UNIVERSIDAD AUTÓNOMA DE CHIHUAHUA

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

ESTRATEGIA DE RECUPERACIÓN DE INFORMACIÓN CON EL USO DE HERRAMIENTAS TECNOLÓGICAS PARA EL DESARROLLO DE PERICIALES INFORMÁTICAS.

POR:

JESÚS ALBERTO LEINER MENDOZA

TESIS PRESENTADA COMO REQUISITO PARA OBTENER EL GRADO DE

DOCTOR EN ADMINISTRACIÓN

CIUDAD JUÁREZ, CHIHUAHUA., MÉXICO **NOVIEMBRE DE 2023**

Universidad Autónoma de Chihuahua
Facultad de Contaduría y Administración
Secretaria de Investigación y Posgrado

La Tesis **"Estrategia de recuperación de información con el uso de herramientas tecnológicas para el desarrollo de periciales informáticas."** que presenta **Jesús Alberto Leiner Mendoza**, como requisito parcial para obtener el grado de: **Doctor en Administración,** ha sido revisada y aprobada en la **Facultad de Contaduría y Administración** por los miembros del

Comité de Grado:

Dra. Alma Lilia Sapién Aguilar
Director de tesis

Dra. Laura Cristina Piñón Howlet
Asesor de metodología

Dr. Luis Antonio Molina Corral
Asesor de área mayor

Dra. Marilyn Georgia Salcido Sáenz
Asesor de Estadística

Dr. Ricardo Gallegos Murillo
Asesor de área menor

Por las autoridades de la Facultad:

M.A.R.H. Erika Nancy Rodríguez Quintana
Secretaria de Investigación y Posgrado

Dra. Cristina Cabrera Ramos
Directora de la
Facultad de Contaduría y Administración.

DEDICATORIA

A mi familia por ser motivadores y formadores a lo largo de mi vida y ayudarme a ser la persona que ahora soy.

A mi madre por todo su apoyo, estar al pendiente de mí y alentarme a seguir cuando me he dado por vencido, gracias por estar siempre a mi lado.

Mi padre, quien siempre me ha dado un ejemplo a seguir y ayudado a superarme, pero sobre todo el seguir el buen camino y siempre creer en mí.

Mi hija Ariadne, mi princesa, que al ver su rostro me da las fuerzas todos los días de seguir, levantarme y volver a luchar hasta lograr las cosas.

A Dulce, por aguantar, por apoyarme, por estar conmigo, hacerme mejor persona, hacerme feliz y sobre todo por amarme.

AGRADECIMIENTOS

A todas las personas que directa o indirectamente me ayudaron y participaron en la realización de este logro.

A cada uno de los doctores que me ayudaron y contribuyeron en mi formación, a mi directora de tesis, la Dra. Alma Sapién Aguilar por su enorme ayuda, guía, motivación y sobre todo por su disposición para compartir sus conocimientos y experiencia. De igual manera a los asesores Dra. Laura Piñón Howlet, Dr. Luis Molina Corral, Dra. Marilyn Salcido Sáenz y al Dr. Ricardo Gallegos Murillo, por su colaboración y conocimientos en la realización de esta investigación.

RESUMEN

La recuperación de información de dispositivos digitales es el proceso de restaurar datos eliminados, por medio de herramientas informáticas y cuyo propósito es localizar, identificar y restablecer la información deseada, el objetivo de la presente investigación fue proponer una estrategia sistemática que fortalezca la elaboración de una pericial informática en la recuperación de información. El enfoque de la investigación fue de naturaleza mixta, el diseño fue no experimental y transaccional, y el muestreo fue probabilístico. Se realizó un análisis documental de las herramientas tecnológicas, se determinaron las características y por medio de una encuesta a expertos se determinaron las herramientas más adecuadas para realizar el procedimiento de recuperación de información, así mismo se precisó una propuesta metodológica en el desarrollo de una pericial informática, lineamientos establecidos y validados por un panel de expertos por medio del método Delphi. El resultado arrojo dos aplicaciones que en conjunto cubren la totalidad de las características que deben poseer las herramientas tecnológicas diseñadas para la recuperación de información y se determinaron los mejores lineamientos para la elaboración de una pericial informática.

Palabras clave: (Recuperación de información, periciales informáticas, tecnologías de información)

ABSTRACT

The recovery of information from digital devices is the process of restoring deleted data, using computer tools and whose purpose is to locate, identify and restore the desired information. The objective of this research was to propose a systematic strategy that strengthens the development of a computer expert in information recovery. The research approach was mixed in nature, the design was non-experimental and transactional, and the sampling was probabilistic. A documentary analysis of the technological tools was carried out, the characteristics were determined and through a survey of experts the most appropriate tools to carry out the information retrieval procedure were determined, likewise a methodological proposal was specified in the development of an expert informatics, guidelines established and validated by a panel of experts through the Delphi method. The result yielded two applications that together cover all the characteristics that technological tools designed for information retrieval must have and the best guidelines for the preparation of a computer expert were determined.

Key words: (Data recovery, computer forensic experts, information technologies)

ÍNDICE GENERAL

ÍNDICE DE GRÁFICAS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

I. INTRODUCCIÓN

Actualmente las Tecnologías de Información y la Comunicación (TIC) están presentes en el día a día de la sociedad, evolucionando y adaptándose en su vivir, haciendo más fácil las actividades cotidianas, dejando un rastro de cada movimiento realizado, el acceso a ellas y su dependencia tanto en el hogar como en los negocios ha creado diversos riesgos en el manejo de la información, con ello ha surgido la necesidad de administrar los recursos intangibles, así como sistemas y prácticas para recuperar esos activos ante fraudes, ataques, daños o sabotaje que puedan incurrir en un delito (Gaytán et al., 2019).

En la vida diaria, se emplean una variedad de herramientas tecnológicas que van desde lo más elemental hasta lo más sofisticado. Todas estas herramientas facilitan las tareas tanto a nivel individual como en el ámbito empresarial u organizativo. Asistimos a una evolución digital sin precedentes en los últimos años, donde el uso del papel ha quedado obsoleto y desmaterializado. El impacto de las Tecnologías de la Información y la Comunicación (TIC) en el mundo, especialmente en lo que respecta al almacenamiento de información, es incalculable. Esta revolución ha dado lugar a diversos métodos de resguardo, como el almacenamiento en computadoras, dispositivos móviles, correo electrónico, aplicaciones de mensajería, fotografías digitales, opciones en la nube, entre otros. El objetivo general de esta investigación fue proponer una estrategia sistemática que fortalezca la elaboración de una pericial informática en la recuperación de información.

La investigación se dividió en cinco secciones, detalladas a continuación. En la primera sección, se proporciona una descripción de los antecedentes y se presenta el problema que lleva a la formulación de los objetivos e hipótesis, concluyendo con la justificación que destaca la importancia de llevar a cabo esta investigación.
En la segunda sección, se aborda la revisión de la literatura, que incluye tanto el marco conceptual como el estado del arte. En cuanto al tercer apartado, se establecen los criterios metodológicos, así como la recopilación y procesamiento de

datos. El cuarto apartado presenta el análisis de los resultados y la discusión. Finalmente, en el quinto apartado, se exponen las conclusiones y recomendaciones, junto con la propuesta de estrategia. Además, se hacen referencia a las fuentes bibliográficas y a los anexos.

ANTECEDENTES

El creciente impulso del uso de tecnologías ha aumentado la cantidad de equipos que son utilizados cotidianamente, datos del Instituto Nacional de Estadística y Geografía (INEGI, 2021), mencionan que en México se estima que existen 86.6 millones de personas con acceso a internet y 91.7 millones usuarios de telefonía celular, esta condición de disponibilidad de las TIC ha generado un impacto en todas las actividades y con ello la demanda de mano de obra en todos los sentidos, según el INEGI (2020), México cuenta con casi 976 mil personas con formación en ciencias de la computación y TIC, de los cuales solo el 10% realizan funciones de servicios por su cuenta. Si bien este efecto ha ayudado a las empresas en aumentar su productividad.

La informatización de la sociedad también tiene una correlación negativa, de aquí surgen los delitos informáticos en México los cuales han crecido en los últimos años, según la organización editorial El Sol de México (2021) aproximadamente en el año 2015 se reportaron seis mil delitos, entre 2015 y 2021 se estima alrededor de 72 mil delitos informáticos en México, sin considerar la gran cantidad que no llegan a demandas, y a pesar de ello no existen regulaciones o legislaciones informáticas en el país, datos de la página oficial del poder judicial de Michoacán denota que el único estado que tiene una legislación de los delitos informáticos es Sinaloa (Valencia, 2019).

Las reformas Constitucionales en México han sufrido grandes modificaciones en los últimos años, estos cambios han permitido la intervención de especialistas en diferentes materias como apoyo en la intervención legal de los abogados, quienes

con prácticas e investigaciones científicas pueden proporcionar pruebas sólidas en el nuevo sistema de justicia penal que describe el Código Nacional de Procedimientos Penales (CNPP, 2021).

El Gobierno de México establece que cualquier hecho puede ser examinado bajo cualquier medio para comprobar que es lícito, el sistema jurídico en la resolución de conflictos menciona en su artículo 368 que puede ser entregada una prueba pericial que sea relevante y que ésta debe ser realizada por un especialista o consultor en la ciencia, con el fin de ser un apoyo técnico en todos los aspectos de interés de la parte con quien colabora además para esclarecer dudas técnicas ante un ministerio o juez, realizando un informe pericial escrito y sin eximir su declaratoria en la audiencia del juicio tal como lo marca el artículo 272 del CNPP (2021).

Ante los cambios a la Ley en la Reforma Constitucional, México se encuentra en el proceso de desarrollo y construcción en el análisis forense informático, por ello una pericial informática como herramienta cuando es requerida, es una pieza clave en la jurisprudencia, por ello la importancia de ser llevada bajo una metodología estandarizada y adecuada para el análisis y manejo de la información, así como los pasos del proceso de investigación, tal como lo está trabajando la Coordinación de Métodos de Investigación de la Fiscalía General de la República (FGR, 2020).

PROBLEMA DE INVESTIGACIÓN

Las modificaciones de la Reforma Constitucional en materia penal específicamente en el desahogo de las pruebas relacionadas con las TIC han sido modificadas y con ello es más común la necesidad de utilizar profesionales especializados en el tema, actualmente no existe una metodología o estudio específico del proceso del desarrollo de una pericial, ni regulación de las herramientas a utilizar en los mismos o cuales son las más efectivas, de tal modo que el sistema de justicia se enfrenta a un compuesto de diversas metodologías y características en el desarrollo de la ciencia forense informática.

México presenta un rezago en la materia y es un tema que necesita ser estudiado, se deben establecer directrices y estándares en su práctica ya que sin una línea de seguimiento definida el tribunal de justicia no puede establecer un dictamen solo con base en las periciales presentadas en el debate procesal de ambas partes, por lo cual en una demanda establecida donde se tenga incertidumbre o versiones contradictorias se tendrá que recurrir a otro perito llamado tercero en discordia, esto con el fin de tener una opinión sin favoritismos, tal como lo expresa el artículo 1390 del Código de Comercio.

Ante este escenario es importante un estudio de las consideraciones legales para la creación de una estrategia para el análisis y recuperación de elementos digitales como apoyo en periciales informáticas forenses, así como realizar un estudio de cuales herramientas pueden ser más eficientes en el proceso del investigador. Por lo que se plantean las siguientes preguntas de investigación:

Pregunta general

¿De qué manera una estrategia sistemática fortalece la elaboración de una pericial informática en la recuperación de información?

Preguntas específicas

¿Cuáles son las principales características de las herramientas tecnológicas utilizadas para la recuperación de información en elementos de almacenamiento digital?

¿Cuáles herramientas tecnológicas son las más utilizadas en los procesos de recuperación de información en elementos de almacenamiento digital?

¿Cuáles son los lineamientos y metodologías trascendentes para la elaboración de una pericial informática?

¿Cómo puede una estrategia de recuperación de información con el uso de herramientas tecnológicas fortalecer una pericial informática?

OBJETIVOS DEL ESTUDIO

Objetivo general

Proponer una estrategia sistemática que fortalezca la elaboración de una pericial informática en la recuperación de información.

Objetivos específicos

1. Describir las principales características de las herramientas tecnológicas utilizadas para la recuperación de información en elementos de almacenamiento digital.

2. Establecer cuáles herramientas tecnológicas son las más utilizadas en los procesos de recuperación de información en elementos de almacenamiento digital.

3. Determinar los lineamientos y metodologías trascendentes para la elaboración de una pericial informática.

4. Diseñar una estrategia de recuperación de información con el uso de herramientas tecnológicas aplicadas en una pericial informática.

JUSTIFICACIÓN

En la vida cotidiana se utilizan diversas herramientas tecnológicas, desde lo más básico hasta lo más complejo, todas ellas facilitan las labores tanto de los individuos como de las empresas u organizaciones, una evolución digital sin precedentes en los últimos años, donde el uso del papel es cosa del pasado, ha quedado desmaterializado, el impacto de la utilización de las TIC en el mundo para el almacenamiento de información es inmedible y con ello ha traído diversos mecanismos de resguardo, existen datos guardados en computadoras, dispositivos móviles, correo electrónico, aplicaciones chat, fotografías digitales, opciones en la nube, entre otros métodos, según la empresa Statista en 2019, se estima que la información alrededor del mundo al año 2018 es de aproximadamente 33 zettabytes (Moreno, 2019).

La generación de toda la información esta almacenada y limitadamente compartida, pero en ocasiones puede trascender en problemas como ser reemplazada, destruida o modificada, lo cual puede llegar a ser una tarea compleja incluso para un profesional, sin embargo, existen técnicas, métodos o estrategias para realizar un proceso de recuperación.

En efectos dentro del marco jurídico éste proceso tiene como objetivo el esclarecimiento de hechos delictivos bajo el derecho penal como la marca la CNPP en sus artículos tanto para la parte actora como la demandada con el fin del desarrollo de una pericial informática forense la cual brinda una perspectiva del

suceso, es importante aclarar que dentro del marco legal ésta no tiene y no existen un proceso o lineamiento a seguir para llevarla a cabo, por lo cual el fin de esta tesis es proponer una estrategia metodológica eficaz en la recuperación de elementos digitales que impacte en la elaboración de la misma, buscando realizar los procesos de un perito de manera más estratégica y dentro de los lineamientos del Sistema de Justicia Mexicano.

La importancia de seguir un lineamiento en los procesos para la obtención de pruebas con un soporte de herramientas informáticas y una revisión por una auditoria forense, tal como está establecido en los estándares internacionales ISO27037, UNE71505, UNE71506, RFC3227, IOCE y la normativa mexicana NMX-I-289-NYCE-2016, tendrá un impacto positivo en los resultados de las investigaciones, dando como resultado una pericial informática sustentada bajo una legitimidad y poder ser cabalmente reconocida ante los tribunales.

DELIMITACIÓN DEL ESTUDIO

La presente investigación pretende generar una propuesta de estrategia para el análisis, recuperación y reconstrucción de elementos digitales de dispositivos de almacenamiento para el desarrollo de periciales en materia de informática como medio probatorio a presentarse en procesos judiciales, realizada durante el periodo de enero de 2023 a noviembre de 2023.

FORMULACIÓN DE LA HIPÓTESIS

Hipótesis General

Una estrategia sistemática fortalece la elaboración de una pericial informática en la recuperación de información.

Hipótesis Específicas

1. Las principales características de las herramientas tecnológicas utilizadas para la recuperación de información en elementos de almacenamiento digital permitirán crear el instrumento de evaluación para la selección de la herramienta más optima.

2. Las herramientas tecnológicas más utilizadas por expertos para la recuperación de información en elementos de almacenamiento digital son Stellar Data Recovery y Wondershare Recoverit.

3. El cumplimiento de los lineamientos y metodologías fortalece la elaboración de una pericial informática.

4. Una estrategia de recuperación de información con el uso de herramientas tecnológicas fortalece un dictamen pericial informático.

II. FUNDAMENTACIÓN

Marco conceptual

Tecnologías de Información y la Comunicación:

Benfeld (2020b) menciona que son elementos materiales e inmateriales conectados entre sí, que permiten el procesamiento, gestión y almacenamiento de información, conjuntos de programas que hacen posible que dispositivos físicos realicen tareas. Por su parte, Chen (2019) y para efectos de la presente tesis, lo describe como un conjunto de tecnologías, recursos, herramientas, programas, equipos, redes y medios relacionados con la transmisión, consumo y generación de información como: Texto, imágenes, video, datos y voz.

Datos:

Los datos o información en términos de informática se les puede considerar lo mismo todo depende de la perspectiva del hecho en que tenga mención, es decir un dato puede ser un solo elemento, como puede ser el concepto de un término como edad, fecha, etc., por si sola es una representación simbólica, atributo o característica, sin un valor semántico, al ser procesado ese dato se convierte información, la información puede referirse a los datos ya almacenados o procesados, otra conceptualización de datos puede ser el almacenamiento de información en conjunto (Rae, 2022).

Evidencia Digital

El principal objetivo de la informática forense es encontrar evidencias, en este caso todo las pruebas y aspectos relacionados que pueden ser ofrecidos como elementos materiales probatorios en un proceso legal, los cuales puede ser cualquier contenido en dispositivos digitales de almacenamiento, por medio de las técnicas que permitan asegurar la integridad y disponibilidad de la información, y tienen validez ante un

juez siempre y cuando se cumplan los requisitos administrativos establecidos por el código penal (PGR, 2018).

Delito informático:

Refiere a todo acto o conducta delictiva donde está presente el uso de la tecnología o dispositivos de comunicación, dando lugar a la violación de los derechos o transgresiones reconocidas por la autoridad y sancionado según sea aplicables bajo el código penal 2023.

Informe pericial:

Documento como medio de prueba en un juicio, este es redactado bajo un análisis especializado con base en los hechos, fundamentos, métodos y técnicas empleadas para expresar conclusiones y emitir un punto de vista profesional, este es ajeno al proceso penal y es realizado por un experto en la materia, denominado perito, y tiene como objetivo aclarar dudas que un juez pueda tener (Sandoval Silva, 2021; Vázquez, 2022a).

Análisis forense informático:

Investigación realizada por un experto informático que participa en la comisión de un delito, con el fin de esclarecer circunstancias e identificar a un autor y su grado de responsabilidad, arrojando un informe pericial (Haro, 2021), lo conceptualiza como, procedimientos estandarizados para el análisis de evidencias en búsqueda de la creación de pruebas. El periodista especializado en tecnología Hernández (2023) la describe como la aplicación de técnicas para realizar una investigación y análisis de un dispositivo informático con el fin de recopilar pruebas, no necesariamente para esclarecer un delito, sino que también como proceso de recuperación de información, este último más acertado y utilizado para fines de la presente.

Herramientas tecnológicas:

Nebreda (2023) lo define como un proceso para la obtención, manejo, creación y búsqueda de información por medio de un instrumento, puede ser cualquier software o hardware que ayude a cumplir con un determinado objetivo de la manera más sencilla, fiable y rápida.

Marco teórico

La información

La definición de información es básica y fundamental para el desarrollo de esta investigación, partiendo del concepto básico de acción y efecto, donde se le puede describir como un conjunto de elementos o una relación entre elementos que generan conocimiento (Real Academia Española [RAE], 2022), existen diversas conceptualizaciones dependiendo de la disciplina de estudio, en el caso de la informática es importante tener clara la diferencia entre datos e información. Un dato es una representación simbólica, un valor que por sí solo no tiene sentido, mientras que la información son datos procesados, entendidos y almacenados, tal como menciona Marcial (1996) en la propuesta conceptual, donde explica la construcción de la información desde un punto de vista informático y menciona que no es una condición exclusiva del hombre, sino que describe que es un desarrollo del mismo en la creación de registros y almacenamiento, con el fin de adecuar, interpretar y utilizar los datos a sus necesidades.

Con ejemplo de los conceptos mencionados, se puede describir que en la rama de Tecnologías de Información (TI), al conjunto de datos procesados y manipulados se le considera información y en este momento se le puede dar un significado y valor, es decir una representación simbólica e intangible almacenada en un dispositivo físico, es importante tener en cuenta que un conjunto de datos puede representarse como tradicionalmente se le conoce como un documento, pero también puede representarse en conjunto como elementos visuales o auditivos como es una

imagen, video o sonido, de aquí parte la importancia de sobre guardar la información de toda organización en diversos dispositivos de almacenamiento, este proceso es crítico, ya que en la mayoría de los casos es el activo intangible más valioso.

Los elementos digitales

Mascarell (2019) comenta que las TIC son los medios tecnológicos y la digitalización y no solo incluyen letras y textos, sino que además las imágenes, continua con la explicación que facilitan el almacenamiento y procesamiento digital de la información audiovisual, agregando a ello el uso de dispositivos que facilitan el acceso y la comunicación.

Cabero (1998) desde su perspectiva describió años antes y de manera similar al pensar de Mascarell, como el diseño, producción y gestión digital de lo que llamó el manejo de la materia inmaterial de la información. Por lo general diversos autores concuerdan en el enfoque que le dan a dicho término. La importancia de la conceptualización ayuda a la comprensión de lo que son los elementos digitales como: información que puede contener texto, sonido, imágenes, videos u otros elementos, que están almacenados en un dispositivo y que requieren de una interfaz para materializarse en algún sentido.

IBM(2023a) y RedHat(2018) explican que los elementos digitales pueden ser guardados de diversas maneras y que estos pueden ser acumulados en medios magnéticos (cintas), discos ópticos (CD) o mecánicos (Discos Duros), además de unidades de estado sólido (SSD) y los tipos pueden ser: repositorios como servidores en la nube o de forma local directa sin necesidad de comunicación con otros equipos; los elementos externos al entorno donde se encuentra, esto independientemente de la forma o tipo de almacenamiento, cada uno de estos procesos necesita forzosamente de un dispositivo físico (hardware) y las formas o configuración de almacenamiento de los datos es controlada por un programa manejador y como interprete (software).

El manejo del almacenamiento de información es un tema delicado, para prevenir daños y la pérdida de información existen desventajas en el uso de cada uno de ellos, por ejemplo los dispositivos magnéticos (como las cintas) pueden sufrir borrado de información o daños cuando algún campo electromagnético intenso está presente a su alrededor y puede ocasionar incluso que no sea recuperable, el resguardo en unidades de discos compactos no sufren alteraciones por estos campos, pero están expuestos a rayaduras o deterioro por el tiempo y aspectos como la humedad (Farfán, 2020) , en los disco duros afectan los campos magnéticos, impactos, uso excesivo, sobrecalentamiento y fallas eléctricas o mecánicas en su funcionamiento, en el almacenamiento de estado sólido pueden ser ocasionados principalmente por sobrecalentamiento, uso excesivo y fallas eléctricas, todo este tipo de fallas se le consideran físicas, por último en cada una de ellas la eliminación intencional o por un problema de software, nombradas fallas lógicas.

Medios de almacenamiento

El almacenamiento informático es el proceso de mantener y guardar información por medio de un proceso tecnológico, es decir salvaguardar datos, estos son la unidad mínima referencia y ellos al ser agrupados se llaman archivos, los cuales pueden ser documentos, fotografías, audio, video, de sistema, y otras variaciones de ellos, por lo general agrupados en carpetas o folders digitales, los cuales pueden tener jerarquías de más subfolders o subdirectorios, los sistemas informáticos almacenan esta información bajo dos esquemas: texto o binario, los archivos de texto contienen letras, números y símbolos especiales un total de 256 diferentes caracteres disponibles en su uso, mientras que el esquema binario pueden contener los mismos caracteres pero por una operación matemática por ceros y unos, conteniendo la información de su propia estructura y que tipo de archivo es para ser interpretado por un programa en específico para ser visualizado (IBM, 2023b).

La información se puede guardar en distintos tipos de dispositivos, los cuales pueden ser magnéticos, ópticos u electrónicos. Los dispositivos magnéticos pueden

ser los ya obsoletos disquetes o cintas magnéticas, los discos compactos en sus diversas versiones catalogados como ópticos y los electrónicos, los más utilizados en la actualidad, en los cuales se ubican las memorias USB (Bus Universal en Serie), tarjetas de memorias, discos duros y unidades de estado sólido (Concepto, 2021).

Las unidades de almacenamiento se manejan por registros los cuales identifican donde se encuentra cada dato, existe el almacenamiento volátil que es la memoria RAM que se pierde o elimina automáticamente cuando un equipo es apagado, la cual en ocasiones queda almacenado en memoria virtual, almacenada temporalmente en la memoria secundaria o de almacenamiento, el almacenamiento secundario es donde se guarda la información principal, como datos, archivos, sistema etc., por lo general es el disco duro o unidad de estado sólido y medios extraíbles como unidades USB, tarjetas, CD, DVD, entre otros (Crucial, 2023).

Los discos duros consisten en discos metálicos giratorios, con un brazo mecánico y un cabezal magnético que funge como lector y dispositivo de escritura, con una tablilla controladora que sirve para comunicarse con los equipos de cómputo, cada disco posee pistas de forma circular y cada circulo a su vez está conformado por sectores, esta es la unidad más mínima de almacenamiento y esta se realiza con cargas magnéticas en el orden que se requiere, es decir la información esta almacenada por partes en distintas ubicaciones.

Por otra parte, las unidades de almacenamiento solido al igual que las tarjetas y memorias USB consisten en un almacenamiento electrónico, al contrario que el almacenamiento circular de los discos duros, estos guardan la información en forma de cuadrantes y bloques de manera secuencial, lo que hace más rápida su localización, esto aumenta la velocidad en su manejo y por lo tanto los equipos de cómputo son más rápidos (Crucial, 2023).

Fallo físico en Unidades de almacenamiento

Las principales fallas físicas en dispositivos de almacenamiento son causadas por daño en los mecanismos, humedad, golpes o descargas eléctricas, en estas situaciones se debe de determinar el grado de daño, en ocasiones se pude recuperar parte de la información por medio de aplicaciones aun cuando están dañados pero es posible acceder a ellos, pero cuando no es posible una restauración por aplicación, se debe realizar un proceso de recuperación complejo, el primer paso es el diagnóstico de cual pieza es la dañada, este es un proceso complicado y es necesario el uso de herramientas físicas, esta recuperación es a nivel hardware y este proceso es realizado por compañías dedicadas y con equipos en laboratorios especializados donde pueden ser reparadas las tablillas, cabezales lectores de los discos o con lectores de las memorias de almacenamiento, aun así estos procesos utilizan programas como interfaz entre la recuperación directa y el armado de información (Datarecoverylab, 2023).

Fallo lógico en Unidades de almacenamiento

Un fallo lógico es considerado cualquier aspecto que conlleven a un problema de lectura de información en un dispositivo de almacenamiento, algunos problemas inherentes son: complicaciones en el acceso de las unidades, rendimiento, pérdida de archivos, información dañada, modificaciones en los manejadores de unidades, información borrada o formateo. Cuando existe una falla lógica es posible recuperar la información desde herramientas tecnológicas ya que el fallo no es de hardware y el dispositivo se encuentra en buenas condiciones y es reconocido por el sistema, es importante entender que ningún proceso puede considerarse completamente seguros o afirmar que la información siempre será restaurada ya que cada falla o avería tiene un diferente grado de daño, ya sea físico o a un nivel de aplicación (González Becerril, 2019).

Herramientas Tecnológicas

La recuperación de información puede ser un concepto algo ambiguo, ya que el proceso puede ser desde lo más sencillo hasta el uso de técnicas complejas, los

procesos básicos son la recuperación de información almacenada en distintas ubicaciones de los medios de almacenamiento donde no es necesario el uso de herramientas de recuperación de información, la conceptualización dentro de las tecnologías de información describe a la recuperación de información como un área de las ciencias y tecnología, un proceso mediante el uso de técnicas y herramientas tecnológicas con el fin de realizar una restauración de un sistema de archivos, es decir el proceso de localizar, identificar, restaurar y respaldar datos de un dispositivo de almacenamiento (Quiña et al., 2019).

Las Herramientas de recuperación trabajan bajo sus propias cualidades y características, es por ello que un programa no es capaz de recuperar datos para todos los escenarios de pérdida de información posibles, ya que la gestión de información tiene diversos mecanismos de almacenamiento y diferentes tipos de sistemas de archivos, además de ello la información no se almacena igual a pesar de que sean del mismo tipo ya que cada registro de información es diferente entre sí, como se mencionó anteriormente si la falla no es física la posibilidad de recuperar la información es alta, si no ha sido reutilizado el espacio lógico donde estaba almacenada la información.

Por ello, la selección del adecuado programa especializado en la recuperación de datos es sumamente importante, y esta selección debe de realizarse en función a sus cualidades (Compudiagnosis, 2018), las principales características que se deben tomar en cuenta para elegir unas herramientas tecnológicas son:

- Procesos de exploración: una vista rápida al estado de la unidad evita utilizar tiempo innecesario en caso de que el programa no sea capaz de recuperar la información.
- Compatibilidad: verificar que será compatible con el sistema operativo y el sistema de archivos que tiene la unidad sobre la que se va a trabajar.

- Soporte: es recomendable utilizar programas que tengan un respaldo por parte de empresa desarrolladora, ya que ellos pueden auxiliar en el proceso de recuperación.
- Confiabilidad: realizar un estudio sobre la herramienta seleccionada, revisar si cuenta con recomendaciones o mala reputación, el proceso de recuperación es crítico y durante este se puede llegar a perder la información de manera definitiva.
- Interfaz: un programa con un ambiente amigable e intuitivo ayudará a realizar el proceso y evitará errores en el proceso.
- Costo beneficio: existen herramientas en el mercado gratuitas y de costo, cada una con su beneficios y desventajas, es importante determinar el valor real de la información para realizar una selección entre un programa de paga o uno que no lo es.

Es importante tener en cuenta que las limitantes de las herramientas de recuperación:

- No pueden reparar sectores dañados.
- No pueden recuperar información de sectores dañados aun cuando la falla es lógica.
- Corregir errores en el sistema de lectura o mecánicos.
- No pueden saltar procesos del sistema de la unidad de almacenamiento (SMART).
- Reparar el sistema de funcionamiento de la unidad (Firmware).
- No pueden detectar o reparar errores de comunicación de periféricos.

En estos tipos de fallo es recomendable utilizar empresas especializadas dedicadas a la recuperación de datos, las cuales pueden realizar lecturas directamente de los platos en el caso de discos duros, o bien de las memorias flash de las unidades de estado sólido y de tarjetas de almacenamiento USB o SD (González, 2021).

Las técnicas de restauración de archivos son diferentes entre cada desarrollador de herramientas tecnológicas, pero los procesos son similares, esto se lleva a cabo creando nuevos bloques de archivos y nuevas referencias en el almacenamiento a partir de la información dañada que se recupera de cada sector, este tipo de técnica es llamada File Carving, esto es extraer información de un dispositivo, analizarla en todos los aspectos y reconstruirla (Guiaspracticas, 2023).

Cuando existe un daño lógico ocasionado por causas humanas, fallas en los sistemas, corrupción de datos o formatos, la solución es a nivel de software y para ello las herramientas digitales tienen la finalidad de agilizar las tareas, una selección adecuada pueden facilitar el análisis y recuperación de datos determinando el resultado en los procesos de reconstrucción, por ende las soluciones informáticas existentes deben de ser avaluadas para crear una estrategia adecuada de cada proceso que se desea realizar, a continuación se describen las principales herramientas recomendadas por la revista PC Magazine (Mendelson, 2018) y Forbes (Main, 2023):

Stellar Data Recovery

Empresa con software de licenciamiento que se dedica al restablecimiento de archivos desaparecidos en sistemas operativos Windows, Android, Mac, iPhone o iPad; en el caso de sistemas Windows posee la capacidad de realizar recuperación de discos duros mecánicos o unidades de almacenamiento sólido, incluso cuando están dañados de forma física, igualmente puede localizar información de memorias compactas y externas provenientes de cámaras digitales o de drones, ya sea por error humano, información corrupta, ataques de virus, etc., otra de sus ventajas por lo cual es un atractivo programa es que puede recuperar información de unidades cifradas y de alto almacenamiento o alta definición, algunas otras utilerías se especializan en reparaciones dedicadas en archivos de Excel, SQL, Access, Quickbook, entre más programas, además permite la reconstrucción de bases de datos del directorio activo de usuarios de Windows y archivos de buzones de correo corruptos y un útil rescate de cintas y sus tipos de formato de almacenamiento LTO

1, 2 y 3, agregando unidades virtuales así como la utilería de borrado permanente, características que pocos softwares incorporan en sus funcionalidades, en sistemas Mac se enfoca en recuperar información ante problemas sencillos en los dispositivos de equipos; es una solución ante fallos de disco duro o eliminación, que pueden ser desde la pérdida de la estructura del disco, inicio del sistema o archivos almacenados en cualquier medio de almacenamiento utilizados por el sistema, lo que refiere a las opciones de dispositivos móviles se especializa en la recuperación y restauración de archivos eliminados y de sistema, cada aplicación tiene un costo independiente (Stellar, 2023).

Easeus

Es una aplicación que puede ser de paga o gratuita dependiendo de la necesidad del alcance, y desarrollada para múltiples plataformas con el fin de dar soluciones de optimización, monitoreo, respaldo y de recuperación de datos ante desastres informáticos, restaura archivos ante los diversos escenarios como eliminación, daño, formato, apagados inesperados y en contraparte posee una utilidad para eliminar información, particiones o un disco duro completo, borrando de forma permanente y que no sea posible recuperarla inclusive por el misma compañía, la cual además posee las utilerías para recuperar datos desde diversos dispositivos, incluyendo unidades de almacenamiento de Circuitos Cerrados de Televisión (CCTV), y desde dispositivos IOS o Android como lo son datos, fotos, videos, contactos, notas, chats WhatsApp, registros, y diversas funcionalidades para servidores Exchange y bases de datos en MySQL (Easeus, 2023).

AnyRecover

La aplicación AnyRecover es una aplicación capaz de recuperar información de sistemas operativos Windows, Mac, iOS y Android, describe dentro de sus características la restauración de documentos borrados, dañados o no guardados de Microsoft Office, así como correos electrónicos e incluso el contenedor de datos

personales (PST) específicamente de Outlook, entre sus otras características menciona la utilidad de recuperar datos almacenados en múltiples sistemas operativos e incluso dispositivos móviles, independientemente del medio de almacenamiento de almacenamiento y su formato (AnyRecover, 2023).

OnTrack Easy Recover

Herramienta destinada a la recuperación de datos dañados eliminados o en unidades que fueron eliminadas, formateadas en múltiples ocasiones y más escenarios de fallas, puede soportar unidades de almacenamiento convencionales y dispositivos externos como memorias USB e incluso CD, compatible con sistemas Windows y Macintosh, y el alcance de sus ventajas es acorde al licenciamiento adquirido (Ontrack, 2023).

Disk Drill \ CleverFiles Disk Drill Pro (For Mac)

Un programa con diversos niveles de recuperación, particiones estándar de Windows, MAC OS y Linux, llegando a niveles de recuperación de información en unidades virtualizadas. Incluye recuperación de dispositivos iPhone IOS, diversidad de unidades de almacenamiento, arreglos de discos duros, reconstruye todo tipo de archivos eliminados o dañados sin importar su formato, esta herramienta recupera información eliminada accidentalmente, borrada inclusive de la papelera de reciclaje, disco duro con fallos, unidad formateada, infecciones por virus, particiones borradas o dañadas, sistemas de archivos corruptos como RAW y tarjetas de memoria dañadas. Posee utilerías de recuperación de mensajes de textos borrados y herramientas de copias de seguridad y monitoreo continuo de manera proactiva, todas las funciones están disponibles en virtud de la versión o licencia adquirida (Disk-drill, 2023).

Wondershare Recoverit Data Recovery

Solución ante una supresión de diversos archivos, la empresa cuenta con diversas aplicaciones que por separado son capaces de recuperar videograbaciones, imágenes y archivos de Windows, IOS, Linux o Android, una recuperación que puede ser desde conversaciones hasta sistemas, bloqueos y contraseñas, clonar y borrar permanentemente información, además de restauraciones ante diversos escenarios de fallos, en conjunto todas las utilerías son herramientas muy útiles para la realización de un informe forense informático (Wondershare, 2023).

MiniTool Power Data Recovery

Es un programa capaz de recuperar información almacenada en cualquier dispositivo compatible y detectado por Windows sin importar si el daño fue ocasionado por eliminación, virus, falla del sistema e incluso por daños lógicos en la unidad de almacenamiento, cuenta con la utilería de visor previo a la recuperación de archivos como documentos, gráficos, audio, video, archivos comprimidos, de correo, entre otros, esto con el fin de verificar previamente si son los archivos adecuados, la versión gratuita está limitada a visualizar y recuperar poca información, por lo que la suscripción mensual, anual o perpetua es la opción viable en este programa (Minitool, 2023).

DMDE

Herramienta gratuita diseñada para recuperar archivos que han sido eliminados, no diferencia el tipo de archivo por ser una aplicación que reconstruye la información desde su estructura de directorio, lo que su recuperación puede realizarse con mínimas restricciones, tanto para Windows, Macintosh y Linux (DMDE, 2023).

Wise Data Recovery

Una aplicación gratuita y muy similar en características con las anteriores, pero agregando a sus funcionalidades la restauración del sistema operativo ante archivos eliminados, registros dañados, fallo de actualizaciones, daño físico, particiones eliminadas o formateos, y la característica de soportar varios tipos de formatos de unidades de almacenamiento (Wisecleaner, 2023).

Prosoft Data Rescue (Macintosh)

Programa para el rescate de información ante fallos como la eliminación y pérdida de archivos, compatible con dispositivos de almacenamiento interno y extraíble, múltiples archivos compatibles, con un visor de archivos previo a la recuperación y la opción de realizar una copia entera de la unidad de almacenamiento o una copia de los archivos de arranque del sistema, esto a manera preventiva ante un fallo (Prosoft, 2023a).

Alsoft Diskwarrior

Es un sistema de paga con pocas funcionalidades que se ejecuta desde un dispositivo almacenamiento USB la cual es proporcionada por los desarrolladores, está diseñado específicamente para restaurar el arranque de sistemas operativos Mac y los archivos almacenados en el equipo (Alsoft, 2023).

Prosoft Data Rescue (Windows)

Al igual que el programa para la versión Macintosh sirve para restaurar información de fallas o eliminación, también es compatible con múltiples archivos almacenados en dispositivos internos y externos, cuenta con un visor de archivos y la opción de realizar un respaldo entero de la unidad de almacenamiento o una copia de los archivos de arranque (Prosoft, 2023b).

Recuva

Este programa gratuito está diseñado con el fin de recuperar información eliminada de un equipo de cómputo, ya sea del disco duro o de algún medio extraíble, sin importar si pudo suceder de forma accidental o intencional. Este sistema tiene la capacidad de recuperar archivos eliminados desde sistemas de archivos FAT, FAT32, NTFS, EXFAT, EXT3 y EXT4, entre otros. Recupera archivos borrados de la papelera de reciclaje, de carpetas dañados, de dispositivos removibles, cámaras digitales, celulares, y más dispositivos detectados por el equipo de cómputo como medio de almacenamiento, inclusive discos que tuvieron formato de borrado superficial o daño físico recuperan archivos eliminados en Windows 11,10 y versiones anteriores, pero no cubre la plataforma MAC OS (Recuva, 2023).

Informática Forense

Es una rama de la ciberseguridad, también llamada cómputo forense o análisis forense, surge de una necesidad legal para la resolución en procesos jurídicos donde es necesario el apoyo de un especialista para la comprensión de aspectos técnicos relacionados con la informática, esta disciplina se encarga de administrar la información digital almacenada principalmente en discos duros, móviles, correos u otros dispositivos electrónicos, siendo de suma importancia ya que no se puede determinar su valor. Esta práctica tiene el objetivo de recuperar, recopilar y preservar información ante un fallo, considerando que los datos pueden sufrir modificaciones o ser eliminados, ya sea de manera intencional o sin autorización, principalmente esta práctica es utilizada en conjunto con elementos de derecho fungiendo como una solución legal en un proceso judicial (Ortega, 2022).

Espinoza (2022) expresa que es una rama de las ciencias forenses donde se realiza la aplicación de una metodología y técnicas para identificar, preservar, recuperar, extraer, documentar e interpretar todo lo necesario como evidencias, así mismo

Muñoz et al. (2020) concuerda al describirla como un proceso metodológico con el fin de realizar el análisis de información digital por expertos.

Existen normas utilizadas mundialmente que han profundizado en ello, surgiendo así el ISO27037, UNE71505, UNE71506, RFC3227, IOCE y la normativa mexicana NMX-I-289-NYCE-2016, por mencionar algunas, todas ellas son normas estandarizadas para el desarrollo de periciales, algunos de los países colaboradores son: Estados Unidos, Reino Unido, Europa y Canadá. La informática forense es un proceso y metodología, no un producto como tal, una capacitación, una correcta estructura y una selección adecuada de herramientas tecnológicas. Por lo anterior se puede describir que la informática forense se encarga de la correcta aplicación de técnicas en los procesos de la adquisición de datos, así como su preservación, recuperación en caso de algún suceso y la presentación de un análisis forense detallado para los efectos legales para el cual fue desarrollada.

ISO27037 / 27042

La Normativa ISO 27037 y 27042 en conjunto generan el de cómputo forense necesario para la resolución en procesos jurídicos, el objetivo de esta normalización internacional es la ejecución de prácticas digitales forenses, sus características principales son: identificación, obtención y preservación de la evidencia.

Emitido por la Organización Internacional de Normalización (ISO), esta trata de un Sistema de Gestión de Seguridad de la Información (SGSI), el cual está dedicado a crear, implementar, manejar y supervisar políticas en el manejo de la información y los sistemas de una organización, esta guía refiere al manejo de evidencias digitales en al marco legal con valor probatorio (iso27000.es, 2022). La normativa creada por la ISO y la Comisión Electrotécnica Internacional (IEC) tiene una validez mundial y hace referencia a los procesos del manejo de evidencias digitales para ser admisible en los procesos legales, para que su integridad no se vea afectada tiene que seguir los procesos de identificación, recolección, adquisición y preservación, y a su vez

tener relevancia, ser confiable y tener suficiencia son elementos importantes en el análisis que definirá la calidad de un informe de resultados, esta norma también aclara que es exclusiva para datos digitales y no para la conversión de información a formato digital.

En la figura 1 específica los lineamientos de control del ISO 27037 para las evidencias digitales, el cual solo cubre el proceso inicial del análisis forense, y subsecuente al proceso de control es la norma ISO 27042 que trata sobre las directrices del análisis e interpretación de la evidencia digital (Coronel et al., 2020).

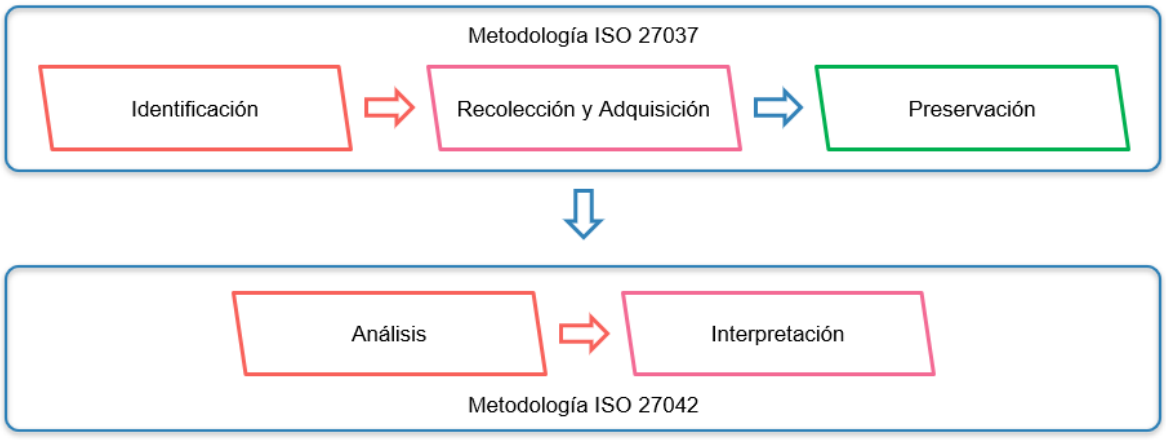


Figura 1. Fases ISO.

Identificación

El primer proceso del análisis forense es la identificación de los elementos digitales, lo cual implica las fases de la indagación, descubrimiento y la documentación.

Identificar la información para la evidencia digital es un proceso complejo dado los factores del entorno, revisar los diversos elementos de almacenamiento es el primer proceso, posteriormente se debe identificar el lugar virtual del almacenamiento, dadas las capacidades de almacenamiento este proceso puede requerir más atención, aunque en ocasiones puede ser muy específica y no requiere de una búsqueda exhaustiva.

Recolectar y adquirir

El proceso de recolectar es el acto de tomar físicamente el dispositivo de almacenamiento o prueba que pueda contener la información de estudio, mientras que adquirir se refiere al procedimiento subsecuente de identificar la información ubicada en el dispositivo de almacenamiento y se genera una copia de seguridad, la cual debe ser creada al mismo tiempo de la adquisición, este proceso es independiente del medio y ubicación de la información, esta copia debe realizarse mediante un estricto proceso y documentado en todo momento, cumpliendo mecanismos de seguridad e integridad con el fin de asegurar que no sufra modificaciones en el proceso, por lo cual este proceso es complejo y crítico.

Preservación

La evidencia digital debe ser preservada, por lo cual la normativa 27037 establece que la conservación es el proceso salvaguardar la información, al igual que su integridad y sin modificaciones, este complicado desarrollo es parte importante, ya que en el análisis en un juicio legal no se puede definir el tiempo de espera y es importante evitar la manipulación o alteración alguna. Los requerimientos generales que debe cumplir son: los mismos principios de auditoría, ser repetible, reproducible y justificable:

Auditable: Debe ser capaz de cumplir con una posible evaluación de cada actividad por las partes involucradas, y al igual que cada paso es indispensable la correcta documentación con cada una de las medidas adoptadas, siempre respondiendo el por qué y cómo en cada criterio.

Repetible: Los mecanismos deben tener la capacidad de ser repetibles en cualquier momento y arrojando los mismos resultados de la prueba original, siempre que sean ejecutados en las mismas condiciones, las cuales se establecen utilizando el mismo procedimiento e instrumentos.

Reproducible: Esto significa que se deben obtener los mismos resultados aun cuando se produce otro tipo de estudio y los instrumentos sean diferentes, es decir, la aplicación de diversos instrumentos y diferentes condiciones arrojara el mismo resultado, esto significa que puede ser reproducible en cualquier momento.

Justificable: El especialista o perito debe ser capaz de mencionar todos los procedimientos y métodos utilizados descritos.

El ISO 27042 establece el examen y sentido de la evidencia digital, para su continuidad y la validez en los procedimientos de análisis forense y su interpretación, es una guía para el desarrollo del cómputo forense de tal modo que las directrices del perito sean admisibles en la presentación en un juicio, el análisis de los datos corresponde a la métodos y técnicas jurídicamente admisibles, mediante una completa documentación de los hallazgos, estudio y procesos realizados, mientras que la interpretación es el informe final de los resultados evidenciados de la investigación.

La ISO/IEC aclara que el seguimiento de sus procesos no sustituye el procedimiento que las jurisdicciones determinen, sino que es presentado como una guía práctica para un especialista en evidencia digital con la finalidad de: establecer cuál es la evidencia, todo lo referente en el manejo de la evidencia, lo que se realizó y finalmente los resultados (ciberseguridad, 2020).

UNE71505 / 71506

España cuenta con un Sistema de Gestión de Evidencia Electrónica (SGEE) llamado UNE71505 (Truchado, 2019), sirve para definir y describir la conceptualización de la información para evidencias electrónicas en un SGSI utilizado previo a un desarrollo, la UNE 71505 define la metodología para realizar un análisis forense con validez jurídica, bajo un sistema de SGEE y un sistema de gestión de seguridad de la información, la cual consta de la revisión de principios generales, prácticas en la diligencia de evidencias y la comprobación de los

formatos y los mecanismos. Los objetivos de la norma son describir y definir los conceptos, identificar las relaciones entre la gestión y la seguridad, y especificar sus controles.

La norma UNE71506 (Guzmán, 2023) es la continuación de la UNE71505 y define toda la metodología para llevar a cabo y presentar un análisis forense, tiene como objetivo el aseguramiento de pruebas electrónicas, su finalidad es seguir el proceso durante el ciclo de vida de las evidencias: preservación, adquisición documentación, análisis y presentación de resultados. Su cumplimiento no representa la validez de certificación de laboratorios forenses, sino que son pautas aplicables en el desarrollo de las actividades periciales como proceso metodológico.
El Sistema de Gestión de Evidencia Electrónica UNE 71505 cumple con los atributos de:

• Autenticación e integridad: refiere a que la evidencia no cambia en el proceso de estudio y manipulación, tanto en contenido, propiedades, características, es decir la información no sufrirá ningún cambio en algún momento.

• Disponibilidad y completitud: garantiza el acceso a la información y la bitácora de cada proceso.

• Calidad y gestión: En cuanto a la calidad de información trata de los procesos técnicos realizados bajo un cuidado minucioso, en el manejo describe la documentación detallada de cada etapa y en la preservación sobre la presentación de la información documental de los resultados, mientras que la gestión menciona los procesos establecidos y verificados previamente al estudio realizado susceptible a ser auditado.

La norma UNE71506, al igual que el ISO 27042, se refiere al proceso de informática forense, específicamente el proceso de gestión, las fases de la norma se pueden observar en la figura 2.

Figura 2. Fases UNE 71506.

Preservación: es la validez y confiabilidad del repertorio de los datos en estudio, así como determinar los aspectos de los entornos físicos que puedan afectar a la evidencia desde el inicio hasta el final del proceso.

Adquisición: garantizar la generación de una copia fiel del original.

Documentación: se realiza una documentación secuencial desde el inicio del análisis hasta el término del informe, detallando cada aspecto incluyendo las herramientas utilizadas en el manejo de las evidencias.

Análisis: son los procesos técnicos realizados durante la recuperación y estudio.

Presentación: proceso final, es el informe detallado en un lenguaje comprensible.

RFC3227

El lineamiento RFC 3227 de Brezinski (2002) es un conjunto de recomendaciones técnicas que sirven como guía en la recopilación de archivos de evidencias relevantes para efectos de seguridad en casos de enjuiciamientos, las directrices tienen el objetivo de ayudar a los peritos en realizar los procesos de recopilación y almacenamiento de las pruebas digitales en materia pericial, el proceso a seguir es:

- Incluir al personal legal y de seguridad necesarios.
- Crear imagen de los medios de análisis desde su mínimo nivel (copia exacta).
- Para evitar supuestos se debe trabajar sobre los medios originales.

- Realizar un registro detallado de la intrusión.
- Registro con fechas y horas.
- Evitar realizar modificación de archivos y registros originales.
- Priorizar la recuperación antes que un análisis y priorizar en la información volátil.
- No apagar el equipo hasta que se analice y recopile las evidencias volátiles.
- Todo proceso debe probarse para garantizar su validez.
- Ser metódico en los procesos.

Y los principios a tomar en cuenta en esta política son:

Recolección: proceso de la recolección en virtud de la volatilidad de las evidencias digitales, dando prioridad en la memoria caché y finalizando en los dispositivos de almacenamiento digital.

Valorar posibilidades: tener en cuenta el riego de la destrucción de evidencias, evitar apagar el equipo, elección adecuada de las herramientas de respaldo que no altere la información original.

Privacidad: tener en cuenta las normas legales, políticas empresariales, información sensible, en caso de existir dudas es recomendable realizar una consulta jurídica.

Consideraciones: determinar si las evidencias pueden ser admisibles en un juicio y a su vez tener la consideración de su autenticidad y aspectos que ayuden a que un juez les tome importancia.

El RFC3227 está enfocado para que los administradores de sistemas obtengan las bases en las políticas de seguridad y considere la correcta documentación ante un incidente, con el fin de seguir una cadena de custodia adecuada. Este lineamiento indica recomendaciones en el proceso de recopilación, realizado de la forma más

detallada posible y precisando cada toma de decisiones durante el procedimiento de recolección de las evidencias.

Una clara metodología en la recopilación, su transparencia y reproducibilidad, la cual establece:

- Documentar las evidencias.
- Determinar la relevancia entre lo admisible o no en un juicio, tener en cuenta que la falta de evidencia es perjudicial, al contrario que la innecesaria solo alarga la documentación.
- Determinar el orden de recuperación de evidencias.
- Aislar el sistema en cuestión.
- Realizar el proceso de respaldo con las herramientas seleccionadas.
- Revisión y depuración de la evidencia.
- Realizar una documentación en todo momento, bitácora de actividades.
- Identificar personal involucrado en el proceso de recopilación.

Es recomendable realizar una documentación con firma digital, con el fin de comprobar la autenticidad de los datos y que no han sido alterados, el aseguramiento digital y la documentación de la cadena de custodia debe ser realizada contestando las preguntas de “Cómo”, ”Dónde”, ”Cuándo”, “Qué”, “Quién” o cualquier pregunta relacionada con el hecho, siguiendo siempre el proceso de selección de la herramienta adecuada con la cual se realizará la copia para su análisis y finalmente la entrega de resultados.

IOCE

Internacionalmente la informática forense también fue regida por la Organización Internacional de Prueba Informática (IOCE) establecida en 1995 y creada para dar cumplimiento a la ley, fue conformada por agencias gubernamentales las cuales desarrollaron una guía para las buenas prácticas en la elaboración de la prueba electrónica, en la cual se establecieron las siguientes fases:

- Recolectar evidencia.
- Verificar la evidencia recolectada.
- Analizar la información sin alterar ningún aspecto.
- Realizar un reporte.

Y su estructura podría resumirse en los siguientes atributos:

- Coherencia para el sistema legal.
- Lenguaje estandarizado.
- Durabilidad.
- Alcances internacionales.
- Integridad de las evidencias.
- Verificable (comparación teórica y metódica).
- Una estandarización aplicable en todos los niveles.

Los principios de la IOCE tenían la finalidad que todas las practicas, técnicas, herramientas y capacitación crearan una computación forense con un acuerdo y una validez internacional, pero estos planes de acción fueron terminados con su disolución en el año 2015 (FBI, 2000).

Normativa Mexicana NMX-I-289-NYCE-2016

La Normativa Mexicana NMX-I-289-NYCE-2016 es un lineamiento fundamentado en la Ley Orgánica de la Administración Pública Federal, la cual pretende dar solución a la problemática que los sectores productivos, sociales y políticos han sufrido con el uso de las TIC, específicamente en la protección de información contra ataques a los sistemas informáticos, lo que implica el uso de técnicas, procedimientos y políticas, en este caso los mecanismos de protección y de seguridad en los dispositivos catalogados como medios digitales ya que en ellos se

almacena grandes cantidades de información personal, financiera y de trabajo (DOF, 2016).

El daño de la información en el sentido de la ciberseguridad se ha convertido en una prioridad para el gobierno mexicano, por lo cual la normativa es una solución para mitigar los ataques en la integridad y disponibilidad de la información, así como de crear un marco en la legislación para fortalecer la ciberseguridad, por la falta de definición de los delitos informáticos y que no existen legislaciones específicas, se crea un modelo que permita fortalecer los procesos del estado mexicano en la impartición de justicia.

El objetivo de la normativa en el manejo de la evidencia tiene como fin garantizar su uso como material probatorio, mediante actividades de control y manejo que cumplan con una metodología establecida en el procesamiento, control, análisis y manejo de contenido en dispositivos digitales.

Los dispositivos digitales tomados en consideración son:

- Memorias USB.
- Reproductores de audio.
- Relojes inteligentes.
- Cámaras fotográficas.
- Dispositivos de vigilancia.
- Tarjetas de memoria.
- Teléfonos inteligentes.
- Unidades de rastreo.
- Dispositivos de seguridad de red.
- Unidades de almacenamiento masivo.

La preservación de evidencia refiere al traslado y entrega de dispositivos a las autoridades de seguridad pública o competentes, aseguramiento de evento y procesamiento del traslado, realizando un informe o dictamen previo.

La cadena de custodia es el sistema de control aplicado en el procesamiento de evidencia, desde el hecho suscitado hasta la investigación del incidente, la cual menciona en el incidente o hecho: identificar, proteger, detectar, responder y recuperar, en la obtención de la evidencia explica la aportación de evidencia como localización y descubrimiento, para finalmente preservar, procesar, trasladar, analizar, almacenar y presentar la evidencia. Cada uno de los protocolos mencionados están basados en el proceso de cadena de custodia y la Cadena de Custodia Guía Nacional (2015), por lo que la normativa es una adaptación para el análisis de evidencia digital.

Cadena de custodia

La correcta recopilación manejo y análisis de información digital por si solas no necesariamente se dará como probatoria en los procesos jurídico-penales para los que tenga lugar, el procedimiento y la evidencia de un especialista puede estar en duda por un juez, por ello la importancia de cumplir una cadena de custodia. Para efectos en esta investigación y basándose en los principios normativos de la Cadena de Custodia Guía Nacional (2015), se puede resumir que la evidencia debe pasar por los siguientes procesos:

- Identificación y aseguramiento.
- Extracción o recolección.
- Preservación.
- Documentación.

Identificar los elementos de estudio y el aseguramiento de la evidencia digital es primordial en el proceso probatorio de un delito informático, en esta atapa se determina cuales elementos son objeto de estudio y pueden ser utilizados en el proceso legal, establecidos los componentes, el desarrollo de la extracción y recolección debe realizarse bajo un adecuado procedimiento, una buena práctica es bajo una copia sin que la creación de la misma altere la información o datos originales, es muy importante la integridad de los datos ya que puede la información puede ser susceptible a una segunda validación y en algunos caso de una tercera revisión, el no tener una preservación integra de este proceso puede llevar a invalidar toda la investigación.

La valoración de las evidencias puede estar en duda ante un juez, por ello, el proceso y como fue realizada una investigación hasta llegar a las conclusiones, incluyendo la cadena de custodia, es base primordial como sustento de validez en un juicio al dictaminar una opinión objetiva, técnica y científica del delito en cuestión por un perito calificado, en conjunto el proceso de técnicas sistematizadas y analíticas darán la veracidad que se busca cumplir y demostrar que lo realizado se encuentra bajo una estandarización de procedimientos al igual que las normas reconocidas mundialmente (Brito y Muñoz, 2023).

Perito

Es un especialista calificado con conocimientos comprobables y experiencia en la ciencia, arte, profesión, técnica, oficio, o industria con el fin de rendir un dictamen para dilucidar a un juez en los procesos jurídicos por la falta de experiencia o conocimiento de la materia, aun cuando la tuviera. En un juicio pueden participar varios especialistas: los peritos de parte que son designados libremente por el demandante o por la defensa (cada parte puede o no, presentar su propio perito), mientras que el perito judicial es designado por el juzgado para dar su punto de vista, por lo general sucede cuando existen puntos de vista encontrados por los peritos de parte, este tercer perito es llamado tercero en discordia y su dictamen es

imparcial, al contrario que los de parte, los cuales son parciales y su inclinación es hacia el cliente que les pagará (Vázquez, 2022b).

Los requisitos de la Secretaria de Gobernación (Diario Oficial de la Federación [DOF], 2021) establecen que los peritos judiciales deben contar con los conocimientos demostrables por medio de constancias que lo acrediten en la especialidad que desean procesar, un mínimo de 5 años de experiencia, no contar con antecedentes o sanciones por el poder judicial, no ser servidores públicos y sujetarse a todas las normas establecidas por la Judicatura Federal (DOF, 2021), mientras que los requisitos para realizar funciones como perito de parte es comprobar su experiencia en la ciencia a desarrollarse por medio de algún documento que certifique o acredite la profesión, tal como lo describen los artículos referentes y establecidos como derecho en el CFPP (2016) Art. 223, en el CNPP (2021) Art. 368 , también en la Ley Federal del Trabajo (2022) Art. 822, en la Ley de Amparo (2021) Art. 120 y en el Código Nacional de Procedimientos Civiles y Familiares Art. 300 (CNPCF, 2023).

Perito Informático

Su trabajo es realizar una peritación bajo su formación y experiencia en ciencias de la computación o una ciencia relacionada con las tecnologías de información, su función es la elaboración de un informe y exponer su punto de vista profesional ante un juez. Un perito informático judicial es imparcial y debe estudiar las periciales presentadas, si las hay, o estudiar los acontecimientos y evidencias para rendir su dictamen, mientras que un perito informático de parte, más allá de realizar su reporte procesal debe preparar a los abogados ya que al igual que el juez, no están familiarizados y no cuentan con los conocimientos técnicos para entender todos los acontecimientos desde un punto de vista científico, el experto en tecnologías a su vez debe tener el asesoramiento jurídico del abogado, ya que en conjunto evalúan y analizan el proceso judicial para una pericial, o en caso contrario, la elaboración de una contra pericial para tratar de rebatir la validez de la entregada por el demandante (Torres, 2020).

El Informe Pericial

El informe pericial consta de un razonamiento experto y debe explicar claramente los métodos y técnicas que dieron las conclusiones presentadas, y no sobre inducciones o deducciones meramente, como lo menciona Vázquez (2022b) en el Manual de Prueba Pericial. Un informe pericial debe de contestar las preguntas realizadas por la parte demandante y demandada, la parte activa del proceso plantea originalmente unas preguntas en su demanda y posteriormente la parte pasiva debe realizar el mismo proceso, es normal que el primer abogado se apoye en el perito para elaborar las cuestiones a versar, así mismo, el segundo abogado consultará a su perito de parte para contestar la demanda y agregar las preguntas necesarias para fortalecer, aclarar o comprobar aspectos que le favorezcan en el proceso del juicio, realizado este proceso la parte actora realiza la contestación de todos los cuestionamientos de las partes de la acción judicial establecida y posteriormente la contraparte puede realizar un análisis de lo expresado y procede a contestar todas las preguntas en la contra pericial, con la ventaja de expresar más allá reafirmando, refutando o comprobando aspectos que le favorezcan a su representado, siempre bajo la ética de decir la verdad.

En México en el CNPP (2021) Art. 228, así como en España o Colombia, se establece que se debe llevar a cabo el procedimiento de la cadena de custodia, esta práctica se realiza durante el proceso de la demanda (Torres, 2020), esto servirá como base para en el futuro próximo realizar la pericial, ya que se debe desempeñar un análisis exhaustivo de todo lo sucedido para contestar los cuestionamientos, además que se deben establecer cuáles fueron los trabajos técnicos, reglas, documentación y estudios que fueron realizados para soportar y contestar cada una de las respuestas a las preguntas como requisito indispensable del informe.

Vázquez (2022b) afirma en su Manual de Prueba Pericial que no existe un formato destinado para la presentación de un informe y mucho menos para los sistemas jurídicos existentes, sin embargo, menciona que todo dictamen debe contener todos

los detalles que van desde las premisas menores a la premisa mayor para así llegar a las conclusiones, por medio de una analogía experta dese la generalización de los hechos por medio del razonamiento dado por las métodos y teorías utilizadas, sin caer en un fundamento inductivo y basándose en un razonamiento deductivo con premisas verdaderas y conclusiones realizadas por una serie de principios, además recalca que el informe debe contener todos los generales relevantes del caso, fundamentos, hechos, inferencias y conclusiones.

En España la Ley de Enjuiciamiento Civil (Boletín Oficial del Estado, 2000), en sus artículos del 335 al 352 establece el derecho de nombramiento de un perito si cumple con los conocimientos científicos o prácticos y título oficial para desempeñar la función, y estipula que la entrega y la secuencia para la pericia científica se debe realizar bajo el concepto de la sana critica. En materia penal define que el trabajo del perito se realizará bajo las reglas de la lógica, la razón y de la experiencia, debe contar con un análisis, recolección de datos o elementos, una metodología, una evaluación de resultados y por ultimo las conclusiones, este proceso servirá como asesoramiento a los magistrados en aspectos especializados que los ayudaran a esclarecer aspectos de un tema en específico, pero sin eximir al juez de sujetarse a las conclusiones del perito (Benfeld, 2020a).

El código General del Proceso en Colombia en su artículo 226 (Leyes.co, 2021) menciona que la prueba pericial es necesaria para verificar los hechos en un proceso que requieran de conocimientos científicos, esta será realizada por un perito que demostrará su conocimiento acreditándolo por medio de documentación y bajo un juramento de ética e imparcialidad, debe de ser un dictamen claro, preciso, exhaustivo y detallado, y contener los datos de quien lo realiza o participo, sus credenciales, publicaciones realizadas, casos en los que ha participado, si ha realizado intervenciones en proceso de la misma parte, declarar variaciones de los métodos o técnicas realizados en otras periciales y justificar el porqué de la variación, además adjuntará toda la documentación e información utilizada para la realización del dictamen.

Derecho informático

El derecho informático trata de una normativa Jurídica relacionada con la tecnología, es decir, las reglas de comportamiento de acuerdo con la ley, derechos y obligaciones, los cuales nos solo integran los delitos informáticos, sino que van más lejos, incluyendo la información sensible de una empresa o una persona física, mejor conocida como la protección de datos personales, y puede proseguir con los derechos intelectuales y otra información personal, como puede ser la intimidad y privacidad, uso de imágenes, videos u otros. Las leyes han sido modificadas en los últimos años y estipulan esta protección, así como su incumplimiento el cual conlleva a sanciones que pueden ser económicas o penales (INFOCDMX,2021).

Mas allá de las leyes del Instituto Nacional de Transparencia Acceso a la información y Protección de Datos Personales (INAI), se deben reforzar las legislaciones, en ello recae el derecho informático y las regulaciones que indirectamente las leyes protegen, donde las reglas y derechos los puede determinar un juez, al no existir connotaciones para todos los sucesos que puedan suscitarse.

Puede tomarse la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (DOF, 2010) como base, en ella se establecen las normativas en el manejo de la información personal y establece que toda acción no contemplada por esta ley será a disposición del Código Federal de Procedimientos Civiles y Familiares (CNPCF, 2023) y de la Ley Federal de Procedimientos Administrativos, así como la Reformación del Código Penal Federal en los artículos 14,16,21 y 73 de la constitución se reformaron para garantizan la seguridad informática, dictaminando la seguridad y protección de la información y su almacenamiento, así como los recursos y procedimientos del manejo por usuarios, recuperación ante desastres y el incumplimiento de las buenas prácticas, para estos fines la principal es el artículo 211 bis 1 el cual establece el acceso ilícito a sistemas y equipos de

informática, el cual describe como delito el acceso sin autorización modifique, destruya o provoque pérdida de información (SENADO, 2007).

Estado del arte

La revisión de los antecedentes demuestra la falta de investigación en México, dando como resultado un bajo contenido o aporte por las instituciones gubernamentales en materia pericial informática, actualmente este tema está poco explorado, el Manual de Prueba Pericial de Carmen Vázquez (2022b) de la Suprema Corte de Justicia de la Nación, aporta los temas sobre el deber de peritos y jueces, la valoración del informe, aspectos legales y su alcance, dejando sesgos importantes en el deber y ser de un perito, mencionando estándares y protocolos, pero el estudio no denota el sentido de como dirigir una pericial. Partiendo de más información en el estudio de las leyes respecto al tema en los artículos del CNPP, CFPP, Ley Federal del Trabajo (LFT, 2022), Ley de Amparo (2021) y la CNPCF, tienen una similitud en sus cláusulas, sin embargo, es incierto en la sistematización a partir del ordenamiento para la reconstrucción de los procesos jurídicos en materia pericial y más en la forma de actuar de los expertos al emitir su informe y rendir declaratoria.

Las recientes investigaciones sobre la materia demuestran que la validación jurídica de una pericial requiere de un perfeccionamiento, Vázquez (2022b) bajo su panorama expresa que se requiere una profesionalización ya que los medios de las pruebas han evolucionado junto con los avances tecnológicos, proporcionando nuevas herramientas para delinquir, por lo que es necesario profesionales que funjan como testigo experto mediante un peritaje, el cual tenga un alcance con valor probatorio. La prueba digital queda en la experticia del profesional, quien deberá contar con los conocimientos, pero especifica que básicos, y continúa aludiendo que podría llegar a fallar.

De aquí se puede tomar como ejemplo el artículo 1390 Bis46 del Código de Comercio (2010) donde habla sobre la pericial, en este no exhibe un procedimental de elaboración, pero aclara que debe estar debidamente ofrecida, bien así, se toma el ejercicio de facultad de atracción, donde el juez inadmite la prueba pericial en la inspección judicial, ya que no existe una legitimación del perito en la ciencia sobre la cual versaría y no especifico su domicilio. Todo lo relativo del ejemplo recae en la reforma al artículo 1390 Bis46 (DOF, 2017), donde se modificó el articulo principal y se establecen los requisitos al ofrecer la prueba pericial y el desahogo en la audiencia de juicio, sobre la nueva modalidad oral.

Por todo lo anterior se puede determinar que existe un perfeccionamiento continuo en los sistemas jurídicos al supeditar las leyes y en la validación jurídica de un perito al cumplir o no con los requisitos necesarios para ejercer, además que es necesario revisar sus habilidades científicas, hecho que es dable solamente en conjunto al valorar su dictamen, rendir sus conclusiones y el desahogo verbal con la contestación de las preguntas por las partes y el juez, así el magistrado podría desvirtuar la pericial en la audiencia de juicio, tal como lo explica en sus conclusiones Vázquez (2022b), recalcando que las instituciones crear un mayor número de reformas y una jurisprudencia más estricta.

Colombia

La finalidad de una pericial informática es igual que en la mayoría de los países, lo que la hace diferente es el proceso que utiliza cada investigador, el contenido, requisitos de presentación y en general su calidad, en el caso de Colombia el Código General del Proceso (2023) en su artículo 226 establece los mismos requisitos del Código de Comercio mexicano en su art 1390 en la cuarta sección, pero a diferencia que los artículos mexicanos, en él se establece que debe cumplir con las características de claridad, precisión, relevancia y ser conciso, además deben describir la metodología, experimentos y toda la investigación realizada, características implícitas en cada pericial, algunos requisitos sobresalientes es

informar las publicaciones de artículos del perito en los últimos 10 años, así mismo listar las periciales realizadas en los últimos 4 años.

Dentro del marco jurídico el gobierno colombiano contempla la cadena de custodia con el fin de salvaguardar la información y la calidad de la pericial, por ello la creación de una normativa que contemple y regule los delitos informáticos, su ley 1273 (Gob.co, 2009) describe la protección de información y de los datos con el fin de tener reglas para prevenir lagunas o supuestos en el caso de hacer cumplir la justicia, donde realiza las modificaciones pertinentes con sucesos que no tenían contemplados, como accesos, obstaculizaciones, interceptación de datos, daño, entre otros, específicamente el artículo 269D referente al daño informático, se refiere a la destrucción o alteración, ya sea de forma parcial o total, artículos no establecidos en México, una investigación forense reciente realizada por Solano (2022), menciona que a pesar de la existencia de leyes en Colombia que integren a la prueba informática, debe de crearse una metodología e integrar buenas prácticas, continua con una propuesta, un proceso de cinco etapas para el análisis forense digital: evaluación, adquisición, examinación, análisis y reporte. Describe que el país no tiene establecido la manera de cómo se debe realizar la adquisición de datos y la forma de presentar la evidencia digital.

España

Como se menciona en el párrafo anterior, la manera de realizar las periciales y de sus normas varían en cada país, España es un país con regulaciones más completas y magistrados mayormente capacitados en la materia tiene el mismo objetivo, la convicción a un juez y proporcionar datos procesales que sus conocimientos no los llevan a deducir, por ello es importante aclarar que la prueba pericial en este caso, no aporta hechos nuevos, sino que debe versar sobre los existentes para convencer y probar que los hechos son ciertos o no, en caso de ser necesaria la creación de evidencia el perito debe de ser auxiliar del juez y bajo un proceso administrativo, en el cual los peritos de parte se convierten en auxiliares, lo

cual sería una pericial directamente proporcionada y no se realizaría informes periciales individuales.

Tornel (2020) con respecto a la ciberdelincuencia menciona que la ley regula la parte tecnológica en la administración de justicia en las normas españolas, pero aclara que las leyes no estipulan como llevar a cabo el proceso de la investigación, manejo de las pruebas o la elaboración de un dictamen pericial, agrega además, en el caso del manejo de información de dispositivos electrónicos, como lo son los discos duros o unidades de almacenamiento, está protegido por la Constitución Española (Senado España, 2022) en el artículo 18, donde protege su acceso por contener información personal, en este caso únicamente se podría acceder a la información bajo autorización de un juez, un claro ejemplo de los sesgos que tiene el país en la impartición de justicia.

III. CRITERIOS METODOLÓGICOS

Enfoque

Los fundamentos del criterio metodológico del presente trabajo se fundamentaron en una investigación de carácter mixto, ya que en las diferentes etapas del trabajo se realizaron métodos cualitativos y cuantitativos, en la parte cualitativa se utilizó un análisis documental para determinar los elementos de estudio y en la parte cuantitativa fue con el fin de evaluar las preferencias del panel de expertos, de tal modo que este proceso se trabajó de forma secuencial derivativa (Hernández-Sampieri y Mendoza, 2020).

El objetivo específico 1 tuvo un enfoque cualitativo, dado que se realizó un análisis documental, un estudio objetivo de los resultados de la muestra especifica, la revisión de material bibliográfico ayudó a identificar las principales características de las herramientas tecnológicas para la recuperación de datos, el propósito es generar los datos secundarios (Finol, 2020).

Para el objetivo específico 2 y basándose en las características obtenidas en el objetivo anterior, se eligió un enfoque cuantitativo dado que la información recolectada de las entrevistas del panel de expertos en la materia fueron datos estructurados que dieron como resultado información estadística, la cual fue la base para determinar las herramientas tecnológicas más utilizadas (Sánchez, 2019).

El objetivo específico 3 de la investigación tuvo un enfoque cualitativo, con un análisis documental dada la revisión de material bibliográfico cuyo fin fue identificar los lineamientos y metodologías de los estándares más utilizados a nivel mundial (Hernández-Sampieri y Mendoza, 2020).

En el último objetivo específico se realizó con un enfoque cualitativo por medio del análisis de resultados cuantitativos, la utilización del método Delphi para recabar la opinión de expertos periciales, abogados y un juez de la suprema corte, los cuales

arrojaron estimaciones como base para validar o anular la estrategia que se pretendía para mejorar los lineamientos y la presentación de informes periciales (Ng, J., 2018), en la figura 3 se pueden observar estas fases y etapas.

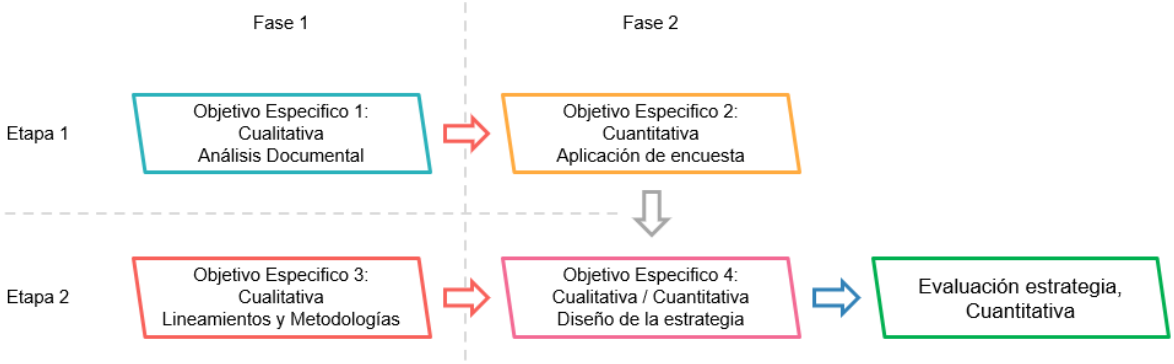


Figura 3. Fases del criterio metodológico.

Diseño de la investigación:

La orientación fue una investigación aplicada porque buscó generar conocimiento de forma sistemática, con un diseño no experimental por no manipular variables, transversal porque el estudio fue basado en situaciones existentes y particulares, y de tipo descriptivo ya que se cuantificaron resultados desde un punto de vista nuevo (Álvarez, 2020).

Método

El alcance de la investigación fue descriptivo, ya que su estudio tuvo la finalidad de trabajar con características específicas, tanto de herramientas, de lineamientos y de métodos. Como menciono Hernández-Sampieri (2020) los estudios descriptivos pueden ser la base de investigaciones correlacionales, en ese estudio el objetivo fue realizar la comparación y análisis para llegar a las conclusiones por medio de la encuesta, en el primer momento la recolección de información cualitativa se realizó con fines descriptivos y con base al análisis e interpretación de estos datos se prosiguió a la recolección de los datos cuantitativos por medio de la encuesta, la integración de ambos métodos fue crucial ya que los datos obtenidos eran necesarios para la construcción de la encuesta, en un segundo momento también

se realizó un análisis descriptivo de lineamientos y metodologías para el desarrollo de actividades, los resultados recogidos de ambas etapas se analizaron con el fin de realizar el diseño de una estrategia y finalmente poderla validar por el método Delphi, tal como lo muestra la figura 4.

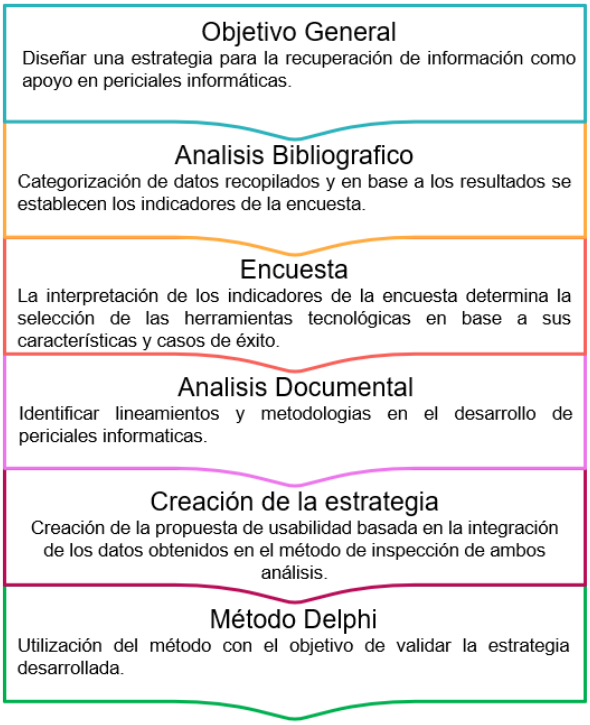


Figura 4. Metodología de los criterios metodológicos.

Población

La población de estudio fue conformada por el estudio de 13 herramientas obtenidas de una revisión bibliográfica, y en su segunda fase fueron encuestados 10 especialistas en recuperación de información dedicados al desarrollo de informes periciales, para la validación de la estrategia se utilizó la consulta de 9 abogados y un Juez de la Suprema Corte de Justicia, el panel de expertos fue seleccionado entre individuos con capacidades y conocimientos superiores, con el fin de clarificar y aportar conocimiento en base a la experiencia en la materia, la selección fue de forma objetiva pero por ser un tema poco explotado económicamente el criterio de selección es limitado y está basado en la disponibilidad y accesibilidad del panel,

el marco muestral se realizó por 10 encuestas enviadas por correo electrónico a los especialistas que han desarrollado procesos de recuperación a empresas, particulares y en desarrollo de periciales informáticas durante los años 2022-2023.

Objetivo específico 1

Identificar las principales características de las herramientas tecnológicas utilizadas para la recuperación de información en elementos de almacenamiento digital.

El propósito fue indicar las características o propiedades y componentes, la información producida por el conocimiento adquirido en la lectura. El método utilizado en este objetivo fue de tipo descriptivo dado que no existían variables, la investigación se realizó por instrumentos de recolección de datos y estudiados bajo criterios sistemáticos (Sabino, 1992), tal como lo describe la figura 5.

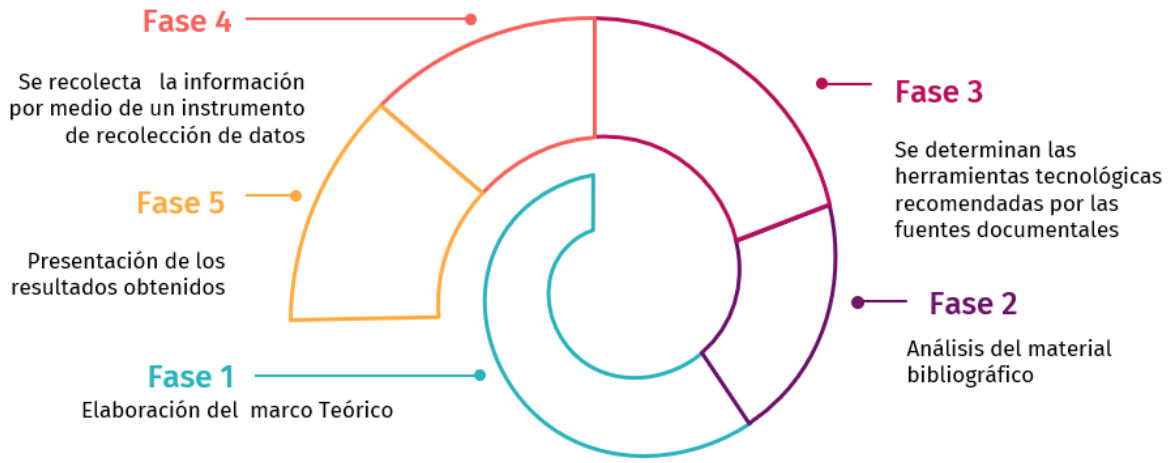


Figura 5. Metodología objetivo específico 1.

En el diagrama describen las fases del objetivo 1 donde:

Fase 1 es la recolección de información presentada para el marco teórico en la sección de herramientas tecnológicas.

Fase 2 refiere al análisis del material bibliográfico.
Fase 3 con base al análisis del material bibliográfico se detectan las herramientas más recomendadas por las fuentes citadas.
Fase 4 se determinan las características de cada herramienta tecnológica y se llena la tabla parametrizada.
Fase 5 se presentan los resultados obtenidos.

Objetivo Especifico 2

Comparar cuáles herramientas tecnológicas son las más utilizadas en los procesos de recuperación de información en elementos de almacenamiento digital.

Para determinar cuáles son las herramientas tecnológicas más utilizadas se realizó la implementación de un instrumento de recolección de datos, la técnica aplicada fue una encuesta y un análisis comparativo para definir cuales tenían una mayor efectividad en los casos de éxito de la recuperación de información, el muestreo fue no probabilístico ya que el tema de estudio no era muy amplio y la cantidad de encuestados fue limitada, por lo cual la muestra es finita (Cisneros-Caicedo et al., 2022).

La encuesta fue elaborada con los tópicos específicos a partir de las características descritas en los resultados del objetivo 1 y los datos obtenidos del cuestionario fueron basados en la experiencia de los profesionales con el fin de obtener datos cuantificables de forma rápida y eficaz, el análisis descriptivo es el método óptimo para el estudio de la información obtenida, las cuales estaban constituidas de preguntas cerradas, con el fin de recopilar todos los datos existentes (Hernández-Sampieri, 2020).

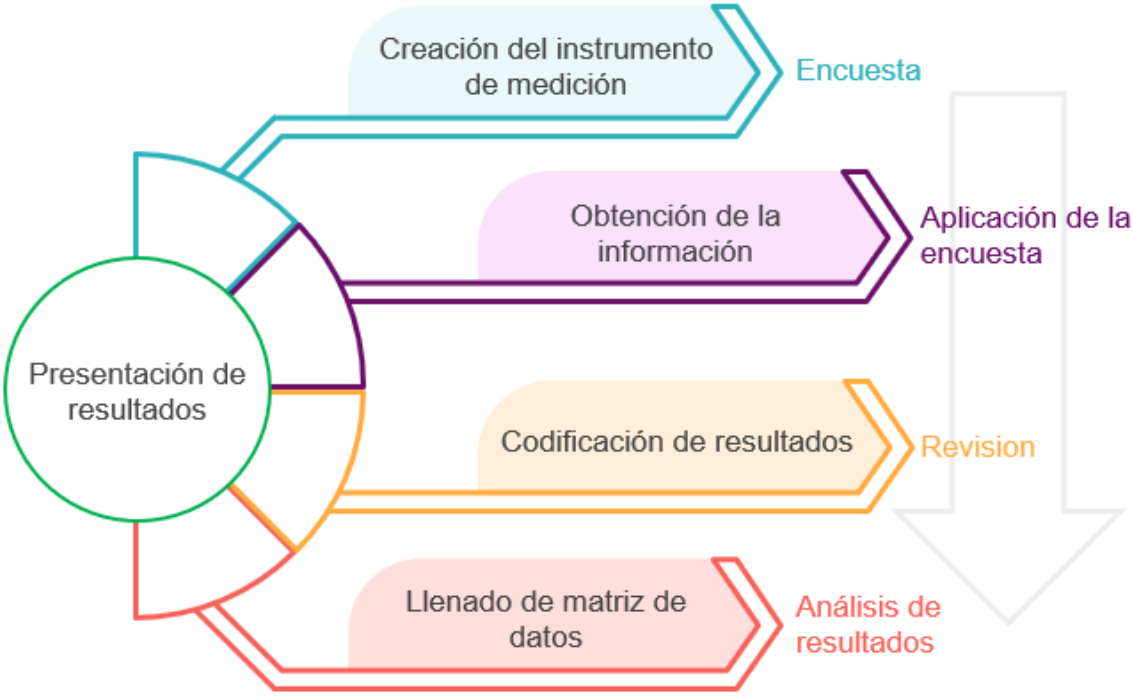


Figura 6. Metodología objetivo específico 2.

El diagrama de la figura 6 describe las fases del objetivo 2 donde:

Fase 1 creación del instrumento de medición, con base de los resultados obtenidos del objetivo 1.

Fase 2 la aplicación de la encuesta proporcionara los datos objeto de estudio, esta etapa pretende medir las herramientas enlistadas e identificar nuevas herramientas y características.

Fase 3 los resultados cuantitativos obtenidos en la encuesta son analizados con el objetivo de crear una matriz de datos, con la finalidad de utilizar los elementos de manera estadística.

Fase 4 se presentan los resultados obtenidos en tablas y gráficas para un mayor entendimiento.

Fase 5 basándose en los resultados se realiza la selección de la o las herramientas óptimas para realizar las funciones descritas.

Objetivo Especifico 3

Determinar los lineamientos y metodologías trascendentes para la elaboración de una pericial informática.

El método fue de tipo descriptivo por un análisis documental, ya que el propósito era indicar los lineamientos fundamentales adquiridos en la lectura y realizados por instrumentos de comparación, desglosando el contenido para realizar el análisis y comprensión profunda de las características, sintetizado de similitudes, patrones, diferencias, enfoques y aspectos más relevantes, generando la reconstrucción del contenido en función a las necesidades del enfoque de esta investigación, es decir una generación de nuevo conocimiento (Peña, 2022).

El objetivo fue identificar los mecanismos o ideas de cada material bibliográfico recabado y elaborar el cuadro comparativo con los elementos y características de las formas de realizar los procedimientos, lo que dio como resultado una organización y síntesis de elementos, esto ayudo a tener una mayor comprensión y beneficios en la creación de una nueva estructura y la integración entre los contenidos, el proceso de ese objetivo puede ser observado en la figura 7.

Figura 7. Metodología objetivo específico 3.

Objetivo Especifico 4

Diseñar una estrategia de recuperación de información con el uso de herramientas tecnológicas aplicadas en una pericial informática validada por el método Delphi.

Para lograr la validación de la estrategia se optó por utilizar el método Delphi, se seleccionó un panel de 10 expertos que determinaron la viabilidad de la propuesta metódica, con base al juicio del grupo se podría verificar su aplicación y visualizar elementos que pudieron ser excluidos en el proceso, de este modo ampliar el conocimiento y tomar mejores decisiones (Ramírez y Rúa, 2018). Las fases del método aplicado se pueden visualizar en la figura 8.

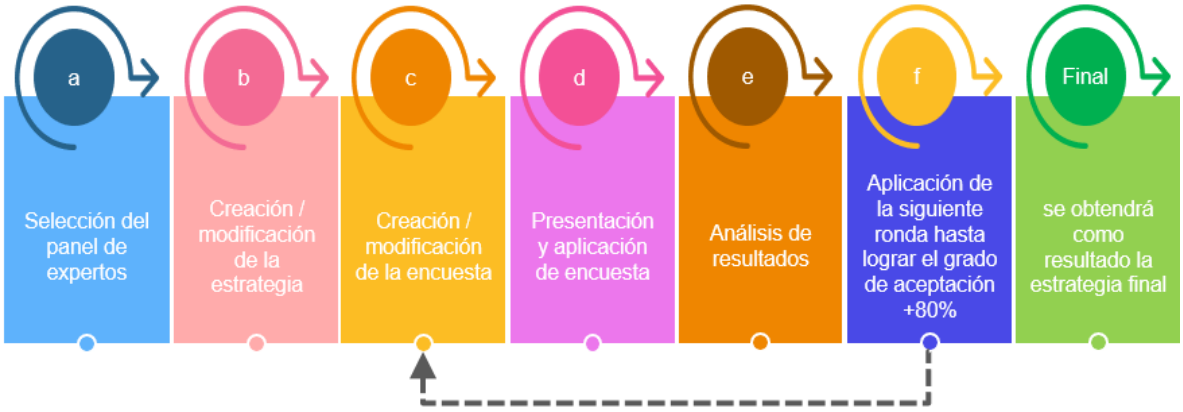


Figura 8. Metodología objetivo específico 4.

a) Selección de 10 especialistas en la recuperación de información, expertos en el desarrollo de periciales informáticas, abogados que han presentado periciales informáticas en los juicios y un Juez de la suprema corte de justicia.

b) Se realiza o modifica la estrategia desarrollada, especificando objetivos, criterios, métricas y el resultado pretendido

c) Creación o modificación de encuesta.

d) Se presenta la estrategia y la encuesta con la ponderación de los criterios considerados en la evaluación.

e) Se recopilaron los resultados y se realizó el análisis de los datos obtenidos de las encuestas.

- El análisis de resultados constó de dos etapas, el estudio del grado de aceptación de cada punto de la encuesta y de las recomendaciones del panel de expertos.
- Se utilizó el método Delphi como retroalimentación, esto ayudó a mejorar el modelo propuesto, de tal modo que las opiniones expresadas fueron un papel importante para mejorar la estrategia desarrollada.
- Se actualiza la propuesta desarrollada con las opiniones recolectadas.

f) Se realizó otra ronda de la encuesta, con la modificación del modelo propuesto y se repitió el proceso desde el inciso inmediato anterior hasta lograr el grado de satisfacción del panel de expertos.

Para fines de la investigación el grado de aceptación establecido debe superar el 80% en cada una de las dimensiones de estudio, por lo consiguiente el número de repeticiones está en función de la aprobación de los 10 especialistas, cuyas medidas seleccionadas son con base a los criterios de estabilidad del modelo Delphi propuestos por Landeta (1999) y donde se expresa que el tamaño óptimo de viabilidad de un panel debe oscilar entre 7 a 30 expertos como máximo, de tal modo que al concluir esas fases se podría obtener como resultado una estrategia final que será el objeto de propuesta en la tesis.

IV. RESULTADOS Y DISCUSIÓN

Los resultados y discusión de la investigación fueron separados por objetivos para su mejor comprensión, los cuales se presentan a continuación:

Resultados del Objetivo específico 1

Se realizo un estudio de las características que deben cumplir las herramientas tecnológicas diseñadas para la recuperación de datos, esto con el fin de ampliar el panorama de la investigación y dar soporte a la entrevista que fue eje en el objetivo 2, en la figura 9 se muestra el proceso realizado, un análisis de contenido específicamente para el estudio de cada uno de los programas, se obtuvo una matriz con las características peculiares que poseen las aplicaciones utilizadas para recuperar información de dispositivos de almacenamiento digital, el proceso fue :

- Se analizaron cada una de las herramientas tecnológicas.
- Se creó una tabla enlistando las herramientas tecnológicas.
- Se identificaron las características de cada una de las herramientas y se agregaron a la tabla.
- Se llenó la tabla verificando cuales herramientas cumplen con cada una de las características.
- Se presentó la matriz de análisis de contenido con los resultados obtenidos.

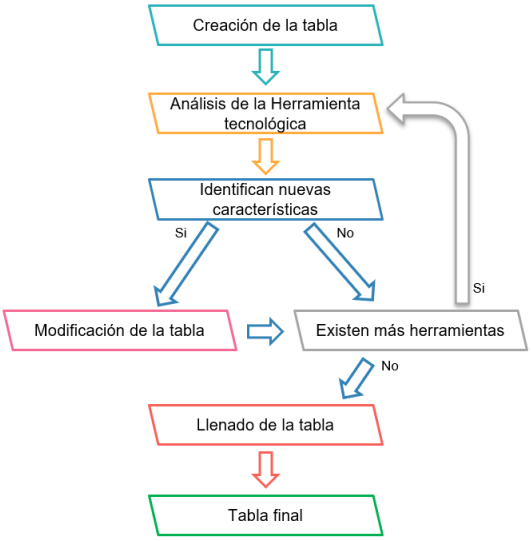


Figura 9. Análisis objetivo específico 1.

Los estudios fueron realizados teniendo en cuenta que se hizo una agrupación de las 16 herramientas, obteniendo una agrupación de 13 por las empresas creadoras, esto por las versiones de las utilerías que tiene su versión para Windows y Macintosh, en la tabla 1 se enlistan las 16 herramientas estudiadas y las 23 funcionalidades.

	Indicadores	Stellar Data Recovery	EASEUS	AnyRecover	OnTrack Easy Recover Kroll Ontrack Easy	Disk Drill CleverFiles Disk Drill Pro for Mac	Wondershare Recoverit Data Recovery	Minitool Power Data Recovery	DMDE	Wise Data Recovery	Prosoft Data Rescue for Mac	Alsoft DiskWarrior For Mac	Prosoft Data Rescue PC4	Recuva
LICENCIAMIENTO	Paga													
	Gratuita													
ALMACENAMIENTO	SSD													
	HD													

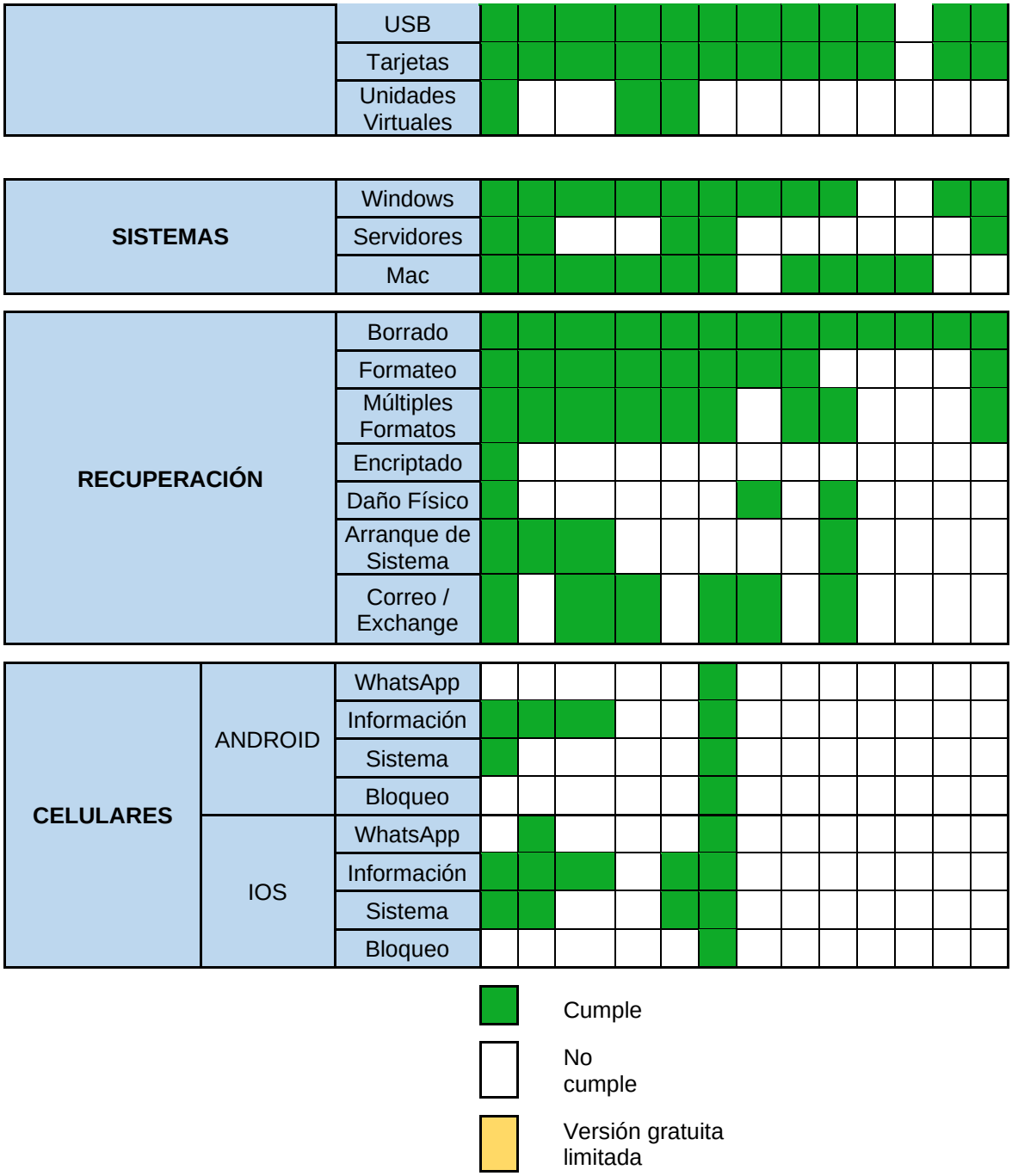


Tabla 1. Comparativo objetivo específico 1.

El análisis de la información obtenida de las páginas desarrolladoras arrojo el listado de las características con las cuales cumplen cada una de ellas, por lo cual podría asumirse que estas características son las que una herramienta de este tipo debe

de cumplir, la información obtenida muestra que la característica general es el recuperado de información borrada, y estas fueron agrupadas en:

Licenciamiento:

- Paga.
- Gratuita.

Almacenamiento:

- SSD (Unidad de Estado Solido).
- HD (Disco Duro).
- USB.
- Tarjetas (SD Tarjeta Digital Segura).
- Unidades Virtuales.

Sistemas:

- Windows.
- Servidores.
- Macintosh.

Recuperación:

- Borrado.
- Formateo.
- Múltiples Formatos.
- Encriptado.
- Daño Físico.
- Arranque de Sistema.
- Correo / Exchange.

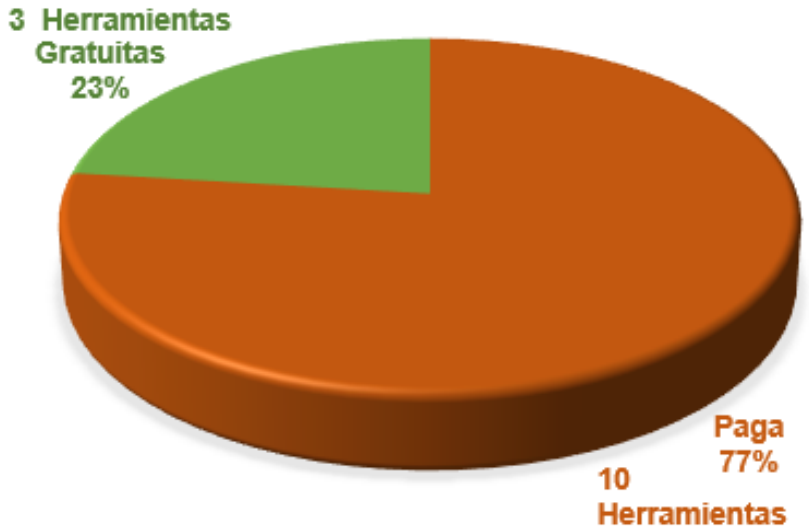
Celulares Android:

- WhatsApp.
- Información.
- Sistema.
- Bloqueo.

Celulares IOS:

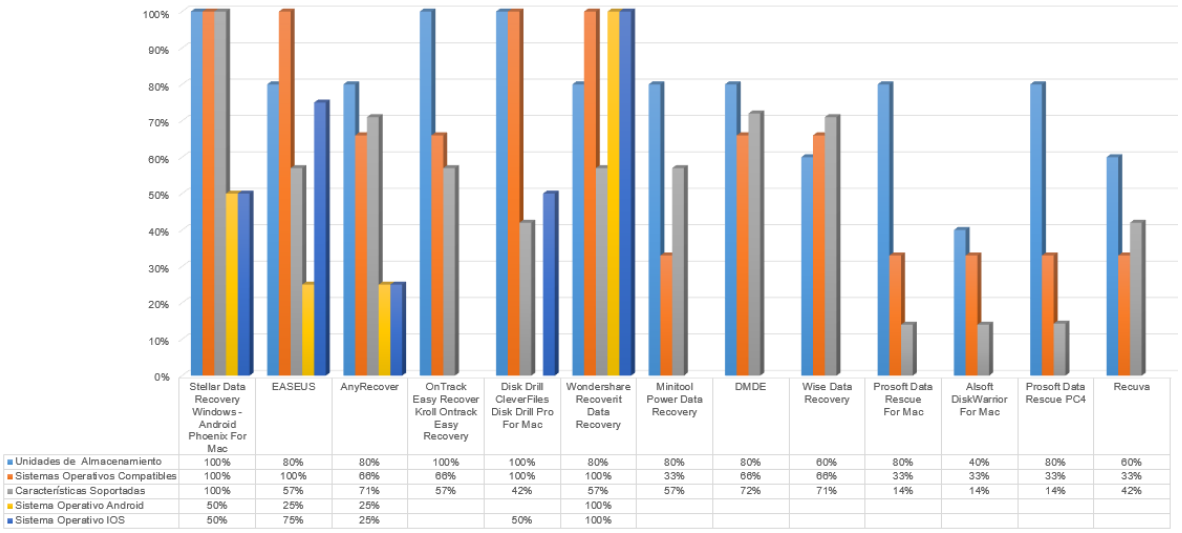
- WhatsApp.
- Información.
- Sistema.
- Bloqueo.

Además los resultados en este objetivo arrojaron que de las herramientas estudiadas el 23% son herramientas gratuitas y el restante 77% son de paga, como lo muestra la gráfica 1, de las cuales en 8 de ellas su funcionalidad depende del tipo de licenciamiento adquirido, consiguiendo deducir que existe mayor uso del software privativo y las características están en función de su costo, no obstante, las 2 herramientas con mayores indicadores, la misma cantidad 19 de 23, es una de costo y una gratuita, se puede deducir que el factor costo no es forzosamente una determinante para la elección de una utilería, por lo cual esta característica será excluida del objeto de estudio.



Gráfica 1. Comparativo licenciamiento.

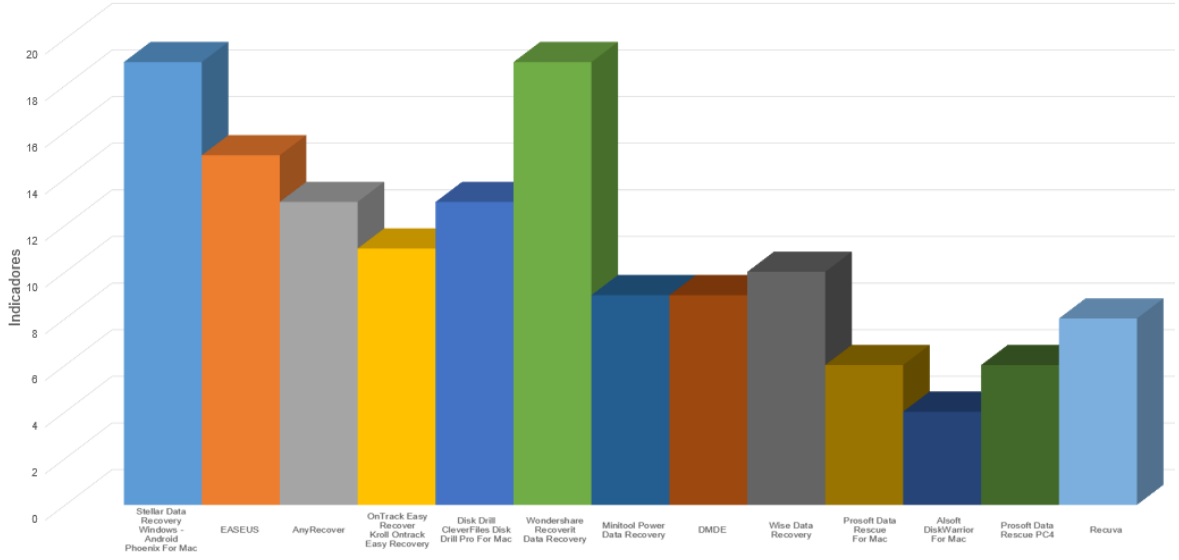
La gráfica 2 excluye la característica de licenciamiento y representa el porcentaje de las funcionalidades agrupadas que cumple cada una de las herramientas:



	Stellar Data Recovery Windows - Android Phoenix For Mac	EASEUS	AnyRecover	OnTrack Easy Recover Kroll Ontrack Easy Recovery	Disk Drill CleverFiles Disk Drill Pro For Mac	Wondershare Recoverit Data Recovery	Minitool Power Data Recovery	DMDE	Wise Data Recovery	Prosoft Data Rescue For Mac	Alsoft DiskWarrior For Mac	Prosoft Data Rescue PC4	Recuva
Unidades de Almacenamiento	100%	80%	80%	100%	100%	80%	80%	80%	60%	80%	40%	80%	60%
Sistemas Operativos Compatibles	100%	100%	66%	66%	100%	100%	33%	66%	66%	33%	33%	33%	33%
Características Soportadas	100%	57%	71%	57%	42%	57%	57%	72%	71%	14%	14%	14%	42%
Sistema Operativo Android	50%	25%	25%			100%							
Sistema Operativo IOS	50%	75%	25%		50%	100%							

Gráfica 2. Soporte funcionalidades por herramienta.

Al agrupar los indicadores por características se puede apreciar la funcionabilidad de cada una de las herramientas, tal como lo muestra la gráfica 3.



Gráfica 3. Funcionalidad general por herramienta.

El estudio anterior mostro una percepción sobre los elementos que deben cumplir las herramientas tecnológicas, así como una introducción a las herramientas

comúnmente utilizadas, estos parámetros fueron fuente para el instrumento de medición del objetivo número 2 donde la opinión de un panel de expertos determino la o las herramientas adecuadas para realizar un proceso de recuperación de información de dispositivos de almacenamiento digital.

Resultados del objetivo específico 2

Se realizo la aplicación del instrumento de medición a los participantes por medio de un formulario, la encuesta “herramientas para recuperación de datos” puede consultar en el anexo 2, así como la descripción de las nuevas herramientas detectadas en el anexo 3, la elaboración fue basada en la revisión del marco referencial de la presente investigación, cuyos indicadores fueron determinados en el objetivo anterior, los resultados de la encuesta arrojaron una diferencia de las herramientas tecnológicas objeto de estudio, dando un total de 11:

- Stellar Data Recovery Windows – Android Phoenix For Mac
- EASEUS
- AnyRecover
- OnTrack Easy Recover Kroll Ontrack Easy Recovery
- Disk Drill CleverFiles Disk Drill Pro For Mac
- Wondershare Recoverit - Data Recovery
- Wise Data Recovery
- GetDataBack
- SDRecovery
- Undelete 360
- Puran File Recovery

Las encuestas no proporcionaron nuevos elementos de evaluación, por lo que se utilizaron los mismos parámetros de estudio, la tabla 2 muestra los resultados de la encuesta.

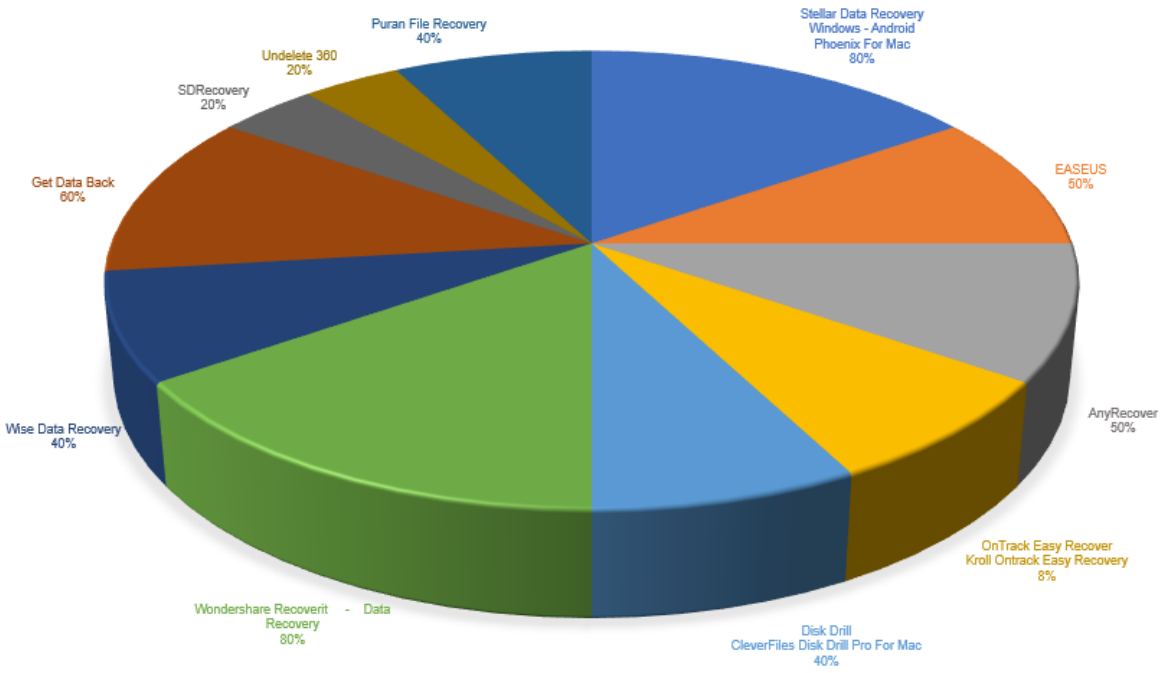
	LICEN-CIA		ALMACENAMIENTO					SISTEMAS			RECUPERACIÓN							CELULARES							
																		ANDROID				IOS			
	Paga	Gratuita	SSD	HD	USB	Tarjetas	Unidades Virtuales	Windows	Servidores	Mac	Borrado	Formateo	Múltiples Formatos	Encriptado	Daño Físico	Arranque de	Correo / Exchange	WhatsApp	Información	Sistema	Bloqueo	WhatsApp	Información	Sistema	Bloqueo
Stellar Data Recovery			8	8	8	5	1	8	1	6	8	8	5	1	5	4	2		4	1			5	5	
EASEUS			5	5	5	3		5	1	3	5	5	5			1			1			2	2	0	
AnyRecover			5	5	3	3		5		2	3	5	3			1	1		1				2		
OnTrack Easy Recover Kroll Ontrack Easy Recovery			4	3	2	2	0	4		0	3	2	3				0								
Disk Drill CleverFiles Disk Drill Pro For Mac			3	3	3	3	0	3	0	1	3	2	2										1	1	
Wondershare Recoverit Data Recovery			8	8	5	6		8	1	4	8	6	5				2	3	3	0	1	4	4	1	1
Wise Data Recovery			4	4	4	4		4		3	4		4		3	1	1								
GetDataBack			6	6	6	4		6	0		6	6	5		5										
SDRecovery			1	1	2	2		2			2		2												
Undelete 360			2	2	1	1		2			2														
Puran File Recovery			4	4	4	4		4			4														

Tabla 2. Resultados objetivo 2.

Por no haberse generado nuevos indicadores, los puntos de estudio fueron las funcionalidades mencionadas en el objetivo específico 1, además de ellos, se obtuvo una evaluación de calidad de cada software, en la tabla anterior se puede

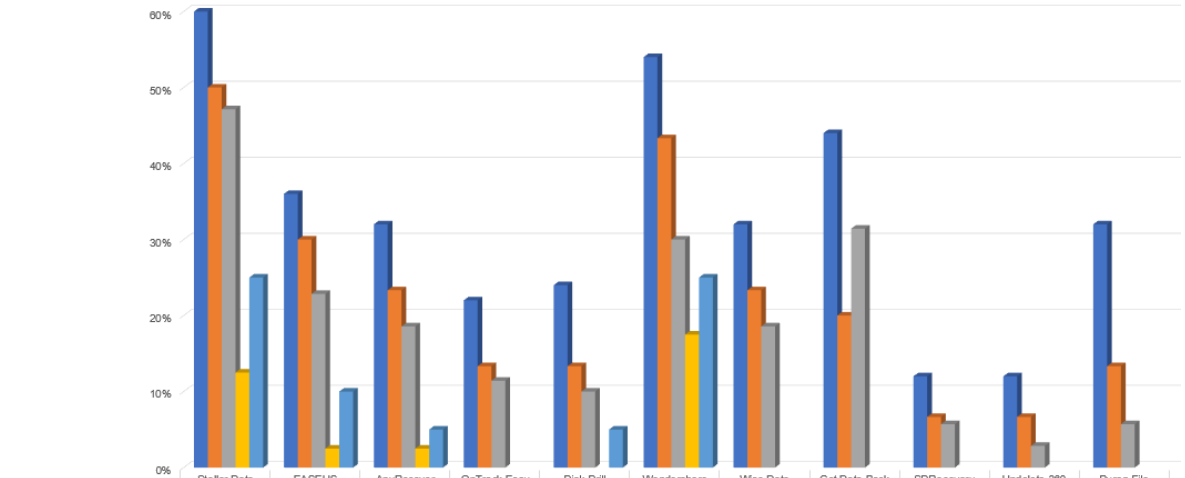
observar en verde el tipo de licenciamiento de la herramienta, en blanco las características o funcionalidades con las que cumple y el numero rojo la cantidad de población de estudio que utiliza dicha funcionalidad, mientras que en color gris son las características con las que no cumple la herramienta tecnológica.

El análisis estadístico como instrumento de medición muestra las preferencias de la usabilidad por herramienta, este resultado se muestra en la gráfica 4.



Gráfica 4. Usabilidad general por herramienta.

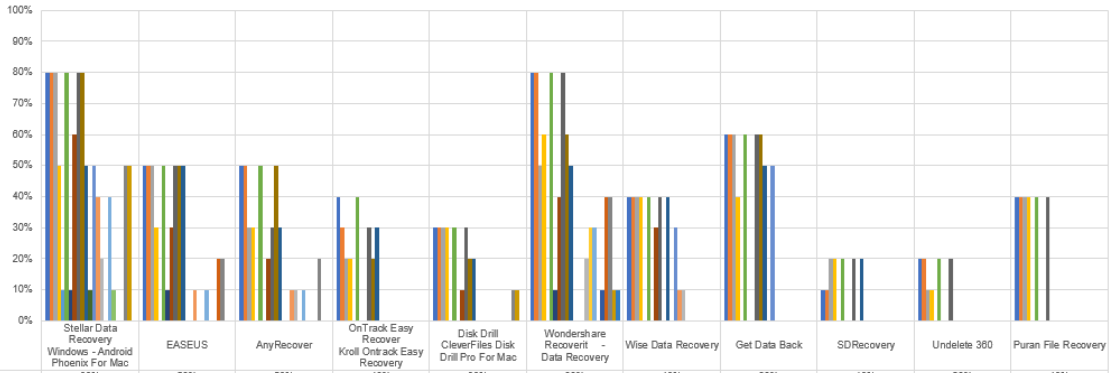
Los resultados porcentuales son el resultado de la agrupación por funcionalidades de las herramientas, en las cuales se realizó una observación de las preferencias del tipo recuperación para el cual se utilizan cada una de las ellas, estos datos pueden observarse en la gráfica 5.



	Stellar Data Recovery Windows - Android Phoenix For Mac	EASEUS	AnyRecover	OnTrack Easy Recover Kroll Ontrack Easy Recovery	Disk Drill CleverFiles Disk Drill Pro For Mac	Wondershare Recoverit - Data Recovery	Wise Data Recovery	Get Data Back	SDRecovery	Undelete 360	Puran File Recovery
Unidades de Almacenamiento	60%	36%	32%	22%	24%	54%	32%	44%	12%	12%	32%
Sistemas Operativos Compatibles	50%	30%	23%	13%	13%	43%	23%	20%	7%	7%	13%
Características Soportadas	47%	23%	19%	11%	10%	30%	19%	31%	6%	3%	6%
Sistema Operativo Android	13%	3%	3%			18%					
Sistema Operativo IOS	25%	10%	5%		5%	25%					

Gráfica 5. Selección por preferencias.

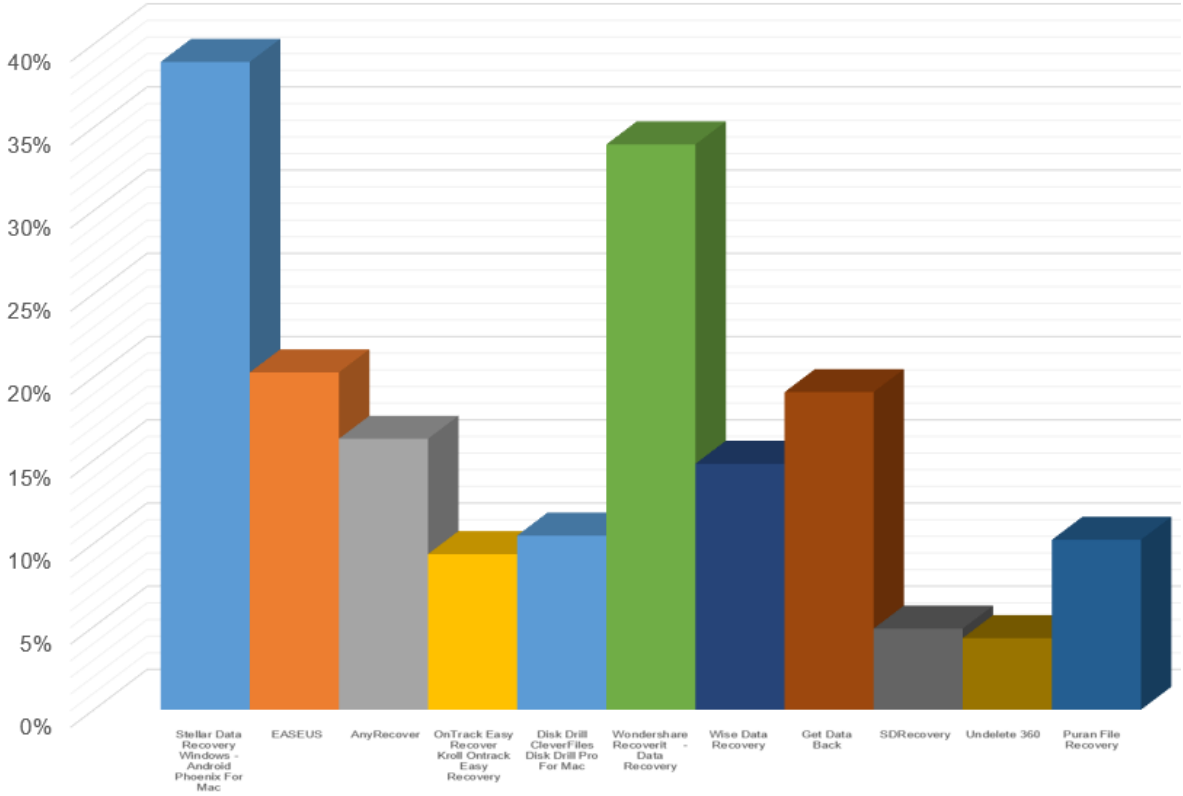
La gráfica 6 describe las características representas por el porcentaje con respecto al uso de las funcionalidades individuales que utilizan los expertos en cada una de las herramientas.



	Stellar Data Recovery Windows - Android Phoenix For Mac	EASEUS	AnyRecover	OnTrack Easy Recover Kroll Ontrack Easy Recovery	Disk Drill CleverFiles Disk Drill Pro For Mac	Wondershare Recoverit - Data Recovery	Wise Data Recovery	Get Data Back	SDRecovery	Undelete 360	Puran File Recovery
SSD	80%	50%	50%	40%	30%	80%	40%	60%	10%	20%	40%
HD	80%	50%	50%	30%	30%	80%	40%	60%	10%	20%	40%
USB	80%	50%	30%	20%	30%	50%	40%	60%	20%	10%	40%
Tarjetas	50%	30%	30%	20%	30%	60%	40%	40%	20%	10%	40%
Unidades Virtuales	10%										
Windows	80%	50%	50%	40%	30%	80%	40%	60%	20%	20%	40%
Servidores	10%	10%				10%					
Mac	60%	30%	20%	0%	10%	40%	30%				
Borrado	80%	50%	30%	30%	30%	80%	40%	60%	20%	20%	40%
Formateo	80%	50%	50%	20%	20%	60%		60%			
Múltiples Formatos	50%	50%	30%	30%	20%	50%	40%	50%	20%		
Encriptado	10%										
Daño Físico	50%						30%	50%			
Arranque de Sistema	40%	10%	10%				10%				
Correo / Exchange	20%		10%			20%	10%				
WhatsApp						30%					
Información	40%	10%	10%			30%					
Sistema	10%										
Bloqueo						10%					
WhatsApp		20%				40%					
Información	50%	20%	20%		10%	40%					
Sistema	50%				10%	10%					
Bloqueo						10%					

Gráfica 6. Resultados uso herramienta.

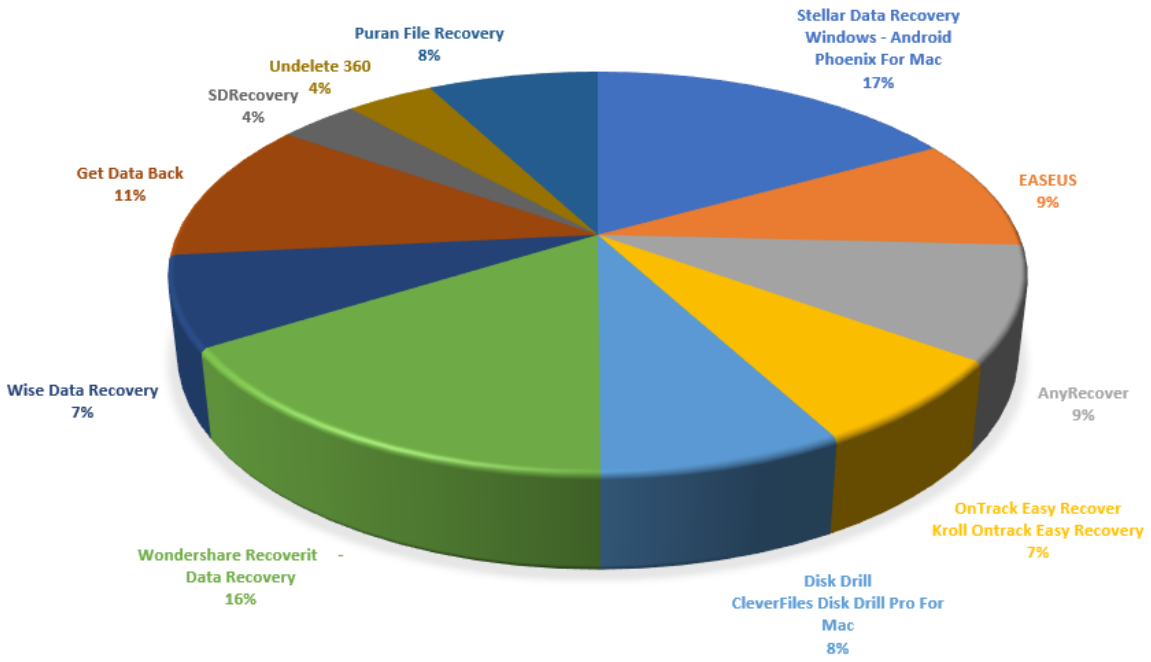
En la gráfica 7 se muestra el porcentaje de la usabilidad de cada una de las herramientas, resultado de las preferencias de los profesionales de la información donde se puede apreciar una tendencia marcada en la selección de software similares.



Gráfica 7. Selección por herramienta.

Los indicadores en la selección y preferencia del panel de expertos arrojaron como resultado que las herramientas Stellar Data Recovery y Wondershare Recoverit son las utilerías más convenientes, por lo cual la recomendación en el uso de alguna de ellas puede ser con base al papel que puede jugar el indicador del costo de licenciamiento o las funcionalidades requeridas, ya que en conjunto pueden cubrir en su totalidad las características que debe tener una herramienta para la recuperación de información.

Para determinar la calidad de las herramientas tecnológicas se utilizó la ponderación determinada por el panel de expertos en las encuestas, estos valores fueron establecidos por la usabilidad, confianza, funcionabilidad, eficiencia, seguridad y satisfacción, estas preferencias se pueden observar en la gráfica 8.



Gráfica 8. Ponderación por herramienta.

Resultados del objetivo específico 3

Se realizó una revisión de los lineamientos y metodologías en el proceso de elaboración de una pericial, se realizó un análisis de contenido, específicamente en el estudio de cada uno de los estándares utilizados internacionalmente, en primer lugar se realizó un análisis de contenido cualitativo en el cual se interpretaron las fases de cada uno, posteriormente se clasificó la información, se identificaron los lineamientos y metodologías, el resultado fue una síntesis entre las fuentes para la elaboración de un nuevo modelo.

En la tabla 3 se puede observar el análisis de contenido documental, donde se abordan los procesos realizados para la recolección de la información o evidencias, análisis de los procesos realizados y las fases del reporte final.

	ISO 27037 / 27042	UNE71505 / 71506	RFC3227	IOCE
Descripción	Establece el examen y sentido de la evidencia digital, para su continuidad y la validez en los procedimientos de análisis forense y su interpretación, es una guía para el desarrollo del cómputo forense de tal modo que las directrices del perito sean admisibles en la presentación en un juicio, el análisis de los datos corresponde a la métodos y técnicas jurídicamente admisibles, mediante una completa documentación de los hallazgos, estudio y procesos realizados, mientras que la interpretación es el informe final de los resultados evidenciados de la investigación.	sirve para definir y describir la conceptualización de la información para evidencias electrónicas en un SGSI utilizado previo a un desarrollo, la UNE 71505 define la metodología para realizar un análisis forense con validez jurídica, bajo un sistema de SGEE y un sistema de gestión de seguridad de la información, la cual consta de la revisión de principios generales, prácticas en la diligencia de evidencias y la comprobación de los formatos y los mecanismos. Los objetivos de la norma son describir y definir los conceptos, identificar las relaciones entre la gestión y la seguridad, y especificar sus controles.	Lineamiento utilizado globalmente, el cual es utilizado como guía en la recopilación de archivos de evidencias relevantes para efectos de seguridad en casos de enjuiciamientos.	Guía para las buenas prácticas en la elaboración de pruebas electrónicas, buscando una estandarización internacional.

Procesos de Recolección de Información	**Identificación**	**Autenticación e integridad**	**Recolección**	**Recolección**
	El primer proceso del análisis forense es la identificación de los elementos digitales, lo cual implica las fases de la indagación, descubrimiento y la documentación. Identificar la información para la evidencia digital es un proceso complejo dado los factores del entorno, revisar los diversos elementos de almacenamiento es el primer proceso, posteriormente se debe identificar el lugar virtual del almacenamiento, dadas las capacidades de almacenamiento este proceso puede requerir más atención, aunque en ocasiones puede ser muy específica y no requiere de una búsqueda exhaustiva.	Refiere a que la evidencia no cambia en el proceso de estudio y manipulación, tanto en contenido, propiedades, características, es decir la información no sufrirá ningún cambio en algún momento. **Documentación**: se realiza una documentación secuencial desde el inicio del análisis hasta el término del informe, detallando cada aspecto incluyendo las herramientas utilizadas en el manejo de las evidencias	Este proceso consiste en realizar una documentación para determinar las posibles evidencias, en este proceso se visualiza y analizar el escenario en su estado natural.	Detección de la evidencia. Análisis del entorno. Informe de procedimientos individuales.
	Recolectar y adquirir	**Disponibilidad y completitud**	**Valoración de posibilidades**	**Verificación de la evidencia**

	El proceso de recolectar es el acto de tomar físicamente el dispositivo de almacenamiento o prueba que pueda contener la información de estudio, mientras que adquirir se refiere al procedimiento subsecuente de identificar la información ubicada en el dispositivo de almacenamiento y se genera una copia de seguridad, la cual debe ser creada al mismo tiempo de la adquisición, este proceso es independiente del medio y ubicación de la información, esta copia debe realizarse mediante un estricto proceso y documentado en todo momento, cumpliendo mecanismos de seguridad e integridad con el fin de asegurar que no sufra modificaciones en el proceso, por lo cual este proceso es complejo y crítico.	Garantiza el acceso a la información y la bitácora de cada proceso	Determinar la relevancia entre lo admisible o no en un juicio, tener en cuenta el riesgo de la destrucción de evidencias, evitar apagar el equipo, elección adecuada de las herramientas de respaldo que no altere la información original.	Identificar todos los indicios o rastros que permitan esclarecer o dar seguimiento al hecho ocurrido. Verificar los procedimientos de seguridad.
	Preservación	**Calidad y gestión**	**Privacidad**	

	La evidencia digital debe ser preservada, por lo cual la normativa 27037 establece que la conservación es el proceso salvaguardar la información, al igual que su integridad y sin modificaciones, este complicado desarrollo es parte importante, ya que en el análisis en un juicio legal no se puede definir el tiempo de espera y es importante evitar la manipulación o alteración alguna. Los requerimientos generales que debe cumplir son: los mismos principios de auditoría, ser repetible, reproducible y justificable:	En cuanto a la calidad de información trata de los procesos técnicos realizados bajo un cuidado minucioso, en el manejo describe la documentación detallada de cada etapa y en la preservación sobre la presentación de la información documental de los resultados, mientras que la gestión menciona los procesos establecidos y verificados previamente al estudio realizado susceptible a ser auditado	Tener en cuenta las normas legales, políticas empresariales, información sensible, en caso de existir dudas es recomendable realizar una consulta jurídica	
	Auditable: Debe ser capaz de cumplir con una posible evaluación de cada actividad por las partes involucradas, y al igual que cada paso es indispensable	**Preservación**	**Consideraciones**	**Consideraciones**

	la correcta documentación con cada una de las medidas adoptadas, siempre respondiendo el por qué y cómo en cada criterio. **Repetible**: Los mecanismos deben tener la capacidad de ser repetibles en cualquier momento y arrojando los mismos resultados de la prueba original, siempre que sean ejecutados en las mismas condiciones, las cuales se establecen utilizando el mismo procedimiento e instrumentos. **Reproducible**: Esto significa que se deben obtener los mismos resultados aun cuando se produce otro tipo de estudio y los instrumentos sean diferentes, es decir, la aplicación de diversos instrumentos y diferentes condiciones arrojara el mismo resultado, esto significa que	Es la validez y confiabilidad del repertorio de los datos en estudio, así como determinar los aspectos de los entornos físicos que puedan afectar a la evidencia desde el inicio hasta el final del proceso. y la adquisición es garantizar la generación de una copia fiel del original.	Considerar y determinar los tiempos para la generación de la línea temporal. Si hay dudas entre recoger y analizar las evidencias, dar prioridad a la recolección. A la hora de recopilar las evidencias, minimizar los cambios que alteren el escenario y eliminar los agentes externos que pueden hacerlo. Por cada tipo dispositivo o sistema operativo puede existir diferentes métodos de recogida de datos. El orden de recogida de datos debe quedar establecido en función de la volatilidad de estos. La copia de la información debería realizarse a nivel binario para no alterar ninguno de los datos	Crear una metodología. Buscar antecedentes. Descripción de procesos y evidencias. Análisis previo. Hallazgos. Deducciones.

	puede ser reproducible en cualquier momento. **Justificable**: El especialista o perito debe ser capaz de mencionar todos los procedimientos y métodos utilizados descritos. **Defendible**. Validez con las herramientas utilizadas.			
Análisis	Análisis: revisión de los datos corresponde a la métodos y técnicas jurídicamente admisibles, mediante una completa documentación de los hallazgos, estudio y procesos realizados	Análisis: refiere a los procesos técnicos realizados durante la recuperación y estudio.	Invalidez de las Evidencias Evitar acciones para no producir invalidez de las evidencias recopiladas: Vulnerar la intimidad o revelar información personal. No ajustarse a las normativas legales o de seguridad de la empresa. Manipular evidencia.	**Analizar la evidencia** Interpretación y evaluación de la evidencia. Verificar protocolos. Realizar procedimientos que no modifiquen la evidencia. Cronograma de actividades. Documentar todos los procesos realizados. Validar las herramientas utilizadas.
	Interpretación: es el último proceso para realizar informe final con los resultados evidenciados de la investigación.			
Reporte Final	Examen inicial desarrollada	Presentación: proceso final, es el	Documentar las evidencias.	Creación del reporte.

	por el perito. Informe incluyendo: Descripción. Fecha y hora. Duración. Lugar. Objetivos. Involucrados en la investigación. Descripción de la evidencia digital y hallazgos. Descubrimientos e implicaciones del proceso. Limitaciones del análisis. Descripción de procedimientos y herramientas a utilizar. Interpretación, conclusiones y recomendaciones del perito.	informe detallado en un lenguaje comprensible. Aseguramiento de la evidencia. Asegurar su autenticidad e integridad. Asegurar su acceso para ser evaluada.	Determinar la relevancia entre lo admisible o no en un juicio, tener en cuenta que la falta de evidencia es perjudicial, al contrario que la innecesaria solo alarga la documentación. Determinar el orden de recuperación de evidencias. Aislar el sistema en cuestión. Realizar el proceso de respaldo con las herramientas seleccionadas. Revisión y depuración de la evidencia. Realizar una documentación en todo momento, bitácora de actividades. Identificar personal involucrado en el proceso de recopilación.	Coherencia en el sistema legal. Lenguaje estandarizado. Integridad de las evidencias. Proceso de comparación y verificación.

Tabla 3. Normativas internacionales.

Dado el análisis documental se elaboró una síntesis de las normativas dando como resultado la siguiente propuesta:

Lineamientos para la estandarización en la elaboración de periciales informáticas
Descripción
Lineamiento para la estandarización en la elaboración de periciales informáticas, estableciendo garantías en el aseguramiento de evidencia digital por medio de una metodología y estructura basada en los estándares internacionales ISO27037, UNE71505, UNE71506, RFC3227, IOCE y la normativa mexicana NMX-I-289-NYCE-2016.

Identificación
Realizar un análisis previo de la situación: • Análisis del entorno. • Detectar posibles evidencias y manipulaciones. • Identificar todos los posibles elementos digitales.
Recolección
Recolectar todo dispositivo susceptible de evidencia o de almacenamiento digital, realizando los más mínimos cuidados de seguridad y manejo de los dispositivos para evitar algún daño que pueda ocasionar pérdida de los datos almacenados. Tener en cuenta información que pueda estar almacenada en la memoria volátil. Determinar lo que es y no evidencia, se debe tener en cuenta que la falta de evidencia es perjudicial, al contrario que la innecesaria solo alarga la documentación, es preferible realizar una documentación más extensa a omitir pruebas relevantes. Evaluar las normativas legales de privacidad y manejo de la información, contar con apoyo jurídico de ser necesario.
Preservación
El respaldo de la información es punto crítico en el proceso, por lo que realizarlo de la manera adecuada es primordial, se debe de cerciorar que la copia de la información o elementos de almacenamiento sea idéntica, realizar un clon bit por bit es la mejor técnica esto asegura que sea una copia exacta respetando hasta el más mínimo dato, lo que asegura que información como la fecha de creación y modificación no sean alteradas.
Calidad y gestión
La calidad refiere a la documentación de cada etapa o proceso, este proceso asegura que la integridad de la investigación pueda ser verificable en cualquier escenario, la validación de las herramientas de recuperación asegura que los procesos tengan un fundamento y al ser auditadas cumplan con las funciones por las que fueron elegidas. La gestión del proceso refiere a que se cumpla la estrategia documentada y sea verificable, por ello la importancia de una minuciosa documentación. Es imperante que estos puedan ser repetibles en cualquier momento y arrojen los mismos resultados que la prueba original, esto significa que cualquier persona con los conocimientos pueda replicar el proceso realizado, siempre y cuando sean ejecutados bajo las mismas condiciones e instrumentos, y así serán iguales aun cuando se realice otro tipo de estudio y los instrumentos sean diferentes, cualquier especialista o perito deberá concordar con los resultados independientemente de los procedimientos, métodos y herramientas utilizadas.

Analizar la evidencia

Los procesos técnicos en la recuperación y estudio de la evidencia:

• Revisión de la evidencia, recuperación de información de la memoria volátil y unidad física de almacenamiento.

• Creación de imágenes de seguridad de las unidades.

• Montar y trabajar sobre las imágenes creadas.

• Previsualizar las imágenes para explorar el contenido de las carpetas y archivos de estudio.

• Extraer la información necesaria.

• Comprobar todo el proceso desarrollado.

Reporte final

Generar reportes y la documentación de todo lo realizado, se deben de incluir los datos como fechas, horas, duración, dirección física de la información, además de la descripción de las herramientas utilizadas en cada proceso.

El reporte debe de ser encaminado a contestar la pericial en función, lo que significa que debe de realizarse la contestación de cada pregunta en materia pericial sin importar si son repetitivas o su proceso es redundante.

El informe pericial debe de ser claro, directo, escrito en un lenguaje entendible y debe contener:

Presentación.
Debe contener los criterios establecidos por el sistema jurídico:

• Fecha y lugar.
• Presentación personal, experiencia, grados de estudio, número de cedula profesional y la vertiente del perito.
• Anexar cedula profesional de estudios con copia certificada e identificación oficial.
• Domicilio del perito.
• Aceptación del cargo.
• Información del juicio, número de expediente, nombrar la parte actora y demandada.

Antecedentes.
• Resumen de los hechos, una descripción breve del motivo y objetivos.

Documentación.
• Descripción de todo el material de estudio, evidencias presentadas por las partes y aclarar los nuevos hallazgos.

Criterios.
• Describir todo el procedimiento realizado por el perito, herramientas utilizadas y conclusiones en cada una.

Cuestionario.
• Es la base del informe que permite al juez tener un panorama de la situación y hechos en litigio.
• El perito debe contestar todas las preguntas especificadas por la parte actora y demandada, sin importar si son repetitivas o similares.

Conclusiones.
• En esta parte el perito debe realizar su dictamen profesional con base a todo lo realizado y puede agregar su punto de vista de acuerdo a la experiencia personal.

Anexos.
• Toda la documentación que sea relevante para la realización del informe debe de ser agregada para dar sustento a la investigación, es importante señalar la referencia de cada una de ellas.

Firma.
• Nombre.
• Firma.
• Lugar y fecha.

Tabla 4. Normativa propuesta.

Se determinaron los elementos necesarios en la elaboración de un informe pericial, este prototipo de aplicación fue una síntesis de los puntos relevantes de las normativas de estudio, los resultados esperados fueron completados, dado que se sustrajeron los puntos relevantes de cada norma y se integraron con el fin de homologar el proceso pericial, la gestión de estos lineamientos tienen como destino ser evaluados por los expertos con el objetivo de tener una normalización en desarrollos futuros.

Resultados del Objetivo Especifico 4

Se utilizo la técnica Delphi en el proceso de consenso con el fin de obtener la opinión del grupo de especialistas y expertos en el área, de tal modo que la aplicación fue realizada de la siguiente manera:

1.- Se conformo un panel de expertos integrados por especialistas en la recuperación de información, abogados y un juez de la suprema corte.

2.- Se entrego el formato de la propuesta realizada con el cuestionario para una evaluación de los criterios abordados, detallando los objetivos de cada parámetro y la opción para que expresaran sus recomendaciones, el formato del cuestionario puede consultarse en el anexo 4 del presente trabajo de investigación.

3.- Se analizaron los resultados de cada parámetro de evaluación.

4.- La valoración de los parámetros fueron basados en una escala de Likert para obtener una mejor comprensión de los resultados, estos oscilaron entre 1 y 5, dando 1 al valor mínimo y 5 a la mayor puntuación de satisfacción.

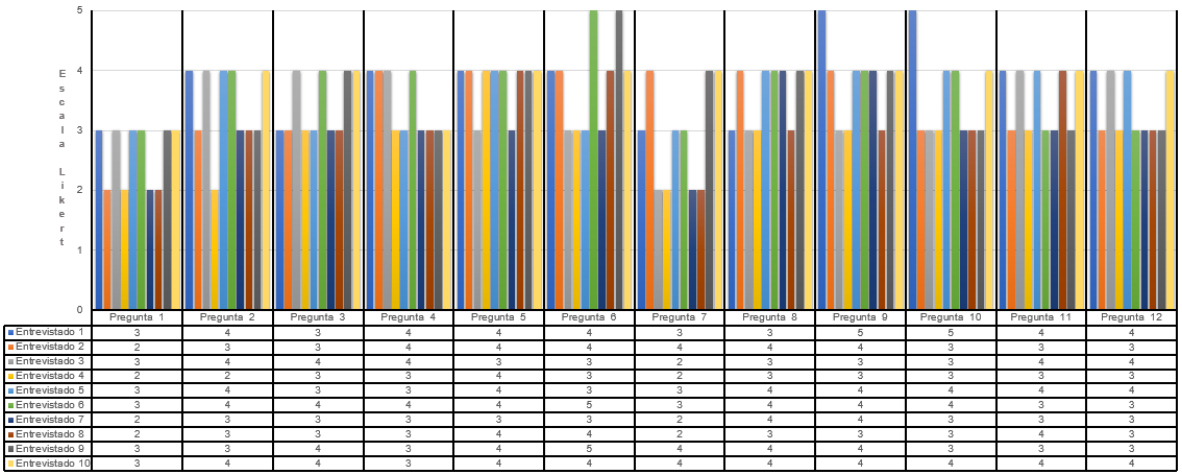
Los resultados finales obtenidos de la primera ronda y las ponderaciones descritas con las letras P1 hasta la P12, representan cada pregunta realizada en la selección de la herramienta tecnológica, tal como se muestran en la tabla 5.

	RONDA 1											
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**	**P11**	**P12**
Entrevistado 1	3	4	3	4	4	4	3	3	5	5	4	4
Entrevistado 2	2	3	3	4	4	4	4	4	4	3	3	3
Entrevistado 3	3	4	4	4	3	3	2	3	3	3	4	4
Entrevistado 4	2	2	3	3	4	3	2	3	3	3	3	3
Entrevistado 5	3	4	3	3	4	3	3	4	4	4	4	4
Entrevistado 6	3	4	4	4	4	5	3	4	4	4	3	3
Entrevistado 7	2	3	3	3	3	3	2	4	4	3	3	3
Entrevistado 8	2	3	3	3	4	4	2	3	3	3	4	3
Entrevistado 9	3	3	4	3	4	5	4	4	4	3	3	3
Entrevistado 10	3	4	4	3	4	4	4	4	4	4	4	4
Media	2.6	3.4	3.4	3.4	3.8	3.8	2.9	3.6	3.8	3.5	3.5	3.4

Tabla 5. Resultados Delphi primer ronda.

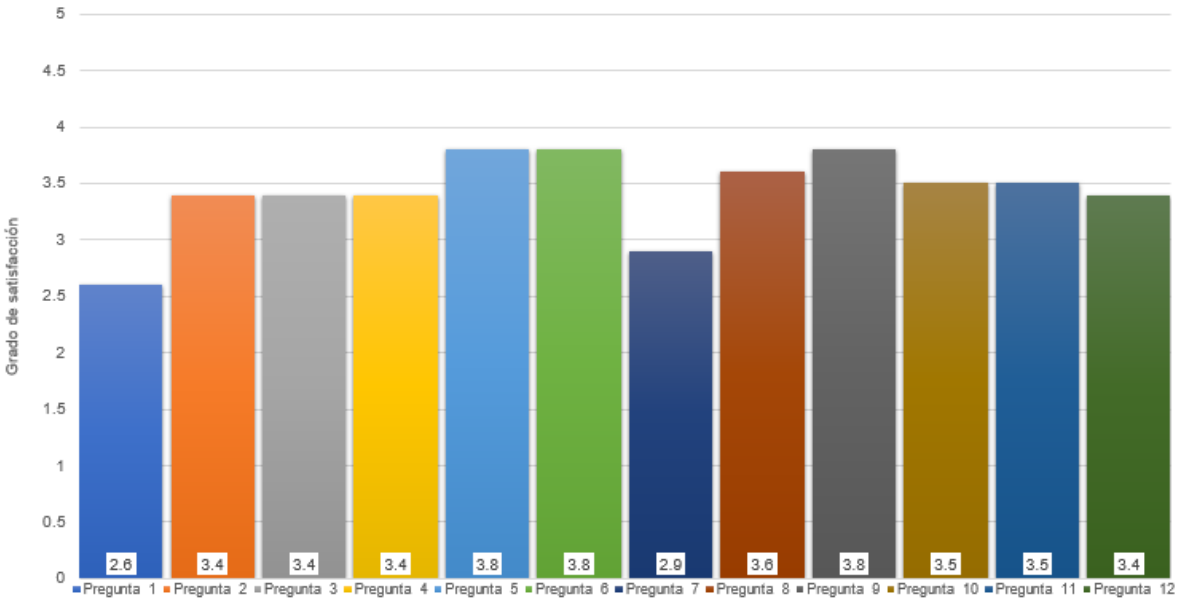
Los resultado arrojan poca aceptación en la propuesta, la cual obtuvo un apoyo significativo por parte de los participantes dadas las recomendaciones recabadas en el cuestionario, la tabla siguiente muestra las preferencias de los involucrados, donde en promedio el resultado fue 3.42, un valor aun no aceptable ya que la

métrica establecida fue del 80% lo que refiere que la puntuación en promedio fue menor de 4 en la escala de Likert, por lo cual no se puede determinar como una propuesta aceptable, en las gráficas 9 y 10 se puede observar el comportamiento de los participantes por cada pregunta realizada y la media.



	Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 7	Pregunta 8	Pregunta 9	Pregunta 10	Pregunta 11	Pregunta 12
Entrevistado 1	3	4	3	4	4	4	3	3	5	5	4	4
Entrevistado 2	2	3	3	4	4	4	4	4	4	3	3	3
Entrevistado 3	3	4	4	4	3	3	2	3	3	3	4	4
Entrevistado 4	2	2	3	3	4	3	2	3	3	3	3	3
Entrevistado 5	3	4	3	3	4	3	3	4	4	4	4	4
Entrevistado 6	3	4	4	4	4	5	3	4	4	4	3	3
Entrevistado 7	2	3	3	3	3	3	2	4	4	3	3	3
Entrevistado 8	2	3	3	3	4	4	2	3	3	3	4	3
Entrevistado 9	3	3	4	3	4	5	4	4	4	3	3	3
Entrevistado 10	3	4	4	3	4	4	4	4	4	4	4	4

Gráfica 9. Resultados Delphi primer ronda.



Gráfica 10. Resultados media primera ronda.

Las recomendaciones fueron evaluadas y se realizó una reestructuración de la propuesta original, las respuestas obtenidas están simplificadas y enlistadas con base al grupo perteneciente, tal como se muestra en la tabla 6.

Identificación
Determinar cuáles son las evidencias admisibles. Realizar documentaciones. Documentación de fecha y horario como si tratara de una bitácora. Agregar los posibles elementos catalogados como evidencia. Evaluar la situaciones y evidencias. Reportes.
Recolección
Documentación. Evaluar la manipulación. Realizar una bitácora. Hacer un inventario. Estudio de la situación.
Preservación
Explicar técnicas. Como se cumple?
Calidad y gestión
Mencionar como puede ser susceptible de una auditoria. Documentación en todo momento. Proponer un proceso de verificación.
Analizar la evidencia
Determinar la manipulación de evidencia. Deben mencionar los reportes de elementos encontrados. Generar un registro.
Reporte final
Describir las técnicas que se realizaron. Agregar un listado de mecanismos de seguridad. Tratar de analizar si pueden asignarse responsabilidades. Propuesta de escenarios. Agregar la copia de recuperación. Mencionar el respaldo.

Tabla 6. Recomendaciones primera ronda.

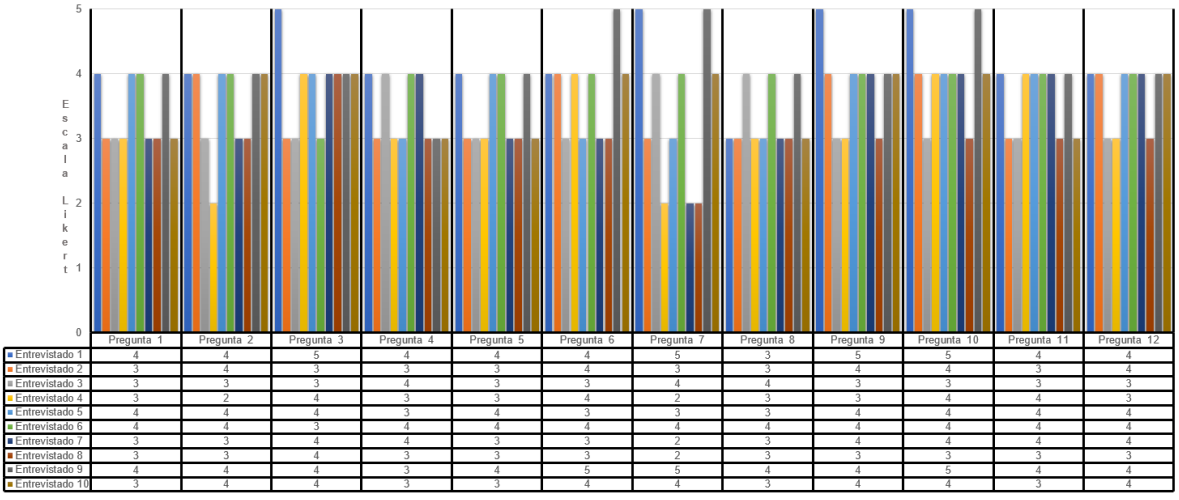
Finalizada la primera ronda y modificada la propuesta original se realizó un segundo consenso, en el cual se obtuvo diferente ponderación, esta tuvo una mejor aceptación por el grupo de expertos, estos resultados se presentan a continuación en la tabla 7.

RONDA 2

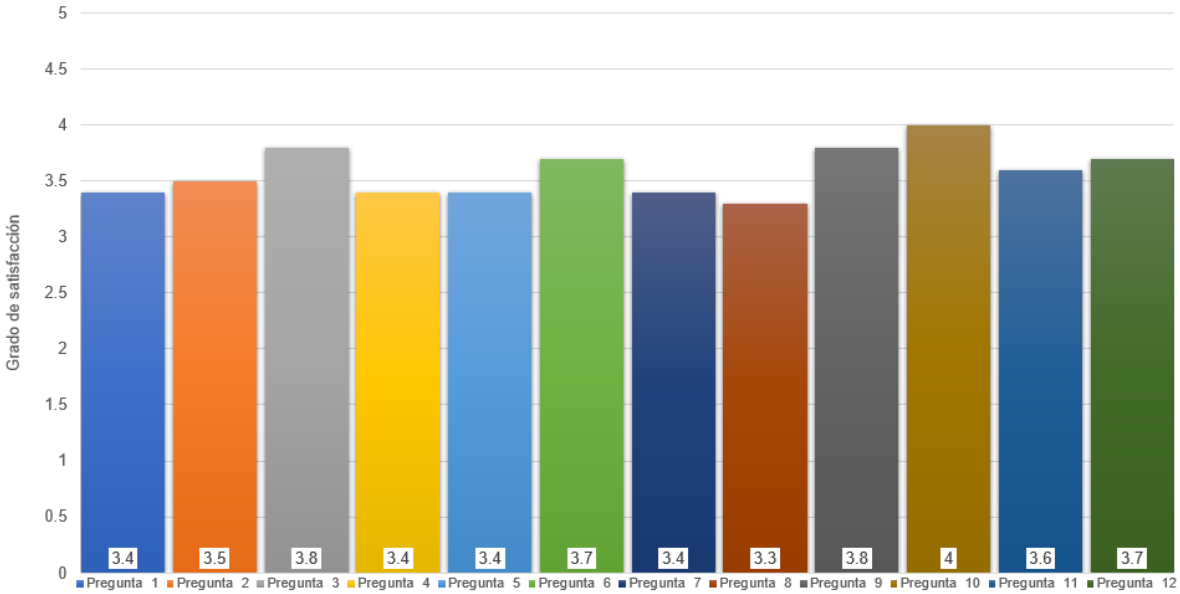
	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12
Entrevistado 1	**4**	4	**5**	4	4	4	**5**	3	5	5	4	4
Entrevistado 2	**3**	**4**	3	3	3	4	3	3	4	**4**	3	**4**
Entrevistado 3	3	3	3	4	3	3	**4**	**4**	3	3	3	3
Entrevistado 4	**3**	2	**4**	3	3	**4**	2	3	3	**4**	**4**	3
Entrevistado 5	**4**	4	**4**	3	4	3	3	3	4	4	4	4
Entrevistado 6	**4**	4	3	4	4	4	**4**	4	4	4	**4**	**4**
Entrevistado 7	**3**	3	**4**	**4**	3	3	2	3	4	**4**	**4**	**4**
Entrevistado 8	**3**	3	**4**	3	3	3	2	3	3	3	3	3
Entrevistado 9	**4**	**4**	4	3	4	5	**5**	4	4	**5**	**4**	**4**
Entrevistado 10	3	4	4	3	3	4	4	3	4	4	3	4
Media	3.4	3.5	3.8	3.4	3.4	3.7	3.4	3.3	3.8	4	3.6	3.7

Tabla 7. Resultados Delphi segunda ronda.

Los resultados obtenidos muestran mejoría en la aceptación de la propuesta con los cambios realizados de la primera ronda, la tabla describe en color amarillo una mejor aceptación por parte de los encuestados, mientras que las casillas en rojo bajo la calificación que asignaron y además se obtuvieron más recomendaciones, la tabla inmediata anterior muestra las preferencias con un promedio general de 3.58, apenas un 0.16 arriba del resultado de la primer encuesta, valor no aceptable comparado con el 80% establecido como aceptable, las gráficas 11 y 12 muestran la valoración de las preguntas de la segunda ronda.



Gráfica 11. Resultados Delphi segunda ronda.



Gráfica 12. Resultados media segunda ronda.

Nuevamente las recomendaciones realizadas por el panel de expertos fueron evaluadas y se realizó una segunda reestructuración en la propuesta, las recomendaciones realizadas se muestran en la tabla 8.

Identificación
Evaluar las evidencias. Evaluación de la situación. Reporte de anomalías.
Recolección
Indagar registros.
Analizar la evidencia
Generar una bitácora de la información encontrada. Registro de información recuperada. Realizar un trazo de información. Reporte de análisis.
Reporte final
Los lineamientos están encaminados a un perito de parte. Revisión de expediente para un panorama general de los hechos. Se debe ser Imparcial. Ser objetivo y no guiarse por criterios personales.

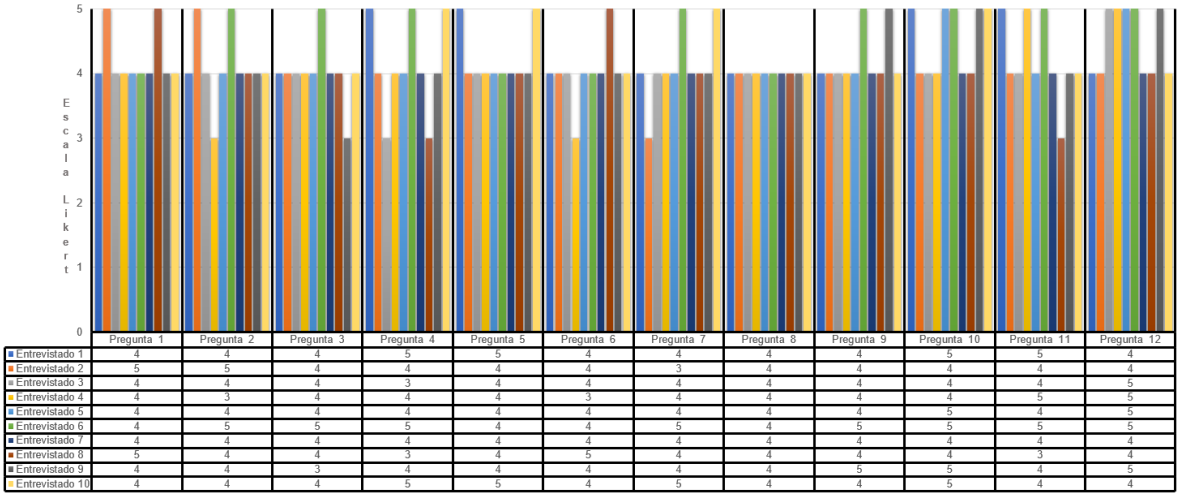
Tabla 8. Recomendaciones segunda ronda.

Se realizo una tercera ronda de la encuesta, los resultados se pueden observar en la tabla 9, donde se evaluaron todas las modificaciones realizadas en la valoración de los procesos propuestos.

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12
Entrevistado 1	**4**	4	4	5	**5**	4	4	**4**	4	5	**5**	4
Entrevistado 2	**5**	**5**	**4**	**4**	**4**	4	3	**4**	4	**4**	**4**	**4**
Entrevistado 3	**4**	**4**	**4**	3	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**5**
Entrevistado 4	**4**	**3**	4	**4**	**4**	3	**4**	**4**	**4**	**4**	**5**	**5**
Entrevistado 5	4	4	**4**	**4**	4	**4**	**4**	**4**	4	**5**	4	**5**
Entrevistado 6	**4**	**5**	**5**	**5**	4	4	**5**	4	**5**	**5**	**5**	**5**
Entrevistado 7	**4**	**4**	4	4	**4**	**4**	**4**	**4**	4	**4**	**4**	**4**
Entrevistado 8	**5**	**4**	**4**	3	**4**	**5**	**4**	**4**	**4**	**4**	3	**4**
Entrevistado 9	**4**	**4**	3	**4**	4	4	4	4	**5**	5	**4**	**5**
Entrevistado 10	**4**	4	4	**5**	**5**	4	**5**	**4**	4	**5**	**4**	4
Media	4.2	4.1	4	4.1	4.2	4	4.1	4	4.2	4.5	4.2	4.5

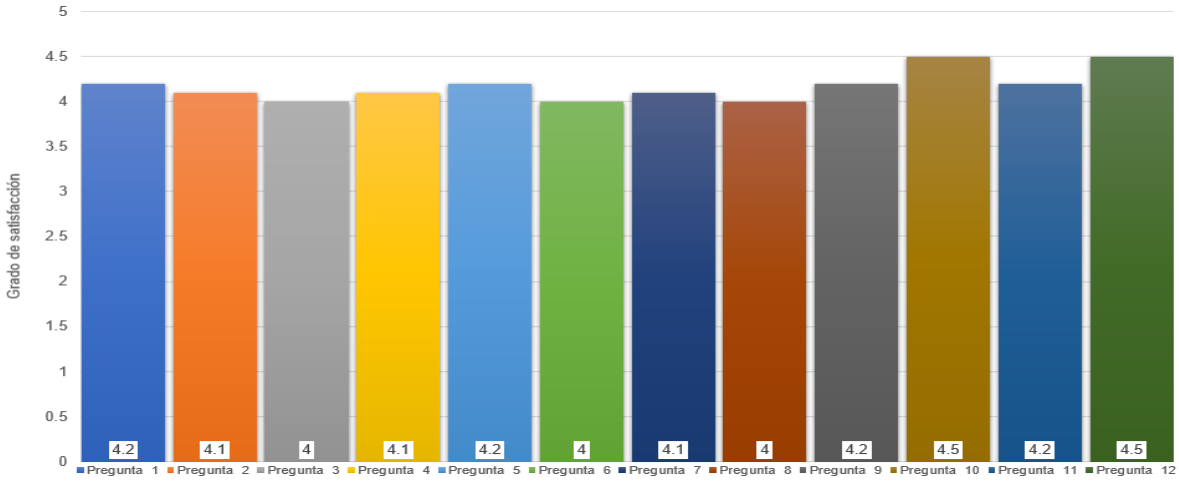
Tabla 9. Resultados Delphi tercera ronda.

Los resultados obtenidos de la tercer ronda mostraron cambios significativos, indican mejoría en la aceptación de la propuesta comparada con los obtenidos en la segunda ronda, la tabla muestra en color amarillo una mejor aceptación por parte de los encuestados, mientras que las casillas en rojo son puntuaciones que bajaron, no obstante la tabla anterior muestra que todas las medias en cada pregunta superaron el valor deseado para obtener una propuesta aceptable, con una media superior a 4, con un promedio general de 4.17, lo que es un 0.59 arriba del resultado anterior y 0.75 de la primer encuesta, obteniendo el 83.5% de aceptación por el panel de especialistas, superando lo establecido como aceptable en los criterios metodológicos, a continuación en la gráfica 13 se presentan el comportamiento de los resultados obtenidos.



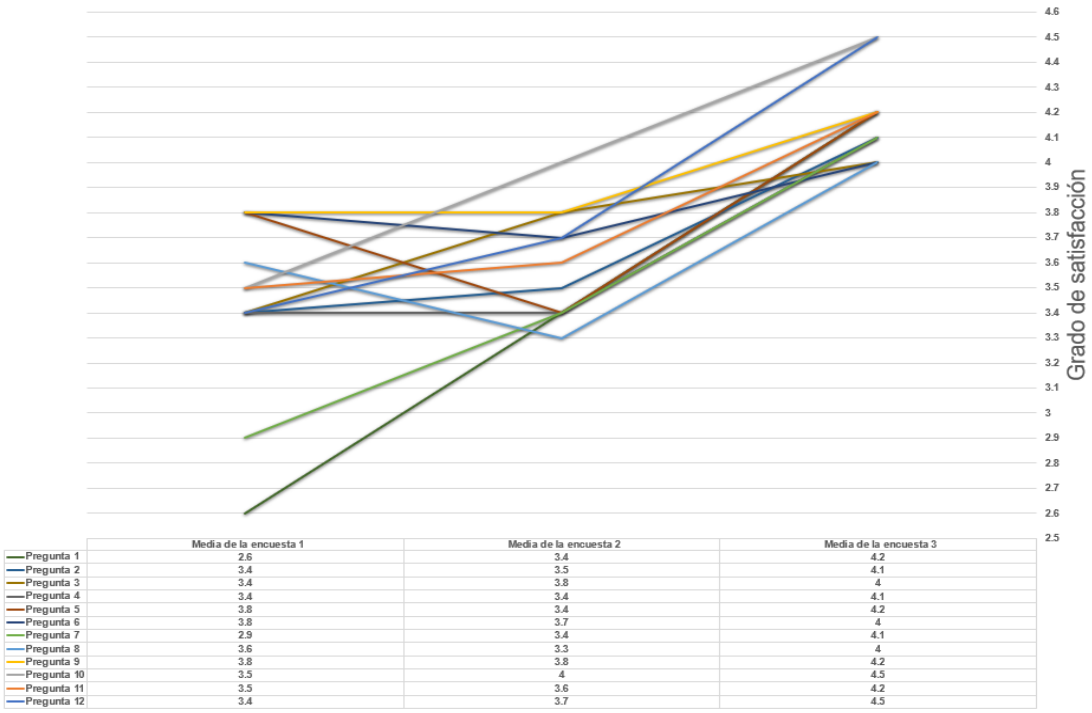
	Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 7	Pregunta 8	Pregunta 9	Pregunta 10	Pregunta 11	Pregunta 12
Entrevistado 1	4	4	4	5	5	4	4	4	4	5	5	4
Entrevistado 2	5	5	4	4	4	4	3	4	4	4	4	4
Entrevistado 3	4	4	4	3	4	4	4	4	4	4	4	5
Entrevistado 4	4	3	4	4	4	3	4	4	4	4	5	5
Entrevistado 5	4	4	4	4	4	4	4	4	4	5	4	5
Entrevistado 6	4	5	5	5	4	4	5	4	5	5	5	5
Entrevistado 7	4	4	4	4	4	4	4	4	4	4	4	4
Entrevistado 8	5	4	4	3	4	5	4	4	4	4	3	4
Entrevistado 9	4	4	3	4	4	4	4	4	5	5	4	5
Entrevistado 10	4	4	4	5	5	4	5	4	4	5	4	4

Gráfica 13. Resultados Delphi tercera ronda.



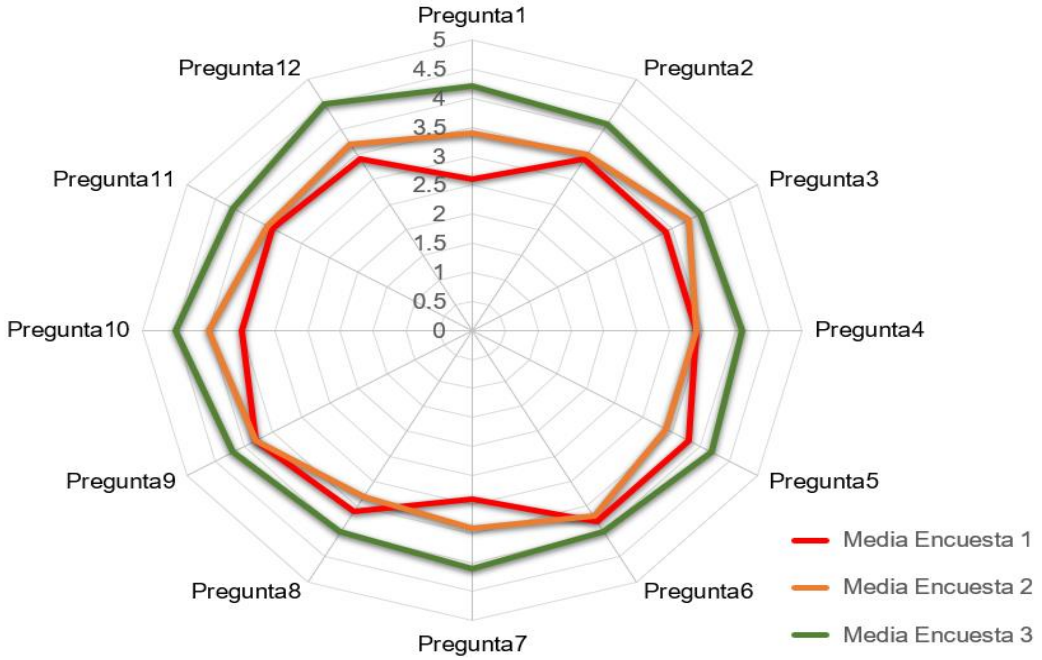
Gráfica 14. Resultados media tercera ronda.

Los resultados obtenidos muestran una aceptación de la propuesta de estrategia, a continuación, en la gráfica 15 se presenta el análisis de la evolución por pregunta y en general.



	Media de la encuesta 1	Media de la encuesta 2	Media de la encuesta 3
Pregunta 1	2.6	3.4	4.2
Pregunta 2	3.4	3.5	4.1
Pregunta 3	3.4	3.8	4
Pregunta 4	3.4	3.4	4.1
Pregunta 5	3.8	3.4	4.2
Pregunta 6	3.8	3.7	4
Pregunta 7	2.9	3.4	4.1
Pregunta 8	3.6	3.3	4
Pregunta 9	3.8	3.8	4.2
Pregunta 10	3.5	4	4.5
Pregunta 11	3.5	3.6	4.2
Pregunta 12	3.4	3.7	4.5

Gráfica 15. Aceptación por pregunta.



Gráfica 16. Evolución de percepción por pregunta.

En el gráfico 16 se puede apreciar visualmente la evolución de la aprobación del panel de expertos, así como los cambios de decisión en cada una de las encuestas realizadas, dando como resultado la siguiente propuesta final, la cual se presenta en la tabla 10 como propuesta final.

Lineamientos para la estandarización en la elaboración de periciales informáticas
Descripción
Lineamiento para la estandarización en la elaboración de periciales informáticas, estableciendo garantías en el aseguramiento de evidencia digital por medio de una metodología y estructura basada en los estándares internacionales ISO27037, UNE71505, UNE71506, RFC3227, IOCE y la normativa mexicana NMX-I-289-NYCE-2016
Identificación
Realizar una evaluación general de la situación: •Análisis del entorno. •Detectar cuales pueden ser las posibles evidencias admisibles. •Detectar las manipulaciones que puedan detectarse a simple vista. •Identificar todos los posibles elementos digitales. •Realizar una documentación minuciosa agregando fecha y hora. •Elaborar un inventario de todos los elementos y aspectos detectados. •Realizar un reporte de hallazgos incluyendo anomalías.
Recolección
•Recolectar todo dispositivo susceptible de evidencia o de almacenamiento digital. •Revisión de inventario. •Realizar protocolos de seguridad. •Extremar manejo de los dispositivos para evitar daños que puedan ocasionar pérdida de los datos almacenados en el proceso. •Evitar manipulación externa. •Recuperar información almacenada en la memoria volátil. •Determinar lo que es y no evidencia y evitar demoras en la recuperación. •Evaluar las normativas legales de privacidad y manejo de la información, contar con apoyo jurídico de ser necesario. •Creación de bitácora. •Documentación. •Tener en cuenta que la falta de evidencia es perjudicial, al contrario que la innecesaria solo alarga la documentación, es preferible realizar una documentación más extensa a omitir pruebas relevantes.
Preservación
El respaldo de la información es punto crítico en el proceso, por lo que realizarlo de la manera adecuada es primordial, se debe de cerciorar que la copia de la información o elementos de almacenamiento sea idéntica, realizar un clon a unidad de bit por bit es la mejor técnica, esto

asegura que sea una copia exacta respetando hasta el más mínimo dato, lo que asegura que información como la fecha de creación y modificación no sean alteradas.

•Realizar la copia de seguridad.
•Verificar que la copia sea exacta.

Calidad y gestión

• La calidad refiere a la documentación de cada etapa o proceso, este proceso asegura que la integridad de la investigación pueda ser verificable en cualquier escenario, la validación de las herramientas de recuperación asegura que los procesos tengan un fundamento y al ser auditadas cumplan con las funciones por las que fueron elegidas.

• La gestión del proceso refiere a que se cumpla la estrategia documentada y que sea verificable, por ello la importancia de una minuciosa documentación.

• Los procesos realizados pueden ser susceptibles a ser auditados, por lo que cada actividad o paso realizado en cada uno de los procedimientos debe ser documentado y verificado.

• Es imperante que estos puedan ser repetibles en cualquier momento y arrojen los mismos resultados que la prueba original, esto significa que cualquier persona con los conocimientos pueda replicar el proceso realizado, siempre y cuando sean ejecutados bajo las mismas condiciones e instrumentos, y así serán iguales aun cuando se realice otro tipo de estudio y los instrumentos sean diferentes, cualquier especialista o perito deberá concordar con los resultados independientemente de los procedimientos, métodos y herramientas utilizadas.

Analizar la evidencia

Los procesos técnicos en la recuperación y estudio de la evidencia:

- Revisión de la evidencia
- Recuperación de información de la memoria volátil.
- Recuperación de unidades físicas de almacenamiento.
- Creación de imágenes de seguridad de las unidades durante los procesos.
- Montar y trabajar sobre las imágenes creadas.
- Previsualizar las imágenes para explorar el contenido de las carpetas y archivos de estudio.
- Generar un registro de contenido.
- Extraer la información necesaria.
- Generar una bitácora de la información encontrada.

- Registro de información recuperada.
- Realizar un historial de la recuperación.
- Generar un reporte del análisis de la herramienta.
- Comprobar todo el proceso desarrollado.
- Determinar si existió manipulación de los elementos.
- Reporte de elementos encontrados o hallazgos.

Reporte final

Generar reportes y la documentación de todo lo realizado, se deben de incluir los datos como fechas, horas, duración, dirección física de la información, además de la descripción de las herramientas utilizadas en cada proceso.

El reporte debe de ser encaminado a contestar la pericial en función, lo que significa que debe de realizarse la contestación de cada pregunta en materia pericial sin importar si son repetitivas o su proceso es redundante.

Se debe realizar una revisión del expediente para un panorama general de los hechos.

Se debe ser Imparcial y objetivo, no debe guiarse por criterios personales.

El informe pericial debe de ser claro, directo, escrito en un lenguaje entendible y debe contener:

Presentación.

Contener los criterios establecidos por el sistema jurídico:

•Fecha y lugar.

•Presentación personal, experiencia, grados de estudio, número de cedula profesional y la vertiente del perito.

•Anexar cedula profesional de estudios con copia certificada e identificación oficial.

•Domicilio del perito.

•Aceptación del cargo.

•Información del juicio, número de expediente, nombrar la parte actora y demandada.

Antecedentes.

•Resumen de los hechos, una descripción breve del motivo y objetivos.

Documentación.

•Descripción de todo el material de estudio.

• Enlistar evidencias presentadas por las partes y aclarar los nuevos hallazgos.

• Mencionar los mecanismos de seguridad que poseían y los recomendados.

• Describir la recuperación de información y agregar una copia de la recuperación.

Criterios.
• Describir todo el procedimiento y técnicas realizadas por el perito. • Mencionar las herramientas utilizadas, procedimiento y conclusiones en cada una.
Cuestionario.
• Es la base del informe que permite al juez tener un panorama de la situación y hechos en litigio. • El perito debe contestar todas las preguntas especificadas por la parte actora y demandada, sin importar si son repetitivas o similares.
Conclusiones.
• En esta parte el perito debe realizar su dictamen profesional con base a todo lo realizado y puede agregar su punto de vista basándose en la experiencia personal y posibles escenarios causales del suceso.
Anexos.
• Toda la documentación que sea relevante para la realización del informe debe de ser agregada para dar sustento a la investigación, es importante señalar la referencia de cada una de ellas.
Firma.
•Nombre. •Firma. • Lugar y fecha.

Tabla 10. Propuesta final.

Discusión

Las periciales informáticas cada día son una técnica más utilizada en los procesos jurídicos, ya que aporta el punto de vista objetivo de expertos en la materia, ya que los jueces o abogados no pueden comprender los procesos informáticos, la importancia de realizar este procedimiento adecuadamente es primordial, donde no solo el cumplimiento de los objetivos es importante, sino llevar los lineamientos y metodología de forma adecuada, asegurando el cumplimiento de una correcta cadena de custodia, procesos y resultados.

En México no existe una regulación o lineamiento que estipule el cumplimiento de una normativa estandarizada o proceso a seguir en la elaboración de periciales, por lo que es necesario definir una estrategia, de tal modo que el proceso realizado por los peritos no siempre es el adecuado, ya que la elaboración de pericial se puede confundir con el desarrollo de una auditoria o un simple informe, tal como lo describe Vázquez (2022b) en el manual de la suprema corte sobre la pericial digital, donde menciona que puede tener o existir un contenido mínimo, identificar el objetivo y la información relevante, lo cual por la revisión bibliográfica no es posible, ya que para lograr un informe pericial se deben revisar hasta los mínimos detalles, la prueba pericial informática parte de lo particular para realizar una generalización de hechos y emitir una conclusión por el experto, caso contrario a lo mencionado en su manual.

En España, se encuentra en funcionamiento un Sistema de Gestión de Evidencia Electrónica (SGEE) denominado UNE71505, según lo señalado por Truchado (2019). Este sistema tiene como finalidad definir y describir la conceptualización de la información destinada a evidencias electrónicas en un Sistema de Gestión de Seguridad de la Información (SGSI) utilizado previo al desarrollo de un proyecto. La norma UNE 71505 establece la metodología para llevar a cabo un análisis forense con validez jurídica, integrando tanto el sistema de SGEE como el sistema de gestión de seguridad de la información. Esta metodología abarca la revisión de

principios generales, prácticas en la diligencia de evidencias, así como la verificación de formatos y mecanismos.

Tal es el caso de las normativas internacionales las cuales refieren al mismo objetivo de la cadena de custodia, pero los procedimientos son distintos entre ellos, una integración de los aspectos más sobresalientes de cada una para la creación de una estrategia o procedimiento dará como resultado un fortalecimiento en el desarrollo del informe pericial, la limitante en el desarrollo son las posibles variantes de la pericial, no todas las periciales tratan del mismo tema o tratan de resolver los mismos problemas.

La integración de normativas internacionales tiene la limitante principal de que no puede ser un estándar general para todas las periciales informáticas, para lo cual sería necesaria una reestructuración de la propuesta e integra más variantes de periciales informáticas, sin mencionar que las leyes deben ser más claras en los requisitos o lineamientos necesarios en la presentación de un informe pericial, ya que cada código de procedimientos tiene y puede tener lineamientos propios y los jueces pueden establecer el cómo proceder.

V. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

El objetivo general de la presente tesis fue el proponer una estrategia sistemática que fortalezca la elaboración de una pericial informática en la recuperación de información, ya que los resultados y análisis de la evaluación Delphi arrojaron el grado de madurez o de aprobación esperados, se puede determinar que la hipótesis planteada resultó aprobada, pero cabe resaltar que los resultados del objetivo general se determinaron por los resultados derivados de los objetivos específicos.

El primer objetivo planteado fue describir las principales características de las herramientas tecnológicas utilizadas para la recuperación de información en elementos de almacenamiento digital, ya que los programas o herramientas tecnológicas poseen características propias, se realizó un análisis documental para identificar las características más sobresalientes, por lo tanto la hipótesis específica que menciona las principales características de las herramientas tecnológicas utilizadas para la recuperación de información en elementos de almacenamiento digital permitirán crear el instrumento de evaluación para la selección de la herramienta más optima fue aceptada.

Para resolver el segundo cuestionamiento de la presente investigación, ¿Cuáles herramientas tecnológicas son las más utilizadas en los procesos de recuperación de información en elementos de almacenamiento digital? Se obtuvieron los resultados necesarios por medio de una encuesta para determinar las herramientas más utilizadas por el panel de expertos, por lo que la hipótesis específica dos fue aceptada ya que con el análisis de resultados se determinaron que las herramientas más utilizadas que fueron Stellar Data Recovery y Wondershare Recoverit.

Con respecto al objetivo específico tres de determinar los lineamientos y metodologías trascendentes para la elaboración de una pericial informática, se

partió de un análisis documental donde se determinaron los indicadores de las diversas normativas estudiadas, los cuales fueron agrupados para determinar las similitudes entre ellos en una tabla comparativa, al realizar un análisis de las normas ISO27037, UNE71505, UNE71506, RFC3227, IOCE y la normativa mexicana NMX-I-289-NYCE-2016, se desarrolló una incorporación de lineamientos y procedimientos, con el fin de realizar una propuesta estratégica considerando el objetivo principal de cada una de ellas, es decir sin cambiar el objetivo principal que debe cumplir una pericial y una cadena de custodia de la información. Por lo que la hipótesis específica tres que señala que el cumplimiento de los lineamientos y metodologías fortalece la elaboración de una pericial informática fue aprobada.

Con el fin de dar cumplimiento al objetivo cuatro; Diseñar una estrategia de recuperación de información con el uso de herramientas tecnológicas aplicadas en una pericial informática validada por el método Delphi, se cumplió en su totalidad, los resultados que lo comprueban pueden ser consultados en las conclusiones, los cuales dieron respuesta al objetivo, el panel de expertos bajo la retroalimentación aportaron el conocimiento necesario para perfeccionar la normativa propuesta, la cual tuvo finalmente su aprobación.

En conclusión, esta investigación abordo temas actuales y de utilidad, tanto en la gestión de procesos tecnológicos y documentales en el ámbito administrativo de los peritajes informáticos, específicamente en la recuperación de información, resaltando los principales aspectos de las técnicas, leyes y procedimientos. Se concluye que la propuesta de la creación de una estandarización en las técnicas de recuperación y lineamientos para la elaboración de una pericial puede garantizar beneficios en el desarrollo y presentación de los informes periciales.

Recomendaciones

No obstante, el resultado de esta metodología está encaminado a la gestión de información almacenada digitalmente, las pericias informáticas tienen muchas vertientes, es imposible estandarizar una normativa que aplique para cada una de ellas, sin embargo, el estudio en esta metodología puede ampliarse o adecuarse para ser utilizado en diversos temas relacionados con el análisis forense, para el objetivo uno se puede indagar sobre mas características que pueden tener las herramientas tecnológicas, continuando con el objetivo específico dos podría tomarse una muestra mayor de especialistas para realizar un estudio en más herramientas que la población de estudio no utiliza. El objetivo específico tres estudia estandarizaciones internacionales, es necesario indagar sobre más normas que pudieran adecuarse en la recuperación de elementos digitales y finalmente para el objetivo específico cuatro se puede realizar la propuesta formal al colegiado de abogados local para la implementación, de esta manera dar seguimiento y continuidad a esta investigación en trabajos futuros, además de los problemas legales, donde la falta de estandarización en los códigos de los procedimientos penales, laborales y de comercio, entre otros, muestran que debe existir una reestructuración en colaboración con expertos de las vertientes tecnológicas y jurídicas.

BIBLIOGRAFÍA

Alsoft. (2023). The world's most advanced repair and data recovery tool. https://www.alsoft.com/

Anyrecover. (2023). Best Data Recovery Software for Hard drive. https://www.anyrecover.com/

Arellano, J., Blanco, R., Cora, L., Decap, M., Gallardo, E., Guzmán, F. y Quilichini, M. (2020). Tecnología, proceso penal, audiencias y juicio oral. CEJA–Centro de Estudios de Justicia de las Américas, Universidad Alberto Hurtado. https://sistemasjudiciales.org/wp-content/uploads/2021/10/13.-SJ24.-Arellano-et-al.pdf

Benfeld, J. S. (2020a). La sana crítica en materia penal, laboral y de derecho de familia. Variaciones normativo-institucionales. Revista de derecho (Valparaíso), (55), 65-97. https://www.scielo.cl/scielo.php?pid=S0718-68512020000200065&script=sci_arttext&tlng=en

Benfeld, J. S. (2020b). Profesión legal y tecnologías de la información y las comunicaciones: Una discusión necesaria. Revista chilena de derecho y tecnología, 9(2), 5-31. https://www.scielo.cl/scielo.php?pid=S0719-25842020000200005&script=sci_arttext

Boletín Oficial del Estado. (8 de enero de 2000). Ley de Enjuiciamiento Civil. Anexo Legislativo: artículos 335 a 352 de la ley 1/2000, de 7 de enero, de enjuiciamiento Civil. https://www.boe.es/buscar/pdf/2000/BOE-A-2000-323-consolidado.pdf

Brezinski, D. y Killalea, T. (2002). RFC3227: Guidelines for Evidence Collection and Archiving. https://dl.acm.org/doi/pdf/10.17487/RFC3227

Brito-Febles, O. P., y Muñoz-Alfonso, Y. (2023). La cadena de guarda y custodia de las pruebas materiales. Revista Metropolitana de Ciencias Aplicadas, 6(S1), 57-67. http://remca.umet.edu.ec/index.php/REMCA/article/download/632/638

Cabero, J. (1998). Impacto de las nuevas tecnologías de la información y la comunicación en las organizaciones educativas. Grupo Editorial

Universitaria. https://cmapspublic2.ihmc.us/rid=1MZF0MGPJ-DW0C5J-NB1S/TICS%20EN%20EDUCACION.pdf

Cadena de Custodia Guía Nacional. (2015). Conferencias nacionales conjuntas de procuración de justicia de secretarios de seguridad pública. http://www.secretariadoejecutivo.gob.mx/docs/pdfs/normateca/protocolos/VF10GuaNacionalCadenadeustodia28-10-2015.pdf

Chen, C. (2019). TIC (Tecnologías de la información y la comunicación). Significados. https://www.significados.com/tic/

ciberseguridad. (2020). ISO/IEC 27037 Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital. https://ciberseguridad.com/normativa/espana/iso-iec-27037-evidencia-digital/

Cisneros-Caicedo, A. J., Guevara-García, A. F., Urdánigo-Cedeño, J. J. y Garcés-Bravo, J. E. (2022). Técnicas e Instrumentos para la Recolección de Datos que apoyan a la Investigación Científica en tiempo de Pandemia. Domino de las Ciencias, 8(1), 1165-1185. https://dominiodelasciencias.com/ojs/index.php/es/article/view/2546/5714

Código Federal de Procedimientos Penales [CFPP]. (2016), Reformada, Diario Oficial de la Federación [D.O.F.], 17 de junio de 2016, (México). https://www.diputados.gob.mx/LeyesBiblio/abro/cfpp/CFPP_abro.pdf

Código Federal Penal [2023]. (2023), Reformada, Diario Oficial de la Federación [D.O.F.], 18 de octubre de 2023, (México). www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

Código Nacional de Procedimientos Civiles y Familiares [CNPCF]. (2023), Reformada, Diario Oficial de la Federación [D.O.F.], 7 de junio de 2023, (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/CNPCF.pdf

Código Nacional de Procedimientos Penales [CNPP]. (2021), Reformada, Diario Oficial de la Federación [D.O.F.], 25 de abril de 2023, (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP.pdf

Compudiagnosis. (2018). Características que debe tener una buena herramienta de recuperación de datos.

https://compudiagnosis.com/wp/2018/01/16/caracteristicas-que-debe-tener-una-buena-herramienta-de-recuperacion-de-datos/

Concepto. (2021). Dispositivos de almacenamiento. https://concepto.de/dispositivos-de-almacenamiento/

Concepto. (2022). Software. https://concepto.de/software/

Coronel-Rojas, L. A., Areniz-Arévalo, Y., Cuesta-Quintero, F., y Rico-Bautista, D. (2020). Definición de una metodología de adquisición de evidencias digitales basada en estándares internacionales. Revista Ibérica de Sistemas e Tecnologías de Información, (E29), 266-282. https://www.researchgate.net/publication/340617686_Definition_of_a_digital_evidence_acquisition_methodology_based_on_international_standards

Crucial. (2023). ¿Qué es un dispositivo de almacenamiento de datos informáticos?. https://www.crucial.mx/articles/about-ssd/what-is-a-computer-data-storage-device

Datarecoverylab. (2023). Datarecoverylab. https://datarecoverylab.com.mx/

de Haro Olmo, F. J. (2021). Crimen, cibercrimen y análisis forense informático. Scientia Omnibus Portus, 1(1), 2. https://dialnet.unirioja.es/servlet/articulo?codigo=8180667

De La Cruz, R. (2023). Security analysis between Windows, Linux and macOS. Innovatus: A Journal on Computing Technology Innovations, 6(1), 19-19. https://zenodo.org/record/7894245/files/rizapaper1rev7.pdf?download=1

de la Garza, J. M. S., y de los Santos Olivo, I. (2018). La dinámica del cambio constitucional en México. https://archivos.juridicas.unam.mx/www/bjv/libros/10/4828/34.pdf

Diario Oficial de la Federación [D.O.F.]. (2010). Ley Federal de Protección de Datos Personales en posesión de los particulares, 5 de julio de 2010, (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Diario Oficial de la Federación [D.O.F.]. (2016). Declaratoria de vigencia de la Norma Mexicana NMX-I-289-NYCE-2016, 19 de septiembre de 2016, (México). https://www.gob.mx/cms/uploads/attachment/file/836067/Anexo_11_Evidencia_Digital.pdf

Diario Oficial de la Federación [D.O.F.]. (2017). Diario Oficial de la Federación, 21 de enero de 2017, (México). https://dof.gob.mx/nota_detalle.php?codigo=5469925&fecha=25/01/2017#gsc.tab=0

Diario Oficial de la Federación [D.O.F.]. (2021). Diario Oficial de la Federación, 15 de septiembre de 2021, (México). https://www.dof.gob.mx/nota_detalle.php?codigo=5630010&fecha=15/09/2021#gsc.tab=0

Díaz-Diez, C. A. (2019). Significados del acto administrativo en la jurisprudencia de la Corte Constitucional. Estudios Socio-Jurídicos, 21(2), 259-291. http://www.scielo.org.co/scielo.php?pid=S0124-05792019000200259&script=sci_arttext

Dieterich, H. (2021). Nueva guía para la investigación científica. Grupo Editor Orfila Valentini. https://books.google.es/books?hl=es&lr=&id=6VxQEAAAQBAJ&oi=fnd&pg=PT9&dq=define+Investigaciones+cient%C3%ADficas&ots=bkA0RpaCGz&sig=IByvLVJkkVuKk8Ue7EZYniQNb-4#v=onepage&q=define%20Investigaciones%20cient%C3%ADficas&f=false

Digitalrecovery. (2023). Qué es la cinta magnética. https://digitalrecovery.com/es/que-es-la-cinta-magnetica/

Disk-drill. (2023). Disk Drill - the premium data recovery software. https://www.disk-drill.com/

DMDE. (2023). DMDE New Version 4.0.6. https://dmde.com/

Easeus. (2023). EaseUS Data Recovery Wizard. https://es.easeus.com/

Espinoza Mina, M. (2019). Informática forense: una revisión sistemática de la literatura. Revista de Ciencias Humanísticas y Sociales (ReHuSo), 4(2), 126-

145.http://scielo.senescyt.gob.ec/scielo.php?pid=S2550-65872019000200126&script=sci_arttext

Farfán Burga, E. (2020). Estudio y comparativa de condiciones ambientales de almacenamiento óptimas para la preservación de archivos magnéticos, ópticos y fílmicos. https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/18493

FBI. (2000). Forensic science communications. April 2000 - Volume 2 - Number 2. https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm#Proposed

FGR (2020). Desarrollo de las ciencias forenses en la investigación de hechos delictivos. https://www.gob.mx/cms/uploads/attachment/file/527390/12_FGR_C_FORENSES_CAPACITACI_N_2020.pdf

Gaytán Martínez, A., Pérez Pinto, J. A., Martínez Ponce, I. N. y Caamal Torres, F. J. I. (2019). Uso de las TIC en el estudio del Derecho Penal. http://148.217.50.3/jspui/bitstream/20.500.11845/1039/1/v20_n3_a9_Uso-de-las-TIC-en-el-estudio-del-derecho-penal.pdf

Getdata (2023). GetData Software Company. https://getdata.com/

González Becerril, K. (2019). Estudio Comparativo para Demostrar las Ventajas y Desventajas de las Unidades de Almacenamiento: Disco Duro y Unidad de Estado Sólido. http://ri.uaemex.mx/handle/20.500.11799/106032

González-Beltrán, V. A. (2022). Estrategia Didáctica para el Aprendizaje de la Legislación Informática con uso de la Tecnología Educativa. Revista Docentes 2.0, 15(1), 75-79. https://ojs.docentes20.com/index.php/revista-docentes20/article/view/277/800

Guiaspracticas. (2023). File carving. https://www.guiaspracticas.com/recuperacion-de-datos/file-carving

Guzmán Molina, A. A. (2023). Implementación de herramientas para la extracción de evidencia digital (Bachelor's thesis, Quito: EPN, 2023.). https://bibdigital.epn.edu.ec/bitstream/15000/23797/1/CD%2013084.pdf

Hernández, A. (13 de enero de 2023). El llamativo encanto de la informática forense https://empresas.blogthinkbig.com/el-llamativo-encanto-de-la-informatica-forense/#:~:text=De%20procesos%20y%20t%C3%A9rminos,ciberforense%2C%20digital%20forensics%2C%20etc.

Hernández-Sampieri, R., y Mendoza, C. (2020). Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta. Mcgraw-hill. https://www.academia.edu/download/64591365/Metodolog%C3%ADa%20de%20la%20investigaci%C3%B3n.%20Rutas%20cuantitativa,%20cualitativa%20y%20mixta.pdf

IBM (2023a). ¿Qué es el almacenamiento de datos? https://www.ibm.com/mx-es/topics/data-storage

IBM. (2021). Sistemas de archivos. https://www.ibm.com/docs/es/i/7.2?topic=system-file-systems

IBM. (2023b). ¿Qué es el almacenamiento de datos? https://www.ibm.com/mx-es/topics/data-storage

INFOCDMX. (2021). La legislación en materia de datos personales requiere ajustes ante el constante uso de TIC´S: enríquez rodríguez. Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México. https://infocdmx.org.mx/index.php/2-boletines/7131-dcs-079-21.html

Instituto Nacional de Estadística y Geografía [INEGI]. (2020).Estadísticas a propósito de las personas formadas en las ciencias de la computación y las TIC en México. INEGI. https://www.inegi.org.mx/contenidos/saladeprensa/aproposito/2020/FormacionTIC.pdf

Instituto Nacional de Estadística y Geografía [INEGI]. (2021). En hogares. México: INEGI. https://www.inegi.org.mx/temas/ticshogares/

ISO27000.es (2022). Serie "27000". https://www.iso27000.es/iso27000.html

León-Martínez, D. (2021). El desahogo de la prueba pericial en el juicio oral mercantil. Revista de Investigaciones Universidad del Quindío, 33(S2), 12-17. https://revistas.uniquindio.edu.co/ojs/index.php/riuq/article/view/605/611

Ley de Amparo. (2021) Reformada, Diario Oficial de la Federación [D.O.F.], 7 de junio de 2021, (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/LAmp.pdf

Ley Federal del Trabajo, [LFT.]. (2022), Reformada, Diario Oficial de la Federación [D.O.F.], 27 de diciembre de 2022, (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/LFT.pdf

leyes.co. (11 de septiembre de 2023). Código General del Proceso Artículo 226, Procedencia. https://leyes.co/codigo_general_del_proceso/226.htm

Main, K. (2023). The Best Data Recovery Software Of 2023. Forbes. https://www.forbes.com/advisor/business/software/best-data-recovery-software/

MARCIAL, N. (1996). Información: una propuesta conceptual. Ciencias de la información. – Vol. 27, nº 1, dic. 1996. – p. 190-195. https://www.academia.edu/download/33747341/Angulo_Marcial_Noel_-_Informacion_una_nueva_propuesta_conceptual_(2).pdf

Martín, A. (2014). La era del Zettabyte: así será Internet en 2015. Computer Hoy. https://computerhoy.com/noticias/internet/era-del-zettabyte-asi-sera-internet-2015-8521

Mascarell Palau, D. (2019). El concepto TIC en la educación en Artes Visuales en nuestra contemporaneidad. Influjos educativos en el aprendizaje en movilidad en el siglo XXI. Quaderns Digitals, 2019, núm. 89, p. 50-64. https://roderic.uv.es/bitstream/handle/10550/74054/138198.pdf?sequence=1&isAllowed=y

Mendelson, E. (2018). The Best Data Recovery Software. PC Magazine. https://www.pcmag.com/picks/the-best-data-recovery-software

Microsoft. (2021). ¿Qué es una cuenta de Microsoft Exchange?. https://support.microsoft.com/es-es/office/-qu%C3%A9-es-una-cuenta-de-microsoft-exchange-47f000aa-c2bf-48ac-9bc2-83e5c6036793

Minitool. (2023). MiniTool System Booster. https://www.minitool.com/

Moreno, G. (2019). Infografía: A la espera de un Big Bang de datos. Statista Infografías. https://es.statista.com/grafico/17734/cantidad-real-y-prevista-de-datos-generados-en-todo-el-mundo/

Muñoz, H., Canabal, J. D., Galindo, S. G., Zafra, B. S. Y Benítez, Y. J. (2020). Informática y auditoría forenses: Nuevas perspectivas en tiempos de COVID-19. Revista Espacios, 41(42). http://w.revistaespacios.com/a20v41n42/a20v41n42p32.pdf

Navarro, J. (junio, 2015). Definición de Ciencias de la Computación. DefiniciónABC. Desde https://www.definicionabc.com/tecnologia/ciencias-computacion.php

Nebreda, M. (2023). ¿Qué son las herramientas tecnológicas? Campus Training. https://www.campustraining.es/noticias/que-son-herramientas-tecnologicas/

Ng, J. (2018). Delphi method: a qualitative approach for quantitative results. Value in Health, 21, S54. https://www.valueinhealthjournal.com/article/S1098-3015(18)30747-2/fulltext

Oracle. (2023). ¿Qué es una base de datos?. https://www.oracle.com/mx/database/what-is-database/

Ortega, K. (2022). ¿Qué es la informática forense?. Saint Leo. https://worldcampus.saintleo.edu/noticias/que-es-la-informatica-forense-analisis-forense-informatico

Peña Vera, T. (2022). Etapas del análisis de la información documental. Revista Interamericana de Bibliotecología, 45(3). http://www.scielo.org.co/scielo.php?pid=S0120-09762022000300004&script=sci_arttext

PGR. (2018). Guía Técnica de cadena de custodia de evidencia digital. Unidad de investigaciones cibernéticas y operaciones tecnológicas. http://www.coahuilatransparente.gob.mx/disp/documentos_disp/GUÍA%20TÉCNICA%20DE%20CADENA%20DE%20CUSTODIA%20DE%20EVIDENCIA%20DIGITAL.pdf

Porto, J., Gardey, A. (2021). Definición de sistema jurídico - Qué es, Significado y Concepto. Definicion.de. Última actualización el 15 de julio de 2021. https://definicion.de/sistema-juridico/

Prosoft. (2023a). Mac Data Recovery Software. Data Rescue 6. https://www.prosofteng.com/mac-data-recovery

Prosoft. (2023b). Windows Data Recovery Software. Data Rescue 6. https://www.prosofteng.com/windows-data-recovery

Puransoftware. (2023). Puran File Recovery Description. https://www.puransoftware.com/File-Recovery.html

Quiña, G. N., Yoo, S. G. y Guarda, T. (2019). Recuperación de Datos en Dispositivos de Almacenamiento SSD Utilizando File Carving. Revista Ibérica de Sistemas e Tecnologías de Información, (E17), 490-498. https://www.researchgate.net/profile/Teresa-Guarda/publication/331178555_Data_recovery_on_SSD_storage_devices_using_file_carving/links/5fabe6be299bf18c5b64e129/Data-recovery-on-SSD-storage-devices-using-file-carving.pdf

Real Academia Española. (2018). Zettabyte. Diccionario de la lengua española (5a ed.). https://www.rae.es/dhle/zettabyte

Real Academia Española. (2022). Información. Diccionario de la lengua española. https://dle.rae.es/informaci%C3%B3n

Recuva. (2023). Recuva - easy way to recover deleted files. https://www.recuva.site/

RedHat (2018). El concepto del almacenamiento de datos. https://www.redhat.com/es/topics/data-storage

Ruíz, H. M. G. (2019). El nuevo sistema de justicia penal y sus incentivos y desafíos para el profesionalismo de la función policial. Desacatos. Revista de Ciencias Sociales, (60), 94-109. www.redalyc.org/journal/139/13964890006/13964890006.pdf

Sabino, C. (2014). El proceso de investigación. Editorial Episteme. http://paginas.ufm.edu/sabino/ingles/book/proceso_investigacion.pdf

Sánchez, F. (2019). Fundamentos epistémicos de la investigación cualitativa y cuantitativa: Consensos y disensos. Revista digital de investigación en docencia universitaria, 13(1), 102-122. http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2223-25162019000100008

Sandoval Silva, F. I. (2019). El perito, el informe pericial y la prueba científica: admisibilidad, criterios cualitativos e igualdad de armas. https://www.ateneo-odontologia.org.ar/articulos/lxiii02/articulo4.pdf

Senado España. (7 de octubre de 2022). Constitución Española. https://www.senado.es/web/conocersenado/normas/constitucion/detalleconstitucioncompleta/index.html#t1c2s1

SENADO. (2007). Gaceta del Senado. Comunicaciones de Ciudadanos Senadores. LX/2PPO-121-396/13967. https://www.senado.gob.mx/65/gaceta_del_senado/documento/13967

Significados.com. (2023). Hardware. https://www.significados.com/hardware/

Solano Oviedo, D. S., Roldán Álvarez, M. Á. y Vargas Montoya, H. F. (2023). Investigación forense digital en entidades del Estado colombiano: acercamiento a la Ley 1952 de 2019. Revista Logos Ciencia y Tecnología, 15(1), 122-140. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2422-42002023000100122

Stallman, R. (2021). Linux y el sistema GNU. Proyecto GNU - Free Software Foundation. https://www.gnu.org/gnu/linux-and-gnu.es.html

Stellar. (2023). Stellar Data Recovery. Best Data Recovery Software. https://www.stellarinfo.com/

Tornel Estrada, M. (2022). La ciberdelincuencia y las especialidades procesales de la prueba. https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/58083/TFG%20Tornel%20Estrada%2c%20Marina.pdf

Torres, M. E. (2020). Informática forense y el camino de la Evidencia digital. http://www.cyta.com.ar/biblioteca/bddoc/bdlibros/informatica_forence.htm

Truchado, J. (2019). UNE 71505; sistemas de gestión de evidencias electrónicas - govertis. https://www.govertis.com/une-71505-sistemas-de-gestion-de-evidencias-electronicas

Undelete360. (2022). Undelete 360. restore files accidentally deleted from your Computer, Recycle Bin, digital camera, flash drive. https://undelete360.com/

Valencia, A. (2019). La necesidad de contemplar los delitos informáticos en el Código Penal del estado de Michoacán. Poder Judicial Michoacán. Biblioteca, Libros y artículos electrónicos. https://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/indice.htm

Vázquez, A. (2022a). El panorama actual de la prueba digital en el contexto de la justicia electrónica en México en materia penal. Universita Ciencia, (27), 43-71. https://universita.ux.edu.mx/universita-ciencia/article/view/802/1330

Vázquez, C. (2022b). El juez ante el perito. Una breve introducción a los tema s tradicionales de la prueba pericial. Sistema Bibliotecario de la Suprema Corte de Justicia de la Nación Catalogación, 1. https://www.scjn.gob.mx/derechos-humanos/sites/default/files/Publicaciones/archivos/2022-04/MANUAL%20DE%20PRUEBA%20PERICIAL_DIGITAL.pdf

WhatsApp. (2023). Stay connected. https://www.whatsapp.com/stayconnected

Winmagic. (2022). SecureDoc V9.0. https://winmagic.com/en/data-security-support/release-notes/securedoc-v9/

Wisecleaner. (2023). Wise Data Recovery. https://www.wisecleaner.com/wise-data-recovery.html

Wondershare. (2023). Wondershare Recoverit. https://recoverit.wondershare.com/free-data-recovery/free-windows-10-data-recovery-software.html

ANEXOS**:**

ANEXO I: Glosario de términos

Ciencias de la computación:

Son todas las ramas de estudio de la informática, tanto hardware como software, uso de datos, sistematización lógica de procesos, metodologías, programación y análisis, que intentan dar soluciones a todas las esferas del conocimiento (Navarro, 2015).

Informatización de la sociedad:

O sociedad de la información, es la implantación de las tecnologías de información y comunicación (TIC) en la sociedad y en la vida cotidiana, en todas las relaciones sociales, culturales y económicas, sin las barreras del espacio y el tiempo con el fin de facilitar la comunicación (Etecé, 2021).

Legislaciones informáticas:

Disciplina derivada del uso de las TIC en el ámbito jurídico, es un conjunto de reglas jurídicas para la resolución de problemáticas (González-Beltrán ,2022).

Reformas Constitucionales:

Actividad normativa que contempla la modificación de las reglas de convivencia que rigen a la sociedad desde el ordenamiento jurídico (de la Garza, 2018).

Nuevo sistema de Justicia penal:

Son las audiencias en las que el juez, litigantes, testigos, acusado y peritos están presentes (Ruíz, 2019).

Código Nacional de Procedimientos Penales:

Normas para el procesamiento y sanción de delitos con el fin de esclarecer los hechos, asegurar la justicia, resolver el conflicto y resarcir los daños (CNPP, 2021).

Sistema jurídico:

Conjunto de normas constitucionales, métodos, procedimientos y reglas que constituyen el derecho, apoyadas en la jurisprudencia de los tribunales (Porto y Gardey, 2021).

Jurisprudencia:
Conjunto de sentencias, decisiones o fallos dictados por autoridades y los tribunales de justicia (Diaz-Diez, 2022).

Investigaciones científicas:
Proceso de reflexión, control y critica, busca aportar nuevos datos, se debe de contar con los elementos necesarios para sustentar la investigación y encontrar las causas, los pasos son: observación, recolección, formulación de hipótesis, experimentación y conclusión (Dieterich, 2021).

Audiencia:
Procedimiento en el cual un juez instruye y escucha los alegatos de las partes en un pleito con el fin de emitir un juicio, el lugar donde es realizado se denomina juzgado o tribunal (Arellano et al., 2020).

Desahogo de pruebas:
Proceso del análisis de los medios, evidencias y declaraciones de testigos o peritos, con el fin de tener valor probatorio ante un juez (León-Martínez, 2021).

Zettabytes:
Unidad de medida de información en dispositivos almacenamiento digital informáticos (RAE, 2018), un byte equivale a un carácter o letra y un Zbyte son 1 180 591 620 717 411 303 424 bytes, es difícil dimensionar lo que significa esta cantidad de información, un ejemplo de almacenamiento de 1 Zbyte seria tener un video de 36 millones de años en calidad de alta definición (Martín, 2014).

Hardware:

Termino en ingles que se refiere a equipos o componentes electrónicos tangibles en los sistemas informáticos (Significados.com, 2023).

Software:

Proviene del vocablo inglés y se refiere a lo intangible en informática como datos, aplicaciones, programas o toda la información almacenada en un dispositivo (Concepto,2022).

Sistemas de archivos

Estructura de clasificación y almacenamiento de información, referente a la asignación de espacio disponible para crear, archivar, administrar y mantener los datos de manera eficaz, existiendo diversos tipos de formato diferenciadas por su seguridad y técnicas de gestión: FAT, FAT32, NTFS, EXFAT, EXT3, EXT4, RAW, entre otras (IBM, 2021).

Sistema Operativo

Es un software que controla la comunicación de una computadora, este proporciona los medios para la interfaz entre un usuario y la máquina, un intermediario como traductor en las funciones y control del hardware (De la Cruz, 2023).

MAC OS

Sistema operativo de la compañía Apple, diseñado específicamente para componentes de la misma empresa como IPhone, iPad, MAC y más (De la Cruz, 2023).

Windows

Sistema de información más utilizado en el mundo, es una colección de programas de cómputo destinados al uso y manejo de información tecnológica por medio de una computadora (De la Cruz, 2023).

LINUX

Conjunto de aplicaciones informáticas que agrupadas generan un sistema en conjunto, propiciada principalmente a favor de la independencia del monopolio de compañías desarrolladoras, sistema creado por la colaboración y participación de una comunidad global de desarrolladores independientes en su mayoría (Stallman, 2021).

WhatsApp

Aplicación para comunicación por mensajería y llamadas, soportado en diversas plataformas de celulares o sistemas de cómputo (WhatsApp, 2023).

Exchange

Sistema manejador de cuenta de correo electrónico de la compañía Microsoft, de la plataforma del sistema operativo Windows (Microsoft, 2021)

Base de Datos

Las bases de datos son un conjunto de información organizada y estructurada, para este efecto de forma electrónica, controlada por un lenguaje manejador que facilita su manejo y consulta, en este caso SQL y por ejemplo software de compañías como Oracle, IBM, MySQL, entre otras. (Oracle, 2023)

Cintas de Almacenamiento

Tienen como objetivo almacenar información en cintas por medio de una inducción magnética, uno de los procesos más antiguos y más fácil de los métodos corporativos para realizar respaldos de información, manejando diversos estándares abiertos de almacenamientos de compresión y cifrado llamados LTO 1,2,3, entre otros (Digitalrecovery, 2023).

ANEXO II: Herramientas de recuperación de datos

ESTRATEGIA DE RECUPERACIÓN DE INFORMACIÓN CON EL USO DE HERRAMIENTAS TECNOLÓGICAS PARA EL DESARROLLO DE PERICIALES INFORMÁTICAS
Presentación
Buen día, La presente encuesta es realizada por Jesús Alberto Leiner Mendoza quien desea obtener el grado de Doctor en Administración en la Facultad de Administración de la Universidad Autónoma de Chihuahua. Solicito de su amable participación para el desarrollo de una investigación doctoral, la cual tiene el objetivo de señalar cuales son las herramientas tecnológicas más utilizadas en los procesos de recuperación de información en dispositivos de almacenamiento, así como su efectividad. La siguiente encuesta es con el fin de recabar información estadística importante para el desarrollo de esta y los datos proporcionados estarán resguardados bajo un estricto control de confidencialidad, por tal motivo es opcional el llenado de información confidencial, de antemano agradezco toda la información que pueda brindar para recabar estos datos, los cuales ayudaran al desarrollo estadístico de la investigación. Cualquier duda o aclaración sobre esta encuesta puede hacerla vía correo electrónico a la dirección alberto.leiner@hotmail.com

Instrucciones
El objetivo es identificar las características de las herramientas tecnológicas que utiliza para la recuperación de información en elementos de almacenamiento digital, en la siguiente tabla: **A)** Indique en la parte superior las Herramientas utilizadas por su empresa en el proceso de recuperación. **B)** Describa en la matriz la funcionalidad que cumple cada una de ellas (X).

		Indicadores													

Escriba el nombre de la(s) herramienta(s) tecnológica (s) que utiliza

LICENCIAMIENTO	Paga														
	Gratuita														
ALMACENAMIENTO	SSD														
	HD														
	USB														
	Tarjetas														
	Unidades Virtuales														
SISTEMAS	Windows														
	Servidores														
	Mac														
RECUPERACIÓN	Borrado														
	Formateo														
	Múltiples Formatos														
	Encriptado														
	Daño Físico														
	Arranque de Sistema														
	Correo / Exchange														
CELULARES	ANDROID	WhatsApp													
		Información													
		Sistema													
		Bloqueo													
	IOS	WhatsApp													
		Información													
		Sistema													
		Bloqueo													
Si detecta más funcionalidades puede enlistarlas a continuación															

Marque con una X solo la(s) característica(s) de cada herramienta (si aplica)

Conteste numéricamente con una escala del 1 al 5 donde:		1 Pésimo	2 Malo	3 Regular	4 Bueno	5 Excelente
Usabilidad / Facilidad en el uso						
Fiabilidad / Confianza						
Funcionabilidad / Estabilidad						
Eficiencia / Tiempo						
Seguridad / Recuperación de información						
Satisfacción						
Prioridad en el uso de cada una de ellas empezando con el No. 1 como la más utilizada						

Se gradece de antemano por su amable colaboración y los minutos que se tomó en responder, se despide Jesús Alberto Leiner Mendoza.

ANEXO III: Herramientas de recuperación

GetDataBack

Esta herramienta de paga está dedicada a la recuperación de información de dispositivos de almacenamiento digital, tanto de discos duros como dispositivos externos, soporta múltiples formatos en sistemas operativos Windows, Linux y Mac, además de realizar reparaciones de sistemas operativos, restaura archivos y carpetas borradas, dañadas o de unidades que perdieron su estructura o fueron formateadas y en el caso de unidades con daño físico puede realizar recuperación de la información si la unidad permite su manejo, trabajando desde la estructura d ellos archivos a su más mínimo nivel (Getdata, 2023).

SDRecovery

Herramienta gratuita dedicada a la restauración de información borrada de discos duros y dispositivos USB, es una potente y rápida pero limitada aplicación (Winmagic, 2023).

Undeleted 360

Programa rápido y eficiente en la recuperación de información eliminada, tiene la limitante que únicamente recupera archivos eliminados en dispositivos compatibles con Windows, su cualidad es la restauración de archivos en cualquier dispositivo que sea detectado como memoria USB (Undelete360, 2022).

Puran File Recovery

Herramienta exclusivamente diseñada para recuperar información de disco duros y memorias extraíbles utilizadas en sistemas operativos Windows, la bondad apremiante de esta utilería es que puede recuperar información incluso de celulares, siempre que su almacenamiento sea compatible con las versiones de archivos FAT y NTFS (PuranSoftware, 2016).

ANEXO IV: Encuesta: Lineamientos Pericial Informática.

Lineamientos para la estandarización en la elaboración de periciales informáticas
Presentación
Buen día, La presente encuesta es realizada por Jesús Alberto Leiner Mendoza quien desea obtener el grado de Doctor en Administración en la Facultad de Administración de la Universidad Autónoma de Chihuahua. Solicito de su amable participación para el desarrollo de una investigación doctoral, la cual tiene el objetivo se establecer los lineamientos adecuados para generar una propuesta en la elaboración de periciales informáticas en el proceso técnico de recuperación de información de dispositivos de almacenamiento digital. La siguiente encuesta es con el fin de recabar información estadística importante para mejorar la propuesta desarrollada, los datos proporcionados estarán resguardados bajo un estricto control de confidencialidad, por tal motivo es opcional el llenado de información confidencial, de antemano agradezco toda la información que pueda brindar para recabar estos datos, los cuales ayudaran al desarrollo estadístico de la investigación. Cualquier duda o aclaración sobre esta encuesta puede hacerla vía correo electrónico a la dirección alberto.leiner@hotmail.com
Instrucciones
El objetivo es que usted evalué la propuesta proporcionada, responda una pequeña encuesta donde se le solicita contestar una serie de preguntas y brindar su percepción y recomendaciones en cada una de ellas. A) Indique numéricamente como califica cada una de las características, utilizando una escala del 1 al 4, donde 1 es la menor ponderación y 5 es excelente. B) Así mismo se le solicita realizar una recomendación en cada pregunta si lo considera necesario. C) Finalmente, se le solicita realizar una breve critica general de la estrategia propuesta.

Lineamientos para la estandarización en la elaboración de periciales informáticas

¿ Considera que el proceso de identificación de la información cumple con los procesos necesarios?

1 Inaceptable **2** Regular **3** Satisfactorio **4** Notable **5** Excelente **Respuesta:**

Recomendaciones:

¿Considera que las directrices mencionadas en la recolección de la evidencia son adecuadas?

1 Muy inadecuada **2** Inadecuada **3** Moderada **4** Algo adecuada **5** Muy adecuada **Respuesta:**

Recomendaciones:

¿Usted considera que la técnica de preservación de la evidencia es la adecuada?

1 Muy inadecuada **2** Inadecuada **3** Moderada **4** Algo adecuada **5** Muy adecuada **Respuesta:**

Recomendaciones:

¿Cree que el cumplimiento de preservacion de la evidencia de estas directrices asegura la integridad total de los datos?

1 Muy deficiente **2** Deficiente **3** Medio **4** Bueno **5** Excelente **Respuesta:**

Recomendaciones:

¿Cree que la Calidad y la gestión descritas cumplen con los objetivos del proceso?

1 Muy deficiente **2** Deficiente **3** Medio **4** Bueno **5** Excelente **Respuesta:**

Recomendaciones:

¿ Considera que el proceso de análisis de la evidencia es el adecuado?

1 Muy inadecuado **2** Inadecuado **3** Moderado **4** Algo adecuado **5** Muy adecuado **Respuesta:**

Recomendaciones:

¿Cree que el reporte final contempla todos los puntos necesarios para su presentación en el informe pericial?

1 No del todo **2** Algo **3** Moderado **4** Bastante **5** Completamente **Respuesta:**

Recomendaciones:

¿Considera que la correcta aplicación de esta propuesta influiría de manera positiva en el desarrollo de futuras periciales informáticas?

1 Escasa **2** Justa **3** Buena **4** Muy buena **5** Excelente **Respuesta:**

Recomendaciones:

¿Considera que la propuesta descrita menciona buenas practicas en cada uno de los procesos?

1 Escasa **2** Justa **3** Buena **4** Muy buena **5** Excelente **Respuesta:**

Recomendaciones:

¿Cómo considera la calidad de los lineamientos descritos?

1 Inaceptable **2** Regular **3** Satisfactorio **4** Notable **5** Excelente **Respuesta:**

Recomendaciones:

¿Considera que la presente propuesta es eficiente y eficaz?

1 Escasa **2** Justa **3** Buena **4** Muy buena **5** Excelente **Respuesta:**

Recomendaciones:

¿Considera en términos generales que la aplicación de esta guía en el sistema jurídico cumpliría con las normativas o estándares que requieren para la elaboración de una pericial informática?

1 No del todo **2** Algo **3** Moderado **4** Bastante **5** Completamente **Respuesta:**

Recomendaciones:

Se gradece de antemano por su amable colaboración y los minutos que se tomó en responder, se despide Jesús Alberto Leiner

ANEXO V: Matriz de congruencia

Objetivo General	Hipótesis General	Preguntas de investigación	Objetivos específicos	Hipótesis	Método
Proponer una estrategia sistemática que fortalezca la elaboración de una pericial informática en la recuperación de información.	Una estrategia sistemática fortalece la elaboración de una pericial informática en la recuperación de información	¿Cuáles son las principales características de las herramientas tecnológicas utilizadas para la recuperación de información en elementos de almacenamiento digita?	Identificar las principales características de las herramientas tecnológicas utilizadas para la recuperación de información en elementos de almacenamiento digital.	Describir las principales características de las herramientas tecnológicas utilizadas para la recuperación de información en elementos de almacenamiento digital para preparar el instrumento de evaluación.	análisis Documental
		¿Cuáles herramientas tecnológicas son las más utilizadas en los procesos de recuperación de información en elementos de almacenamiento digita?	Establecer cuáles herramientas tecnológicas son las más utilizadas en los procesos de recuperación de información en elementos de almacenamiento digital.	Las herramientas tecnológicas más utilizadas por expertos para la recuperación de información en elementos de almacenamiento digital son Stellar Data Recovery y Wondershare Recoverit.	Encuesta

		¿Cuáles son los lineamientos y metodologías trascendentes para la elaboración de una pericial informática?	Determinar los lineamientos y metodologías trascendentes para la elaboración de una pericial informática.	El cumplimiento de los lineamientos y metodologías fortalece la elaboración de una pericial informática.	análisis Documental
		¿Cómo puede una estrategia de recuperación de información con el uso de herramientas tecnológicas fortalecer una pericial informática?	Diseñar una estrategia de recuperación de información con el uso de herramientas tecnológicas aplicadas en una pericial informática validada por el método Delphi.	Una estrategia de recuperación de información con el uso de herramientas tecnológicas fortalece un dictamen pericial informático.	Método Delphi