, la hipótesis nula fue rechazada, en consecuencia, se concluye que al implementar el ISO 27037:2012 mejora significativamente la extracción de datos del análisis forense en la empresa DG Service, Lima-2021.

Los resultados contrastan con los siguientes antecedentes: Heloıse (2019), el ISO 27037 nos muestra los pasos que se deben seguir para adquirir los datos almacenados en los dispositivos móviles comenzando con la información más volátiles que se encuentra la RAM de los dispositivos móviles después, continuar con la información almacenada en la memoria interna y la SD card para extraer la mayor cantidad de datos y evitar perder algún tipo de información que se dé suma intereses para resolver el incidente informático.

Por otra parte, Ahmad (2018), El ISO 27037 nos da la seguridad de obtener la mayor cantidad de información que puede almacenar en un dispositivo electrónico porque la información se copia bit a bit y se almacena en una imagen forense, el cual contendrá datos relevantes al momento de realizar el análisis forense al dispositivo móvil incluso aquellos datos que hayan borrados en un tiempo corto podrán ser recuperados y estudiados para descubrir cómo se ocasiono el ataque informático.

Y adicionalmente para Sugiantoro (2018), al momento de recolectar información de los medios electrónicos el uso del ISO 27037 es imprescindible porque nos ayuda no solo a recuperar data tradicional que simplemente se puede se puede copiar de un dispositivo de almacenamiento a otro sino también los datos almacenados en el mismo sistema Operativo Android, el cual solo se puede extraer aplicando el ISO 27037 los cual nos permite acceder a información que es aparentemente es invisible como por ejemplo las aplicaciones instaladas o borradas del dis-

positivo, el historial de mensajes almacenados en un archivo db, todos estos archivos se extraen del móvil se extraen con un software forense para su posterior análisis.

Respecto al indicador de número de casos resueltos, en el análisis descriptivo se realizó una toma de 30 observaciones tanto en el pretest y el postest, donde se observó una mejoría de un 38.23%, es decir, los números de casos resueltos se ha incrementado considerablemente al aplicar el ISO 27037:2012, la diferencia numérica en la media fue de 0.3467, lo que significa que existe un aumento casos resueltos en el análisis forense aplicando el ISO 27037:2012.

En el análisis inferencial referente a la prueba de normalidad se tuvo los siguientes resultados: para el pretest fue de 0.003, para el postest fue de 0.001, y como ambos son menores al valor p que es 0.05, se concluye que la distribución es no normal. En consecuencia, para la contrastación de la hipótesis se utilizó la prueba no paramétrica de rango de Wilcoxon y se obtuvo que el valor de la significancia es de 0.001, el cual definitivamente es menor que el valor p de 0.05, por lo tanto, la hipótesis nula fue rechazada, en consecuencia, se concluye que al implementar el ISO 27037:2012 mejora significativamente los números de casos resueltos del análisis forense en la empresa DG Service, Lima-2021

Los resultados contrastan con los siguientes antecedentes: Ferreyros (2019), debido a los diferentes incidentes informáticos que pueden ocurrir dentro de cualquier dispositivo móvil. Al principio se hacía muy complicado como recolectar la información y solo pocas veces se lograba conseguir el objetivo de resolver el caso, por ello se juntaron las mejores prácticas del tratamiento de la evidencia digital en el ISO 27037 para el análisis forense, lo cual ayudo a los investigadores a tener una idea de cómo tratar la evidencia y los pasos a seguir para resolver un incidente informático, quienes fueron los posibles usuarios del ataque, como se realizado, la fechas entre otras datos que ayudan a encontrar una solución al incidente.

Además, para Singh (2019), nos indica que el ISO 27037 contribuye al aumento de los casos resueltos el cual se ver reflejado en la fase de presentación donde si el investigador siguió los pasos establecidos en la metodología podrá dar solución al incidente informático que se haya ocasionado en el dispositivo móvil, incluso si es un ataque sofisticado se podrá trazar una línea del tiempo indicado cuales fueron los programas usados para vulnerar la seguridad del medio electrónico, conocer cuáles fueron los datos implicados en el ataque como por ejemplo usuarios, contraseñas, mensajes de texto, correos electrónicos, si bien no siempre se puede detectar al culpable al menos se pueden tomar medidas correctivas para evitar que el dispositivo móvil se vea atacado frecuentemente.

Asimismo Dimpe y Kogeda (2017), indica que el análisis forense digital para móviles puede ser complicado de realizar si no se cuenta con una guía adecuada como el ISO 27037, el cual puede adaptarse a las nuevas tecnologías presentes en los dispositivos electrónicos independientemente de si sea Android o iPhone porque sus buenas prácticas pueden aplicarse a ambos siendo lo único que cambia el software forense al utilizar para poder resolver el caso de manera satisfactoria hace énfasis en que se debe cumplir la metodología en todo momento desde la aseguración de la escena hasta la presentación del caso, lo cual garantiza que el análisis forense se realizó cumpliendo los estándares establecidos y no hubieron incidentes relevantes que impidieron la realización de la investigación, además la evidencia digital de contar son su correspondiente hash para asegurar su integridad y sus respectivas copia de seguridad para mantener la disponibilidad de la información.

Con respecto al objetivo general se observó que la aplicación del ISO 27037:2012 en el análisis forense en la empresa DG Service, Lima-2021, obtuvo resultados positivos como es el indicador de tiempos de trabajo donde se obtuvo una mejoría de 28.39%, esto indica que se realiza el proceso del análisis forense de manera confiable y segura en un menor tiempo.

Asimismo, también se visualizó que sucedió algo similar en el indicador de extracción de datos, ya que el valor que se obtuvo de mejoría después de la implementación de dicha herramienta es de un 27.25%, este dato señala el ISO 27037 permite una mayor cantidad de captura de información de los dispositivos móviles en comparación a la metodología tradicional, por lo que se convierte en un beneficio significativo para la variable dependiente. Finalmente, los resultados obtenidos en el tercer indicador que son número de casos resueltos confirma un aumento en la finalización satisfactoria de casos forenses, esta mejora representa un 38.23%, con relación al escenario anterior.

Por lo tanto, se concluye que el ISO 27037:2012 mejora significativamente el análisis forense en la empresa DG Service., Lima 2021. Estos resultados contrastan con los antecedentes siguientes: Según Sadiku, Tembely, Musa (2017), la estandarización para la toma de datos digitales con el ISO 27037 de las pruebas almacenadas en un medio electrónico es de gran ayuda para los investigadores forenses porque permite estar alineado a las leyes pueden restringir la capacidad de los analistas para llevar a cabo investigaciones, además permite reducir los tiempos de trabajo, recuperar más información al momento de la extracción de datos y resolver más casos complejos que antes, lo cual nos ayuda a realizar un mejor análisis forense en los dispositivos móviles.

Con respecto a la metodología utilizada esta permitió fortalecer la investigación, ya que, al ser del diseño de investigación experimental puro, posibilita controlar la validez interna del experimento mediante la asignación aleatoria. Asimismo, mediante las pruebas pretest y postest se pudo medir el cambio aplicado con mayor exactitud, con el propósito de describir sus resultados, identificando la relación de causa y efecto, es decir, la relación directa entre las variables de la investigación. Además, permitió conocer la situación actual sobre el proceso del análisis forense en la empresa gracias a los indicadores. Es importante señalar que el uso de las fichas de observación como instrumento de recolección de datos favoreció en gran medida la obtención de estos; finalmente, los indicadores establecidos en el trabajo

de investigación permitieron conocer que la empresa en estudio se encuentra preocupada por disponer de la información necesaria para la medición de la variable dependiente. En cuanto a la relevancia social científica, la investigación proporciona la expansión de conocimiento en el área del análisis forense con el ISO 27037; por otro lado, esta metodología puede ser aplicada en otros procesos similares de la organización y empresas interesadas que estén interesadas en desarrollar sus propias investigaciones relacionadas al análisis forense.

VI: Conclusiones

Primero: A raíz de los resultados obtenidos en esta investigación realizada en la empresa DG Service, se determina que con la implementación del ISO 27037, mejora significativamente el análisis forense, donde los puntos fuertes de mejora son los indicadores, como se demuestra en el indicador de tiempos de trabajo, el cual tuvo una disminución en horas empleadas al realizar el análisis forense, lo cual significa que el proceso se realiza en un menor tiempo, también la extracción de datos mejoró en su promedio gracias al ISO 27037 porque permite la captura de una mayor cantidad de datos almacenados en los dispositivos móviles y por último el indicador de número de casos resueltos obtuvo una mejora el cual se ve reflejado en el aumento de investigaciones finalizadas satisfactoriamente por los analistas forenses.

Segundo: En cuanto al primer indicador que es tiempos de trabajo se visualizó la mejora después de la aplicación del ISO 27037 en el Análisis forense, ya que disminuyó un 28.39% en promedio, lo que nos indica que se pueden realizar el análisis forense en un menor tiempo aplicando el ISO 27037, lo cual es una ventaja porque al aplicar esta metodología los casos que tomaban días para ejecutarse ahora solo toman horas.

Tercero: Para el segundo indicador que es extracción de datos hubo una mejora después de la aplicación del ISO 27037 en el análisis forense, ya que aumentó en un 27.25% en promedio, lo que nos indica que el ISO 27037 contribuye a una mejor captura de datos cuando se realiza en análisis forense porque los datos ocultos y volátiles son recolectados de forma sencilla gracias a la metodología aplicada.

Cuarto: Para el tercer indicador que es número de casos resueltos, se visualizó una mejora después de la aplicación del ISO 27037 en el análisis forense, ya que aumentó en un 38.23%, lo cual se ve reflejado en el aumento de investigaciones finalizadas sobre incidentes informáticos que afectan a los dispositivos móviles, gracias a esto se detectó los ataques informáticos a los que están expuestos los móviles de la compañía y que contramedidas se deben aplicar para mitigar estas amenazas.

VII. Recomendaciones

Primero: Para sostener los resultados positivos en los tres indicadores, obtenidos por la investigación realizada a la empresa DG Service, Lima 2021, después de la aplicación del ISO 27037 para el análisis forense, se precisa al gerente de sistemas que debe solicitar al área de recursos humanos coordinar capacitaciones sobre las nuevas tecnologías relacionadas a los dispositivos móviles y sobre los nuevos ataques informáticos que afectan a esta como por ejemplo el SQL Injection Hexadecimal, Ransomware, entre otras para que el personal tenga conocimiento sobre los nuevos tipos de análisis forense.

Segundo: En cuanto al indicador de tiempos de trabajo si bien el ISO 27037 reduce el tiempo de investigación, se le recomienda al gerente de sistemas contar con una bitácora de los incidentes más comunes que pueden servir como lecciones aprendidas para que los nuevos investigadores puedan adaptarse más rápido para poder realizar análisis forense de manera eficiente y en menor tiempo.

Tercero: Para el indicador extracción de datos, si bien la adquisición de datos ha mejorado, se recomienda al gerente de sistemas contar son software forense especializado y actualizado en técnicas antiforense debido a que estas se están empezando a popularizar entre los crackers y que están empezando a encriptar o destruir información al momento que se realiza la extracción de datos.

Cuarto: Para el indicador número de casos resueltos, se recomienda al gerente de sistemas que la metodología basada en el ISO 27037 debe ser actualizada por lo menos cada 6 meses para evitar estar desfasada ante las nuevas tecnologías y que este afecta las futuras investigaciones del análisis forense.

REFERENCIAS

Antón Bayona Jorge Antonio (2018), “propuesta de manual de políticas y procedimientos de auditoría forense para mejorar la gestión administrativa en la beneficencia de Piura. Recuperado de: http://repositorio.unp.edu.pe/bitstream/handle/unp/1234/con-ant-bay-18.pdf?sequence=1&isallowed=y

Ahmad Al Mutawa Noora (2018), Integrating behavioral analysis within the digital forensics’ investigation process. Recuperado de: http://clok.uclan.ac.uk/25412/1/25412%20al-mutawa%20noora%20final%20e-thesis%20(master%20copy).pdf

Arshad Humaira (2018), Digital forensics: review of issues in scientific validation of digital evidence. Recuperado de: https://www.researchgate.net/profile/humaira-ar-shad/publication/327644306_digital_forensics_review_of_issues_in_scientific_validation_of_digital_evidence/links/5b9b298592851ca9ed06467d/digital-forensics-review-of-issues-in-scientific-validation-of-digital-evidence.pdf

Boasiako Albert Antwi (2018), A Model for digital evidence admissibility assessment. Recuperado de: https://repository.up.ac.za/bitstream/handle/2263/70619/antwiboasiako_model_2019.pdf?sequence=1

Cajamarca Sánchez Armando (2016), implementación de un laboratorio de informática forense en el órgano rector del sistema de inteligencia nacional. Recuperado de: http://repositorio.usil.edu.pe/bitstream/usil/2754/2/2016_cajamarca.pdf

De La Cruz Jo Frans Renzo (2015), Aplicación de metodologías y herramientas de la informática forense para reducir el riesgo de la seguridad informática en la dirección nacional de comunicación y criminalística de la policía nacional del Perú. Recuperado de: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahukewjopq-yvblwahvyqpu-chytobg8qfjaeeg-qigbad&url=http%3a%2f%2frepositorio.unasam.edu.pe%2fbitstream%2fhandle%2funasam%2f2626%2ft033_41010567_m.pdf%3fsequence%3d1%26isallowed%3dy&usg=aovvaw0maxuyhibklsios7duk4o8

De La Cruz Kaykoshida María (2017), Las estrategias metodológicas del docente y su influencia en el logro de las competencias del curso de matemática básica de los alumnos del primer ciclo de la Universidad Nacional de Cañete. Recuperado de: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjYu-uMhMjxAhWxrpU-

CHag7DmQQFnoECAMQAA&url=https%3A%2F%2Freposito-rio.une.edu.pe%2Fbitstream%2Fhandle%2FUNE%2F1761%2FTM%2520CE-Du%25203429%2520R1%2520-%2520Re-yes%2520de%2520la%2520Cruz.pdf%3Fsequence%3D1%26isA-llowed%3Dy&usg=AOvVaw3oAY-qbJ5Rr9rxFPAOWds8

Dimpe Precilla M., Kogeda Okuthe P. (2017), Impact of using unreliable digital forensic tools. Recuperado de: https://www.researchgate.net/publication/320922374_impact_of_using_unreliable_digital_forensic_tools

Du Xiaoyu (2020), Alleviating the digital forensic backlog: a methodology for automated digital evidence processing. Recuperado de: https://markscanlon.co/papers/phdthesis-methodologyautomateddigitalevidenceprocessing.pdf

Eset, (2020), Reporte de seguridad 2020 para Latinoamérica. Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

Ferreyros Corcuera Jorge Enrique (2019), La auditoría forense como herramienta preventiva y de investigación para combatir el fraude y la corrupción financiera pública en el Perú. Recuperado de: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved

=2ahukewjn0ud3wllwahupqpuchbu2aeeqfjakeg-qihxad&url=http%3a%2f%2freposito-rio.uigv.edu.pe%2fbitstream%2fhandle%2f20.500.11818%2f4660%2fte-sis_ferreyros_jorge.pdf%3fsequence%3d1%26isallowed%3dy&usg=ao-vvaw2twkg96lzc6hex4_zk3bux

Hajar Akbar Muh (2020), Analysis of steganographic on digital evidence using general computer forensic investigation model framework. Recuperado de: https://www.researchgate.net/profile/imam-riadi-2/publication/346527069_analysis_of_steganographic_on_digital_evidence_using_general_computer_forensic_investigation_model_framework/links/5fc62f2e92851c301299e7a0/analysis-of-steganographic-on-digital-evidence-using-general-computer-forensic-investigation-model-framework.pdf

Harbawi Malek, Varol Asaf (2016), The role of digital forensics in combating cybercrimes. Recuperado de: https://www.researchgate.net/publication/303393656_the_role_of_digital_forensics_in_combating_cybercrimes

Heeren Herrera, Maximiliano (2019), Epistemic problem of pedagogy: some definitions and approximations. Recuperado de: http://repositorio-digital.uct.cl/handle/10925/2506

Heloıse Pieterse (2019), Evaluation and identification of authentic smartphone data. Recuperado de: https://repository.up.ac.za/handle/2263/70669

Hernández, R, Fernández. C y Baptista. P (2014*), Metodología de la investigación (6ta)*, México D. C.: MacGraw Hill - Interamericana Editores S.A.

Asha Joseph, Singh John (2016), Review of digital forensic models and a proposal for operating system level enhancements. Recuperado de: https://www.researchgate.net/publication/312287362_review_of_digital_forensic_models_and_a_proposal_for_operating_system_level_enhancements

Karabiyik Umit, Akkaya Kemal (2018), Digital forensics for iot and wsns. Recuperado de: https://core.ac.uk/download/pdf/158373118.pdf

Kävrestad Joakim (2018), Fundamentals of digital forensics: theory, methods, and real-life applications. Recuperado de: https://books.google.com.pe/books?id=bfpmdwaaqbaj&printsec=frontcover&hl=es#v=onepage&q&f=true

López Roldan Pedro y Fachelli Sandra (2016), Metodología de la investigación social cuantitativa. Recuperado de: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved

=2ahUKEwjGnfWYicjxAhUyqJUCHXKQA-YQFnoECBo-QAA&url=https%3A%2F%2Fddd.uab.cat%2Fpub%2Fca-plli%2F2016%2F163568%2Fmetinvsoccua_cap3-8a2016.pdf&usg=AO-vVaw2_1ys9Lzd0gYkyFo-NGwl5

Mohamed Elyas, Ahmad Atif, Maynard Sean B. y Lonie Andrew (2015), Digital forensic readiness: expert perspectives on a theoretical. Recuperado de: http://scholar.google.com.pe/scholar_url?url=https://www.resear-chgate.net/profile/atif_ahmad2/publication/275157238_digital_foren-sic_readiness_expert_perspec-tives_on_a_theoretical_frame-work/links/5a21e1824585155dd41ac227/digital-forensic-readiness-expert-perspectives-on-a-theoretical-frame-work.pdf&hl=es&sa=x&ei=8ngsymtwkoxsmag-8ppwbw&scisig=aagbfm38cq-pqiiytqwzb-xthvz5s-_fyg&nossl=1&oi=scholarr

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

Mohammed Hussam, Clarke Nathan, Li Fudong (2016), An Automated Approach for Digital Forensic Analysis of Heterogeneous Big Data. Recuperado de: https://www.researchgate.net/publication/308903458_an_automated_ap-proach_for_digital_forensic_analysis_of_heterogeneous_big_data

Monat Jamie, Gannon Thomas (2018), Applying systems thinking to engineering and design. Recuperado de: https://www.researchgate.net/publication/327758240_applying_systems_thinking_to_engineering_and_design

Montasari Reza, Hill Richard, Carpenter Victoria (2019), The standardised digital forensic investigation process model. Recuperado de: http://nectar.northampton.ac.uk/11862/1/montasari_etal_springer_2019_the_standardised_digital_forensic_investigation_process_model_sdfipm_.pdf

Reza Montasari (2016), The comprehensive digital forensic investigation process model. Recuperado de: http://hdl.handle.net/10545/620799

Mosbah Jalal Mosa (2018), Theory and practice of forensics techniques for smartphones. Recuperado de: http://www.alazhar.edu.ps/arabic/he/files/20163450.pdf

Nye Ryan (2017), Digital forensics report. Recuperado de: http://www.rnyte-cyber.com/uploads/9/8/5/9/98595764/exampledigiforensicsrprt_by_ryan_nye.pdf

Obiora Nweke Livinus (2018), Digital forensics: validation of network artifacts based on stochastic and probabilistic modeling of internal consistency of artifacts. Recuperado de: https://pmworldlibrary.net/wp-content/uploads/2018/07/nweke-digital-forensics-masters-thesis-sapienza-university-italy.pdf

Jeetendra Pandey, Prasad Ajay (2016), Digital forensics. Recuperado de: https://www.researchgate.net/publication/300474145_digital_forensics

Prasad Prabhu (2020), Role of the computers in digital forensics. Recuperado de: https://www.researchgate.net/publication/343323877_role_of_the_computers_in_digital_forensics

Prayudi Yudi, Riadi Imam, Subektiningsih Subektiningsih (2018), Digital forensics workflow as a mapping model for people, evidence, and process in digital investigation. Recuperado de: https://www.researchgate.net/publication/326741793_digital_forensics_workflow_as_a_mapping_model_for_people_evidence_and_process_in_digital_investigation

Proffitt Timothy (2019), A digital forensics capability maturity model for organizations. Recuperado de: http://ijofcs.org/v14n1-pp003-a-digital-forensics.pdf

Raja Ashif (2021), Active and Passive Detection of Image Forgery: A Review Analysis. Recuperado de: https://www.ijert.org/research/active-and-passive-detection-of-image-forgery-a-review-analysis-IJERTCONV9IS05089.pdf

Rani Sudesh (2018), Digital forensic models: a comparative analysis. Recuperado de: https://www.ijmra.us/project%20doc/2018/ijmie_june2018/ijmra-14015.pdf

Riadi Imam (2017), Identification of digital evidence on android's blackberry messenger using nist mobile forensic method. Recuperado de: https://www.researchgate.net/profile/imam-riadi-2/publication/317620078_identification_of_digital_evidence_on_android%27s_blackberry_messenger_using_nist_mobile_forensic_method/links/5943f0cd0f7e9b6910ee2624/identification-of-digital-evidence-on-androids-blackberry-messenger-using-nist-mobile-forensic-method.pdf

Rochmadi Tri, Riadi Imam, Prayudi Yudi (2017), Live forensics for anti-forensics analysis on private portable web browser. Recuperado de: https://www.researchgate.net/profile/yudi_prayudi/publication/316172830_live_forensics_for_anti-foren-sics_analysis_on_private_portable_web_browser/links/59f80b67a6fdcc075ec7cc7d/live-forensics-for-anti-forensics-analysis-on-private-portable-web-browser.pdf

Roussev Vassil (2019), Forensics knowledge area. Recuperado de: https://www.cybok.org/media/downloads/forensics_issue_1.0.pdf

Sadiku Matthew N. O., Tembely Mahamadou, Musa Sarhan M. (2017), Digital forensics. Recuperado de: https://www.researchgate.net/publication/318665422_digital_forensics

Sarwar Mir Sara, Shoaib Umar, Shahzad Sarfraz Muhammad (2016), Analysis of digital forensic investigation models. Recuperado de: https://www.academia.edu/download/51340536/30_paper_31101673_ijcsis_camera_ready_pp._292-301.pdf

Sathiyanarayanan Mithileysh (2016), Introduction to digital forensics. Recuperado de: https://www.academia.edu/37613861/introduction_to_digital_forensics

Scanlon Mark (2017), Evaluation of digital forensic process models with respect to digital forensics as a service. Recuperado de: https://www.researchgate.net/publication/318981575_evaluation_of_digital_forensic_process_models_with_respect_to_digital_forensics_as_a_service

Shalaginov Andrii, Iqbal Asif, Olegård Johannes (2020), Iot digital forensics readiness in the edge: a roadmap for acquiring digital evidence from intelligent smart applications. Recuperado de: https://ntnuopen.ntnu.no/ntnu-

xmlui/bitstream/handle/11250/2729970/_edge_2020__iot_digital_forensics_readiness_in_the_edge.pdf?sequence=1

Singh Avinash (2019), A digital forensic readiness approach for ransomware forensics. Recuperado de: https://repository.up.ac.za/bitstream/handle/2263/75610/singh_digital_2019.pdf?sequence=1&isallowed=y

Singh Neha, Joshi Sandeep (2015), Digital image forensics: progress and challenges. Recuperado de: https://www.researchgate.net/publication/299367087_digital_image_forensics_progress_and_challenges

Stelly Christopher D. (2019), A domain specific language for digital forensics and incident response analysis. Recuperado de: https://scholarworks.uno.edu/cgi/viewcontent.cgi?article=3872&context=td

Sudyana Didik, Prayudi Yudi, Sugiantoro Bambang (2019), Analysis and evaluation digital forensic investigation framework using iso 27037:2012. Recuperado de: https://www.researchgate.net/publication/328281191_analysis_and_evaluation_digital_forensic_investigation_framework_using_iso_270372012

Sugiantoro Bambang (2018), Digital forensic analysis on android smartphones for handling cybercrime cases. Recuperado de: https://www.researchgate.net/publication/330558290_digital_forensic_analysis_on_android_smartphones_for_handling_cybercrime_cases

Taubmann Benjamin (2019), Improving digital forensics and incident analysis in production environments by using virtual machine introspection. Recuperado de: https://www.researchgate.net/publication/343600647_Improving_Digital_Forensics_and_Incident_Analysis_in_Production_Environments_by_Using_Virtual_Machine_Introspection

Valderrama Mendoza Santiago Rufo (2013), Guía para elaborar la tesis universitaria escuela de posgrado. Recuperado de: https://www.academia.edu/37024919/gu%c3%8da_para_elaborar_la_tesis_universitaria_escuela_de_posgrado

Varoj asaf, Sonmez yesim ulgen (2017), Review of evidence analysis and reporting phases in digital forensics process. Recuperado de: https://www.researchgate.net/publication/320829880_review_of_evidence_analysis_and_reporting_phases_in_digital_forensics_process

Veber Jaromir, Smutny Zdenek (2015), Standard iso 27037:2012 and collection of digital evidence: experience in the Czech Republic. Recuperado de:

https://www.researchgate.net/profile/zdenek-smut-ny/publication/283226153_standard_iso_270372012_and_collection_of_digital_evidence_experience_in_the_czech_republic/links/569a87dd08ae6169e55b844f/standard-iso-270372012-and-collection-of-digital-evidence-experience-in-the-czech-republic.pdf

Yeboah-Boateng Ezer Osei y Akwa-Bonsu Elvis (2016), Digital forensic investigations: issues of intangibility, complications and inconsistencies in cyber-crimes. Recuperado de: https://www.researchgate.net/publication/294277641_digital_forensic_investigations_issues_of_intangibility_complications_and_inconsistencies_in_cyber-crimes

Yopla Mercado Yolanda, Yopla Mercado Alberto (2014), Metodología para la colecta de la evidencia digital. Recuperado de: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/114/1020052-1020056.pdf?sequence=6&isallowed=y

ANEXOS

Anexo 1: Matriz de Consistencia

TÍTULO: ISO 27037:2012 en la mejora del análisis forense en la empresa DG Service, Lima-2021

AUTOR: Ramos Anampa Bruno

<table>
<tr><th>PROBLEMA</th><th>OBJETIVOS</th><th>HIPÓTESIS</th><th colspan="2">VARIABLES E INDICADORES</th></tr>
<tr><td rowspan="5">Problema principal:
¿De qué manera el ISO 27037:2012 mejora el análisis forense en la empresa DG Service, Lima 2021?

Problemas específicos:
PE 1: ¿De qué manera el ISO 27037:2012 mejora los tiempos de trabajo del análisis forense en la empresa DG Service, Lima 2021?

PE 2: ¿De qué manera del ISO 27037:2012 mejora la extracción de datos del análisis forense en la empresa DG Service, Lima 2021?</td><td rowspan="5">Objetivo principal:
Determinar que el ISO 27037:2012 mejora el análisis forense en la empresa DG Service, Lima 2021.

Objetivos específicos:
OE 1: Determinar que el ISO 27037:2012 mejora los tiempos de trabajo del análisis forense en la empresa DG Service, Lima 2021.

OE 2: Determinar que el ISO 27037:2012 mejora la extracción de datos del análisis forense en la empresa DG Service, Lima 2021</td><td rowspan="5">Hipótesis principal:
El ISO 27037 :2012 mejorara significativamente el análisis forense en la empresa DG Service, Lima 2021.

Hipótesis específicas:
HE 1: El ISO 27037:2012 mejorara significativamente los tiempos de trabajo del análisis forense en la empresa DG Service, Lima 2021

HE 2: El ISO 27037:2012 mejorara significativamente la extracción de datos del análisis forense en la empresa DG Service, Lima 2021.</td><td colspan="2">Variable - 1: ISO 27037:2012</td></tr>
<tr><td colspan="2">Variable - 2: Análisis Forense</td></tr>
<tr><td>Indicadores</td><td>Unidad de medida</td></tr>
<tr><td>tiempos de trabajo</td><td>Porcentaje</td></tr>
<tr><td>extracción de datos</td><td>Porcentaje</td></tr>
<tr><td>número de casos resueltos</td><td>Porcentaje</td></tr>
</table>

TÍTULO: ISO 27037:2012 en la mejora del análisis forense en la empresa DG Service, Lima-2021 AUTOR: Ramos Anampa Bruno			
PROBLEMA	**OBJETIVOS**	**HIPÓTESIS**	**VARIABLES E INDICADORES**
PE 3: ¿De qué manera el ISO 27037:2012 mejora el número de casos resueltos del análisis forense en la empresa DG Service, Lima 2021?	OE 3: Determinar que el ISO 27037:2012 mejora el número de casos resueltos del análisis forense en la empresa DG Service, Lima 2021	HE 3: El ISO 27037:2012 mejorara significativamente el número de casos resueltos del análisis forense en la empresa DG Service, Lima 2021	

Metodología

TIPO Y DISEÑO	POBLACIÓN Y MUESTRA	TÉCNICAS E INSTRUMENTOS	ESTADÍSTICA POR UTILIZAR
Tipo: Aplicada **Diseño: E**xperimental-experimental puro	**Población:** 30 Observaciones **Muestreo:** probabilístico del tipo aleatorio simple	**Técnicas:** Observación **Instrumentos:** Guía de observación	**Descriptiva:** Para el análisis descriptivo, se usará tablas y figuras, exponiendo medidas de tendencia central usando la media, se realizará su interpretación o lectura por cada indicador, datos emitidos por el instrumento, lo cual ayudará a fijar de manera visual y estructurada la comprensión sencilla de lodos los datos numéricos **Inferencial:** Para el análisis inferencial, se comprobó la normalidad de los datos obtenidos mediante la prueba Test de Shapiro Wilk, Además, se utilizó para la contrastación de hipótesis las pruebas de los rangos con signo de Wilcoxon

Anexo 2: Matriz de Operacionalización de Variables

TÍTULO**: ISO 27037:2012 en la mejora del análisis forense en la empresa DG Service, Lima 202**1

AUTOR: R**amos Anampa Bruno Dudu**

INDICADOR	DEFINICIÓN	INSTRUMENTO	UNIDAD DE MEDIDA	FÓRMULA
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	$x = \frac{Datos\ extraidos}{Datos\ Totales} x100$
Número de 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 3: Instrumento de Recolección de Datos

Guía de observación N° 1: Tiempos de Trabajo

Guía de observación de medición del indicador índice de Tiempos de Trabajo					
Investigador:			Ramos Anampa Bruno		
Proceso observado:			Análisis Forense		
Pre-Test					
N° de Obs.	Dispositivo	Fecha	Horas De Trabajo Empleado	Horas De Trabajo Proyectada	Tiempos de Trabajo = (Horas De Trabajo Empleado) / (Horas De Trabajo Proyectada)

Guía de observación de medición del indicador *Tiempos de Trabajo*					
Investigador:			Ramos Anampa Bruno		
Proceso observado:			Análisis Forense		
Post-Test					
N° de Obs.	Dispositivo	Fecha	Horas De Trabajo Empleado	Horas De Trabajo Proyectada	Tiempos de Trabajo = (Horas De Trabajo Empleado) / (Horas De Trabajo Proyectada)

Guía de observación N° 2. Indicador de Extracción de Datos

Guía de observación de medición del indicador de Extracción de Datos					
Investigador:			Ramos Anampa Bruno		
Proceso observado:			Análisis Forense		
Pre-Test					
N° de Obs.	Dispositivo	Fecha	Datos extraídos (MB)	Datos Totales (MB)	Extracción de Datos= (Datos extraídos) / (Datos Totales) x 100

Guía de observación de medición del indicador de Extracción de Datos					
Investigador:			Ramos Anampa Bruno		
Proceso observado:			Análisis Forense		
Post-Test					
N° de Obs.	Dispositivo	Fecha	Datos extraídos (MB)	Datos Totales (MB)	Extracción de Datos= (Datos extraídos) / (Datos Totales) x 100

Guía de observación N° 3. Indicador Número De Casos Resueltos

Guía De Observación De Medición Del Indicador Número De Casos Resueltos					
Investigador:			Ramos Anampa Bruno		
Proceso observado:			Análisis Forense		
Pre-Test					
N° de Obs.	Dispositivo	Fecha	Nivel de Actual	Nivel Deseado	Número de Casos resuel-tos= (Nivel de Actual) / (Nivel Deseado) x 100

Guía de observación de medición del indicador Número de Casos resueltos					
Investigador:			Ramos Anampa Bruno		
Proceso observado:			Análisis Forense		
Post-Test					
N° de Obs.	Dispositivo	Fecha	Nivel de Actual	Nivel Deseado	Número de Casos resuel-tos = (Casos resueltos) / (Casos totales) x 100

Anexo 4: Certificado de Validación del Instrumento de Recolección de Datos

Validación del Experto n°1

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO

VARIABLE: ANÁLISIS FORENSE

N.º	INDICADORES	Claridad [1]		Pertinencia [2]		Relevancia [3]		Sugerencias
		Si	No	Si	No	Si	No	
1	**Tiempos De Trabajo** x= (horas de trabajo empleado) / (horas de trabajo proyectada) x 100	X		X		X		
2	**Extracción De Datos** x= (Datos extraídos) / (Datos Totales) x 100	X		X		X		
3	**Número De Casos Resueltos** x= (Nivel de Actual) / (Nivel Deseado) x 100	X		X		X		

Observaciones (precisar si hay suficiencia): Si hay Suficiencia

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

24 de mayo del 2021

Apellidos y nombres del juez evaluador: Inquilla Quispe Ricardo Carlos DNI: 00515158

Especialista: Metodólogo [ ] Temático [X]

Grado: Maestro [X] Doctor [ ]

[1] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2] **Pertinencia:** Si el ítem pertenece a la dimensión.
[3] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

Validación del Experto n°2

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO

VARIABLE: ANÁLISIS FORENSE

N.º	INDICADORES	Claridad [1]		Pertinencia [2]		Relevancia [3]		Sugerencias
		Si	No	Si	No	Si	No	
1	**Tiempos De Trabajo** x= (horas de trabajo empleado) / (horas de trabajo proyectada) x 100	X		X		X		
2	**Extracción De Datos** x= (Datos extraídos) / (Datos Totales) x 100	X		X		X		
3	**Número De Casos Resueltos** x= (Nivel de Actual) / (Nivel Deseado) x 100	X		X		X		

Observaciones (precisar si hay suficiencia): Hay Suficiencia

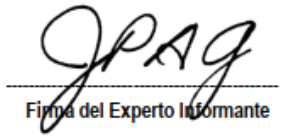
Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

24 de mayo del 2021

Apellidos y nombres del juez evaluador: Anampa García Jhon Paul **DNI: 70005373**

Especialista: Metodólogo [ ] Temático [X]

Grado: Maestro [X] Doctor [ ]



[1] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2] **Pertinencia:** Si el ítem pertenece a la dimensión.
[3] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Validación del experto n°3

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO

VARIABLE: Análisis Forense

N°	INDICADORES	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
		Si	No	Si	No	Si	No	
1	**Tiempos De Trabajo** x= (horas de trabajo empleado) / (horas de trabajo proyectada) x 100	X		X		X		
2	**Extracción De Datos** x= (Datos extraídos) / (Datos Totales) x 100	X		X		X		
3	**Número De Casos Resueltos** x= (Nivel de Actual) / (Nivel Deseado) x 100	X		X		X		

Observaciones (precisar si hay suficiencia):__SUFICIENTE_____

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

29 de mayo del 2021

Apellidos y nombres del juez evaluador: JOEL MARTIN VISURRAGA AGÜERO DNI: 10192315

Especialista: Metodólogo [X] Temático [X]

Grado: Maestro [ ] Doctor [X]

[1] **Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2] **Pertinencia**: Si el ítem pertenece a la dimensión.
[3] **Relevancia**: El ítem es apropiado para representar al componente o dimensión específica del constructo
Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Dr. Joel Martin Visurraga Agüero

Anexo 5: base de datos

	Indicador 01		Indicador 02		Indicador 03	
	I1PreTest	I1PostTest	I2PreTest	I2PostTest	I3PreTest	I3PostTest
1	1.07	0.8	77.83	89.53	0.6	1
2	1.11	0.91	82.66	92.61	0.6	0.8
3	1.07	0.84	79.09	96.6	0.8	1
4	1.02	0.67	45.51	87.52	0.6	1
5	1.38	0.88	43.02	72.18	0.6	0.8
6	1.33	0.93	76.48	95.79	0.6	1
7	1.02	0.93	39.53	79.89	0.6	0.8
8	1.02	0.67	42.32	93.33	0.6	1
9	1.18	0.8	63.41	94.71	0.8	1
10	0.98	0.73	78.41	94.53	0.6	1
11	1.02	0.84	42.61	79.89	0.6	0.8
12	1.15	0.75	76.48	99.08	0.6	1
13	1.33	1.02	90.35	94.53	0.4	0.6
14	1.58	0.93	52.91	80.64	0.6	1
15	1.07	0.78	84.1	94.78	0.2	0.6
16	1.16	0.84	38.92	79.57	0.6	1
17	1.11	0.91	39.97	89.54	0.6	0.8
18	1.11	0.93	82.78	96.6	0.6	1
19	1.15	0.8	90.81	97.7	0.6	1
20	1.22	0.89	41.64	82.94	0.4	0.8
21	1.33	0.96	77.72	97.72	0.6	1
22	1.2	0.89	79.07	97.28	0.4	0.8
23	1.09	0.67	60.59	93.75	0.6	1
24	1.18	0.83	82.16	94.71	0.6	1
25	1.02	0.73	57.95	82.35	0.4	1
26	1.22	0.8	66.46	97.28	0.6	0.8
27	1.11	0.67	76.48	97.78	0.6	1
28	1.5	1.1	84.1	94.53	0.4	0.8
29	1.4	0.89	63.93	88.61	0.4	1
30	1.05	0.8	72.08	98.66	0.6	0.8

Anexo 6: Autorización de la Investigación

AUTORIZACIÓN DE INVESTIGACIÓN EN LA EMPRESA DG SERVICE

Gerente General Lucio Gonzalez Martines

Autoriza

Al Sr. Bruno Dudu Ramos Anampa, identificado con el DNI 46255583 se le autorizo la aplicación del instrumento de recolección de datos a través de la ficha de observación de los siguientes indicadores: tiempos de trabajo, extracción de datos, y número de casos resueltos. Para el proceso de Análisis Forense con la finalidad de lograr la mejora a través del ISO 27037 en la empresa DG Service

Tras lo mencionado se afirma que el ISO 27037 mejora el en la mejora del Análisis Forense en la empresa DG Service, Lima-2021.

Se expresa el agradecimiento por la mejora y se expide el presente documento a solicitud del interesado para los fines que estime conveniente.

Anexo 7: Pruebas de Normalidad

Según López y Fachelli (2016), se hará uso de la prueba de Shapiro-Wilk, al contar esta investigación con un numero de 30 de observaciones; para esta prueba se aplicó el software IBM SPSS V25, con un nivel de confianza del 95%, en donde si el valor de significancia es menor a 0.05 se obtiene una distribución no normal, lo cual significa que se debe usar la prueba de Wilcoxon para este caso y si se presenta una distribución normal se debe usar la prueba t de Student.

Prueba de normalidad del indicador tiempos de trabajo

A continuación, se describen los resultados de las pruebas de normalidad de tiempos de trabajo antes y después de aplicar el ISO 27037.

Formulación de hipótesis estadística:

H_o: Los datos del indicador tiempos de trabajo presentan una distribución normal.

H_1: Los datos del indicador tiempos de trabajo no presentan una distribución normal

Tabla 1

Pruebas de normalidad del Indicador tiempos de trabajo

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pretest01	.896	30	.007
Postest01	.962	30	.345

Nota: Elaborado con asistencia de IBM SPSS V25.

En la tabla 1, los resultados alcanzados en la prueba reflejaron que el valor de significancia de la muestra del indicador tiempos de trabajo en el pretest 01 es

de 0.007 y en el postest 01 es de 0.345 cuyo valor es mayor al error asumido de 0.05 entonces se acepta la hipótesis nula, deduciendo que el indicador se distribuye normalmente

Prueba de normalidad del indicador extracción de datos

Formulación de hipótesis estadística

Ho: Los datos del indicador de extracción de datos presentan una distribución normal.

H1: Los datos del indicador extracción de datos no presentan una distribución normal

Tabla 2

Pruebas de normalidad del indicador de extracción de datos

	Shapiro-Wilk		
	Estadístico	gl	Sig.
PreTest02	.880	30	.003
PosTest02	.855	30	.001

Nota: Elaborado con asistencia de IBM SPSS V25.

los resultados reflejados en la tabla 2 indica que el valor de significancia de la muestra del indicador de extracción de datos en el pretest02 es de 0.03 y en el postest 02 es de 0.001 cuyos valores es menor al error asumido de 0.05 entonces por lo tanto se rechazó la hipótesis nula y se concluyó que el indicador no se distribuye normalmente.

Prueba de normalidad del indicador número de casos resueltos

Formulación de hipótesis estadística:

Ho: Los datos del indicador de número de casos resueltos presentan una distribución normal.

H1: Los datos del indicador número de casos resueltos no presentan una distribución normal.

Tabla 3

Pruebas de normalidad del indicador de número de casos resueltos

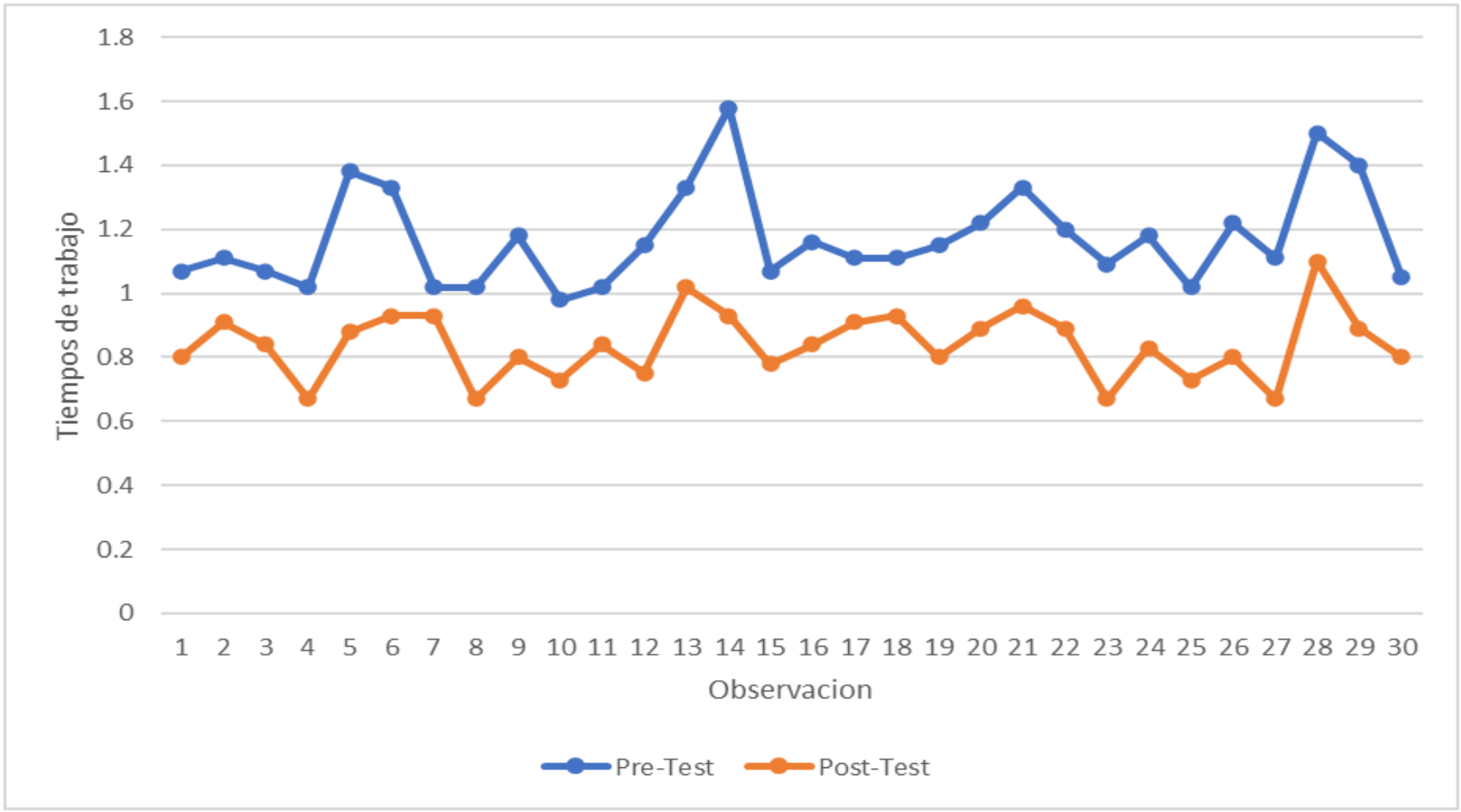
	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pretest03	.733	30	.001
Pretest03	.701	30	.001

Nota: Elaborado con asistencia de IBM SPSS V25

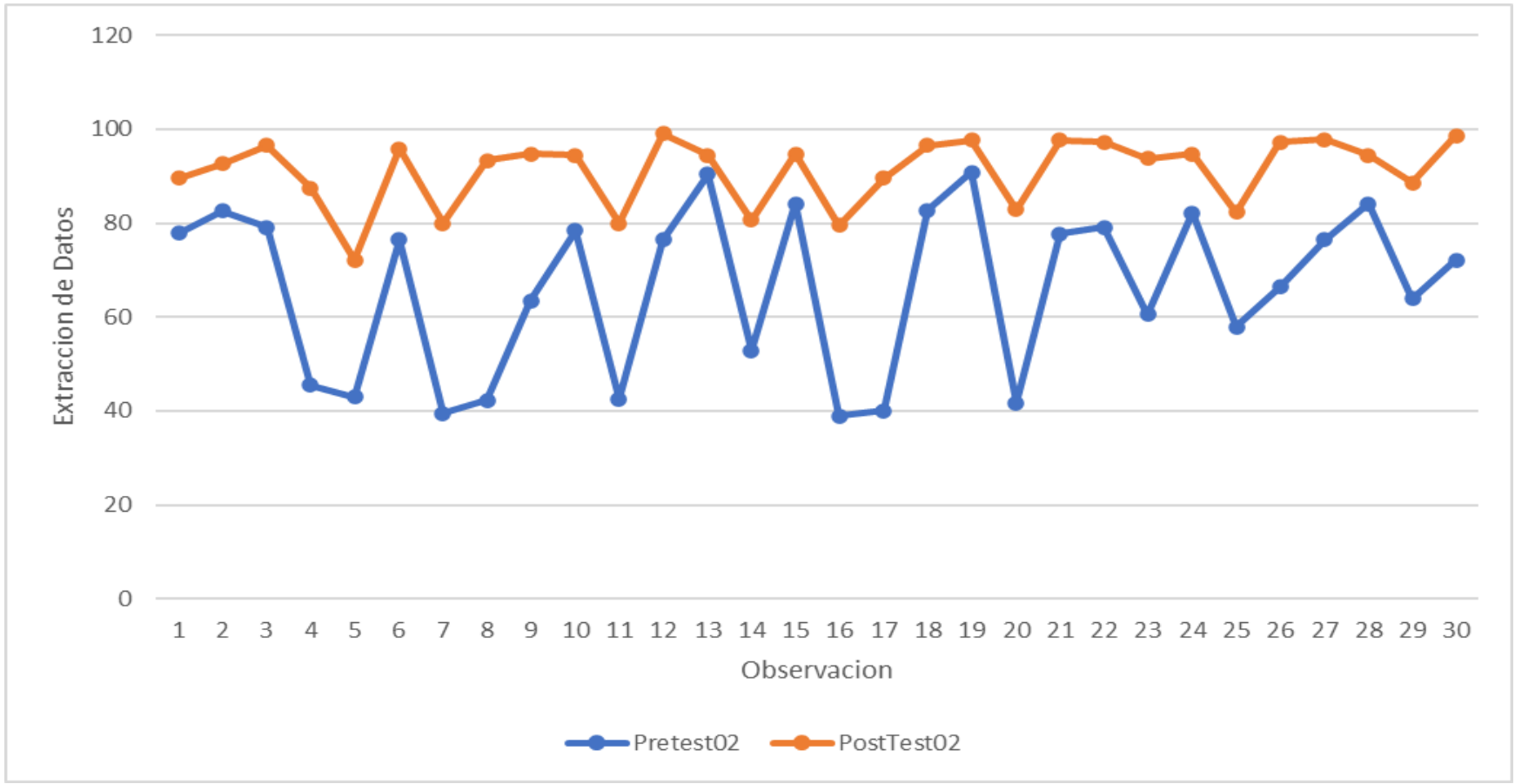
Según los resultados mostrados en la tabla 3 se muestra que el valor de significancia de la muestra del indicador de número de casos resueltos en el pretest 03 fue de 0.01 y en postest 03 fue de 0.001 cuyos valores es menor al error asumido de 0.05 entonces se rechaza la hipótesis nula, deduciendo que el indicador no se distribuye normalmente

Anexo 8: Comportamiento de las medidas descriptivas

Indicador 1: Tendencias de las medidas descriptivas del indicador tiempos de trabajo antes y después de aplicar el ISO 27037:2012



Indicador 2: Tendencias de las medidas descriptivas del indicador de extracción de datos antes y después de aplicar el ISO 27037:2012



Indicador 3: Tendencias de las medidas descriptivas del indicador números de casos resueltos antes y después de aplicar el ISO 27037:2012