UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

ESCUELA DE POSGRADO

TESIS

PERITAJE INFORMÁTICO BASADO EN UNA NUEVA METODOLOGÍA HÍBRIDA EN 2M & J INGENIEROS – HUARAZ 2019

PRESENTADO POR

CRISTHIAN MAX CACHA ARANA

PARA OPTAR EL GRADO ACADÉMICO DE

MAESTRO EN GESTIÓN TECNOLÓGICA DE LA INFORMACIÓN

ASESOR

Mg. CARLOS ALBERTO ZEGARRA SANCHEZ

LÍNEA DE INVESTIGACIÓN

GESTIÓN DE SISTEMAS DE INFORMACIÓN

LIMA - PERÚ

2020

Dedicatoria

A mis padres y hermana por su incondicional apoyo, por ser los motivos para esforzarme y seguir siempre mejorando a nivel profesional y personal.

El Autor.

Agradecimiento

A los docentes de la Escuela de Posgrado de la Universidad Peruana de Ciencias e Informática por el apoyo en todo el proceso.

El Autor.

Índice

Lista de tabla

Lista de figuras

Resumen

El objetivo de la presente investigación fue demostrar cual es el efecto de la informática forense basado en una nueva metodología híbrida en el Peritaje Informático en la Empresa 2M&J Ingenieros, 2019.

Es una investigación aplicada, con diseño experimental, de manera específica, diseño preexperimental, en una muestra censal de 15 computadoras. Se aplicó la prueba del pretest al grupo único y, obtenidos los resultados se realizó la aplicación de la nueva metodología en actividades, para volver a ser evaluada en la fase de postest. En el tratamiento estadístico se utilizó el software SPSS 25.

La descripción de los resultados se hizo desde una mirada descriptiva (Figuras y gráficas de barras) mientras en la parte inferencial se utilizó en el contraste de hipótesis la prueba no paramétrica de rangos con signos de Wilcoxon que se utiliza para muestras relacionadas. El resultado hallado demostró el efecto de la informática forense con la aplicación de una nueva metodología en la mejora del peritaje informático en la Empresa 2M&J INGENIEROS, 2019, al obtener un valor Z = -3.425 < -1.96 (95%), por lo que se evidencia diferencias significativas en el contraste de hipótesis en la fase de pretest y postest, al obtenerse un valor p = 0 .001 < 0.05.

Palabras clave: Nueva metodología híbrida, peritaje informático, estudio informático, evidencia digital, delito informático.

Abstract

The objective of the present investigation was to demonstrate the effect of forensic informatics based on a new hybrid methodology in Computer Expertise in the Company 2M & J Ingenieros, 2019.

It is an applied research, with experimental design, specifically, preexperimental design, in a census sample of 15 computers. The pretest test was applied to the single group and, after obtaining the results, the application of the new methodology in activities was carried out, to be reassessed in the posttest phase. The SPSS 25 software was used in the statistical treatment.

The description of the results was made from a descriptive perspective (tables and bar graphs) while in the inferential part the non-parametric test of ranges with Wilcoxon signs used for related samples was used in the hypothesis test. The result found demonstrated the effect of forensic informatics with the application of a new methodology in the improvement of computer expertise in the Company 2M & J ENGINEERS, 2019, when obtaining a value Z = -3.425 <-1.96 (95%), so significant differences in the hypothesis contrast are evidenced in the pretest and posttest phase, when obtaining a value p = 0 .001 <0.05.

Keywords: New hybrid methodology, computer expertise, computer study, digital evidence, computer crime.

Introducción

La información es el activo más valioso que se posee en la sociedad actual. Cada vez es más importante para el desarrollo de las empresas y de negocios a través de la implementación de sistemas de información y redes de cómputo, permitiendo mantener de forma ininterrumpida los flujos de información que luego han de convertirse en conocimiento nuevo y, posteriormente, adoptar decisiones. Sin embargo, este bucle retroalimentador que funciona en el interior de la organización muchas veces se ve expuesto a ataques invasivos, violando de esta manera, la seguridad del sistema de información.

De otro lado, la proliferación de redes y sistemas informáticos permiten al mundo mantenerse globalmente "conectado", a través de la telaraña mundial se pueden mantener conversaciones, intercambiar correos o realizar transacciones monetarias con prácticamente cualquier persona en diversas partes del planeta de una forma rápida, sencilla y económica. Las ventajas son evidentes, mayor facilidad en el manejo de la información, rapidez en la recolección y análisis de la misma, alta disponibilidad tanto en tiempo como en localidad. Sin embargo, así como las Tecnologías de Información y Comunicaciones (TIC's) han cambiado la forma tradicional de hacer las cosas y representan una herramienta cada vez más importante en las organizaciones, no obstante, este cambio ha traído consigo también, nuevas formas de cometer delitos y por lo tanto se torna primordial hablar de seguridad en cuanto a computación y redes se refiere. La seguridad de la información y de los sistemas es un punto crítico en una sociedad en la que cada día la información electrónica o digital se torna más indispensable.

Por ello, operar los sistemas de información implica correr el riesgo de que la información sea sustraída, destruida o utilizada de forma delictiva. Ante estos imponderables es preciso tener una manera de protegerse de los delincuentes cibernéticos. De manera que,

ante este panorama que se torna cada día más complejo, los profesionales de las TIC's y en aplicación de la ley, deben cooperar y trabajar juntos en la defensa, detección y procesamiento de las personas que hacen uso de las TIC's para dañar individuos, organizaciones, empresas o sociedad en general.

Sin embargo, para poder garantizar las políticas de seguridad y la protección de la información y las tecnologías que facilitan la gestión de la misma, surge la Informática Forense. De acuerdo con Cano (2006) la informática forense constituye una disciplina auxiliar a la justicia moderna cuyo objetivo es enfrentarse a los intrusos informáticos que cometen crímenes cibernéticos, en ese sentido esta disciplina busca garantizar el conocimiento de la verdad en torno de una evidencia digital requerida en un proceso judicial. Como disciplina que se ha ido perfilando en las últimas dos décadas ha desarrollado un conjunto de estándares que han permitido desarrollar una metodología propia y, que se ve reflejada en los diversos modelos de análisis forense de evidencias digitales.

En base a lo expresado anteriormente, el presente estudio, ha considerado conveniente proponer como título: Peritaje informático basado en una nueva metodología híbrida en 2M & J Ingenieros – Huaraz 2019, la misma que se expone de manera detallada en los siguientes apartados:

En el capítulo I, se aborda el Planteamiento del Problema, mediante la descripción de la realidad problemática, definición del problema, objetivos de la investigación, las hipótesis, variables y dimensiones, además de la justificación de la investigación.

A continuación, se presenta las consideraciones del capítulo II, albergando la presentación del Marco Teórico, donde se presentan: los antecedentes nacionales e internacionales que sirven de soporte a la presente investigación, además de las conceptualizaciones teóricas sobre la variable de estudio.

Asimismo, se desarrolla el capítulo III, en el que se detalla la metodología comprendido en el: tipo y diseño de la investigación, asimismo la descripción de la población y la muestra elegida, además de la aplicación de las técnicas para la recolección y procesamiento de la información, la misma que se obtuvo a través de la implementación y levantamiento de datos en base a dos cuestionarios: cuestionario de estrategias de aprendizaje universitario y el cuestionario de logro de competencias genéricas.

En efecto, en el capítulo IV, se muestran los resultados obtenidos de la aplicación de los instrumentos presentados en Figuras y gráficos, asimismo el contraste de las hipótesis, información obtenida a través de los datos, habiendo sido procesados través del software estadístico SPSS.

En consecuencia, en el capítulo V, se presenta la discusión tomando en consideración los antecedentes y los resultados obtenidos, además de las conclusiones y recomendaciones que se generan de las mismas en la presente investigación.

Finalmente, se presenta las referencias bibliográficas que permitieron la construcción de fuentes de información para el presente estudio, basándose en fuentes bibliográficas y electrónicas.

Capítulo I

1. PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

La evolución de las tecnologías de la información y comunicación (en adelante, TIC) representa un avance significativo para la humanidad, porque está creando nuevos entornos sociales basado en la movilidad y facilidad para los usuarios. En efecto, se está experimentando una nueva realidad: la de un mundo en el que las personas están conectadas digitalmente, un mundo impulsado por la tecnología, en el que las TIC engloban y afectan el entorno que viene labrando el siglo XXI. Dichos avances tecnológicos están conllevando a la reorganización de la realidad de personas, Estados y empresas. Todo ello hace que aumente el número de delincuentes informáticos que, en líneas generales, son personas que realizan actividades delictivas en internet como robar información, acceder a redes privadas, correos, chats, estafas, pornografía infantil, entre otros crímenes. En suma, todo lo que tiene que ver con los delitos e ilegalidad donde posteriormente pueden

intentar eliminar todo rastro y poder librarse de la justicia.

A nivel internacional, Dmitry Bestuzhev, director del equipo de Investigación y Análisis para América Latina de la empresa rusa de seguridad informática Kaspersky, dio a conocer que, dentro de este escenario, Brasil es el país más expuesto a los crímenes cibernéticos al haber sido víctima en 2013 de entre el 33 y el 43% de los ataques en la región, sostuvo el experto.

Además de Brasil, ciudadanos y organizaciones de México, Venezuela y Perú son víctimas de entre el 26 y 36% de los ataques en la red, añadió Bestuzhev durante la cuarta Cumbre Latinoamericana de Analistas de Seguridad organizada por Kaspersky y que se realizó en la ciudad colombiana de Cartagena. Estos delitos incluyen robo de información financiera y personal, ciberespionaje, sabotaje, eliminación de datos o daños a la reputación corporativa, siguió añadiendo el especialista tecnológico.

En la actualidad no se cuenta con una metodología estandarizada que se pueda aplicar a todo el proceso de peritaje informático, dependiendo de las diferentes metodologías para poder aplicar la informática forense y el país donde resida la empresa o el interesado en aplicarla. Si no se cuenta con una metodología estandarizada para poder aplicarla, no se podrá realizar la evaluación exhaustiva y precisa de los diferentes casos que se presente, el análisis no será preciso al comparar con otros casos similares y, por ende, los resultados no tendrán los mismos indicadores a evaluar.

Por ello, se propone plantear una nueva metodología para aplicarse en el proceso de peritaje informático y se maneje un estándar en los estudios a realizarse, logrando tener una guía de procedimientos para la mejor evaluación y presentación de resultados del estudio.

1.2. Definición del problema

1.2.1. Problema general

¿En qué medida la informática forense aplicando una nueva metodología mejora el Peritaje Informático en la Empresa 2M&J INGENIEROS, 2019?

1.2.2. Problemas específicos

P1. ¿En qué medida el proceso de peritaje aplicando una nueva metodología mejora el estudio Informático en la Empresa 2M&J INGENIEROS, 2019?

P2: ¿En qué medida el proceso de peritaje aplicando una nueva metodología mejora la evidencia digital en la Empresa 2M&J INGENIEROS, 2019?

P3: ¿En qué medida el proceso de peritaje aplicando una nueva metodología recupera las evidencias del delito informático en la Empresa 2M&J INGENIEROS, 2019?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Demostrar que la informática forense aplicando una nueva metodología mejora significativamente el Peritaje Informático en la Empresa 2M&J INGENIEROS, 2019.

1.3.2. Objetivos específicos

O1. Demostrar que el proceso de peritaje aplicando una nueva metodología mejora significativamente el estudio Informático en la Empresa 2M&J INGENIEROS, 2019.

O2: Demostrar que el proceso de peritaje aplicando una nueva metodología mejora significativamente la evidencia digital en la Empresa 2M&J INGENIEROS, 2019.

O3: Demostrar que el proceso de peritaje aplicando una nueva metodología recupera las evidencias del delito informático en la Empresa 2M&J INGENIEROS, 2019.

1.4. Hipótesis de la investigación

1.4.1. Hipótesis general

HG: La informática forense aplicando una nueva metodología mejora significativamente el Peritaje Informático en la Empresa 2M&J INGENIEROS, 2019

1.4.2. Hipótesis específicas

H1. El proceso de peritaje aplicando una nueva metodología mejora significativamente el estudio Informático en la Empresa 2M&J INGENIEROS, 2019.

H2: El proceso de peritaje aplicando una nueva metodología mejora significativamente la evidencia digital en la Empresa 2M&J INGENIEROS, 2019.

H3: El proceso de peritaje aplicando una nueva metodología recupera las evidencias del delito informático en la Empresa 2M&J INGENIEROS, 2019.

1.5. Variables y dimensiones

Tabla 1

Operacionalización de las variables

VARIABLES		ITEMS	ESCALA DE
VI: Informática Forense	1.1 Uso de la Metodología 1.2 Uso del Hardware 1.3 Uso del Software 1.4 Uso de la Auditoría	Actividades tareas Subproceso Procesos	
VD: Peritaje	2.1. El estudio Informático	1,2,3,4	Dicotómica
	2.2. La Evidencia Digital	5,6,7,8	Correcto: 1
	2.3. El Delito Informático	9, 10,11, 12	Incorrecto: 0

Fuente: Elaboración propia.

1.6. Justificación de la investigación

Conveniencia

La investigación es conveniente para la elaboración de un nuevo modelo de análisis informático forense que puede ser aplicado a procesos de peritaje informático, este modelo nos ayudará a realizar mejor el proceso, contribuyendo al estudio minucioso y detallado que se requiera en equipos de cómputo, ya sea en empresas o instituciones estatales y privadas.

Relevancia Social

Uno de los temas principales en los últimos tiempos en nuestro país es el delito informático, personas con malas intenciones logran acceder a los equipos de cómputo para realizar modificaciones que afecten al usuario o institución, eliminar información relevante, configurar para generar fallas o errores irreparables, robar información, etc. Esto no solo afecta al usuario del equipo, sino a toda la institución, generando problemas y que nunca puedan encontrar al culpable de dicho daño. Esta nueva propuesta va orientado al mejor estudio y resultados precisos en el proceso de peritaje informático.

Dado que en Perú no se tiene claro una metodología en la Informática Forense, de acuerdo a la experiencia personal, se concluyó realizar una investigación orientada a la exploración de documentos relacionados con el manejo de la evidencia digital, los distintos países y el Perú tienen su propio sistema legal sobre delitos informáticos y que no es correcto la utilización de metodologías de otros países forzando su aplicación al nuestro, motivo por el cual es necesario disponer y conocer de manera precisa la metodología que se adecúe mejor a la realidad Peruana respecto a la informática forense.

Implicaciones Prácticas

La presente investigación ayuda a resolver de manera práctica el proceso de peritaje informático, ya que se les presenta una nueva metodología aplicada al análisis informático forense que se puede aplicar en el Perú, contribuyendo con la metodología que dará un mejor resultado y tener en claro todo el proceso, pasos, herramientas, técnicas, etc.

Valor Teórico

Con esta investigación se podrá obtener un modelo general para el análisis informático forense, reforzando y dando robustez al proceso de peritaje informático con los pasos y procedimientos definidos. En este sentido, este trabajo forma un precedente de un modelo a seguir cuando una entidad necesite aplicar un modelo para el análisis informático forense.

Utilidad Metodológica

Se va a elaborar una nueva metodología para el análisis informático forense aplicado al proceso de peritaje informático, como base para desarrollar el análisis y disponer de una metodología que nos pueda guiar en el desarrollo hasta la elaboración del informe final, cuyos datos puedan ser lo más exactos posibles.

Capítulo II

2. MARCO TEÓRICO

2.1. Antecedentes de la investigación

En el Ámbito nacional

Hernández, G. (2018), en Lima Perú, hizo una investigación titulada: *La auditoría forense como medio para instrumentalizar la prueba en el lavado de activos en el sistema financiero, período 2018.* El objetivo de la investigación fue determinar si la auditoría forense puede convertirse en un medio para instrumentalizar la prueba en el lavado de activos en el sistema financiero, durante el periodo del 2018. Este trabajo se desarrolló y aplicó al personal de las entidades del sistema financiero en Lima Metropolitana, comprendido por personal administrativo, personal contable, auditores y asistentes de auditoría, entre otros relacionados con operaciones financieras y control de lavado de activos de las referidas entidades. Como resultados obtenidos se midieron las variables de estudio: La aplicación de Auditoría Forense y la Instrumentalizar la prueba en el lavado de

activos.

Hipólito, R. (2018), en Lima Perú, hizo una investigación titulada: *El empoderamiento de la auditoría forense en la lucha contra la corrupción en los gobiernos regionales del Perú, propuesta actual.* El objetivo de la investigación fue determinar la manera de como el empoderamiento de la auditoría forense podría facilitar la lucha contra la corrupción en los Gobiernos Regionales del Perú. Este trabajo se desarrolló tomando como muestra a los gobiernos regionales, un análisis de los diferentes delitos que pudiera cometer el personal de las instituciones públicas. Como resultados obtenidos del estudio fueron:

Establecer la forma como los procedimientos de auditoría forense podrán estimular la lucha contra la corrupción de los Gobiernos Regionales.

Determinar el modo como la prueba o evidencia de la auditoría forense podrá instrumentalizar la lucha contra la corrupción en los Gobiernos Regionales del Perú.

Establecer la manera cómo el informe de auditoría forense podrá enarbolar la lucha contra la corrupción en los Gobiernos Regionales del Perú.

En el ambito internacional

Arnedo, P. (2014), en la Universidad Internacional de La Rioja, hizo una investigación titulada: *Herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos*. Su objetivo de la investigación fue servir como marco de referencia para estudiantes, docentes e investigadores de la informática forense en sus procesos de peritaje y enseñanza, demostrando mediante pruebas simuladas la efectividad y aplicabilidad de herramientas de software según la función que desarrolla cada uno de ellas. Se estudió tres delitos informáticos, como primer delito fue el Incidente DELINF0951 – El servidor de la Clínica, accedieron a información de los pacientes, el segundo fue el Incidente DELINF0957 – Empresa Internacional de Refrescos, correos de chantaje de hacer circular información

secreta y confidencial relacionada con la lógica del negocio de la empresa; y como tercer delito fue el Incidente DELINF0998 – Empresa internacional dedicada a la venta de ropa femenina, intentaron hacer un fraude por una suma considerable a través de internet. Todos los delitos fueron analizados mediante software especializado, como resultados obtenidos se midieron las variables de estudio:

Identificar herramientas informáticas de gran valor para la investigación forense.

Demostrar la funcionalidad de algunas herramientas informáticas durante la investigación forense.

Desglosar las etapas que se dan en una investigación de informática forense.

Palacios, A. (2013), en México D. F. Hizo una investigación titulada: *Metodología para el análisis forense informático en sistemas de redes y equipos de cómputo personal.* Su objetivo de la investigación fue proponer una metodología con el enfoque sistémico para el análisis forense informático en sistemas de redes y equipos de cómputo personal. Se realizó el estudio de dos discos duros, el primer disco duro fue la "Imagen del disco duro objeto de estudio.ad1" y el segundo disco duro fue "Imagen del disco duro objeto de estudio.ad2" los cuales se procedió a montarlos (adicionarlos como evidencia en el software) en el software forense, con el fin de llevar a cabo una búsqueda exhaustiva de toda la información. Finalmente, los resultados obtenidos se midieron las variables:

Analizar las metodologías y estándares en cuanto a evidencia digital se refiere para efectuar una evaluación y diagnóstico de la situación actual.

Aplicar la metodología propuesta en un caso de estudio real para iniciar la evaluación de su implementación.

Tocados, J. (2015) en Castilla – La mancha, España. Hizo una investigación titulada: *Metodología para el desarrollo de procedimientos periciales en el ámbito de la información forense.* Su objetivo de la investigación fue proponer un manual de

procedimientos para la elaboración de informes periciales, que sea lo suficientemente genérico para abordar la gran variedad de dispositivos y tecnologías existentes que pueden ser sometidos a análisis. Se realizó el análisis de una computadora portátil que usaba una usuaria que fue despedida de la empresa por la supuesta utilización de un período de baja laboral (permiso) comprendido del 1 al 5 de Abril del 2015 para realizar un viaje de ocio.

Se realizó el análisis minucioso de la portátil, obteniendo como resultado:

Se realizó en análisis del hardware usando software para la realización del peritaje informático.

Se realizó las actividades de la nueva metodología propuesta para el proceso de peritaje en el ámbito de la información forense.

2.2. Bases teóricas

Según Gallardo, Fuentes y Fuentes (2016) definen informática forense como aquella disciplina que se "basa en tecnologías que tienen capital importancia para la recolección de evidencias que quizás configurarán un hecho real y tangible. La escena del crimen, es la red o la computadora en sí" (p. 2). Por tanto, la informática forense se orienta al análisis de dispositivos informáticos en base a un método con el propósito de obtener evidencias digitales.

Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Como la definición anterior lo indica, esta disciplina hace uso no solo de tecnologías de punta para poder mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar dentro de cualquier dispositivo

electrónico lo que ha sucedido. El conocimiento del informático forense abarca el conocimiento no solamente del *software* sino también de *hardware*, redes, seguridad, hacking, cracking y recuperación de información.

La informática forense ayuda a detectar pistas sobre ataques informáticos, robo de información, conversaciones o pistas de emails y chats.

La importancia de estos y el poder mantener su integridad se basa en que la evidencia digital o electrónica es sumamente frágil. El simple hecho de darle doble clic a un archivo modificaría la última fecha de acceso del mismo.

Es muy importante mencionar que la informática forense o cómputo forense no tiene parte preventiva, es decir, la informática forense no tiene como objetivo el prevenir delitos, de ello se encarga la seguridad informática, por eso resulta imprescindible tener claro el marco de actuación entre la informática forense, la seguridad informática y la auditoría informática".

Metodología NIST

El Departamento de Justicia de los Estados Unidos, es un ministerio, parte del Gobierno de los Estados Unidos, diseñado para hacer cumplir las leyes, defender los intereses del país de acuerdo con la ley y para asegurar una administración de justicia imparcial y justa para todos los estadounidenses.

El Laboratorio de Cibercrimen en la Sección de Propiedad Intelectual y Crimen Computacional (Computer Crime and Intellectually Property Section) desarrolló un diagrama de flujo en el cual se describe la Metodología de Análisis Forense Digital, dicho trabajo se realizó después de consultar con numerosos analistas forenses de varias agencias federales. Los elementos clave del Cómputo Forense se listan a continuación:

- El empleo de métodos científicos.
- Recolección y Preservación.

- Validación.
- Identificación.
- Análisis e Interpretación.
- Documentación y Presentación.

Metodología DOJ

El modelo del DOJ (Eloff et al., 2008) no hace distinción entre los métodos forenses aplicados a computadores o a algún otro dispositivo electrónico. Intenta construir un modelo general para aplicarlo a la mayoría de dispositivos electrónicos.

El Departamento de Justicia de Estados Unidos también intenta describir el proceso de computación forense, pero ha realizado el beneficio de abstraerse de tecnologías específicas. Este conjunto de procesos incluye las faces de: colección, examinación, análisis y reporte. Este modelo identifica de manera significativa los aspectos centrales del proceso forense y construyendo los pasos para soportarlo, más que caer en los detalles de una tecnología o metodología particular. En resumen, el modelo del DOJ (Department Of Justice) no hace distinción entre los métodos forenses aplicados a computadores o algunos otros dispositivos electrónicos. En vez de esto, intenta construir un proceso generalizado que será aplicado a la mayoría de los dispositivos electrónicos. La identificación de potenciales tipos de evidencia y las posibles ubicaciones en diferentes tipos de dispositivos es un buen paso para quienes desean desarrollar un proceso generalizado que puede ser instanciado con una tecnología para producir resultados significativos en una corte.

Hardware

La palabra *hardware* en informática se refiere a las partes físicas tangibles de un sistema informático; sus componentes eléctricos, electrónicos, electromecánicos y mecánicos. Los cables, así como los gabinetes o cajas, los periféricos de todo tipo, y cualquier otro elemento físico involucrado, componen el hardware o soporte físico; contrariamente, el

soporte lógico e intangible es el llamado *software*.

El término es propio del idioma inglés, y su traducción al español no tiene un significado acorde, por tal motivo se lo ha adoptado tal cual es y suena. La Real Academia Española lo define como «Conjunto de los componentes que integran la parte material de una computadora».El término, aunque sea lo más común, no solamente se aplica a las computadoras, también es a menudo utilizado en otras áreas de la vida diaria y la tecnología. Por ejemplo, *hardware* también se refiere a herramientas y máquinas, y en electrónica *hardware* se refiere a todos los componentes electrónicos, eléctricos, electromecánicos, mecánicos, cableados y tarjetas de circuitos impresos.

Software

Se conoce como *software* al soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados *hardware*. La interacción entre el software y el hardware hace operativo un ordenador (u otro dispositivo), es decir, el Software envía instrucciones que el Hardware ejecuta, haciendo posible su funcionamiento.

Auditoría.

Naranjo (2009) afirma: "La palabra auditoría viene del latín auditorius y de esta proviene la palabra auditor, que en español significa aquel que tiene la virtud de oír y revisar cuentas. La auditoría debe estar encaminada a un objetivo específico que es el de evaluar la eficiencia y eficacia con que se está operando el área analizada, para que por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien, mejorar la forma de actuación." (p. 3)

También se puede definir al término auditoria como la evaluación desarrollada por un grupo de profesionales a una entidad, del orden público o privado, con el fin de detectar fallas y

hacer las respectivas sugerencias para subsanarlas.

Historia: La auditoría es tan antigua como lo es la aparición del hombre sobre la tierra. En sus inicios esta se desarrollaba de manera empírica. En la época de la conquista estaban los "oidores" de la corona, que en el fondo eran auditores, ya que vigilaban el pago de tributos a la corona española.

En la era moderna la auditoria se implementa en cualquier empresa o entidad para encontrar falencias misionales y posteriormente proseguir con implementar el correctivo necesario.

Aplicabilidad: La aplicabilidad de un proceso de Auditoria abarca un rango amplio de entidades, de procesos, de procedimientos y de ejecuciones. Se aplica a cualquier entidad o empresa que desee detectar falencias en su lógica de negocio para su posterior corrección o como mínimo alcanzar su mayor mitigación.

Peritaje Informático

Según García (2015) refiere que peritaje informático "se caracterizará por proporcionar al juez esos argumentos o razones acerca de los aspectos que resulten controvertidos en una determinada situación de un sistema informático y que tengan relevancia jurídica" (p. 7). Es decir, se trata de experticia informática que tiene la facultad de alegar informes técnicos en relación con delitos relacionados con computadoras o sistema de redes ante una contienda judicial.

Son también los estudios e investigaciones usados en asuntos privados para la búsqueda de pruebas y argumentos que sirvan a una de las partes en discusión para decantar la discrepancia a su favor. Habitualmente se recurre a pruebas periciales informáticas en asuntos penales en los que la infraestructura informática media como herramienta del delito, por ejemplo la pornografía infantil en Internet. Son otros asuntos los delitos contra la propiedad privada e intelectual, espionaje industrial, protección de datos personales,

fraudes, sabotajes, etc.

Informática

El diccionario de la Real Academia de la Lengua Española (2001), presenta la siguiente definición: “Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores”.

La palabra Informática tiene su origen en Francia, procede de la palabra francesa informatique, formada por la conjunción de las palabras "information" y "automatique". La historia nos dice que esta palabra fue utilizada por primera vez por el ingeniero Philippe Dreyfus en el año 1962.

Una definición más acorde con lo que esta palabra representa en la actualidad sería decir que la informática es la ciencia que estudia el tratamiento automático y racional de la información en equipos de cómputo, equipos electrónicos y sistemas de información, la cual se basa en múltiples ciencias como la física, la matemática, la electrónica, entre otras.

Historia y Evolución: La informática nació para hacerle las cosas más fáciles al hombre, ya que gracias a ella podemos realizar procedimientos complejos con gran exactitud, minimizando la probabilidad del error y con una rapidez imposible de alcanzar de forma manual o mecánica. Desde sus inicios ha ido evolucionando en forma progresiva y sin latencia. Podemos señalar como un momento fundamental en el desarrollo de la informática el momento en que IBM mostró en sociedad el primer computador personal, con un procesador Intel 8088 y software desarrollado por Bill Gates y Paul Allen, específicamente sistema operativo D.O.S y lenguaje de desarrollo BASIC.

Luego llego ARPANET, la cual derivó en Internet y en 1990 aparecería la World Wide Web. En 1996 nace la segunda versión de Internet, más rápida, con más capacidad de carga y transporte de archivos, luego llegaría la conexión por modem, por microondas y actualmente por fibra óptica y vía satélite.

Actualmente la informática está involucrada en casi todos los procesos humanos de la vida cotidiana, llámese familiar, social, laboral, intelectual, etc., a tal punto que no se concibe la creación de un negocio o microempresa sin el acompañamiento de una plataforma informática.

En lo que tiene que ver con la vida académica podemos decir que la informática es prácticamente un aspecto inalienable a ella, desde la educación básica hasta la doctoral, donde el computador y el internet se han convertido en algo imprescindible para cualquier estudiante.

Delito informático

La enciclopedia en línea Wikipedia, presenta la siguiente definición: "Un delito informático o ciberdelicuencia es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.".

También lo podemos definir como el acto u hecho, ya sea voluntario o involuntario, que viola una norma o ley y utiliza medios tecnológicos para su consecución y que están encaminados a atacar la integridad, confidencialidad y disponibilidad de los activos de información en un sistema informático.

Historia y Evolución: Podemos decir que el primer tipo de delito informático que se dio fue el de robo de información en un computador, por rompimiento de contraseña. Hoy en día los delitos han evolucionado hasta tal punto que actualmente existe toda una ramificación de tipos y subtipos.

Entre algunos delitos informáticos encontramos:

Fraude informático: es inducir a otro a hacer o a restringirse en hacer alguna cosa de lo cual el criminal obtendrá un beneficio, casi siempre económico, utilizando medios informáticos.

Contenido obsceno u ofensivo: Cuando se envían mensajes a través de internet con

contenido que atenta contra la integridad de una o más personas u organizaciones (por medio de redes sociales, emails, etc.).

- Hostigamiento / acoso: Delito que se concreta cuando se contacta a una persona para que realice o entregue algo bajo una situación de amenaza.
- Terrorismo Virtual: Se da cuando se ataca una organización o estado para hacer daño a su sistema de información (ataques 0-days, denegación de servicio, acceso no autorizado, etc.).
- Pornografía Infantil: Delito que se comete cuando se envían archivos de imágenes o video por la web con contenido sexual explicito con menores de edad.
- Propiedad Intelectual: Delito que se comete en el momento que se accede a información privada o confidencial sin la autorización expresa de su autor, ya sea para su difusión gratuita o comercialización.

Evidencia digital

"Información de valor probatorio almacenada o transmitida en forma digital" (Cano, 2005, p.186). En otras palabras la podemos definir como las pruebas digitales encontradas en una escena de un delito que pueden servir en un proceso judicial como evidencia probatoria.

La evidencia digital se puede dividir en tres categorías:

Registros almacenados en un equipo informático: Correos electrónicos, imágenes, documentos ofimáticos, etc.

Registros generados por un equipo informático: Logs de Eventos, logs de errores, logs de transacciones, etc.

Registros parcialmente generados y almacenados en un equipo informático: por ejemplo aquellos archivos generados temporalmente por el navegador de internet mientras consultamos el ciberespacio o aquellos archivos generados cuando se ejecuta un procedimiento por lotes o un procedimiento almacenado en una base de datos.

Tabla 2

Propuesta de solución, según proceso y metodología

	Metodología		
		DOJNIST	PROPUESTA
Evaluación de Material		*	*
Recolectar y conservar / extracción	*	*	*
Identificación / Revisión	*	*	*
Examen y/o análisis	*	*	*
Demostración			*
Diagnóstico y Evaluación			*
Reporte / Informe	*	*	*

Fuente: Elaboración propia.

La metodología propuesta debe tener un Enfoque Sistémico realizando primero el reconocimiento del requerimiento y material para la intervención pericial; es decir Fase I: Requerimiento; lo anterior, servirá como punto de partida para iniciar el proceso del peritaje y poder hacer una Fase II: Recolección y Conservación, identificar los recursos para realizar la investigación. A partir de la identificación de los recursos disponibles, preservarla; para posteriormente proceder a realizar la Fase III: Identificación de la evidencia, de debe extraer la evidencia sin dañarla; así mismo, el perito en informática forense deberá asegurar que la evidencia sea igual a la original sin alteraciones, De esta manera se podrá realizar la Fase IV: Examen y Análisis de Datos, es identificar la interacción de la información extraída del material motivo de estudio o equipo cuestionado. Para poder realizar la siguiente fase. Fase V: Demostración. Es la fase donde se entregará lo obtenido de los análisis realizados. La FASE VI. Diagnóstico y Evaluación Crítica, en esta fase se evalúa lo obtenido, identifica y analiza la información obtenida con todas las pruebas realizadas. La FASE VII. Se muestra los reportes y resultados demostrados luego de todas las fases anteriormente trabajadas. Todas las fases consideradas son minuciosamente trabajadas junto a una cadena de custodia, que garantiza la Confidencialidad, Integridad y Disponibilidad de los datos e información, a continuación,

se presenta en un esquema general la Metodología Planteada para el Proceso de Peritaje Informático:

Figura 1. Análisis de la metodología como Sistemas

(*Fuente*: Elaboración propia)

Figura 2. Secuencia de Metodología Propuesta

(*Fuente*: Elaboración propia)

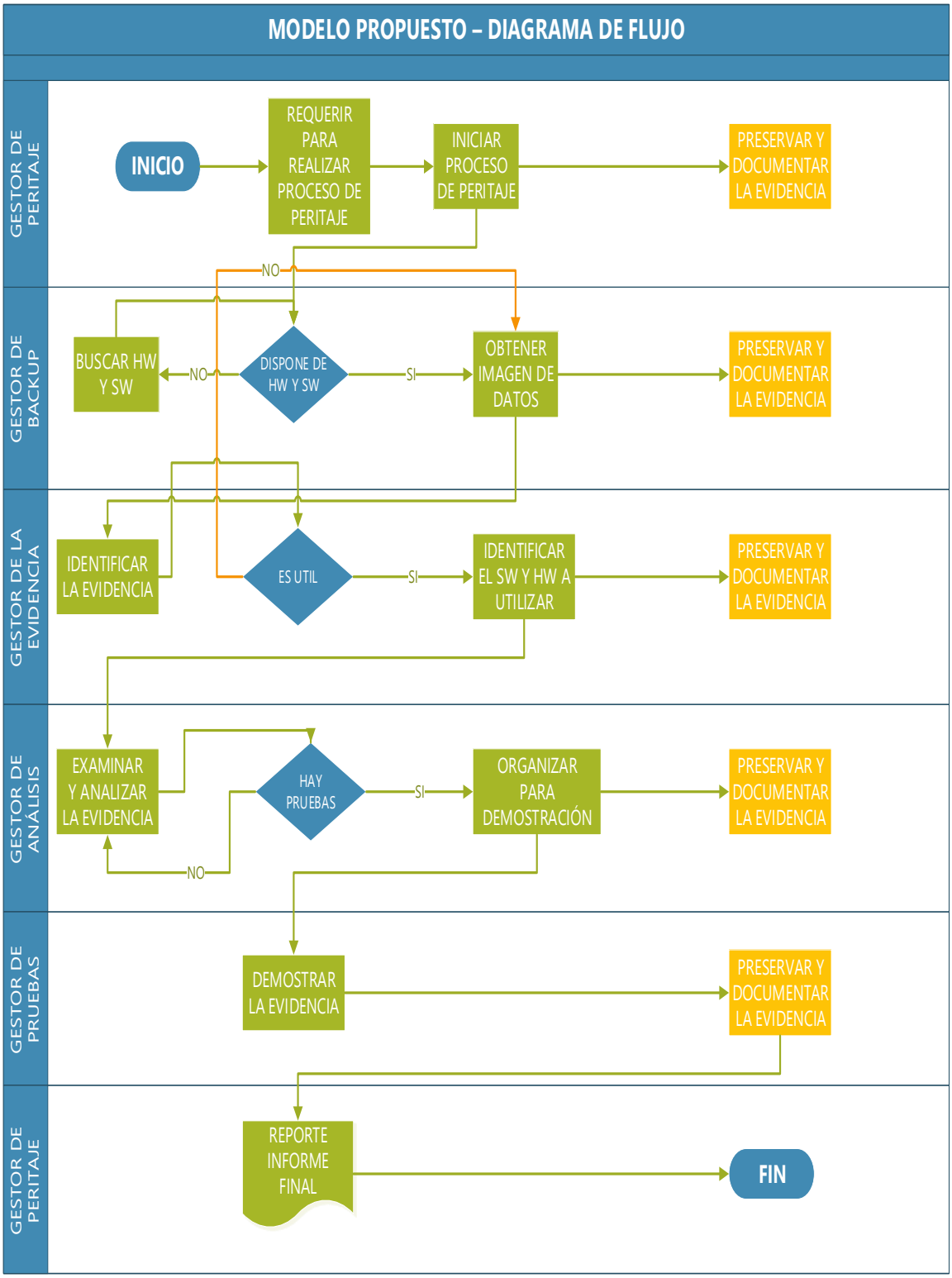


Figura 3. Diagrama de flujo de Metodología Propuesta

Tabla 3
Actividades de cada fase de la Metodología Propuesta.

REQUERIMIENTO	RECOLECCIÓN Y CONSERVACIÓN	IDENTIFICACIÓN DE LA EVIDENCIA	EXAMEN Y ANÁLISIS	DEMOSTRACIÓN	DIAGNÓSTICO Y EVALUACIÓN	REPORTE / INFORME
Actividad 1.1. Definir adecuadamente el requerimiento para iniciar el proceso.	**Actividad 2.1.** Recolectar las posibles fuentes de información y objetos de estudio .	**Actividad 3.1.** Identificar detalladamente el material objeto de estudio.	**Actividad 4.1.** Obtener los datos para su análisis.	**Actividad 5.1.** Explicar el material estudiado.	**Actividad 6.1.** Evaluar la información obtenida.	**Actividad 7.1.** Considerar todas las actividades llevadas a cabo.
Actividad 1.2. Evaluar si disponemos del material adecuado.	**Actividad 2.2.** Conservar los materiales de estudio.	**Actividad 3.2.** Identificar que Hardware y Software a utilizar.	**Actividad 4.2.** Examinar que datos y material de estudio.	**Actividad 5.2.** Indicar el Software y Hardware utilizado y su utilidad.	**Actividad 6.2.** Diagnosticar el delito informático.	**Actividad 7.2.** Considerar todas las sub actividades llevadas a cabo.
	Actividad 2.3. Realizar el backup del material objeto de estudio.	**Actividad 3.3.** Identificar la forma de extracción de información.	**Actividad 4.3.** Analizar el material de estudio.	**Actividad 5.3.** Explicar los datos y la información obtenida.	**Actividad 6.3.** Mostrar la evidencia digital.	**Actividad 7.3.** Elaboración del reporte e informe final del peritaje informático.
		Actividad 3.4. Identificar las consideraciones necesarias.	**Actividad 4.4.** Utilizar Software y Hardware para la extracción de datos.	**Actividad 5.4.** Demostrar la información útil para el caso.	**Actividad 6.4.** Evaluar cómo se realizó el delito.	
			Actividad 4.5. Extraer información del material de estudio.		**Actividad 6.5.** Evidenciar al responsable del delito informático.	
			Actividad 4.6. Analizar la información obtenida.			
			Actividad 4.7. Seleccionar la información útil al caso.			
Actividad 1.3. Preservar y documentar la evidencia	**Actividad 2.4.** Preservar y documentar la evidencia	**Actividad 3.5.** Preservar y documentar la evidencia	**Actividad 4.8.** Preservar y documentar la evidencia	**Actividad 5.5.** Preservar y documentar la evidencia	**Actividad 6.6.** Preservar y documentar la evidencia	**Actividad 7.4.** Preservar y documentar la evidencia

FLUJO FASE I. Requerimiento

En esta Fase, se le presenta al forense informático de una manera clara y precisa el requerimiento para poder realizar la investigación, es decir el fin que tendrá su intervención como especialista.

Para cumplir con el requerimiento se sugieren llevar a cabo las siguientes actividades:

Actividad 1.1. Definir adecuadamente el requerimiento para iniciar el proceso.

Actividad 1.2. Evaluar si disponemos del material adecuado.

Actividad 1.3. Preservar y documentar la evidencia.

FASE II. Recolección y conservación

Para poder realizar cualquier estudio, el forense informático necesita realizar la recolección y conservación previamente del material objeto de estudio, es importante que la recolección y conservación cumplan con la Confidencialidad, Integridad y Disponibilidad de los datos, dónde estarán localizados y cómo están almacenados.

Al ser un universo tan heterogéneo el de los sistemas de información donde se pueden encontrar evidencias digitales, se hace necesaria una clasificación para poder organizar las mismas.

Para tal, fin se requiere llevar a cabo las siguientes actividades:

Actividad 2.1. Recolectar las posibles fuentes de información y objetos de estudio.

Actividad 2.2. Conservar los materiales de estudio.

Actividad 2.3. Realizar el backup del material objeto de estudio.

Actividad 2.4. Preservar y documentar la evidencia.

FASE III. Identificación DE LA EVIDENCIA

Ahora bien, para este propósito se han creado categorías a fin de hacer una necesaria distinción entre el elemento material de un sistema informático o hardware (evidencia electrónica) y la información contenida en este (evidencia digital).

Esta distinción es útil al momento de diseñar los procedimientos adecuados para tratar cada tipo de evidencia y crear un paralelo entre una escena física del crimen y una digital. En este contexto el hardware se refiere a todos los componentes físicos de un sistema

informático, mientras que la información, se refiere a todos los datos, programas almacenados y mensajes de datos trasmitidos usando el sistema informático.

Es importante considerar el Hardware y Software adecuado para la realización del peritaje, identificar el procedimiento y forma de extraer los datos y/o información del material en estudio, toda la fase tiene que estar resguardada con el CID (Confidencialidad, Integridad y Disponibilidad)

Actividad 3.1. Identificar detalladamente el material objeto de estudio.

Actividad 3.2. Identificar que Hardware y Software a utilizar.

Actividad 3.3. Identificar la forma de extracción de información.

Actividad 3.4. Identificar las consideraciones necesarias.

Actividad 3.5. Preservar y documentar la evidencia.

FASE IV. Examen y análisis

Esta es, la fase más importante y crítica de la aplicación de la metodología propuesta, puesto que una vez que se haya comprobado que existió el delito informático el interesado, la empresa o institución dañada normalmente deseará llevar a un proceso judicial al atacante bajo las evidencias encontradas en el peritaje informático. Para ello es necesario poseer evidencias digitales adquiridas y preservadas de forma adecuada para que no exista duda alguna de su verosimilitud y siempre de acuerdo a las leyes vigentes de nuestro país. En general la realización del examen digital, la evidencia deberá poseer las siguientes características para ser considerada una evidencia real, de acuerdo a los criterios que requiere la autoridad competente actualmente:

- Admisible.
- Integridad.
- Confidencialidad.

- Disponibilidad.
- Creíble.

Este proceso de examinación y análisis se debe realizar tan pronto como sea posible. Siempre que sea posible hay que evitar los cambios en las evidencias y si no se logra, registrarlo, documentarlo y justificarlo, siempre que sea posible con la autoridad competente y/o testigos que puedan corroborar las acciones.

El concepto de evidencia digital está formado por el contenido de los archivos (datos) y la información sobre los archivos (metadatos). La evidencia almacenada debe ser analizada para extraer la información relevante para la investigación y recrear la cadena de eventos sucedidos. El análisis requiere un conocimiento profundo de lo que se está buscando y como obtenerlo, logrando registrar todo lo necesario para el caso en investigación. Hay que asegurarse que la persona que analiza la evidencia está totalmente cualificada para ello y experiencia en el proceso. Analizar las evidencias digitales va a depender del tipo de datos a analizar que son importante para el estudio que se está realizando, del tipo de sistema en el cual se clasifique el dispositivo comprometido (ordenadores, dispositivos móviles, etc.). Además, en función del tipo de delito (fraude, pornografía infantil, drogas, etc.) se deberán analizar unos tipos de evidencias y en un determinado orden (el orden permitirá al investigador forense llegar lo antes posible y de la forma más precisa a las evidencias digitales para llegar a resolver el delito informático).

Para tal fin, se requiere llevar a cabo las siguientes actividades:

Actividad 4.1. Obtener los datos para su análisis.

Actividad 4.2. Examinar que datos y material de estudio.

Actividad 4.3. Analizar el material de estudio.

Actividad 4.4. Utilizar Software y Hardware para la extracción de datos.

Actividad 4.5. Extraer información del material de estudio.

Actividad 4.6. Analizar la información obtenida.

Actividad 4.7. Seleccionar la información útil al caso.

Actividad 4.8. Preservar y documentar la evidencia.

FASE V. Demostración

La importancia de la evidencia digital reside en la necesidad de demostrarle al juez la prueba fehaciente que convierte en responsable al sospechoso. Por eso, es fundamental la correcta selección de la prueba relevante por parte del experto para no ser sobre abundante o superflua, se tiene que demostrar de forma clara y precisa toda la información relevante obtenida. El correcto tratamiento de la evidencia digital es fundamental para que sea admisible: haber sido obtenida respetando las garantías y procedimientos legales, basada en una previa autorización judicial o del director de investigación, justificando su tratamiento en los procedimientos de obtención, preservación, análisis y presentación ante el tribunal, respetando la cadena de custodia, cuyos pasos deberá desprenderse de un manual de buenas prácticas.

Asimismo, deben poder justificarse todos los métodos y acciones realizadas en el tratamiento de la evidencia digital, a través de la demostración de la validación de los métodos utilizados y de los procesos realizados.

También se deberá documentar las acciones realizadas y justificar todas las decisiones en las etapas del proceso, y se deben obtener los mismos resultados en caso de aplicar el mismo procedimiento, pero con herramientas diferentes, en cualquier momento.

Para tal fin se requiere llevar a cabo las siguientes actividades:

Actividad 5.1. Explicar el material estudiado.

Actividad 5.2. Indicar el Software y Hardware utilizado y su utilidad.

Actividad 5.3. Explicar los datos y la información obtenida.

Actividad 5.4. Demostrar la información útil para el caso.

Actividad 5.5. Preservar y documentar la evidencia.

FASE VI. Diagnóstico y evaluación

En esta fase se realiza el diagnóstico y evaluación de la información extraída mediante procesos que anteriormente se describieron, en esta fase tenemos la primera idea el delito informático cometido por un intruso, todo este delito informático se muestra en la evidencia digital, quién sería el resultado del análisis previo.

Se puede identificar el proceso de cómo el intruso accedió a nuestros datos, se identifica de cómo vulneró la seguridad logrando ver toda la información que tenemos en nuestros equipos ya sea a nivel individual o empresarial, una vez analizado todo lo antes mencionado, tenemos la capacidad de identificar quién es el culpable de todo el daño generado a tu información, podemos en evidencia al culpable de la intrusión, cambio o eliminación de información de los equipos.

Cómo último proceso de documenta todo realizado y encontrado mediante un reporte. Para tal fin se requiere llevar a cabo las siguientes actividades:

Actividad 6.1. Evaluar la información obtenida.

Actividad 6.2. Diagnosticar el delito informático.

Actividad 6.3. Mostrar la evidencia digital.

Actividad 6.4. Evaluar cómo se realizó el delito.

Actividad 6.5. Evidenciar al responsable del delito informático.

Actividad 6.6. Preservar y documentar la evidencia.

FASE VII. Reporte / informe

Se presenta el resultado final de todo el estudio con la nueva metodología planteada, se

considera todas las actividades desde la Fase I hasta la fase VII, se describen detalladamente, así como las sub actividades considerando los procedimientos que se realizaron y lo que se obtuvo de dichas actividades. Dicho informe final es para que pueda ser considerado como evidencia encontrando al culpable, o se pueda llevar a cabo en un proceso Judicial en busca de algún delito.

Para tal fin se requiere llevar a cabo las siguientes actividades:

Actividad 7.1. Considerar todas las actividades llevadas a cabo.

Actividad 7.2. Considerar todas las sub actividades llevadas a cabo.

Actividad 7.3. Elaboración del reporte e informe final del peritaje informático.

Actividad 7.4. Preservar y documentar la evidencia

Aplicación de la nueva metodología en la empresa 2M&J INGENIEROS S.R.L

Debido a la eliminación de archivos de una de los equipos de cómputo, se hizo urgente la necesidad de recuperar dichos archivos, ya que, correspondían a un avance de un trabajo de estudios de pre inversión que se estaban desarrollando, para lo cual se requería contar con dichos archivos para culminar el trabajo.

FASE I. Requerimiento

La necesidad de contar con el archivo, hace que sea necesario la recuperación de los avances realizados para la entrega de un trabajo.

Para cumplir con el requerimiento se sugieren llevar a cabo las siguientes actividades:

Actividad 1.1. Se necesita con urgencia los archivos que contenía la carpeta donde se estaba desarrollando un proyecto de pre inversión a nivel de Expediente Técnico.

Actividad 1.2. Se identifica que si se dispone con el equipo informático (Laptop) donde se almacenaba cada avance del archivo, dicho equipo sería el material en estudio en este caso.

Actividad 1.3. Se guarda con cuidado el equipo y documenta el equipo con sus

características técnicas para su posterior evaluación.

FASE II. Recolección y conservación

Es importante la recolección y conservación del equipo informático en estudio, evitar en todo momento la manipulación del equipo ya que pueden alterar el contenido de los archivos almacenados y registros dentro del equipo que dificultarían y cambiarían al proceso de recuperación de información.

Es importante tener en cuenta la trilogía del CID (Confidencialidad, Integridad y Disponibilidad de los datos)

Para tal, fin se requiere llevar a cabo las siguientes actividades:

Actividad 2.1. El equipo informático debe estar en un lugar seguro donde se evite la manipulación.

Actividad 2.2. Conservar el Disco Duro, que es el dispositivo donde se encuentra la información que necesitamos analizar.

Actividad 2.3. Realizar el backup del material objeto de estudio con un programa, ya sea realizando el backup completamente igual al original, esto es, con la finalidad de no manipular nuestro material objeto en estudio y evitar cambios indeseados, para ello se puede utilizar el software ENCASE FORENSIC.

Actividad 2.4. Preservar el material objeto de estudio, preservar también el backup realizado del Disco Duro del equipo informático y documentar la evidencia, asignando los datos como el software utilizado, tamaño del backup, fecha, etc.

FASE III. Identificación de la evidencia

En esta fase tenemos que identificar qué tipo de evidencia contamos, como primera parte tenemos la evidencia electrónica que es el Disco Duro, pero al momento de realizar el backup de la información que tiene el Disco duro, se estaría contando con una Evidencia

digital.

Entonces desde ahora en adelante nuestro material en estudio es el backup del Disco duro (Evidencia Digital), de dicha evidencia se realizará el análisis para la extracción de los datos que posteriormente organizados nos dan la información que estamos buscando.

Actividad 3.1. Hemos identificado que el material en estudio desde este punto es una Evidencia Digital (Backup del Disco Duro).

Actividad 3.2. El hardware utilizado es Ugreen de conector Sata a Usb 3.0 para poder examinar el backup que hemos realizado a otro Disco duro y el software a utilizar serán Encase Forensic, Foca Forensic, Recuva y el Autopsy.

Actividad 3.3. La forma de extracción de datos se realizará con los softwares mencionados, analizando en base a los archivos que se contaba, para este caso en la carpeta se contaba con archivos de las siguientes extensiones:

- .docx
- .xlsx
- .dwg
- .mpp
- .s2k
- .wtg

Actividad 3.4. Es necesario que se disponga de todos los softwares necesarios para poder recuperar la información eliminada y disponer de nuestros archivos para poder trabajarlos o usarlos.

Actividad 3.5. Preservar las aplicaciones, los archivos extraidos y documentar la evidencia.

FASE IV. Examen y análisis

Esta es, la fase más importante y crítica de la aplicación de la metodología propuesta,

puesto que en esta etapa se centra todo el proceso de examinar el backup realizado para, analizar todas las fuentes que se cuenta con los diferentes softwares planteados, cada uno del software tiene una finalidad e identifican los archivos que deseamos. En general la realización del examen digital, la evidencia deberá poseer las siguientes características para ser considerada una evidencia real:

- Admisible.
- Integridad.
- Confidencialidad.
- Disponibilidad.
- Creíble.

Este proceso de examinación y análisis se debe realizar tan pronto como sea posible con la finalidad de evitar la pérdida de datos e información relevante para la empresa.

La evidencia almacenada debe ser analizada para extraer la información relevante para la investigación y recrear la cadena de eventos sucedidos. El análisis requiere un conocimiento profundo de lo que se está buscando y como obtenerlo, logrando registrar todo lo necesario para el caso en investigación. Hay que asegurarse que la persona que analiza la evidencia está totalmente cualificada para ello y experiencia en el proceso. Analizar las evidencias digitales va a depender del tipo de datos a analizar que son importante para el estudio que se está realizando para la empresa, en este caso el análisis se realiza al backup realizado al Disco duro del equipo de cómputo.

Para tal fin, se requiere llevar a cabo las siguientes actividades:

Actividad 4.1. La obtención de los datos se realizará del backup realizado al Disco duro del equipo de cómputo.

Actividad 4.2. Se examina que cantidad de datos se dispone de donde se va a extraer la información.

Actividad 4.3. Analizar qué es lo que queremos conseguir del backup objeto en estudio para este caso.

Actividad 4.4. Se utilizará diferentes softwares para poder extraer la información que se requiere, para ello se usarán Foca Forensic, Recuva y el Autopsy

Actividad 4.5. Se inicia el proceso de extracción de la información, este proceso puede tomar su tiempo dependiendo de la cantidad y cuán pesado es el backup, cuanta más data se tenga, demorará más el proceso de extracción de información.

Actividad 4.6. Analizar la información obtenida, consiste en identificar toda la información que se logró recuperar, los archivos con las diferentes extensiones según este caso planteado.

Actividad 4.7. Seleccionar la información útil, esto es para identificar si los archivos recuperados nos son útiles al caso, es decir si nos va a servir y contribuirá con el objetivo planteado, para el caso es que nuestros archivos sean los archivos del estudio de pre inversión que fueron eliminados.

Actividad 4.8. Preservar los archivos en un dispositivo externo y documentar la evidencia que se logró extraer e identificar como útil.

FASE V. Demostración

En este caso la demostración comprende en mostrar la información recuperada del caso en estudio, la información debe estar completa donde cada archivo recuperado debe poder mostrar el contenido, así mismo se muestra los procedimientos realizados para que el procedimiento realizado sea exitoso, así como el el hardware y software utilizado.

También se deberá documentar las acciones realizadas y justificar todas las decisiones en las etapas del proceso, y se deben obtener los mismos resultados en caso de aplicar el mismo procedimiento, pero con herramientas diferentes, en cualquier momento.

Para tal fin se requiere llevar a cabo las siguientes actividades:

Actividad 5.1. Explicar el material estudiado, el material de estudio se realizó solamente en el backup realizado, ya que es importante que la fuente principal no debe ser manipulada.

Actividad 5.2. Indicar el Software y Hardware utilizado, los softwares utilizados fueron los siguientes:

- Encase Forensic.
- Foca Forensic.
- Recuva.
- Autopsy.
- Chronological View

Actividad 5.3. Explicar los datos y la información obtenida, es importante mostrar toda la información obtenida en base al caso en estudio, para este ejemplo se muestra el contenido de la carpeta donde se encontraba el contenido del estudio de pre inversión de un proyecto de saneamiento.

Actividad 5.4. Demostrar la información útil para el caso, la información es importante que se seleccione, ya que la información recuperada puede ser amplia, pero se tiene que seleccionar la información importante para el caso, los demás no son tomado en cuenta para el caso en estudio.

Actividad 5.5. Preservar la información obtenida, con todo el cuidado necesario para evitar pérdidas y documentar la evidencia indicando todo lo recuperado y todo lo usado para el proceso.

FASE VI. Diagnóstico y evaluación

En esta fase logramos identificar quién fue el que eliminó los archivos, en esta oportunidad se descubrió que fue un error del equipo de trabajo, pero gracias a la utilización de los softwares se pudo recuperar la información eliminada y así también identificar al

usuario quién eliminó el contenido de la carpeta.

Los detalles de la eliminación, la hora, la fecha, que acción realizó, el usuario, el equipo, etc.

Cómo último proceso de documenta todo realizado y encontrado mediante un reporte. Para tal fin se requiere llevar a cabo las siguientes actividades:

Actividad 6.1. Evaluar la información obtenida, verificar si la información obtenida está completa, comprobar si los archivos se pueden visualizar, leer el contenido, que no se encuentren dañados, etc.

Actividad 6.2. Diagnosticar el delito informático para poder saber quién fue el que realizó y conocer la acción que realizó.

Actividad 6.3. Mostrar la evidencia digital, indicando en el software los detalles que muestra y resultados obtenidos con el análisis.

Actividad 6.4. Evaluar cómo se realizó el delito, identificar qué acción realizó la persona que eliminó el archivo.

Actividad 6.5. Evidenciar al responsable del delito informático, para conocer quién es el responsable de haber eliminado el archivo y mostrar con el software la identificación de la persona.

Actividad 6.6. Preservar la información recuperada y documentar la evidencia donde indica los reportes y responsable del caso.

FASE VII. Reporte / informe

Se presenta el resultado final de todo el estudio con la nueva metodología planteada, se considera todas las actividades desde la Fase I hasta la fase VII, se describen detalladamente todas las actividades realizadas, así como las sub actividades, considerando los procedimientos que se realizaron y lo que se obtuvo de dichas actividades.

Para tal fin se requiere llevar a cabo las siguientes actividades:

Actividad 7.1. Considerar todas las actividades llevadas a cabo, describiendo el proceso como tal a fin de documentar todo el peritaje informático.

Actividad 7.2. Considerar todas las sub actividades llevadas a cabo, describiendo el proceso a fin de documentar todo el proceso de peritaje informático.

Actividad 7.3. Elaboración del reporte e informe final del peritaje informático, el reporte indicará si se logró el objetivo, en este caso, recuperar el archivo eliminado por error y también identicar al responsable que eliminó la carpeta que contenía el proyecto de pre inversión.

Actividad 7.4. Preservar la información y documentar la evidencia encontrada, en este caso con éxito.

2.3. Definición de términos básicos

Informática. Conjunto de conocimientos técnicos que se ocupan del tratamiento automático de la información por medio de computadoras.

Peritaje. Informe técnico con valoración económica que realiza un perito

Peritaje informático. El Peritaje Informático se refiere a los estudios e investigaciones orientados a la obtención de una prueba o evidencia electrónica de aplicación en un asunto judicial o extrajudicial para que sirva para decidir sobre la culpabilidad o inocencia de una de las partes.

Capítulo III

3. DISEÑO METODOLÓGICO

3.1. Tipo de investigación

El enfoque usado en la presente investigación, es cuantitativo, ya que "utiliza la recolección de información para experimentar y comparar supuestos, con base en la medición numérica y el estudio estadístico, para establecer modelos de conducta y probar teorías y su respectiva validación." (Hernández et al, 2014, p.4.)

Asimismo, el nivel y las características de la investigación se orientan a un estudio de tipo aplicada, porque, "la investigación puede cumplir dos intenciones, fines o finalidades fundamentales: a) producir inteligencia, juicio, razón, discernimiento y teorías y b) resolver dificultades e incertidumbres, preguntas o disyuntivas prácticas (investigación aplicada).

Gracias a estos dos tipos de investigación y conocimiento la humanidad se ha desarrollado y avanzado". (Hernández, R. y Mendoza, C., 2018, p. 36). En ese sentido el estudio se enfoca en proponer una tecnología que demuestre la robustez en el manejo de los datos. Para ello se ha estructurado una situación de control en la que es preciso la manipulación de forma intencional.

3.2. Diseño de la investigación

Diseño: El diseño de la investigación es preexperimental. Es decir, se procede a la manipulación de una variable independiente (informática forense) sobre otra variable dependiente: peritaje informático. Al respecto, Hernández et al (2014) refieren que esta clase de diseño de un solo grupo el grado de control es mínimo. Generalmente es útil como un primer acercamiento al problema de investigación en la realidad

GU ——— O1 X O2

3.3. Población y muestra de la investigación

Población

Es un conjunto de casos que tienen características en común. Al respecto Hernández et al (2014, p. 174) sostiene que se trata de un conjunto de casos que concuerdan con determinadas especificaciones. En este caso, la unidad de muestreo son en este caso computadores al que se le cargó la nueva metodología, para medir su robustez

Tabla 4

Población

DESCRIPCIÓN	TOTAL
Computadoras	15
TOTAL	15

Fuente: Elaboración propia.

Muestra

Siguiendo con Hernández et al. (2014, p. 173), sostienen que la muestra es un subgrupo de la población del cual se recolectan los datos. Por tanto, se consideró una muestra por conveniencia, es decir, se trata der aquella que se ajuste al interés del investigador. En este caso la muestra es similar a la población

Tabla 5

Muestra

DESCRIPCIÓN	TOTAL
Computadores	15
TOTAL	15

Fuente: Elaboración propia

Muestreo

Para la presente investigación, el tipo de muestreo es intencional o por conveniencia. Según, Hernández et al (2014), se cataloga por una labor voluntaria de lograr y obtener muestras modelo mediante inclusión en la muestra de sectores supuestamente típicos o convenientes en accesibilidad, la técnica no es automática ni con base en reglas de probabilidad, depende del suceso de toma de determinaciones del observador o de un grupo de observadores y, desde luego, las muestras seleccionadas obedecen a otros criterios de la investigación.

Criterios de inclusión

Computadores con la nueva tecnología.

3.4.Técnicas para la recolección de datos

3.4.1. Descripción de los instrumentos

En este punto de la investigación respecto a descripción de los instrumentos el usado para obtener datos para el procesamiento de información se llevó a cabo mediante el reporte técnico

3.4.2. Validez y confiabilidad de instrumentos

Criterios de jueces para la validez

Para establecer la validez del contenido de la técnica desarrollada se llevó a cabo un proceso de juicio de especialistas, la misma que se garantiza por el criterio de un conjunto de personas conocedoras y estudiosos en el asunto de la presente investigación, los mismos que ofrecen sus valoraciones y puntos de vista respectivos.

Para esta investigación se tuvo en consideración el juicio de estudiosos compuestos por tres especialistas los mismos que llenaron la ficha de validación, la que se evidencia en su respectivo anexo, asimismo se presenta el juicio de aplicabilidad del instrumento en la siguiente Figura:

Validez: La validez de los instrumentos se realizó a través del juicio de estudiosos conformado por tres ingenieros de sistemas expertos que tienen grado de maestría y doctor.

Confiabilidad: La confiabilidad del instrumento se realizará mediante el estudio del coeficiente de KR 20 realizándose una prueba piloto.

Tabla 6

Opinión de aplicabilidad basada en el juicio de expertos

Juez evaluador	**Opinión de aplicabilidad del instrumento de medición**
Mg. Olga Tomasa Talledo	Aplicable
Dr. William Eduardo Mory Chiparra	Aplicable
Dr. Jubenal Fernández Medina	Aplicable

Fuente: Elaboración propia

Tabla 7

Confiabilidad de dimensiones y variable peritaje informático

Dimensiones y Variable	Nº de sujetos	KR 20	Nº de ítems
Estudio informático	10	0.610	4
Evidencia digital	10	0.700	4
Delito informático	10	0.550	4
Peritaje informático	10	0.830	12

Fuente: Elaboración propia

En la Figura 6 se visualiza la confiabilidad del instrumento determinada a los ingenieros en la prueba piloto. Identificándose para la variable peritaje informatico (KR 20 = 0.830), el cual es considerado altamente confiable. En tal sentido, el instrumento sujeto a la prueba piloto, en una oficina de las mismas características que se estudia en muestra objetivo, resultó altamente confiable (0.830), quedando probado de esta manera la consistencia interna de los ítems del instrumento desarrollado en la presente investigación.

3.4.3. Técnicas para el procesamiento y análisis de los datos

En el presente estudio, se consideró procedimientos estadísticos para el análisis de la información, razón por la cual se consideró las siguientes fases: 1) estadística descriptiva, orientada a establecer distribuciones de frecuencias o histogramas, gráficos de barras en el que se representen las fase de pretest y postest, a fin de poder efectuar los paralelos pertinentes para un correcto análisis y comprensión; 2) estadística inferencial, para la cual se empleó la prueba de normalidad con el propósito de instaurar la naturaleza de la información, certificando, si proceden de una distribución paramétrica o no paramétrica; en segundo, lugar, se aplicó la prueba W de Wilcoxon, que es un estadístico que permite disponer comparaciones de valores categóricos y definir contrastes de manera adecuada los datos procesados del levantamiento de información realizada a los profesores a través de los cuestionarios e instrumentos de información.

Argumenta, Valencia, et al., (2015, p. 252), que el procesamiento de la información se desarrolla primero: verificación de la calidad de los datos, enseguida, el orden de los elementos, finalmente, clasificación, tabulación y, por último, gráficos de datos.

Se aplicó el instrumento en base a los ítems del reporte estructurado para el experimento, cuyas respuestas son dicotómicas.

Tabla 8

Categorías por respuestas en cuestionario: peritaje informático

Respuesta	**Categoría**
Si	1
No	0

Fuente: Elaboración propia

Capítulo IV

4. PRESENTACION DE RESULTADOS

4.1. Presentación e interpretación de resultados en tablas y figuras

4.1.1. Resultados descriptivos por variables y dimensiones

En este apartado se presentan los resultados obtenidos del trabajo de campo, razón por el cual se organizaron en distribuciones de frecuencias absolutas y porcentuales univariadas, además de gráficas de barras, con sus respectivas interpretaciones. De la misma manera, se realizó la parte inferencial de los resultados, siendo importante para ello determinar la naturaleza de los datos, es decir, si proceden de una distribución paramétrica o no paramétrica, recurriendo para ello a la prueba de normalidad, para luego efectuarse el contraste de hipótesis.

4.1.2. Tablas cruzadas por variables y dimensiones

Peritaje informático

Tabla 9

Distribución de frecuencias absoluta y porcentual, según nivel de robustez del peritaje informático en la empresa 2M&J INGENIEROS, 2019

Nivel		Pretest		Postest	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	8	53.3	0	0,0
	Medio	7	36,7	2	13.3
	Alto	0	0	13	86.7
	Total	15	100,0	15	100.0

Fuente: elaboración propia

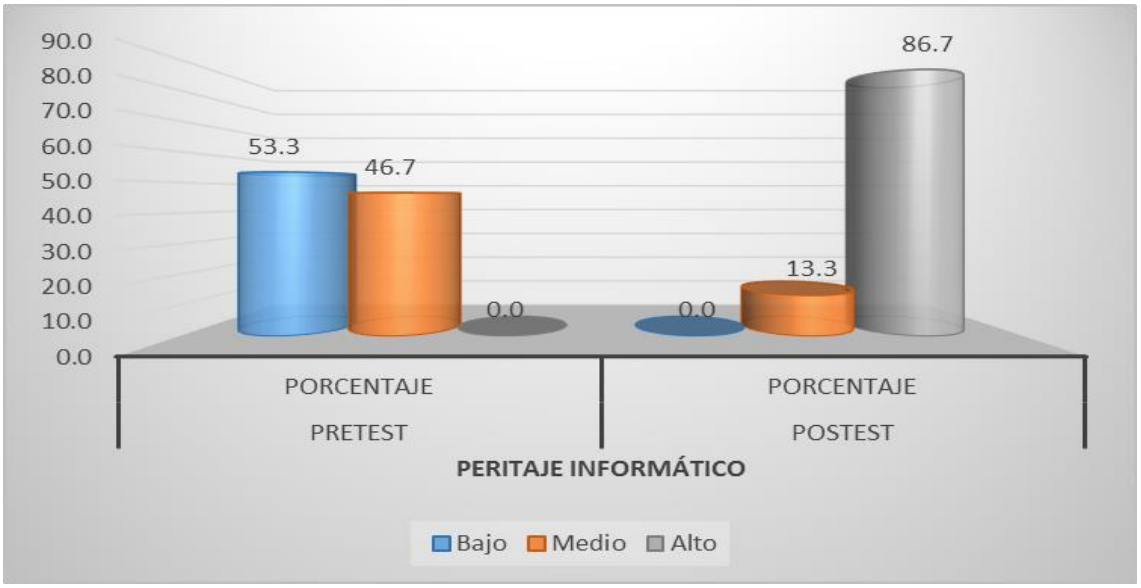


Figura 4. Peritaje informático, según niveles en la fase de pretest y postest en la empresa 2M&J INGENIEROS, 2019.

Interpretación:

En la fase de pretest se evaluó la robustez del peritaje informático y se encontró una baja robustez que representó 53.3%, y, otro medio que significó el 46.7%. En el nivel alto no se

encontró resultado alguno. Luego se implementó la nueva metodología como propuesta y se obtuvo en el nivel bajo en la fase de postest ningún resultado, luego en el nivel medio un 13.3% y en el nivel alto un 86.7%. Por tanto, la nueva metodología logra resultados favorables en cuanto a la robustez de la metodología.

Dimensión: Estudio informático

Tabla 10

Distribución de frecuencias absoluta y porcentual, según nivel de robustez del estudio informático en la empresa 2M&J INGENIEROS, 2019.

Nivel		Pretest		Postest	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	7	46.7	0	0.0
	Medio	8	53.3	0	0.0
	Alto	0	0.0	15	100.0
	Total	15	100.0	15	100.0

Fuente: elaboración propia.

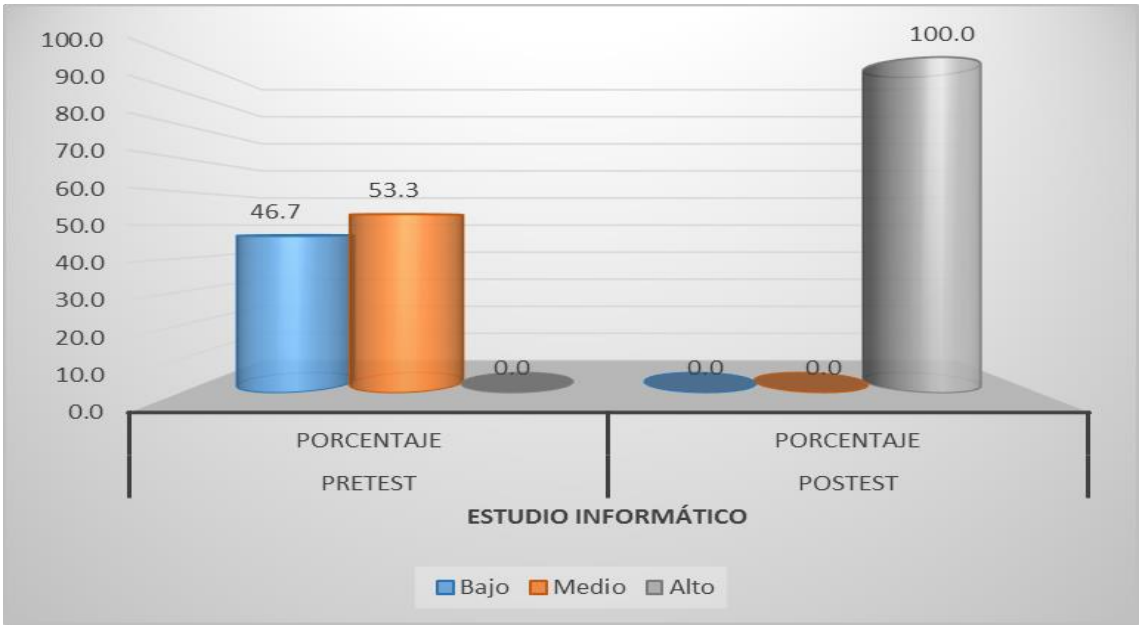


Figura 5. Estudio informático, según niveles en la fase de pretest y postest en la empresa 2M&J INGENIEROS, 2019.

Interpretación:

En la fase de pretest se evaluó la robustez del estudio informático y se encontró una baja robustez que representó 46.7%, y, otro media que significó el 53.3%. En el nivel alto no se encontró resultado alguno. Luego se implementó la nueva metodología como propuesta y se obtuvo en el nivel bajo en la fase de postest ningún resultado, luego en el nivel medio tampoco resultado alguno, sin embargo, en el nivel alto un 100.0%. Por tanto, la nueva metodología híbrida logró resultados favorables en cuanto a la robustez del estudio informático

Dimensión: Evidencia digital

Tabla 11

Distribución de frecuencias absoluta y porcentual, según nivel de robustez de la evidencia digital en la empresa 2M&J INGENIEROS, 2019.

Nivel		Pretest		Postest	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	8	53.3	0	0.0
	Medio	7	46.7	1	6.7
	Alto	0	0.0	14	93.3
	Total	15	100.0	15	100.0

Fuente: elaboración propia.

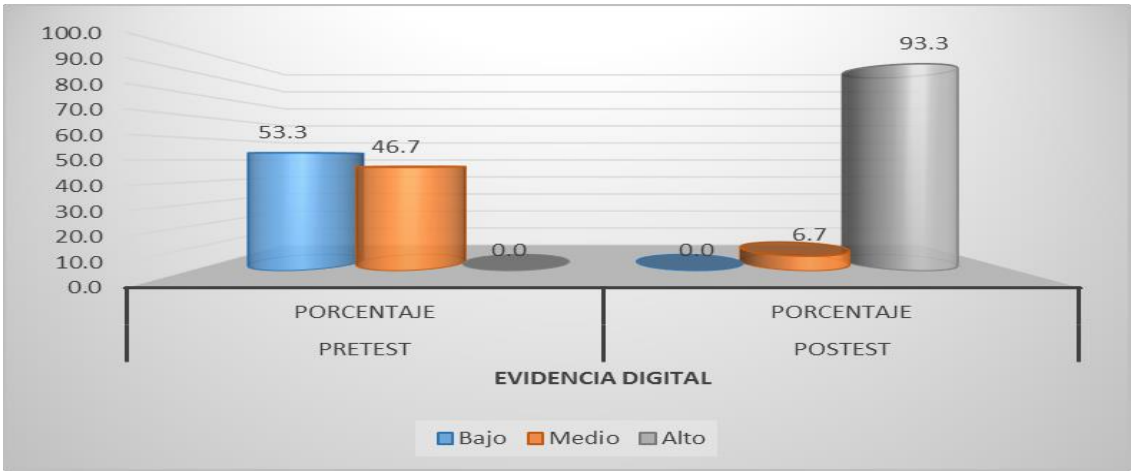


Figura 6. Evidencia digital, según niveles en la fase de pretest y postest en la empresa 2M&J INGENIEROS, 2019.

Interpretación:

En la fase de pretest se evaluó la robustez del estudio informático y se encontró una baja robustez que representó 53.3%, y, otro media que significó el 46.7%. En el nivel alto no se encontró resultado alguno. Luego se implementó la nueva metodología como propuesta y se obtuvo en el nivel bajo en la fase de postest ningún resultado, luego en el nivel medio se obtuvo un 6.7%, sin embargo, en el nivel alto se logró un 93.3%. Por tanto, la nueva metodología híbrida logró resultados favorables en cuanto a la robustez de la evidencia digital.

Dimensión: Delito informático

Tabla 12

Distribución de frecuencias absoluta y porcentual, según nivel de robustez del delito informático en la empresa 2M&J INGENIEROS, 2019.

Nivel		Pretest		Postest	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	9	60.0	0	0.0
	Medio	6	40.0	2	13.3
	Alto	0	0.0	13	86.7
	Total	15	100.0	15	100.0

Fuente: elaboración propia.

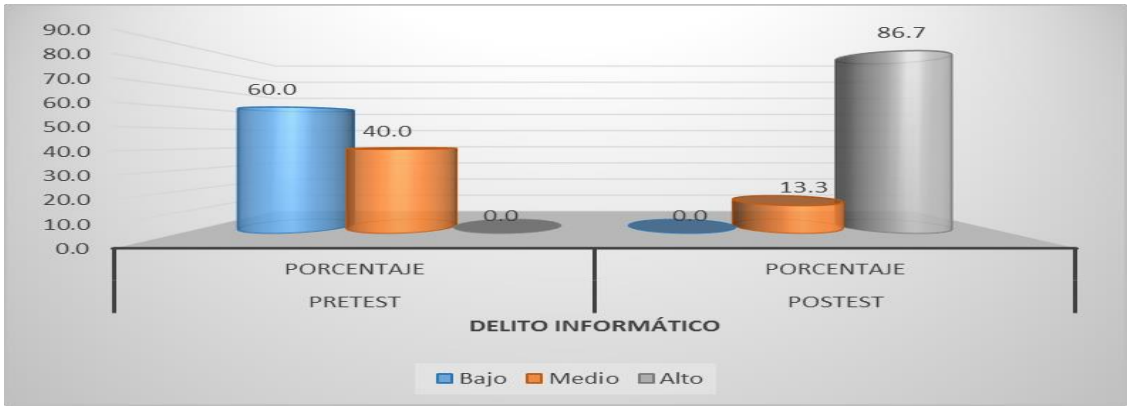


Figura 7. Evidencia digital, según niveles en la fase de pretest y postest en la empresa 2M&J INGENIEROS, 2019.

Interpretación:

En la fase de pretest se evaluó la robustez del delito informático y se encontró una baja robustez que representó 60.0%, y, otro media que significó el 40.0%. En el nivel alto no se encontró resultado alguno. Luego se implementó la nueva metodología como propuesta y se obtuvo en el nivel bajo en la fase de postest ningún resultado, luego en el nivel medio se obtuvo un 13.3%, sin embargo, en el nivel alto se logró un 86.7%. Por tanto, la nueva metodología híbrida logró resultados favorables en cuanto a la robustez de la lectura del delito informático

4.1.3. Prueba de normalidad

Tabla 13

Prueba de normalidad en la fase de pretest y postest

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Peritaje informático Pretest	,185	15	,177	,907	15	,123
Peritaje informático Postest	,226	15	,039	,859	15	,023

a. Corrección de significación de Lilliefors

Como la muestra es de 15 ordenadores, se considera en este caso la prueba de Shapiro Wilk, porque corresponde a una muestra menor a 30. En la fase de pretest, se pudo constatar, de acuerdo con la prueba de normalidad de S-W un valor p 0 123> 0.05, siendo normal su distribución, pero en la fase de postest el valor de p = 0.023 > 0.05, por lo que se rechaza la hipótesis de normalidad, por tanto corresponde adoptar un estadístico no paramétrico. En este caso, la prueba W de Wilcoxon.

4.1.4. Contrastación de las hipótesis de investigación

Hipótesis general

HG: La informática forense aplicando una nueva metodología mejora significativamente el Peritaje Informático en la Empresa 2M&J INGENIEROS, 2019

Ho: La informática forense aplicando una nueva metodología no mejora el Peritaje Informático en la Empresa 2M&J INGENIEROS, 2019

Tabla14

Tabla de contraste de hipótesis mediante W de Wilcoxon en la variable peritaje informático.

		N	Rango promedio	Suma de rangos
peritaje_postest - peritaje_pretest	Rangos negativos	0[a]	,00	,00
	Rangos positivos	15[b]	8,00	120,00
	Empates	0[c]		
	Total	15		

a. peritaje_postest < peritaje_pretest

b. peritaje_postest > peritaje_pretest

c. peritaje_postest = peritaje_pretest

Estadísticos de prueba[a]

	peritaje_postest - peritaje_pretest
Z	-3,425[b]
Sig. asintótica(bilateral)	,001

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

En la tabla 14 se aprecia que el valor Z = -3.425 < -1.96 (95%), por lo que se evidencia diferencias significativas en el contraste de hipótesis en la fase de pretest y postest, al obtenerse un valor p 0 .001 < 0.05.

Por tanto, la informática forense aplicando una nueva metodología mejora significativamente el Peritaje Informático en la Empresa 2M&J INGENIEROS, 2019

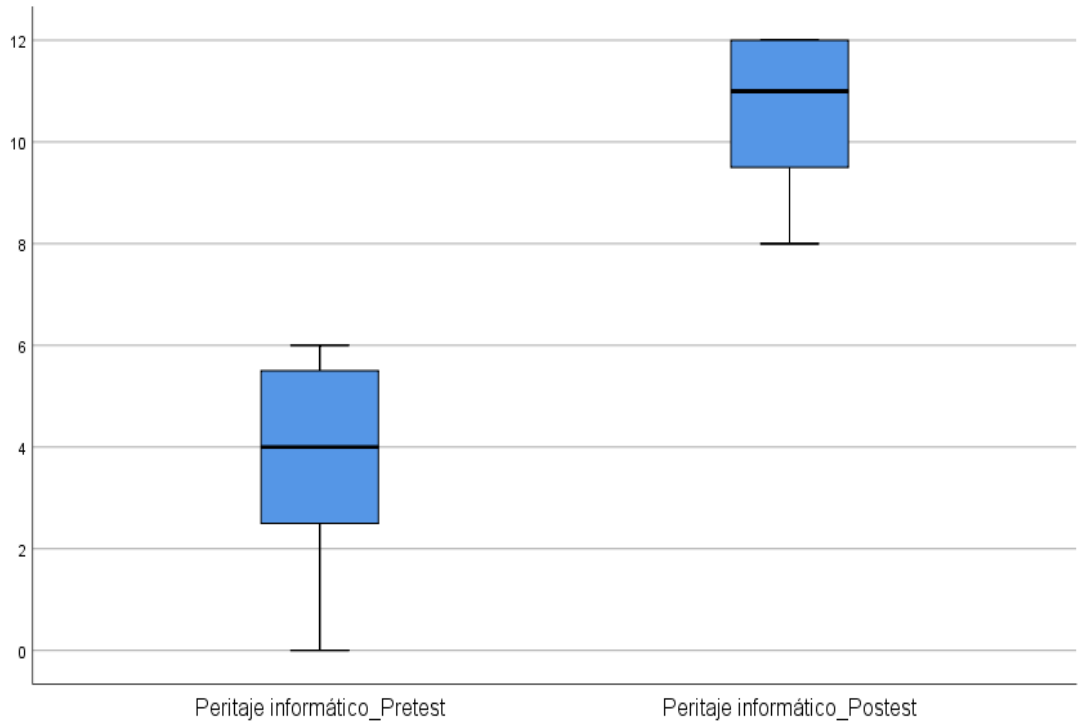


Figura 8. Diagrama de cajas en la fase de pretest y postest de peritaje informático.

En la figura se aprecia que en la fase de pretest y postest se evidenció una diferencia significativa en las medianas lo que significa que la nueva metodología ejerce un cambio notorio entre una fase y otra al experimentar con los ordenadores.

Hipótesis específica 1

H_0: El proceso de peritaje aplicando una nueva metodología no mejora significativamente el estudio Informático en la Empresa 2M&J INGENIEROS, 2019.

H1: El proceso de peritaje aplicando una nueva metodología mejora significativamente el estudio Informático en la Empresa 2M&J INGENIEROS, 2019.

Tabla 15

Tabla de contraste de hipótesis mediante W de Wilcoxon en la variable estudio informático

		N	Rango promedio	Suma de rangos
Estudio_informático_postest - Estudio_informático_pretest	Rangos negativos	1[a]	2,00	2,00
	Rangos positivos	10[b]	6,40	64,00
	Empates	4[c]		
	Total	15		

a. Estudio_informático_postest < Estudio_informático_pretest

b. Estudio_informático_postest > Estudio_informático_pretest

c. Estudio_informático_postest = Estudio_informático_pretest

Estadísticos de prueba[a]

	Estudio_informático_postest - Estudio_informático_pretest
Z	-2,778[b]
Sig. asintótica(bilateral)	,005

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

En la tabla 15 se aprecia que el valor Z = -2.778 < -1.96 (95%), por lo que se evidencia diferencias significativas en el contraste de hipótesis en la fase de pretest y postest, al obtenerse un valor p = 0 .005 < 0.05.

Por tanto, El proceso de peritaje aplicando una nueva metodología mejora significativamente el estudio Informático en la Empresa 2M&J INGENIEROS, 2019.

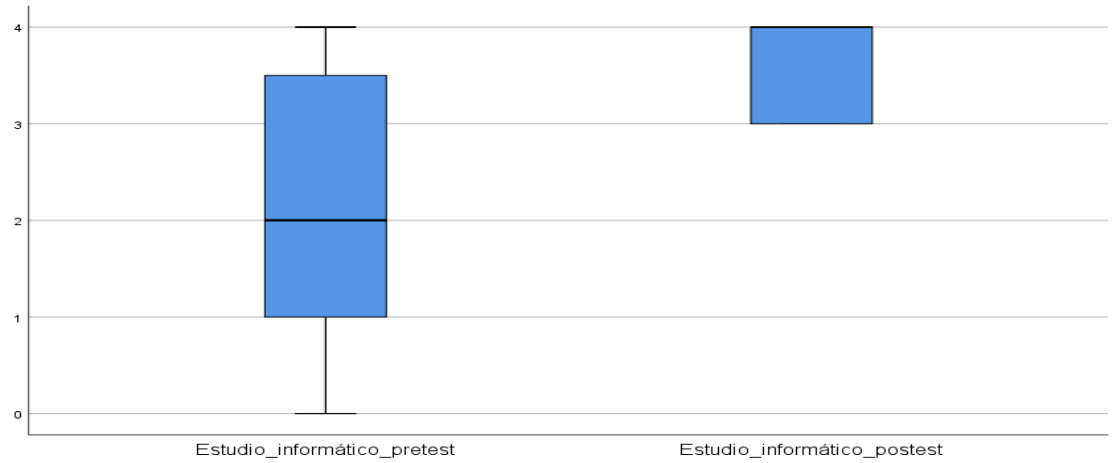


Figura 9. Diagrama de cajas en la fase de pretest y postest de estudio informático.

En la figura se aprecia que en la fase de pretest y postest se evidenció una diferencia significativa en las medianas lo que significa que la nueva metodología ejerce un cambio notorio entre una fase y otra al experimentar con los ordenadores.

Hipótesis específica 2

H0: El proceso de peritaje aplicando una nueva metodología no mejora significativamente la evidencia digital en la Empresa 2M&J INGENIEROS, 2019.

H2: El proceso de peritaje aplicando una nueva metodología mejora significativamente la evidencia digital en la Empresa 2M&J INGENIEROS, 2019.

Tabla16

Tabla de contraste de hipótesis mediante W de Wilcoxon en la variable evidencia digital

		N	Rango promedio	Suma de rangos
Evidencia_digital_Postest - Evidencia_digital_Pretest	Rangos negativos	0[a]	,00	,00
	Rangos positivos	15[b]	8,00	120,00
	Empates	0[c]		
	Total	15		

a. Evidencia_digital_Postest < Evidencia_digital_Pretest

b. Evidencia_digital_Postest > Evidencia_digital_Pretest

c. Evidencia_digital_Postest = Evidencia_digital_Pretest

Estadísticos de prueba[a]

	Evidencia_digital_Postest - Evidencia_digital_Pretest

Z	-3,457[b]
Sig. asintótica(bilateral)	,001

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

En la tabla 16 se aprecia que el valor Z = -3.457 < -1.96 (95%), por lo que se evidencia diferencias significativas en el contraste de hipótesis en la fase de pretest y postest, al obtenerse un valor p = 0 .005 < 0.05.

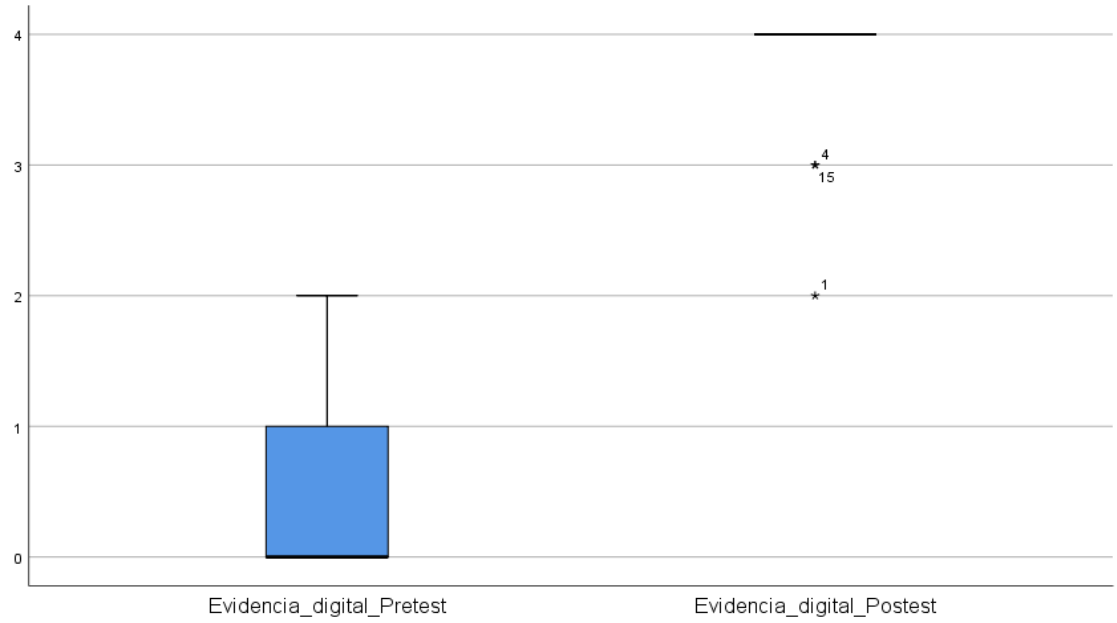


Figura 10. Diagrama de cajas en la fase de pretest y postest de evidencia digital.

En la figura se aprecia que en la fase de pretest y postest se evidenció una diferencia significativa en las medianas lo que significa que la nueva metodología ejerce un cambio notorio entre una fase y otra al experimentar con los ordenadores.

Por tanto, El proceso de peritaje aplicando una nueva metodología mejora significativamente la evidencia digital en la Empresa 2M&J INGENIEROS, 2019.

Hipótesis específica 3

H0: El proceso de peritaje aplicando una nueva metodología no recupera las evidencias del delito

informático en la Empresa 2M&J INGENIEROS, 2019.

H3: El proceso de peritaje aplicando una nueva metodología recupera las evidencias del delito informático en la Empresa 2M&J INGENIEROS, 2019.

Tabla 17

Tabla de contraste de hipótesis mediante W de Wilcoxon en la variable delito informático

		N	Rango promedio	Suma de rangos
Delito_Infomático_Postest - Delito_Informático_Prestest	Rangos negativos	1[a]	2,50	2,50
	Rangos positivos	13[b]	7,88	102,50
	Empates	1[c]		
	Total	15		

a. Delito_Infomático_Postest < Delito_Informático_Prestest

b. Delito_Infomático_Postest > Delito_Informático_Prestest

c. Delito_Infomático_Postest = Delito_Informático_Prestest

Estadísticos de prueba[a]

	Delito_Infomático_Postest - Delito_Informático_Prestest
Z	-3,182[b]
Sig. asintótica(bilateral)	,001

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

En la tabla 17 se aprecia que el valor Z = -3.182 < -1.96 (95%), por lo que se evidencia diferencias significativas en el contraste de hipótesis en la fase de pretest y postest, al obtenerse un valor p = 0 .001 < 0.05.

Por tanto, El proceso de peritaje aplicando una nueva metodología recupera las evidencias del delito informático en la Empresa 2M&J INGENIEROS, 2019.

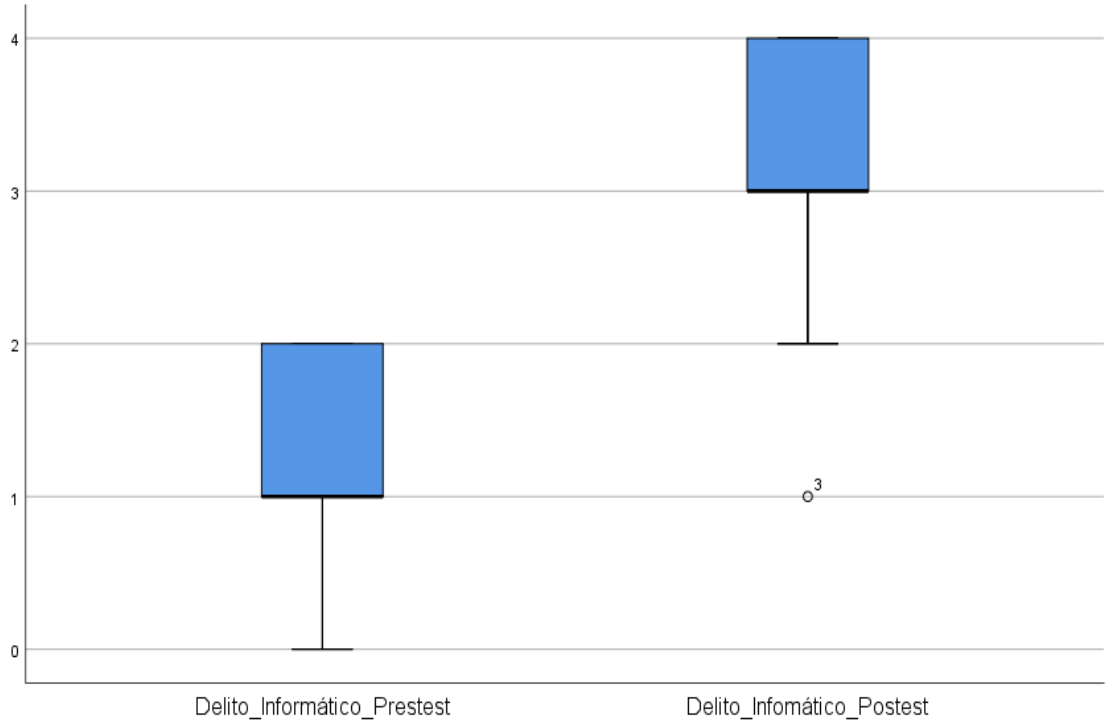


Figura 11. Diagrama de cajas en la fase de pretest y postest de delito informático.

En la figura se aprecia que en la fase de pretest y postest se evidenció una diferencia significativa en las medianas lo que significa que la nueva metodología ejerce un cambio notorio entre una fase y otra al experimentar con los ordenadores.

Capítulo V

4. DISCUSIÓN

5.1. Discusión de resultados obtenidos

El objetivo de la investigación fue demostrar el efecto de la informática forense aplicando una nueva metodología que mejora el proceso de Peritaje Informático en la Empresa 2M&J INGENIEROS, 2019. Los resultados hallados coinciden con Hernández (2018) quien encontró que la aplicación de Auditoría Forense y la Instrumentalizar la prueba en el lavado de activos, se convierte en un medio para instrumentalizar el lavado de activo en el sistema financiero.

Con respecto a la hipótesis general

De acuerdo con los resultados descriptivos, se encontró que un 53.3% se encontraron en el nivel bajo, mientras un 46.7% se hallaron en el nivel medio, y, ninguno en el nivel alto; con este resultado obtenido en la fase de pretest, fue necesario aplicar actividades de mejora

en base a una nueva metodología híbrida en el peritaje informático. Luego de aplicarse a los procesos, se volvió a evaluar y se encontró en la fase de postest que el 86.7% si situó en el nivel alto, esto quiere decir que hubo un diferencial favorable de 86.7% de mejora en relación a la fase de pretest en este mismo nivel; del mismo modo, se observó una variación positiva en el nivel medio de 13.3%, lo que significó también una mejora en relación a la fase de pretest en este mismo nivel de 33.4%. Estas variaciones solo pueden deberse a la aplicación de las actividades de la metodología híbrida. Dicho resultado se confirma al efectuarse el contraste de hipótesis mediante la prueba de Wilcoxon para datos emparejados, obteniendo para la hipótesis general un valor Z = -3.425 < -1.96, p = .001 < .05. Por lo tanto, la informática forense aplicando una nueva metodología mejora significativamente el Peritaje Informático en la Empresa 2M&J INGENIEROS, 2019. Los resultados hallados coinciden con Hernández (2018) quien encontró que la aplicación de Auditoría Forense y la Instrumentalizar la prueba en el lavado de activos, se convierte en un medio para instrumentalizar el lavado de activo en el sistema financiero. Lo hallado en este estudio se engarza con lo dispuesto por Hernández (2018) quien se planteó como objetivo determinar si la auditoría forense puede convertirse en un medio para instrumentalizar la prueba en el lavado de activos en el sistema financiero, durante el periodo del 2018, concluyendo que la aplicación de Auditoría Forense es un medio importante para instrumentalizar la prueba en el lavado de activos; adicionalmente, cabe destacar el aporte de Hipólito (2018), enfocándose de manera resuelta en establecer la forma como los procedimientos de auditoría forense podrían estimular la lucha contra la corrupción de los Gobiernos Regionales. En tanto, Arnedo (2014), demostró mediante pruebas simuladas la efectividad y aplicabilidad de herramientas de software según la función que desarrolla cada uno de ellas. Enfocándose en tres delitos informáticos, como primer delito fue el Incidente DELINF0951 – El

servidor de la Clínica, accedieron a información de los pacientes, el segundo fue el Incidente DELINF0957 – Empresa Internacional de Refrescos, correos de chantaje de hacer circular información secreta y confidencial relacionada con la lógica del negocio de la empresa; y como tercer delito fue el Incidente DELINF0998 – Empresa internacional dedicada a la venta de ropa femenina, intentaron hacer un fraude por una suma considerable a través de internet. Todos los delitos fueron analizados mediante software especializado, en la cual lo que se buscó fue identificar herramientas informáticas de gran valor para la investigación forense.

Con respecto a la hipótesis específica 1:

De acuerdo con los resultados descriptivos, se encontró que un 53.3% se encontraron en el nivel medio, mientras un 46.7% se hallaron en el nivel bajo, y, ninguno en el nivel alto; con este resultado obtenido en la fase de pretest, fue necesario aplicar actividades de mejora en base a una nueva metodología híbrida en el peritaje informático, de manera específica en la dimensión estudio informático. Luego de aplicarse a los procesos, se volvió a evaluar y se encontró en la fase de postest que el 100.0% si situó en el nivel alto, esto quiere decir que hubo un diferencial favorable de 100.0% de mejora en relación a la fase de pretest en este mismo nivel. Estas variaciones solo pueden deberse a la aplicación de las actividades de la metodología híbrida. Dicho resultado se confirma al efectuarse el contraste de hipótesis mediante la prueba de Wilcoxon para datos emparejados, obteniendo para la hipótesis específica 1 un valor $Z = -2.778 < -1.96$, $p = .005 < .05$. Por lo tanto, la informática forense aplicando una nueva metodología mejora significativamente el Peritaje Informático en la Empresa 2M&J INGENIEROS, 2019. Estos resultados hallados se inscriben en la misma línea que Palacios (2013) cuyo estudio tuvo como objetivo proponer una metodología con el enfoque sistémico para el análisis forense informático

en sistemas de redes y equipos de cómputo personal. Se realizó el estudio de dos discos duros, el primer disco duro fue la "Imagen del disco duro objeto de estudio.ad" y el segundo disco duro fue "Imagen del disco duro objeto de estudio.ad2" los cuales se procedió a montarlos (adicionarlos como evidencia en el software) en el software forense, con el fin de llevar a cabo una búsqueda exhaustiva de toda la información.

Con respecto a la hipótesis específica 2:

De acuerdo con los resultados descriptivos, se encontró que un 46.7% se encontraron en el nivel medio, mientras un 53.3% se hallaron en el nivel bajo, y, ninguno en el nivel alto; con este resultado obtenido en la fase de pretest, fue necesario aplicar actividades de mejora en base a una nueva metodología híbrida en el peritaje informático, de manera específica en la dimensión evidencia digital. Luego de aplicarse a los procesos, se volvió a evaluar y se encontró en la fase de postest que el 93.3% si situó en el nivel alto, esto quiere decir que hubo un diferencial favorable de 93.3% de mejora en relación a la fase de pretest en este mismo nivel. De la misma manera se encontró otro 6.7% ubicado en el nivel medio. Estas variaciones solo pueden deberse a la aplicación de las actividades de la metodología híbrida. Dicho resultado se confirma al efectuarse el contraste de hipótesis mediante la prueba de Wilcoxon para datos emparejados, obteniendo para la hipótesis específica 1 un valor $Z = -3.457 < -1.96$, $p = .001 < .05$. Por lo tanto, el proceso de peritaje aplicando una nueva metodología mejora significativamente la evidencia digital en la Empresa 2M&J INGENIEROS, 2019. En esa línea, Palacios (2013) realizó una investigación centrada en proponer una metodología con el enfoque sistémico para el análisis forense informático en sistemas de redes y equipos de cómputo personal. Se realizó el estudio de dos discos duros, el primer disco duro fue la "Imagen del disco duro objeto de estudio.ad1" y el segundo disco duro fue "Imagen del disco duro objeto de estudio.ad2"

los cuales se procedió a montarlos (adicionarlos como evidencia en el software) en el software forense, con el fin de llevar a cabo una búsqueda exhaustiva de toda la información. Obteniendo como resultado que demostrar a través del análisis que las metodologías y estándares en cuanto a evidencia digital se refiere le permitieron efectuar una evaluación y diagnóstico de la situación actual.

Con respecto a la hipótesis específica 3

De acuerdo con los resultados descriptivos, se encontró que un 40.0% se encontraron en el nivel medio, mientras un 60.0% se hallaron en el nivel bajo, y, ninguno en el nivel alto; con este resultado obtenido en la fase de pretest, fue necesario aplicar actividades de mejora en base a una nueva metodología híbrida en el peritaje informático, de manera específica en la dimensión delito digital. Luego de aplicarse a los procesos, se volvió a evaluar y se encontró en la fase de postest que el 86.7% si situó en el nivel alto, esto quiere decir que hubo un diferencial favorable de 86.7% de mejora en relación a la fase de pretest en este mismo nivel. De la misma manera se encontró otro 13.3% ubicado en el nivel medio. Estas variaciones solo pueden deberse a la aplicación de las actividades de la metodología híbrida. Dicho resultado se confirma al efectuarse el contraste de hipótesis mediante la prueba de Wilcoxon para datos emparejados, obteniendo para la hipótesis específica 3 un valor $Z = -3.182 < -1.96$, $p = .001 < .05$. Por lo tanto, el proceso de peritaje aplicando una nueva metodología recupera las evidencias del delito informático en la Empresa 2M&J INGENIEROS, 2019. En esa línea de estudio, el trabajo de Tocados (2015) se enlaza con los resultados hallados, porque el objetivo de la investigación fue proponer un manual de procedimientos para la elaboración de informes periciales, que sea lo suficientemente genérico para abordar la gran variedad de dispositivos y tecnologías existentes que pueden ser sometidos a análisis. Se realizó el análisis de una computadora portátil que usaba

una usuaria que fue despedida de la empresa por la supuesta utilización de un período de baja laboral (permiso) comprendido del 1 al 5 de Abril del 2015 para realizar un viaje de ocio. Se realizó el análisis minucioso de la portátil, obteniendo como resultado que tanto el hardware como el software sin elementos importantes para la realización del peritaje informático.

Por tanto, el objetivo planteado en la presente investigación a través del trabajo de campo, permitió validar las hipótesis de investigación, pero, sobre todo, hacer que las dimensiones del peritaje informático se muestren robustas ante la aplicación de la nueva metodología híbrida.

5.2. Conclusiones

Primera: Se demostró el efecto de la informática forense con la aplicación de una nueva metodología en la mejora del peritaje informático en la Empresa 2M&J INGENIEROS, 2019, al obtener un valor Z = -3.425 < -1.96 (95%), por lo que se evidencia diferencias significativas en el contraste de hipótesis en la fase de pretest y postest, al obtenerse un valor p = 0 .001 < 0.05.

Segunda: Se demostró el efecto de la informática forense con la aplicación de una nueva metodología en la mejora del estudio informático en la Empresa 2M&J INGENIEROS, 2019, al obtener un valor Z = -2.778 < -1.96 (95%), por lo que se evidencia diferencias significativas en el contraste de hipótesis en la fase de pretest y postest, al obtenerse un valor p = 0 .005 < 0.05.

Tercera: Se demostró el efecto de la informática forense con la aplicación de una nueva metodología en la mejora de la evidencia digital en la Empresa 2M&J INGENIEROS, 2019, al obtener un valor Z = -3.457 < -1.96 (95%), por lo que se evidencia diferencias significativas en el contraste de hipótesis en la fase de pretest y postest, al obtenerse un valor p = 0 .001 < 0.05.

Cuarta: Se demostró el efecto de la informática forense con la aplicación de una nueva metodología en la mejora de la recuperación de evidencias del delito informático en la Empresa 2M&J INGENIEROS, 2019, al obtener un valor Z = -3.182 < -1.96 (95%), por lo que se evidencia diferencias significativas en el contraste de hipótesis en la fase de pretest y postest, al obtenerse un valor p = 0 .001 < 0.05.

5.3. Recomendaciones

Primera: Recomendar al gerente general de la Empresa 2M&J INGENIEROS, 2019, realizar una prueba piloto durante un promedio de tres meses (90 días) con la finalidad de documentar las actividades de la nueva metodología híbrida para dar robustez a los resultados del peritaje informático.

Segunda: Recomendar al gerente general de la Empresa 2M&J INGENIEROS, 2019, desplegar en la prueba piloto durante un promedio de tres meses (90 días) con la finalidad de extraer información en relación con la nueva metodología híbrida y de esta forma validar el estudio informático.

Tercera: Recomendar al gerente general de la Empresa 2M&J INGENIEROS, 2019, desplegar en la prueba piloto durante un promedio de tres meses (90 días) con la finalidad de analizar información en relación con la nueva metodología híbrida y de esta forma validar las evidencias digitales.

Tercera: Recomendar al gerente general de la Empresa 2M&J INGENIEROS, 2019, desplegar en la prueba piloto durante un promedio de tres meses (90 días) con la finalidad de realizar la reconstrucción del proceso de peritaje informático en relación con la nueva metodología híbrida y de esta forma identificar el delito informático.

FUENTES DE INFORMACIÓN

Acurio, S., 2009. *Perfil sobre los delitos informáticos en el Ecuador. Pontificia Universidad Católica del Ecuador* (Ecuador). Disponible en http://www.criptored.upm.es/guiateoria/gt_m592d.htm.

Arnedo, P. (2014). Herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos (Tesis de Maestría). La Rioja, España: Universidad Internacional La Rioja. Recuperado de https://reunir.unir.net/bitstream/handle/123456789/2828/arnedo%20blanco.pdf?sequence=1&isAllowed=y

Cano, J. (2006). *Introducción a la informática forense.* Revista ACIS.

Eloff, J., Kohn, M. y Olivier, M. (2008). Information and computer security architectures (ICSA). Research Group. Department of Computer Science, University of Pretoria, South Africa. Disponible en http://icsa.cs.up.ac.za/issa/2008/Proceedings/Full/25.pdf.

Gallardo, R., Fuentes, A. y Fuentes R. (2016). Un enfoque básico sobre informática forense. *En Researchgate, pp. 1 - 4.* Recuperado de https://www.researchgate.net/publication/311581737_Un_enfoque_basico_sobre_Informatica_Forense/link/584eae9a08ae4bc899395c3a/download

García, J. (2015). *Informe sobre el Peritaje Informático* (Tesis de Maestria). Madrid, España: Universidad Carlos III de Madrid.

Hernández, R., Fernández, C. y Baptista, P. (2014). *Metodología de la investigación.* (6ª edición). México: McGraw Hill Education.

Hernández, R. y Mendoza, C. (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta.* México: McGraw Hill Interamericana Editores.

Hernández, V. (2018). *La auditoría forense como medio para instrumentalizar la prueba*

en el lavado de activos en el sistema financiero, período 2018 (Tesis de Maestría). Lima, Perú: Universidad Nacional Federico Villarreal. Recuperado de http://repositorio.unfv.edu.pe/handle/UNFV/2148

Hipólito, R. (2018). El empoderamiento de la auditoría forense en la lucha contra la corrupción en los gobiernos regionales del Perú, propuesta actual (Tesis de Maestría). Lima, Perú: Universidad Nacional Federico Villarreal. Recuperado de http://repositorio.unfv.edu.pe/handle/UNFV/2116

Naranjo, A. (2009). *Conceptos de la auditoria de sistemas*. Argentina: El Cid Editor.

Palacios, A. (2013). *Metodología para el análisis forense informático en sistemas de redes y equipos de cómputo personal* (Tesis de Maestría). México, D.F.: Instituto Politécnico Nacional.

Redacción Perú21 (18 de agosto de 2014). Kaspersky Lab: Cada segundo se crean tres virus informáticos en el mundo. Recuperado de: https://peru21.pe/mundo/kaspersky-lab-segundo-crean-tres-virus-informaticos-mundo-180763-noticia/

Real Academia Española (2001). *Informática.* En Diccionario de la lengua española (22.aed.). Recuperado de http://lema.rae.es/drae/?val=inform%C3%A1tica

Tocados, J. (2015). *Metodología para el desarrollo de procedimientos periciales en el ámbito de la información forense* (Tesis de Grado). Ciudad Real, España: Universidad Castilla La Mancha. Recuperado de https://ruidera.uclm.es/xmlui/bitstream/handle/10578/6667/TFG_Juan_Miguel_Tocados.pdf?sequence=1&isAllowed=y

ANEXOS

Anexo 1. Matriz de consistencia

Problemas	**Objetivos**	**Hipótesis**	**Variables y dimensiones**	**Diseño metodológico**
General ¿En qué medida la informática forense aplicando una nueva metodología mejora el Peritaje Informático en la Empresa 2M&J INGENIEROS, 2019? **Específicos** P1. ¿En qué medida el proceso de peritaje aplicando una nueva metodología mejora el estudio Informático en la Empresa 2M&J INGENIEROS, 2019? P2: ¿En qué medida el proceso de peritaje aplicando una nueva metodología mejora la evidencia digital en la Empresa 2M&J INGENIEROS, 2019? P3: ¿En qué medida el proceso de	**General** Demostrar que la informática forense aplicando una nueva metodología mejora significativamente el Peritaje Informático en la Empresa 2M&J INGENIEROS, 2019. **Específicos** O1. Demostrar que el proceso de peritaje aplicando una nueva metodología mejora significativamente el estudio Informático en la Empresa 2M&J INGENIEROS, 2019. O2: Demostrar que el proceso de peritaje aplicando una nueva metodología mejora significativamente la evidencia digital en la Empresa 2M&J INGENIEROS, 2019. O3: Demostrar que el proceso de peritaje aplicando una nueva metodología recupera las evidencias del delito informático	**General** HG: La informática forense aplicando una nueva metodología mejora significativamente el Peritaje Informático en la Empresa 2M&J INGENIEROS, 2019 **Específicos** H_1. El proceso de peritaje aplicando una nueva metodología mejora significativamente el estudio Informático en la Empresa 2M&J INGENIEROS, 2019. H_2: El proceso de peritaje aplicando una nueva metodología mejora significativamente la evidencia digital en la Empresa 2M&J INGENIEROS, 2019. H_3: El proceso de peritaje aplicando una nueva metodología recupera las evidencias del delito informático en la Empresa 2M&J	**V1. Informática forense** Uso de la metodología Uso del Hardware Uso del – software Uso de la auditoria **V2. Peritaje** El estudio informático La evidencia digital El delito informático	**Tipo:** Aplicada **Diseño:** Experimental **Enfoque**: Cuantitativo Población y muestra: 15

peritaje aplicando una nueva metodología recupera las evidencias del delito informático en la Empresa 2M&J INGENIEROS, 2019?	en la Empresa 2M&J INGENIEROS, 2019.	INGENIEROS, 2019.		

Anexo 2. Instrumentos para la recolección de datos

Indicadores	Items	Opción de puestas		Niveles y rangos
		No	**Sí**	
Estudio Informático	Identificación de Hardware			Bajo: [0 – 4]
	Identificación de software			
	Componentes de redes de			
	Instrumentos electrónicos			
Evidencia Digital	Evidencia electrónica			
	Evidencia digital			
Delito Informático	Parámetros de la escena del			
	Establezca las medidas de			
	Asegure físicamente la escena			
	Entregar la escena del delito y			

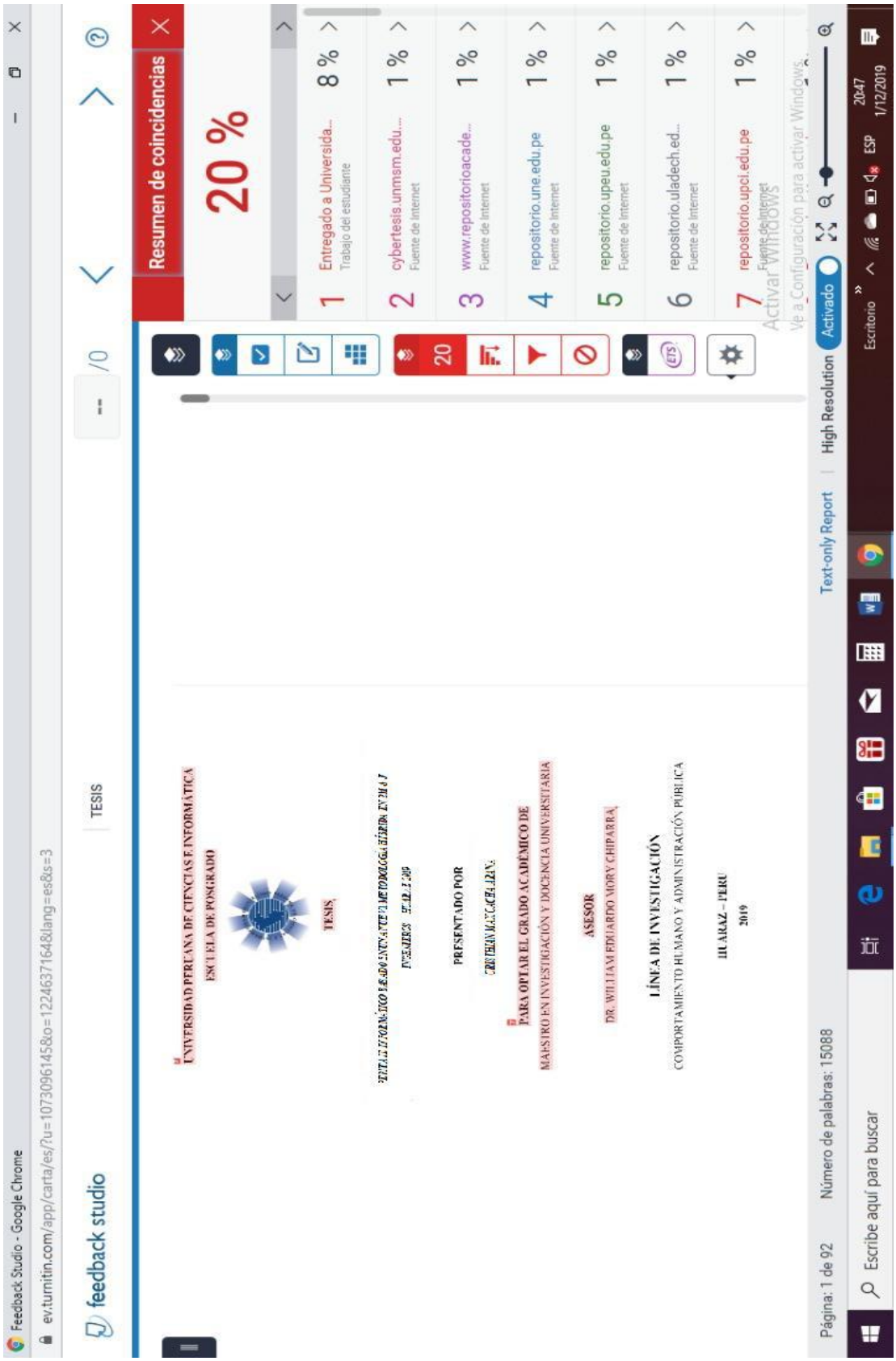
Fuente: Acurio (2909)

Anexo 3. Base de datos

PRETEST													
	ITEM1	ITEM2	ITEM3	ITEM4	ITEM5	ITEM6	ITEM7	ITEM8	1	ITEM10	ITEM11	ITEM12	PD
EE1	1	0	1	0	1	0	0	0	1	0	0	0	4
EE2	1	0	0	1	0	0	1	0	1	0	1	0	5
EE3	1	0	0	0	0	0	1	1	1	1	0	0	5
EE4	0	0	0	0	0	0	0	0	0	0	0	0	0
EE5	1	1	1	1	0	0	0	0	0	1	0	1	6
EE6	1	0	0	0	0	0	0	0	0	0	0	1	2
EE7	1	0	0	0	0	0	0	0	1	0	0	1	3
EE8	0	0	0	0	0	0	0	0	0	0	0	1	1
EE9	0	0	0	0	0	0	0	0	0	0	1	1	2
EE10	1	0	1	1	0	1	1	0	0	0	1	0	6
EE11	1	1	1	1	0	0	0	0	0	0	0	1	5
EE12	1	1	1	1	1	0	0	0	0	0	0	1	6
EE13	1	0	0	0	0	0	0	1	0	0	0	1	3
EE14	1	1	1	1	0	0	0	0	1	0	0	1	6
EE15	1	0	1	0	0	0	0	1	0	0	1	0	4

POSTEST													
	ITEM1	ITEM2	ITEM3	ITEM4	ITEM5	ITEM6	ITEM7	ITEM8	1	ITEM10	ITEM11	ITEM12	PD
EE1	1	1	0	1	0	1	1	0	1	1	1	0	8
EE2	1	1	1	1	1	1	1	1	1	1	1	0	11
EE3	1	1	1	1	1	1	1	1	0	0	0	1	9
EE4	1	1	0	1	1	1	0	1	0	1	1	1	9
EE5	1	1	1	1	1	1	1	1	0	1	1	0	10
EE6	1	1	1	1	1	1	1	1	1	1	1	0	11
EE7	1	1	1	1	1	1	1	1	1	1	1	1	12
EE8	1	1	1	1	1	1	1	1	1	1	1	1	12
EE9	1	1	1	1	1	1	1	1	1	1	1	1	12
EE10	1	0	1	1	1	1	1	1	1	1	1	1	11
EE11	1	1	1	1	1	1	1	1	1	1	1	1	12
EE12	1	1	1	1	1	1	1	1	1	1	1	1	12
EE13	1	0	1	1	1	1	1	1	1	1	1	1	11
EE14	0	1	1	1	1	1	1	1	1	0	1	1	10
EE15	0	1	1	1	1	1	1	0	1	0	1	0	8

Anexo 4. Evidencia digital de similitud



Anexo 5. Autorización de publicaciión en el repositorio

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE INVESTIGACIÓN O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

1.- DATOS DEL AUTOR

Apellidos y Nombres: CACHA ARANA CRISTHIAN MAX

DNI: 45082546 Correo electrónico: cristhian_max88@hotmail.com

Domicilio: Jr. Los Jardines N° 620 - Independencia - Huaraz

Teléfono fijo: 043-426742 Teléfono celular: 956501641

2.- IDENTIFICACIÓN DEL TRABAJO Ó TESIS

Facultad/Escuela: POSGRADO

Tipo: Trabajo de Investigación Bachiller ( ) Tesis (X)

Título del Trabajo de Investigación / Tesis:

PERITAJE INFORMÁTICO BASADO EN UNA NUEVA METODOLOGÍA HÍBRIDA EN 2M & 5 INGENIEROS

3.- OBTENER:

Bachiller ( ) Título ( ) Mg. (X) Dr. ( ) PhD. ( )

4. AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

Por la presente declaro que el documento indicado en el ítem 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencias e Informática para publicar la versión electrónica en su Repositorio Institucional (http://repositorio.upci.edu.pe), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art23 y Art.33.

Autorizo la publicación de mi tesis (marque con una X):
(X) Sí, autorizo el depósito y publicación total.
( ) No, autorizo el depósito ni su publicación.

Como constancia firmo el presente documento en la ciudad de Lima, a los 23 días del mes de Junio de 2020.

Firma