Plan de implementación de un laboratorio de informática forense caso de estudio Universidad Tecnológica de Pereira UTP

Biviana Yulieth Aguirre Arias

Informe final de trabajo de grado presentado como requisito parcial para optar al título de

Magister en seguridad de la información

Director (a):

Esp. Julio Cesar Cano Ramírez

MSc Luis Carlos Correa Ortiz

Seguridad de la información

Grupo de Investigación y Desarrollo en Informática y Telecomunicaciones

Universidad de Manizales

Facultad de Ciencias e Ingeniería

Maestría en seguridad de la información

Manizales, 2023

Resumen

La informática forense es una rama de la ciencia forense que se encarga de la presentación, análisis y recolección de pruebas digitales para ser utilizadas en casos judiciales. En Colombia, la delincuencia informática ha ido en aumento en años recientes, esto ha generado la necesidad de contar con expertos en informática forense capaces de recolectar y analizar pruebas digitales para ser utilizadas en la investigación y enjuiciamiento de delitos cibernéticos. Los laboratorios forenses en Colombia son fundamentales para mejorar la capacidad de investigación de delitos informáticos. A pesar de su importancia, en Colombia no existen suficientes laboratorios de informática forense que puedan hacer frente a la creciente demanda de análisis de evidencia digital. Por tal motivo, este trabajo de investigación se planteó el objetivo de plantear el diseño de un laboratorio de informática forense adecuado para contribuir con las necesidades actuales de seguridad informática en Colombia y cuya aplicación será en la Universidad Tecnológica de Pereira.

El desarrollo de esta propuesta estuvo fundamentado en un enfoque metodológico de paradigma cualitativo. El tipo de investigación se determinó con un alcance propositivo. Se pudo concluir que la planeación y el desarrollo de un laboratorio forense es un ejercicio complejo que no solo requiere pensar en un espacio adecuado, unos equipos especializados y un software específico para el análisis forense, sino también en contar con un equipo especializado de profesionales en el campo que presten servicios con ética y legalidad. Este trabajo es revelador en cuanto a todos los requisitos para la puesta en escena de un laboratorio de informática forense y espera ser una propuesta que se desarrolle a futuro con la universidad.

Palabras clave: informática forense, ciencias forenses, evidencia digital, laboratorio de informática forense, seguridad informática.

Abstract

Computer forensics is a branch of forensic science that deals with the collection, analysis, and presentation of digital evidence for use in legal cases. In Colombia, information technology has been increasing in recent years, which has generated the need for experts in computer forensics capable of collecting and analyzing digital evidence to be used in the investigation and prosecution of cybercrimes. Forensic laboratories in Colombia are essential to improve the capacity to investigate cybercrime. Despite its importance, in Colombia there are not enough computer forensics laboratories that can cope with the growing demand for digital evidence analysis. For this reason, this research work set out the objective of proposing a suitable forensic computer laboratory design to meet the current computer security needs in Colombia and whose application will be at the Technological University of Pereira.

The development of this proposal was based on a qualitative paradigm methodological approach. The type of research continues with a purposeful scope. It was possible to conclude that the planning and development of a forensic laboratory is a complex exercise that not only requires thinking about an adequate space, specialized equipment and specific software for forensic analysis, but also having a specialized team of professionals in the field that provide services ethically and legally. This work is revealing in terms of all the requirements for setting up a forensic computer laboratory and hopes to be a proposal that will be developed in the future with the university.

Keywords: computer forensics, forensic science, digital evidence, computer forensics laboratory, Informatic security.

Contenido

Pág.

Lista de tablas

Lista de figuras

1. Planteamiento del problema de investigación y su justificación

1.1 Descripción del área problemática

La informática forense es una rama de la ciencia forense que se encarga de la recolección, análisis y presentación de pruebas digitales para ser utilizadas en casos judiciales. En Colombia, la delincuencia informática ha aumentado recientemente, lo que ha generado la necesidad de contar con expertos en informática forense capaces de recolectar y analizar pruebas digitales para ser utilizadas en la investigación y enjuiciamiento de delitos cibernéticos.

El área problémica de este trabajo investigativo se centra el diseño de un laboratorio de informática forense para la Universidad Tecnológica de Pereira teniendo en cuenta la falta de recursos y herramientas para la recopilar, analizar y presentar pruebas digitales en casos judiciales en Colombia. Según el Informe de Ciberseguridad 2021 de Kaspersky, Colombia ocupa el quinto lugar en la región latinoamericana en cuanto a incidentes de seguridad cibernética, siendo los ataques de malware, phishing y ransomware los más comunes (Kaspersky, 2021).

La falta de recursos y herramientas adecuadas en los laboratorios de informática forense en Colombia ha sido un problema recurrente que ha dificultado la investigación y enjuiciamiento de delitos cibernéticos. Según un estudio realizado por la Policía Nacional de Colombia, se encontró que esto ha limitado la capacidad de recolección y análisis de pruebas digitales, lo que ha resultado en la pérdida de evidencia digital relevante en casos judiciales (Vargas et al., 2022).

En Colombia, la delincuencia informática ha aumentado en los últimos años, erigiéndose en uno de los problemas más importantes para las autoridades. De acuerdo con la Policía Nacional de Colombia, en el 2020 se registraron más de 14.000 denuncias relacionadas con delitos informáticos, lo que representa un aumento del 66% con respecto al año anterior (Policía Nacional de Colombia, 2021).

A pesar de la gravedad de la situación, en Colombia no existen suficientes laboratorios de informática forense que puedan hacer frente a la creciente demanda de análisis de material digital. Según un estudio de la Fiscalía General de la Nación, existen únicamente 21 laboratorios de informática forense en el país, y estos se encuentran en las ciudades principales, dejando grandes vacíos en áreas geográficas importantes, lo que limita el acceso a la justicia de muchas personas (Fiscalía General de la Nación, 2020).

Esta falta de laboratorios de informática forense también conlleva a que los casos de delitos informáticos se queden sin resolver o se resuelvan de manera deficiente debido a la falta de experiencia y capacitación en informática forense. Además, en muchos casos, la evidencia digital se puede perder debido a la falta de conocimientos en el manejo de la misma, lo que hace que las pruebas no sean admisibles en un juicio (Cuevas & Sánchez, 2018).

Otro problema que enfrenta la informática forense en Colombia es la falta de un marco legal sólido que regule su uso. Aunque existen algunas normativas que se enfocan en salvaguardar datos personales y combatir la delincuencia informática, no hay una ley específica que regule la informática forense, lo que hace que en muchos casos los peritos no estén seguros sobre qué prácticas son legales o no, y los jueces no tengan una base legal sólida para tomar decisiones (Gómez & Rincón, 2020).

Por lo tanto, el diseño de un laboratorio de informática forense acorde a los requerimientos y necesidades de la Universidad Tecnológica de Pereira, en Colombia, es crucial para abordar los problemas mencionados anteriormente. El laboratorio debe estar equipado con tecnología de vanguardia, contar con expertos en informática forense altamente capacitados y procedimientos ajustados tanto al marco legal existente, como a normas nacionales e internacionales, lo que permitiría una mayor eficacia en la recolección, preservación y análisis de la evidencia digital. Esto a su vez, podría ayudar a mejorar la capacidad de la justicia para investigar y resolver casos de delitos informáticos.

La definición de los servicios que se ofrecerán en el laboratorio de informática forense es también importante, ya que esto permitiría identificar las necesidades actuales del mercado y la industria. Según la Cámara de Comercio de Bogotá, los principales sectores afectados por la delincuencia informática en Colombia son el financiero, el de las telecomunicaciones y el de la salud (Cámara de Comercio de Bogotá, 2019).

Por otro lado, uno de los principales desafíos en la construcción de un laboratorio forense en una universidad es la necesidad de contar con un equipo de expertos altamente capacitados y experimentados, tanto en términos de técnicas de análisis forense como en el manejo de evidencias. Según Garrido et al. (2020), el personal encargado de la gestión y operación de los laboratorios forenses debe tener una formación académica sólida en áreas como la química forense, la biología molecular y la criminalística, así como una experiencia considerable en la aplicación de técnicas de análisis y en la interpretación de resultados.

Para respaldar aún más este argumento, se puede citar a otros expertos en el ámbito de la ciencia forense y la investigación criminal. Por ejemplo, según el National Institute of Justice (NIJ)

de los Estados Unidos, el personal de un laboratorio forense debe ser altamente capacitado en una variedad de disciplinas, incluyendo la biología, la química, la física, la informática y las ciencias sociales. Además, deben tener experiencia en la recolección, eventual examen e interpretación de datos forenses, así como en la comunicación clara y efectiva de los hallazgos a los investigadores y el sistema judicial.

Así mismo, la Asociación Americana de Química Forense - AAFS señala que los analistas forenses deben tener una formación sólida en química y conocimientos específicos en técnicas de análisis como la espectroscopia, la cromatografía y la espectrometría de masas, entre otras. También deben estar familiarizados con las buenas prácticas de laboratorio y tener habilidades en la gestión de datos y la interpretación de resultados.

Además, según el Consejo Internacional de Estándares en la Educación Forense - IAFSE, la formación de los profesionales en ciencias forenses debe ser continua y actualizada para mantenerse a la vanguardia con los avances tecnológicos y las nuevas estrategias de análisis. Por lo tanto, los laboratorios forenses en universidades deben proporcionar oportunidades de capacitación y desarrollo profesional para su personal. El equipo que esta idea requiere debe estar altamente capacitado y experimentado en diversas disciplinas, con conocimientos específicos en técnicas de análisis y habilidades en la gestión de datos y la interpretación de resultados. La formación continua y actualizada del personal es esencial para mantener los estándares de calidad y proporcionar servicios forenses confiables a la comunidad.

En definitiva, pensar en el diseño de un laboratorio de informática forense no solo requiere pensar en las herramientas (equipos, recursos y espacios) necesarios para su montaje físico y

logístico, sino también pensar en el personal y su capacitación, para el manejo de la seguridad informática. Es, en cualquier caso, una propuesta que se debe apoyar desde diferentes instancias.

1.2 Formulación del problema

El problema que se aborda en este proyecto de investigación es la necesidad de crear un laboratorio de informática forense en la Universidad Tecnológica de Pereira que satisfaga las necesidades actuales de seguridad informática en Colombia. La falta de este tipo de laboratorios en la universidad y en la región implica una limitación en la capacidad de investigación y resolución de delitos informáticos en el país. Los delitos informáticos están en constante aumento en Colombia, lo que ha llevado a que se incrementen los esfuerzos en la investigación judicial de estos casos. Sin embargo, la falta de recursos y tecnología especializada en los laboratorios de investigación y peritaje digital limitan su capacidad para llevar a cabo investigaciones efectivas. Por tanto, la creación de un laboratorio de informática forense en la Universidad Tecnológica de Pereira permitiría abordar de manera más eficaz los delitos informáticos en la región y mejorar la capacidad de investigación en Colombia.

Para lograr este objetivo, se requiere definir los servicios que se ofrecerán en el laboratorio de informática forense, considerando las necesidades actuales del mercado y la industria. Además, se debe determinar la infraestructura necesaria para el laboratorio, incluyendo equipos de hardware y software, herramientas de estudio y almacenamiento de datos. La escasez de tecnología especializada y recursos limitados para su adquisición son un obstáculo importante en la creación de un laboratorio de este tipo, por lo que se debe buscar una solución adecuada a esta problemática.

Otro aspecto importante para considerar en la creación del laboratorio de informática forense es la necesidad de cumplir con los estándares de calidad y normativas vigentes. Es necesario identificar los protocolos y guías de operación que se aplican en los laboratorios de informática forense en Colombia para garantizar su cumplimiento y así evitar la posibilidad de errores en las investigaciones y la recolección de pruebas. La falta de cumplimiento de estas normas puede llevar a que las pruebas obtenidas no sean válidas en un proceso judicial.

Es necesario seleccionar las herramientas y tecnologías necesarias para la gestión del laboratorio de informática forense. Esto incluye la selección de software especializado para análisis forense y la definición de los procedimientos y protocolos para su uso efectivo. La selección adecuada de estas herramientas y tecnologías será un factor determinante en el éxito del laboratorio de informática forense, por lo que se requiere de expertos en la materia para su selección y utilización adecuada.

Pues bien, existe una necesidad de constituir un laboratorio de informática forense en la Universidad Tecnológica de Pereira que permita asegurar la seguridad informática, especialmente teniendo en cuenta las transformaciones de la sociedad del conocimiento a raíz del uso de las tecnologías. Para lograr este objetivo, se deben definir los servicios que se ofrecerán, determinar la infraestructura necesaria, identificar los protocolos y guías de operación que se aplican en los laboratorios de informática forense en Colombia y seleccionar las herramientas y tecnologías necesarias para la gestión del laboratorio. Esto permitirá mejorar la capacidad de investigación y resolución de delitos informáticos en Colombia y contribuirá a un país más seguro y protegido contra el crimen digital.

En consideración de lo anterior, la pregunta problema que se propone es la siguiente:

¿Cuáles serán las características de una propuesta de desarrollo de un laboratorio de informática forense con infraestructura tecnológica especializada en la Universidad Tecnológica de Pereira que cumpla con las necesidades de seguridad informática en Colombia?

1.3 Justificación

La informática forense se ha erigido en un área crucial en la investigación de delitos informáticos, y su importancia ha aumentado en la última década debido al creciente número de casos de delitos informáticos en todo el mundo. En Colombia, aunque se han hecho esfuerzos significativos para establecer políticas y regulaciones para abordar los delitos informáticos, aún existe una necesidad crítica de mejorar la capacidad forense en este campo. Una de las razones más importantes por las que se necesita mejorar la capacidad forense en Colombia es la complejidad de las investigaciones de delitos informáticos. Este tipo de delitos pueden ser muy complicados y difíciles de investigar debido a la gran cantidad de tecnologías y herramientas informáticas involucradas. Además, la tecnología utilizada en estos casos está en constante evolución, lo que significa que los investigadores y los analistas forenses deben estar actualizados constantemente en las últimas tendencias y técnicas de la informática forense.

En ese orden de ideas, los laboratorios forenses en Colombia son fundamentales para mejorar la capacidad de investigación de delitos informáticos. Estos laboratorios son entornos especializados que permiten a los investigadores y analistas forenses realizar investigaciones más eficientes y efectivas. Se requiere que estén equipados con las últimas tecnologías y herramientas informáticas especializadas en informática forense, y están diseñados para garantizar la seguridad y la originalidad de los datos durante todo el proceso de investigación.

Además, los laboratorios especializados, como se proponen en este estudio, son esenciales para garantizar la adquisición y preservación adecuadas de la evidencia digital. Este tipo de evidencia es extremadamente delicada y puede ser fácilmente alterada o destruida si no se maneja de manera adecuada. En un laboratorio forense, los investigadores y analistas forenses pueden seguir los protocolos y procedimientos establecidos para adquirir y preservar adecuadamente la evidencia digital. Esto garantiza la integridad y autenticidad de la evidencia, lo que es crucial para que cualquier investigación de delitos informáticos llegue a buen puerto.

Otra ventaja importante de los laboratorios forenses es que permiten a los investigadores y analistas forenses trabajar en un entorno seguro y controlado. Los laboratorios están diseñados para garantizar la seguridad física de la evidencia y también están protegidos por medidas de seguridad informáticas avanzadas. Esto significa que los investigadores pueden trabajar sin preocuparse por la seguridad de la evidencia o la integridad de sus propias herramientas y equipos.

Además, la creación de estos espacios tecnológicos se propone como mejorar la eficiencia y eficacia de las investigaciones de delitos informáticos. Los laboratorios forenses permiten a los investigadores y analistas forenses trabajar en equipo, lo que significa que pueden compartir información y conocimientos para resolver casos de manera más rápida y eficiente. Además, el acceso a herramientas especializadas y tecnologías de última generación en informática forense puede acelerar el proceso de análisis y reducir el tiempo necesario para resolver casos.

Cabe destacar que la informática es una disciplina en constante evolución debido que los delitos informáticos y la necesidad de encontrar soluciones a los mismos han incrementado. En este sentido, es crucial contar con una fuerza laboral altamente capacitada en informática forense para poder hacer frente a los retos y desafíos que se presentan en la actualidad.

En la Universidad Tecnológica de Pereira, es necesario contar con más personas especializadas en informática forense debido a que, en cuanto el uso de la tecnología aumenta, también lo hacen los delitos informáticos. Los estudiantes que se especializan en informática forense aprenden a recolectar, analizar y presentar evidencia digital de manera efectiva y ética. Además, son capaces de detectar y prevenir delitos informáticos y de proteger la información digital de las organizaciones. En este sentido, esta propuesta se presenta como una solución viable y necesaria. Un laboratorio de este tipo proporcionaría un espacio físico especializado para la enseñanza y el aprendizaje de la informática forense. Además, ofrecería un entorno controlado y seguro para llevar a cabo pruebas y experimentos con tecnologías forenses.

Ahora, la creciente incidencia de delitos informáticos requiere más cuidado y estudio. Estos delitos van desde la usurpación de identidad y el hurto de información personal hasta el fraude financiero y el ciberacoso. La informática forense es una herramienta esencial en la lucha contra estos delitos, ya que permite la recolección y análisis de pruebas digitales para la resolución de casos. Al mismo tiempo, los laboratorios de informática forense en Colombia pueden ser utilizados por agencias gubernamentales, organizaciones privadas y empresas para proteger sus datos y evitar delitos informáticos. Estos laboratorios pueden ayudar a las organizaciones a establecer políticas de cuidado y protección de la información y a implementar medidas de prevención y respuesta ante incidentes.

En términos técnicos, un laboratorio de informática forense debe contar con una serie de equipos y herramientas diseñadas exclusivamente para llevar a cabo la recolección y análisis de pruebas digitales. Estos equipos incluyen computadoras, dispositivos de almacenamiento, dispositivos móviles, redes y servidores. Además, se requiere software especializado para adquirir,

analizar y presentar la evidencia digital. El personal encargado de trabajar en un laboratorio de informática forense debe estar altamente capacitado y tener experiencia en la recolección y análisis de pruebas digitales. Además, deben tener un conocimiento profundo de las normativas y regulaciones que determinan la recolección de pruebas digitales y la presentación de evidencia en un tribunal.

Además, estos laboratorios permitirían a los investigadores y expertos forenses acceder a tecnología de última generación y herramientas especializadas para la recuperación de datos, análisis de malware, identificación de evidencia digital y análisis de redes. Esto permitiría una investigación más precisa y eficiente, lo que a su vez podría aumentar las tasas de resolución de delitos informáticos y mejorar la capacidad de respuesta de las autoridades frente a este tipo de delitos. Otro beneficio importante, es la posibilidad de colaborar con instituciones y empresas en la protección de la propiedad intelectual, la prevención de fraudes y la protección de la privacidad de los usuarios de internet. Esto podría generar nuevas oportunidades de investigación y desarrollo tecnológico, así como fortalecer la capacidad del país para enfrentar la creciente amenaza de la ciberdelincuencia.

En suma, esos espacios en la Universidad Tecnológica de Pereira y en Colombia en general son una necesidad apremiante, pues, son una inversión estratégica en la formación de profesionales altamente capacitados y en la adopción de tecnologías avanzadas que permitan luchar eficazmente contra los delitos informáticos. Esto no solo aumentaría la capacidad de respuesta del país frente a las amenazas de tipo cibernético, sino que también ayudaría a consolidar a Colombia como un país referente en el ámbito de la seguridad informática a nivel internacional.

2. Objetivos

2.1 Objetivo general

Diseñar un laboratorio de informática forense adecuado para satisfacer las necesidades actuales de seguridad informática de Colombia en la Universidad Tecnológica de Pereira.

2.2 Objetivos específicos

- Definir los servicios que se ofrecerán en el laboratorio de informática forense, considerando las necesidades actuales del mercado y la industria.
- Determinar la infraestructura necesaria para el laboratorio de informática forense, incluyendo equipos de hardware y software, herramientas de análisis y almacenamiento de datos.
- Identificar los protocolos y guías de operación que se aplican en los laboratorios de informática forense en Colombia, para garantizar el cumplimiento de los loneamientos de calidad y las normativas vigentes.
- Seleccionar las herramientas y tecnologías necesarias para la gestión del laboratorio de informática forense, incluyendo la selección de software especializado para análisis forense y la definición de los procedimientos y protocolos para su uso efectivo.

3. Antecedentes

Sobre la seguridad informática y la informática forense se han desarrollado una serie de investigaciones tanto a nivel nacional como internacional, en español e inglés, teniendo en cuenta sobre todo la creciente transformación de la sociedad hacia el permanente uso de las tecnologías de la información y la comunicación. Como se ha venido insistiendo, la seguridad de la información es primordial en estos sistemas, pues muchas veces se trata de datos sensibles que requieren de un tratamiento especial.

En español a nivel latinoamericano se encuentra el trabajo de Di Lorio et al. (2016) con su artículo sobre "Consideraciones para el diseño de un Laboratorio Judicial en Informática Forense" que es especialmente relevante para este trabajo investigativo en la medida en la que propone la creación de un laboratorio forense a través de una guía que presentó cuestiones y desafíos para este tipo de espacios, a través de una metodología de trabajo cualitativa de alcance propositivo. Esta propuesta se ubicó en Argentina, reconociendo la necesidad de este país en materia de seguridad informática y permitió concluir que se requieren una serie de recursos físicos y económicos para lograr consolidar este tipo de laboratorios.

En su artículo "InFo-Lab, un laboratorio mixto de investigación y desarrollo de tecnología en Informática Forense" los autores Lerena et al. (2016) presentaron un proyecto de Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense – InfoLab en colaboración con la Universidad FASTA y el Ministerio Público de la Provincia de Buenos Aires, presentando la importancia del trabajo académico junto con el poder judicial (Estado – Universidad) para la creación de este tipo de recursos. A través de una metodología cualitativa, los autores muestran todos los esfuerzos hechos para la consolidación del laboratorio, por lo cual es un aporte valioso

que resalta, sobre todo, la relación entre el gobierno y las universidades para generar estos laboratorios, que bien se podría replicar en Colombia.

Precisamente, en el contexto colombiano, González- et al. (2019) en su artículo sobre "Laboratorios de informática para mejorar el proceso de cumplimiento fiscal de Colombia" ponen a discusión la importancia de la informática forense para abordar problemáticas como la evasión fiscal. A través de un ejercicio cualitativo de alcance analíticos, reconocen que los procesos de la DIAN para superar esta problemática se verían beneficiados. Este trabajo permite analizar la variedad del uso de un laboratorio de informática forense, revelando todavía más su relevancia dentro del país y la necesidad de crear más laboratorios en alianza con las universidades del país.

Por último, Bustamante (2021) hace una revisión de la información desde el enfoque cualitativo, en su artículo titulado "Avances de la Informática Forense en Colombia en los últimos cuatro años" a través de este tipo de trabajos se puede conocer qué tanto ha avanzado el país en materia de informática forense y cuidado del proceso de custodia de la evidencia digital en delitos informáticos, revelando además los modos de actuar de los delincuentes informáticos tomando como ejemplo algunos casos en la industria colombiana. El autor concluye así que el país necesita involucrar más herramientas tecnológicas en el manejo de los delitos informática, innovando por ejemplo desde sus laboratorios de informática forense; pero también en el sentido académico, brindando mayor capacitación a estudiantes de ingeniería de sistemas y afines, así como dentro del poder judicial para contar con profesionales cada vez más preparados para trabajar con herramientas forenses tecnológicas.

Ahora bien, en cuanto al contexto internacional, en investigaciones en idioma inglés se encuentra una gran variedad que soporta la importancia de la informática forense y el desarrollo d ellos laboratorios de informática forense.

Para empezar, Yudistira y Widijowati (2023) en su artículo "Evidence Using Forensic Laboratory in Revealing the Crime of Murder" revelan la importancia del uso de laboratorios forenses para ayudar a resolver casos de crímenes por homicidio. Este artículo tuvo como objetivo analizar el papel de los laboratorios forenses y los esfuerzos realizados por la Policía Nacional para involucrar a los laboratorios forenses en pruebas que ayuden a esclarecer el delito de homicidio. A través de un análisis descriptivo de enfoque cualitativo, los autores mostraron que la función y papel de los laboratorios forenses en relación al proceso judicial como medio de prueba en los tribunales es corroborar/dar certeza a la información, determinar relaciones de causa y efecto, probar si ciertos factores o fenómenos son o no verdaderos, elaborar argumentos a partir de un fenómeno si se ha demostrado que es cierto, y ser un medio de prueba en los tribunales para definir y explicar las causas de la muerte de una persona, de modo que sea de mayor apoyo en el proceso de justicia penal. Este trabajo evidencia la utilidad que tienen los laboratorios forenses para los órganos judiciales para resolver delitos.

Por otra parte, en el artículo "Laboratory Forensics for Open Science Readiness: an Investigative Approach to Research Data Management" de Lefebvre y Spruit (2021) abren la puerta a temáticas más actuales como el manejo de datos a gran escala, más conocido como Big Data. En este caso, a través de una metodología cualitativa, los autores concluyeron que era necesario que los laboratorios sigan una visión de preparación científica abierta en la gestión de

datos de investigación que se centre en aumentar la calidad de la información para una mayor preservación y difusión de datos de investigación (abiertos).

En el "Role Of Crime Laboratories: Scope And Prospective In Criminal Investigation - Survey Based Analysis", los autores Qureshi y Ramprakash (2022) analizan el rol de los laboratorios de informática forense desde una metodología de revisión de literatura, con el propósito de brindar al lector un estado del arte de la problemática mencionada. De acuerdo con el análisis hecho, se encontró que uno de los obstáculos más frecuentes a la hora de manejar un laboratorio de informática forense se encuentra en la adecuación de espacios seguros, el uso de herramientas (aparatos y sistemas) complejos e innovadores y la seguridad de la información y la evidencia recolectada. Estas problemáticas son más evidentes en el caso de laboratorios que no son preparados adecuadamente y con propósitos de trabajo y práctica manejados por personas que no están suficientemente capacitadas para ello.

Finalmente, Wickenheiser (2021) en su artículo "Reimagining forensic science – The mission of the forensic laboratory" se propone re imaginar la misión de los laboratorios de informática forense. Desde allí plantea una cuestión de la que poco se habla respecto a los laboratorios de informática forense: que su competitividad está mediada por el tiempo que demoran en hacer un análisis y proporcionar un informe final. Por lo tanto, el laboratorio que menos tiempo demore el informe, más posibilidades tendrá de resaltar; sin embargo, esto no es siempre posible porque el manejo de la información y la evidencia digital es un proceso complejo. Esto sin tener en cuenta que en el caso de estar frente a un caso de delito informático, el laboratorio generalmente trabajará con una autoridad judicial, por lo cual se trata de tareas que llevan tiempo y por lo tanto, requieren ser automatizadas o manejadas con un mayor dinamismo. En ese sentido,

los laboratorios deben contar con personal preparado para el manejo de las herramientas y que además le dé un manejo adecuado a la evidencia digital.

De acuerdo con esta evidencia científica, la estructuración de los LIF desde espacios académicos se ha convertido en estrategias de inversión en seguridad cibernética o digital en diferentes países, donde sus resultados han demostrado grandes beneficios en el campo judicial y pericial, sin aun identificarlos o correlacionarlos con los obtenidos desde la academia y su extensión a la innovación.

4. Referente normativo y legal

En Colombia, el marco legal para abordar los delitos informáticos se enmarca dentro de dos campos importantes: la jurisprudencia asociada al concepto y naturaleza jurídica del delito informático y la jurisprudencia y dimensión legal asociada a las evidencias. La necesidad de integrar jurisprudencia al escenario colombiano resulta ser producto de la realidad actual de la violencia y los crímenes, los cuales en su mayoría suponen alguna relación con material digital e informático. Por lo tanto, el acercamiento al marco legal sobre el delito informático supone gran relevancia para la práctica de la informática forense, en la medida que dicta las posibilidades y alcances de la actividad profesional en el marco de acciones judiciales lícitas y validas en cualquier escenario que requiera de dicho material probatorio.

Frente al marco de leyes relacionados con la tipificación del delito informático y la seguridad informática se pueden revisar las siguientes referencias:

Tabla 1. *Marco legal – Delitos informáticos y seguridad informática*

Normativa	Nombre	Descripción y Alcances
Ley 599 de 2000	"Por la cual se expide el Código Penal"	Tiene como propósito regular los delitos penales cometidos en territorio colombiano o en aquellos casos en donde los convenios y tratados internacionales le permitan a Colombia regular. Dentro del código penal, los artículos 192 a 197, tipifican los delitos relacionados con la violación a la intimidad o la acción de intercepción de comunicaciones. Tal tipificación involucra acciones como la violación de la comunicación entre personas mediante medios digitales, el comercio ilegal de equipos para interceptación de comunicaciones, la divulgación de datos confidenciales, el acceso no autorizado a sistemas informáticos y el uso inadecuado de equipos tecnológicos con capacidad para interceptar comunicaciones. Por otra parte, el artículo 219-A es un importante referente de tipificación del delito asociado al uso de los sistemas y la red de internet para la prostitución infantil. Se encuentra también el artículo 257, que relaciona la prestación o uso ilegal de servicios de telecomunicaciones; los artículos 269ª a 272 que relacionan todos los diferentes delitos asociados al cuidado de la información y los datos como también los delitos asociados a la violación de los derechos de autor.

		Lo anterior no supe que ninguno de los artículos no mencianos en esta revisión no pueda involucrar acciones delictivas que comprometan el uso de aparatos informáticos, pero dicho articulado compromete directamente el uso de equipos.
Ley 1273 de 2009	"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".	Esta ley profundiza y detalla con independencia un marco jurídico especial para la tipificación de los delitos asociados al cuidado de la información y los datos. Así, se crean un nuevo conjunto de tipos penales para situaciones delictivas que vulneren información y datos personales de ciudadanos. Algunos casos paradigmáticos que se relacionan con la seguridad informática corresponden a delitos como vulneración de sistemas informáticos y suplantación para el acceso a información bancaria y robo de identidad.
Ley 527 de 1999	"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".	Dicta las disposiciones sobre el uso de mensajes de datos, firmas y comercio digital, dictando disposiciones importantes sobre el valor judicial y los alcances que los mensajes de datos pueden tener en un escenario probatorio.
Ley 600 de 2000	"Por la cual se expide el Código de Procedimiento Penal".	En este código se presenta un articulado relevante para la práctica de la informática, el cual corresponde a la prueba pericial y el valor de las pruebas.

Ley 1564 de 2012	"Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones".	En lo que respecta a la actividad profesional forense, dicta algunas disposiciones generales relacionas con la naturaleza de la prueba pericial y el valor probatorio de ciertos materiales que operan como insumos dentro del proceso de procesamiento de evidencias
Ley 270 de 1996. Art. 96	Ley Estatutaria de la Administración de Justicia	Establece los lineamientos legales y principios de la administración de justicia. Entre estos, manifiesta en su artículo 1° que la administración de justicia es la función que en el ordenamiento público debe cumplir el Estado colombiano por cuenta de lo dispuesto en la Constitución Política de 1991 en pro de hacer efectivos todos los derechos y garantías relacionados con las diferentes libertades de los ciudadanos colombianos, esto con el fin de prestar las condiciones necesarias para una convivencia armoniosa y equilibrada bajo las distintas circunstancias de la vida nacional. El artículo 2° de esta ley afirma que el Estado colombiano debe garantizar el acceso a la justicia para todos los ciudadanos y ciudadanas adscritos a la administración de justicia. Aspectos a tener en cuenta en la búsqueda del orden nacional como el amparo a quienes viven en la pobreza y la defensoría pública estarán a cargo de estas personas, de igual forma establece que, en cada municipio del territorio nacional habrá, al menos, un defensor público. Por su parte, el artículo 3° establece que el derecho a la defensa está garantizado en toda la diversidad de acciones judiciales o administrativas sin que exista algún tipo de excepción. Esto en concordancia con lo dispuesto en la Constitución Política y en los diferentes tratados internacionales a los cuales el Estado colombiano se encuentra adscrito. Por otro lado, los estudiantes de derecho o leyes de universidades debidamente certificadas para impartir estos contenidos podrán ejercer la defensa de los ciudadanos que así lo requieran dentro del marco legal dispuesto para ello. El aspecto relevante para este trabajo que esta ley proporciona está en su artículo 95, el cual establece la relevancia y pertinencia de la inclusión y el consecuente uso de las tecnologías en el campo de la administración de justicia, para ello, el Consejo Superior de la Judicatura debe contemplar la adopción de tecnologías avanzadas a disposición del servicio de la administración pública.
Ley 1437 de 2011. Art. 216	"Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo".	Tiene como razón de ser salvaguardar y garantizar todos los derechos y las libertades de los ciudadanos colombianos, considerando como prioridad el interés o bien general sobre el común bajo la estricta sujeción a la Constitución Política por parte de las autoridades estatales. Para cumplir con dicho fin, el artículo 216 establece que es admisible el uso de los distintos medios electrónicos de avanzada tecnología para robustecer la búsqueda de materiales probatorios (MP), esto, de conformidad con lo dispuesto en la normatividad que regula la incautación y manejo de materiales probatorios y en concordancia con los códigos pertinentes, esto es, Código Penal y Código de Procedimiento Civil y las disposiciones planteadas en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

Decreto 2609* y 2364 del 2012. Decreto 333*** de 2014**	*"Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado". **"Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones". *** "Por el cual se reglamenta el artículo 160 del Decreto-ley 19 de 2012".	Estos decretos hacen refieren importantes disposiciones legales relacionadas con la gestión documental de las pruebas periciales y las firmas electrónicas y digitales.

Fuente: elaboración propia (2023).

Adicionalmente, también se pueden encontrar los siguientes documentos CONPES relacionados con la seguridad informática:

Tabla 2. *Documentos CONPES sobre seguridad informática*

Documento CONPES	Descripción
CONPES 3701 de 2011	Este documento diseñado por el Conpes y los ministerios de Justicia, Relaciones exteriores, Defensa Nacional, TIC, el Departamento Administrativo de Seguridad (DAS) y la Físcalía General de la Nación (FGN) plantea una serie de lineamientos para políticas de ciberseguridad (capacidad estatal para reducir el riesgo de la ciudadanía para ser víctima de amenazas cibernéticas) y ciberdefensa (capacidad estatal para enfrentar amenazas de naturaleza informativa o cibernética). Los lineamientos que este documento plantea buscan establecer un plan de acción interinstitucional en el que, como su nombre lo indica, participa una gran cantidad de instituciones que se encargan, interdisciplinarmente, de aportar con determinadas acciones específicas una función en pro de combatir la delicuencia cibernética y salvaguardar los derechos de la ciudadanía. Por otra parte, este documento incluye aspectos como financiación para los periodos del 2011, 2012, 2013 y 2014, también establece una serie de recomendaciones y cera de 21 pasos, a través de los cuales, se implementan, institucionalmente, las acciones de las entidades involucradas, simultáneamente, expone una serie de requisitos a cumplir antes de brindar la capacitación especializada en las acciones contra estos tipos penales.

CONPES 3854 de 2016	Este documento, a igual del Conpes 3701, fue diseñado mancomunadamente por varias entidades del Estado colombiano tales como el Conpes,los ministerios de Tecnologías de la Información y las Comunicaciones (TIC), Defensa Nacional; Dirección Nacional de Inteligencia (DNI) y el Departamento Nacional de Planeación (DNP). Este documento oficial reconoce y advierte que la creciente cercanía de las diferentes teconologías digitales con la sociedad civil conlleva la posibilidad de nuevas modalidades delictivas que se aprovechen de ello, por ello, el propósito de este documento es plantear una política nacional de seguridad digital en la que se busca robustecer la defensa y soberanía nacional en el entorno digital; propiciar la creación de mecanismos duraderos y estratégicos para impulsar la seguridad digital nacional; implementar el plan de acción que contempla establecer un marco institucional para la seguridad digital que involucre a diversas instituciones del Estado interesadas en una seguridad digital robusta y eficiente, por último, busca que el Gobierno colombiano logre implementar un modelo de riesfgos de seguridad digital (DE3).
CONPES 3995 de 2020	Este documento oficial, al igual que los Conpes 3701 y 3854 fue elaborado por distntas instituciones de Estado colombiano como lo son el DNP, el Ministerio de las TIC y el Departamento Administrativo de la Presidencia de la República (DAPRE). Al igual que sucede con el documento Conpes 3854 de 2016, este documento advierte la importancia de fortalecer las medidas de seguridad para la ciudadanía que ejecuta diversas acciones en el entorno digital y cibernético, por esto, también plantea el diseño de una política de seguridad, en esta se considera el fortalecimiento de las capacidades de seguridad digital dentro de los sectores oficiales y privados con el fin de aumentar la confianza digital dentro del país; preparar al país en materia de seguridad tecnológica de cara al futuro, esto partiendo de un análisis previo de la implementación de modelos, estándares y marcos de trabajo de políticas previas como la de los conpes 3701 y 3854, Además, este documento incluye una sección de financiamiento para los periodos comprendidos entre el 2020 y el 2022, Por últimimo expone 9 puntos con recomendaciones sobre seguridad digital.

Fuente: elaboración propia (2023)

5. Referente teórico

5.1 Ciencias Forenses

La denominada informática forense es parte de la criminalística y se compone por todos los procedimientos y conocimientos científicos y técnicos adoptados en el esclarecimiento y explicación de delitos y asuntos jurídicos (ya sean civiles, penales o administrativos) (Barros et al., 2021).

Esta área tiene como funciones estudiar e interpretar la evidencia de información que caracterizan las infracciones o acciones dolosas que permitan esclarecer los actos delictivos y así colaborar con la autoridad judicial ante la aplicación de la ley. En las indagaciones de orden penal, la el objetivo principal del perito forense es confirmar los roles de los actores involucrados en un crimen o aclarar la participación del presuntos partícipes en pro de evitar sentencias injustas contra personas inocentes a través de estrategias que permitan definir con relativa precisión, un ejemplo de ello es si una persona se encontrada en determinado lugar o en la escena de los acontecimientos (Barros et al., 2021).

El papel principal de este es ayudar a las investigaciones relacionadas con la justicia tanto civil como penal, empleando métodos científicos para determinar perjuicios inexplicables, muerte y crímenes. A partir del análisis de las pruebas reunidas en el marco de la investigación, la criminalística ayuda a individualizar a los sospechosos y aclarar un determinado delito, dando lugar a una posible explicación de lo sucedido. Por ello, esta tiene la tarea de investigar en las pruebas del hecho punible los elementos necesarios para formalizar el peritaje o revisión de los

elementos materiales probatorios, de donde surgen las pruebas para formalizar el proceso penal (Silva et al., 2019).

En los primeros momentos de la reconstrucción de la disciplina, las prácticas criminalísticas eran ejecutadas por profesionales con formación genérica. No obstante, con los avances tecnológicos, algunos delitos se han complejizado, por lo que se requiere que profesionales expertos en otras áreas de la ciencia proporcionen sus conocimientos para llevar a cabo investigaciones más efectivas. Así, muchas áreas como la antropología, la criminología, la entomología, la odontología, la toxicología, la ingeniería, la patología, la psicología y la medicina, entre otras comenzaron a elogiar y asistir a las ciencias forenses, considerando los campos interdisciplinarios. Su área de actividad es, por lo tanto, bastante amplia, buscando contribuir a la justicia y a la sociedad (Espinoza, 2019).

La versatilidad disciplinar en las ciencias forenses es tradicional, lo que proporciona una característica de integralidad, por esto, la ciencia y el derecho logran tener información que genera, como resultado diversas metodologías y estrategias para la ejecución de peritajes. De la misma forma, el juez apela a varios elementos para hacer respetar y acatar la ley, los expertos utilizan el conocimiento de las diversas áreas de la ciencia para analizar los rastros encontrados en la escena de un crimen. A diferencia de otras disciplinas científicas, el derecho es goza de una presencia habitual en el campo criminalístico (González y Cañón, 2017).

Sin embargo, la ciencia y el derecho obtienen información y consecuentes resultados de diversas maneras. A lo largo de la investigación, se propone una hipótesis y se realizan experimentos para una prueba; si los datos encontrados no los contradicen, ganan apoyo, razonamiento y aceptación como razonables y confiables. No obstante, el experto trabaja con algunas dificultades provenientes de la misma ciencia, porque incluso con la evolución

tecnológica, las conclusiones algunas veces son precisas, lo que puede llevar a que los hallazgos sean cuestionados. La ley opera de manera contradictoria, a veces actuando sin requerir ningún dato de respaldo para fundamentar las dudas presentadas por un abogado defensor (Pacheco y Moreno, 2012).

En diversas oportunidades, hay casos en que la fiscalía puede invalidar la aaprobación del método propuesto por la defensa. No obstante, las estrategias de las ciencias forenses han sido validados y probados en el ámbito científico. Como muchas las actividades profesionales, la criminalística se basa por principios y acciones éticas que tienen como objetivo delimitar los las obligaciones y responsabilidades de cada trabajador para proporcionar calidad no solo al área técnica, sino además al espíritu humano de la profesión. Los expertos que no siguen los principios éticos violan las normas éticas, independientemente del campo en el que operen. (González & Cañón, 2017).

En ciencias forenses, los profesionales trabajan con diversos antecedentes, como galenos, biomédicos, dentistas, ingenieros, psicólogos, geólogos, biólogos, químicos, farmacéuticos, antropólogos, arqueólogos, etc. comúnmente, los consejos profesionales de cada disciplina establecen un código de honor propio, haciendo énfasis en los principios que deben cumplirse en cada especialidad. Este asesoramiento tiene el privilegio de aplicar sanciones a los profesionales que violen dichas normas (Barros et al., 2021).

Los expertos que hacen parte de los equipos de trabajo en criminalística deben tener una formación científica alugar para llevar a cabo correctamente los procesos analíticos en el ámbito judicial. Estos profesionales deben ser conscientes de los avances vanguardistas y potenciales que pueden mejorar su práctica en el presente y comportarse desde lo ético para superar los desafíos de este siglo 21, evitando el pasado y enfatizando los intereses de la sociedad. (Oviedo, 2015).

5.2 Evidencia Digital

El principal trabajo de las disciplinas forenses es el de la búsqueda, análisis e interpretación de evidencia. En términos forenses, la evidencia e indicio se pueden interpretar como sinónimos, por ello, conviene utilizar solo uno de estos conceptos. La criminalística considera como evidencia o indicio a todo objeto, huella, marca, señal, es decir, todo aquello que connota un antecedente como razón de haber acontecido. Bajo estos conceptos forenses, la evidencia material o física tiene una estrecha relación con la realización de un hecho presuntamente delictivo, cuyo examen o estudio proporciona las bases científicas para encaminar con buenas bases una investigación y lograr fundamentalmente tres cosas: la identificación del o los autores, las pruebas de cómo se cometió el hecho y de la construcción hipotética de la estrategia que siguió del evento delictivo (Miranda et al., 2019).

Desde el campo jurídico-procesal, se asigna al término indicio un sentido más similar con la jerga común. Según el Diccionario de la Lengua Española, un indicio es un "fenómeno que permite conocer o inferir la existencia de otro no percibido". Esto es, un indicio es un signo aparente y probable de que existe alguna cosa y a su vez es sinónimo de seña, muestra o indicación (Di Lorio et al., 2017).

La denominada evidencia o prueba posee tres características o elementos:

- ✓ un hecho comprobado (hecho indicador, de naturaleza contundente).
- ✓ una operación lógica o juicio de razonamiento y
- ✓ un hecho deducido que es aquel que se busca comprobar y hace parte del objeto de la investigación.

Bajo el marco procesal, una evidencia requiere su adecuada presentación o análisis para transformarse en fuente de pruebas. (Di Lorio et al., 2017).

Desde el punto de vista del proceso penal, las pruebas pueden cumplir dos roles, uno orientador y otro probatorio; una prueba puede cumplir simultáneamente los dos roles (Calderón, 2021). Cabe recordar que, cuando se desea usar pruebas o evidencias con función probatoria, se debe haber cumplido con los aspectos mínimos de relevancia, suficiencia, confiabilidad y validez. En este punto cabe destacar que la inclusión de las tecnologías de información en la vida cotidiana ha conllevado la necesidad de hacer lo mismo con los medios informáticos como herramientas investigativas o probatorias, y, a su vez, para lograr obtener, examinar, interpretar y presentar esta clase de evidencia, esto ha requerido del auxilio de expertos en el campo (Miranda et al., 2019).

5.3 Informática forense y evidencia digital

La informática forense es contemplada como parte de las ciencias forenses y es responsable de identificar, conservar, estudiar y exponer información digital veraz, la cual ha sido procesada electrónicamente y almacenada en medios de su misma naturaleza digital (Lerena et al., 2019).

En otras palabras, es reconocida como la aplicación de la tecnología de la información para recuperar material probatorio digital. En esta área, se consideran diferentes fases y modalidades de actuación, las cuales, a lo largo de un proceso penal, son llevadas a cabo por profesionales tales como peritos, investigadores y profesionales del derecho, los cuales en un trabajo en conjunto se encargarían de la planificación previa, identificación, recopilación, validación, análisis, interpretación, documentación y presentación de pruebas digitales para ayudar a esclarecer o probar hechos de carácter delictivo (Miranda et al., 2019).

Con el desarrollo de la informática forense se crea, a modo de resultado, la denominada evidencia digital, este término, generalmente, se reconocía y asociaba exclusivamente con elementos físicos, que pueden ser capturados con los sentidos y solían ser materiales tangibles. Esto parece contrastar con el término "evidencia digital", por tanto que se considera que relacionado con el término "digital" se asemeja, por extensión, a lo vinculado con el término "virtual", es decir, como lo no real o no tangible (Oviedo, 2015).

Sin embargo, en este orden de ideas es importante también tener en cuenta que los datos o pruebas digitales siempre se almacenan en un medio real, el cual es un elemento físico, por lo tanto, esta tipología también puede considerarse como tangible o física.

Puede deducirse que la evidencia digital es una clase de evidencia física, la cual se construye a partir de información no tangible sumergida en campos magnéticos y pulsos electrónicos. Hay elementos que pueden convertirse en evidencia digital, en ese caso serían un archivo en un medio de almacenamiento, una línea de texto en un registro cibernético, el registro de acceso a u una página web, algunos datos en dentro del peritaje de una aplicación, o información de lo ocurrido en los registros de eventos de un sistema. (González y Cañón, 2017).

De este modo, el trabajo de la informática forense gira principalmente alrededor del material probatorio digital, como fuente de información almacenada o codificada binariamente. (González y Cañón, 2017).

La tarea del profesional especialista o técnico se relaciona directamente con la correcta identificación y recuperación más completa posible de la información, visible e incluso invisible, relacionada con la posible situación delictiva o el hecho de estudio, aplicando las técnicas y herramientas disponibles, para asegurar un proceso de adquisición reproducible, dejando a la vista procedimientos que prueben el examen, el análisis, el cotejo, la conservación y presentación de

pruebas, a fin de reforzar su valor probatorio ante los tribunales o entes judiciales (di Lorio et al., 2017).

En la informática forense, la fiabilidad de la evidencia digital como prueba va a depender de aspectos básicos tales como, el proceso de obtención, el método para conservar y el procesamiento y/o manipulación de la información (di Lorio et al., 2017).

Para el profesional investigador del área judicial, la finalidad de encontrar evidencia será establecer un vínculo que relacione la escena, la víctima y el agresor. Respecto a la informática forense, en respuesta a los principios de criminalística, los profesionales operan bajo modalidades extremadamente variadas, en donde la denominada como escena del evento puede extenderse incluso en diferentes ubicaciones físicas, constituyendo entre ellas un entorno virtual, o escena del entorno virtual (Pacheco y Moreno, 2012).

Adicionalmente se ha logrado identificar que no solo el contenido visible de un documento constituye una evidencia digital, sino además los metadatos, los registros del sistema y otros tipos de material probatorio digital pueden ser importantes para descubrir o probar nexos entre diferentes aspectos de un evento. Cabe resaltar en este contenido, que las diversas huellas digitales que deja el contacto entre la escena, la víctima y el agresor, lo cual consiste en intercambios de información digital, en los que también interactúan otras variables, como momentos, instrumentos, objetos y consecuencias, requieren de un análisis complejo para reconstruir este vínculo (Espinoza, 2019).

Así la aplicabilidad de las ciencias forenses de la informática proporciona los métodos y estrategias que permiten detectar, obtener, analizar e interpretar pruebas de naturaleza digital en el proceso investigativo.

5.3.1 Informática forense

La informática forense es considerada una ciencia joven que se ha encargado de cuidar, determinar, conservar, examinar y exponer un conjunto de datos, también llamados pruebas digitales, de tal modo que estas puedan llegar a ser aceptadas en un proceso legal o judicial (Silva et al., 2019).

De acuerdo con la literatura, la Informática Forense es definida como ciencia, ya que permite el uso de procedimientos de origen científico y analítico especializados a una infraestructura tecnológica con el objetivo de determinar, proteger, estudiar y presentar la información digital obtenida de una forma válida en un proceso legal (Lázaro y Pérez, 2021).

Rivas (2014) afirma que esta ciencia en conjunto con sus técnicas permite o facilita una reestructuración de un equipo informático alterado, así como la evaluación y validación de los datos que se han podido extraer de las escenas o situaciones sospechosas o ilegales.

De acuerdo con Creutzburg et al. (2016) la Informática Forense no se propone la prevención de delitos, aunque entre los análisis e información deducida podría ofrecer información precisos para perfeccionar los mecanismos de seguridad utilizados para asegurar una red. Los estudios forenses, en este orden de ideas, buscan pesquisar lo que ocurrió durante una situación delictiva de carácter digital, en donde buscan la identificación de quién realizó el hecho punitivo, los elementos o activos que se afectaron, la dimensión de lo ocurrido, las fechas de cuándo ocurrió, los lugares relacionados, los cuales se podrían denominar como escenas virtuales, el lugar de origen y finalmente los afectados o los objetivos finales de tal evento delictivo, de donde se buscaran responder los porqué de cada situación (Velásquez y Dávalos, 2016).

En todo este proceso el profesional informático forense, llamado también perito forense, tendrá unas exigencias a cumplir, las cuales pretenden disminuir la probabilidad de sesgos o manipulación de la información tratada, por tanto, de acuerdo con la literatura. Darahuge y

Arellano (2016) mencionan que los peritos forenses en su función no podrán movilizar el equipo físico que contiene la información objeto de análisis, por esto, el estudio se debe efectuar en el lugar de los acontecimientos, así como se debe efectuar la creación de una copia de la información contenida en un repositorio original, los que propicia la transformación de evidencia digital a evidencia física. Esta tarea se deberá realizar minuciosamente, de tal manera que la duplicación o copia generada preserve la validez del contenido original.

Las ventajas de algunos protocolos de manipulación de los datos obtenidos en los procesos investigativos desde la informática forense, permiten el almacenamiento, la lectura o incluso la recuperación de diferente tipo de información que era considerada eliminada, oculta o incluso no generada. La Informática Forense, por medio de la aplicación de procedimientos rigurosos y estrictos, puede contribuir a la resolución de incidentes importantes tanto los estrictamente digitales o los no reconocidos como digitales, ya que a través del apoyo o la implementación del denominado método científico, el cual se aplica a la recolección, análisis y validación de todo tipo de pruebas, permite la abstracción de cualquier tipo de información que haya sido utilizada incluso como comunicación o transacción (Lázaro y Pérez, 2021).

Esta ciencia o disciplina no solo hace uso de tecnologías de punta que permite mantener la integridad de los datos y el procesamiento de estos; adicionalmente da las herramientas necesarias para determinar y hallar, dentro de cualquier dispositivo electrónico, lo que pudo ocurrir, es decir obtener cada uno de los registros de las funciones que ha ejecutado un dispositivo digital, es por esto que requiere de personal formado y especializado con conocimientos avanzados en temas de informática y sistemas (Lázaro y Pérez, 2021).

El alcance de esta ciencia aplicada al medio judicial se extiende hasta capacidades de investigación relacionada con información personal, tal como la identificación de propiedad de

sitios web, o posibles manipuladores de dichos sitios, permite la identificación y ubicación de los presuntos autores de determinados grupos de datos y otros documentos enviados o publicados a través de redes. Son investigables las adulteraciones, sabotajes y otros manejos a las bases de datos de redes internas o externas de un lugar afectado por terceros en delitos cibernéticos (Lázaro y Pérez, 2021).

La manipulación o creación de información digital genera huellas digitales, es así como los archivos informáticos pueden guardar información sobre su autor, la compañía, fecha de creación, etc. de manera inconsciente para el usuario implicado, lo cual facilita en el campo de la informática forense la determinación en algunos casos del dispositivo en donde fue redactado el documento que puede ser material de evidencia judicial (Lázaro y Pérez, 2021).

En este orden de ideas la relevancia de la informática forense se encuentra entonces en la identificación y determinación de las afectaciones ocasionadas por el ataque a quien ha sido víctima de una situación delictiva o una organización en particular con características delictivas (Lázaro y Pérez, 2021)

La capacidad de la cuantificación del alcance del perjuicio recibido e, incluso, la identificación de los responsables del delito, busca elevarse ante las instituciones competentes como se mencionó anteriormente, con el objetivo de buscar la aplicación de la justicia y la debida pena de los responsables correspondiente al delito cometido. Eventualmente, y utilizando la experiencia adquirida en la investigación de delitos o situaciones punitivas de origen cibernético, se puede generar información que haga las veces de un historial para tomar acciones preventivas eventualmente, o establecer protocolos de intervención ante algunos eventos característicos con comportamientos similares (López et al., 2019).

Es importante mencionar que al apelar a la informática forense se hace posible investigar aun, ante la salvedad de la capacidad que brinda el internet para el anonimato y el uso de nombres falsos o apodos sociales, identificar quién es el autor o dueño de alguna página web, quiénes son los autores de determinadas publicaciones y otros documentos enviados a través de alguna red o publicados en la misma. Todo este proceso informático de rastreo que se realiza pretende, inicialmente, indagar, hallar y determinar cada uno de los pasos a través de los cuales se desarrolló el ataque o la acción ilícita. Además, es posible buscar y ubicar a presuntos atacantes externos de diferentes sistemas e, inclusive, en algunos casos se consigue determinar los medios de propagación de los denominados virus cibernéticos o informáticos que buscan el hurto de información personal a nivel digital (Darahugue y Arellano, 2016).

Por medio de procesos de análisis informático forense son medibles y verificables las afectaciones, alteraciones y otros manejos intencionados de bases de información de redes propias o ajenas. Es por esto que, tal como se mencionó anteriormente las exigencias mínimas para la realización de esta tarea, será contar con un conocimiento profesional y eficaz, por lo que se reconoce que comúnmente aquellos que ejercen su función de informáticos forenses, han ejecutado ataques en el pasado o conocen el uso de los sistemas, dispositivos y software de incursión en la web, por lo que conocen las posibles intrusiones por parte de terceros en un sistema, logrando desarrollar así protocolos de detección e intervención inicial mucho más agiles (Frisch y Severi, 1995).

Es así como de acuerdo con la literatura disponible se logra concluir que la finalidad de un análisis forense informático será el de ejecutar una búsqueda detallada y precisa para reconstruir a través de todos los medios digitales o físicos los hechos que tuvieron lugar en el momento en el cual el sistema estuvo en su estado íntegro hasta el momento de detección de un estado anormal.

Cabe recordar que los datos pueden guardar información sobre su creador, empresa, fecha, hora, entre otra información básica, que para el caso jurídico, resulta ser de gran interés. Cabe recordar que esa información suele ser desconocida para una gran mayoría de usuarios, sin embargo, es ideal que, para los profesionales en el campo de la informática forense, ninguna información pueda llegar a ser desconocida u oculta (Cica y Julio, 2021).

5.3.2 Laboratorio de Informática Forense

En el área de informática forense los elementos materiales probatorios digitales tienen que ser analizados y procesados para extraer la mayor cantidad posible de información, para esto se requiere de la infraestructura y la adecuación que faciliten la recolección de pruebas que permitirán la imputación de los delitos identificados. Aquí se refiere entonces a infraestructura en términos de espacio físico, y dispositivos en términos de tecnología para el procesamiento de la evidencia digital (González et al., 2019).

Los laboratorios forenses están dispersos por todo el mundo y se alinean a los términos jurisdiccionales de aplicación de la ley local o estatal, lo cual quiere decir que la disposición de cada laboratorio variaría con relación a su ubicación geográfica y las exigencias legales locales (Di Lorio et al., 2016). En Estados Unidos, la mayoría de estas instalaciones están a cargo de las fuerzas del orden, lo cual varía en algunos países como Colombia, donde estos se encuentran bajo propiedad privada. (González et al., 2019).

La construcción de estos espacios exclusivos para la aplicación de informática forense no debe ser estrictamente de tipo físico, algunos se denominan laboratorios virtuales y estos, por tanto, no deben estar confinados en una sola ubicación. La tecnología actual hace posible operar un

laboratorio “virtual” con los examinadores y el depósito central de evidencia ubicados en lugares geográficamente separados. Este tipo de organización tiene varias ventajas, incluido el ahorro de costos, un mayor acceso a más recursos (herramientas y almacenamiento, por ejemplo), acceso a una experiencia diversa y mayor, y reducción de la duplicación innecesaria de recursos. (Bustamante, 2021).

Las características en términos de capacidad de los laboratorios digitales permitirán la realización de un mejor procesamiento de la prueba digital en diferentes espacios geográficos, además, el beneficio que ofrece la búsqueda y extracción de los datos de un suceso a distancia (Hern et al., 2019).

El estudio de las imágenes o de información forense de tipo digitales realizados en el laboratorio forense digital, permite la identificación ágil de los elementos relevantes de cada caso, mediante el uso de las técnicas informáticas y de datos instauradas en diferentes softwares, para obtener bases de información, hojas de cálculo, documentos, e mails, archivos contables, facturación, entro otros, que podrían demostrar procesos ilegales tales como la evasión de impuestos (di Lorio et al., 2016).

La estructuración e instalación de un laboratorio de informática forense exige el conocimiento de diferentes aspectos claves, tanto desde el punto de vista técnico como desde el legal, estatal, organizacional, metodológico, jurídico, informático y de talento humano. Este producto (laboratorio) puede ser suficiente, aunque aisladamente, disponer del software indicado, contar con el personal adecuado, acatar todos los requisitos técnicos y de infraestructura, y, aun así, no adaptarse a las situaciones en las que está inserto desde el punto de vista estratégico e institucional, lo cual puede resultar muy poco útil. Por esta razón, para la proyección y

estructuración de un producto de este tipo, se deben tener en cuenta ciertas previsiones, las cuales pueden reposar en evidencia científica (di Lorio et al., 2016).

Para la universidad de ciencias informáticas en Cuba, un LIF debería componerse de 6 áreas principales: un área de seguridad de los datos; un área de recuperación de archivos borrados y metadatos; un área de análisis de memoria RAM; un área de análisis de red; un área de análisis de aplicaciones instaladas y un departamento legal y de seguridad que garantice el funcionamiento del laboratorio y sus procedimientos (Lázaro y Pérez, 2021).

El diseño interno de un LIF debe contemplar el suministro de elementos que garanticen un contexto seguro e íntegro para el trabajo diario del personal forense, así como para la manipulación y archivo de las evidencias. Es por esto por lo que el área destinada deberá contar con una fuente eléctrica que debe ser permanente, una condición térmica que proteja los equipos, un circuito cerrado seguimiento de video, sistema de seguridad y detección de incendios, se recomienda que el servicio de internet sea asegurado y permanentemente, así como monitoreado y controlado. Adicionalmente que el uso de dispositivos de almacenamiento de información y celulares de uso personal sea delimitado, así como el ingreso de personal no relacionado con el área, a excepción de aquellos con el aval de los directivos del área y para funciones específicas en las operaciones (Lázaro y Pérez, 2021).

5.4 Diseño de laboratorios de informática forense en la educación.

Para el diseño y construcción de un laboratorio de informática forense existen varios caminos, que se van a diferenciar de acuerdo con la organización para la cual se proyecte. Entre

las múltiples opciones para la determinación del proceso de estructuración, una de las más tradicionales es basarse en prototipos o inspirarse en laboratorios de otras organizaciones similares que manifiestan un buen desempeño (di Lorio et al., 2016).

Otro camino, más exigente, pero igualmente efectivo, comienza con un proceso de investigación inicial, con observación y estudio de la realidad de la organización en la que se agregará al laboratorio, identificando las demandas y necesidades coyunturales, las características del contexto, de la institución principal, previsión de hipotéticos escenarios futuros, entre otros elementos. Como resultado de esta práctica, que debería ser parte de la cultura de una organización, deben surgir algunas preguntas clave: ¿Cuáles son las demandas y necesidades insatisfechas, actuales y futuras, más importantes a las que se enfrenta la organización?, ¿de qué modo podrán ser satisfechas? para, por último, estar en condiciones de discutir y proyectar de forma efectiva el diseño de estructuras informático forenses institucionales (di Lorio et al., 2016).

Cabe destacar que, en este aspecto, no existen guías previas que establezcan los lineamientos sobre los cuales diseñar, implementar y llevar adelante laboratorios forenses en el campo educativo. Se ha dado un primer paso consistente en hacer visible la necesidad de consolidar los laboratorios forenses como estrategia frente a la investigación criminal por parte del poder judicial, y, en especial, cuando es llevada para los Ministerios Públicos, sin embargo, en el campo de la educación o de la academia, aun no se ha conseguido identificar evidencia científica que permita preestablecer un patrón para la proyección o estructuración de este tipo de espacios (di Lorio et al., 2016).

Es necesario considerar que, para la proyección de estos laboratorios, es importante establecer la visión, la misión, la y finalidades de la organización para fundamentar la razón de su existencia, y, eventualmente, vincularla con la construcción de los espacios destinados para el área

de informática forense. En cuanto al escenario estatal, la implementación de un laboratorio de informática forense encuentra los principios articuladores de su labor, estructura y razón de ser tanto en la Constitución Política Nacional y Provincial como en las regulaciones orgánicas que regulan el funcionamiento de los entes gubernamentales (Ministerio de Justicia y Derechos Humanos, 2016).

La implementación de un laboratorio mixto es decir un espacio donde se consiga interaccionar el poder judicial, el poder ejecutivo y la academia, se considera un espacio y un proceso multidisciplinar tanto en el plano provincial como municipal, el cual fortalece y potencia los alcances de las funciones allí desempeñadas (di Lorio et al., 2016)

De acuerdo con Lerena et al. (2019) estructuración de estos espacios físicos a nivel institucional académico resulta en una contribución concreta del mundo científico tecnológico al desarrollo regional y nacional, a través de la co-creación de conocimiento en el trabajo por el cubrimiento de las necesidades encontradas en la sociedad o institución.

Así la incorporación de una actividad extra, de transferencia y cooperación entre instituciones lo cual es muy tradicional en el ámbito universitario, pero no en los campos judiciales relacionados con la informática forense, robustecen la capacidad de investigación y resolución de problemas y desarrollo de tecnología. Así mismo permite el intercambio de experiencias y el diseño de soluciones en forma conjunta con pares de otras jurisdicciones, logrando compartir los productos y enriquecerlos, gestionando un cambio de paradigma en la manera de abordar y resolver los problemas en la Justicia (Lázaro y Pérez, 2021)

La aptitud de ayuda entre universidades para ayudar a la Justicia, formalmente comprometida mediante la puesta en escena de laboratorios forenses, se considera una iniciativa y

un avance significativo desde lo funcional y metodológico, para el crecimiento social y tecnológico de cualquier población.

6. Metodología

6.1 Enfoque Metodológico

Esta propuesta está fundamentada desde lo metodológico en el paradigma cualitativo, esto se da como consecuencia de la relación de la naturaleza de las variables aquí tenidas en cuenta, el diseño de unos objetivos de alcance propositivo y las características de dicho paradigma cuya esencia cualitativa nace de la particular cualidad "circular" entre el descubrimiento de las preguntas de investigación más apropiadas y sus posibles respuestas. Hernández, Fernández y Sampieri (2014) explican el proceso cualitativo desde una característica cíclica en la que la fase de partida es el surgimiento de una idea susceptible de ser investigada; desde ahí se crea un planteamiento del problema a través de una pregunta o hipótesis; esto conlleva eventualmente a un diseño de estudio que debe marcar las pautas para la recolección de datos; posterior a esto último se podrá plantear un análisis de ellos para obtener un reporte de resultados y así dar respuesta a los objetivos planteados y a la pregunta de investigación.

El planteamiento de esta propuesta considera los elementos del estudio cualitativo anteriormente descrito, en donde el interés sobre la relación entre la informática forense y el aporte que esta puede dar a una sociedad caracterizada por la carencia de recursos o alternativas para garantizar la seguridad de sí misma lleva a plantear la posibilidad de instaurar espacios que permitan posibilitar el desarrollo de esta herramienta con el fin de conocerla, entenderla e influir en su evolución en pro de la seguridad de cientos de ciudadanos vulnerables en sus contextos virtuales, en especial teniendo en cuenta el auge del uso de las redes sociales y una creciente actividad digital que acoge, incluso una nueva forma de desarrollo y actividades económicas,

escenario propicio para la supervivencia de la criminalidad. Ante esto, es menester plantear las características y la importancia que tiene el construir laboratorios de informática forense en espacios académicos identificando y definiendo los servicios, la infraestructura y los protocolos y guías ya documentadas.

6.2 Tipo de Estudio

En concordancia con lo planteado en el enfoque metodológico, el tipo de investigación se determinó con un alcance propositivo, dado que el objetivo primario de este trabajo es, precisamente, plantear una propuesta para el diseño de laboratorio de informática forense para la Universidad Tecnológica de Pereira, esto como respuesta a la necesidad de fortalecer los espacios para el estudio y desarrollo de este campo de la informática que se considera útil para el bienestar de una sociedad desbordada por la inseguridad, además de la ausencia de este tipo de escenarios en la academia colombiana, La propuesta aquí pretendida buscó definir los aspectos más básicos como los servicios, la infraestructura, los protocolos y guías que un laboratorio debe cumplir para poder aportar al sistema acusatorio desde lo académico y a la academia nacional como uno de los pocos espacios existentes para formar profesionales en este campo.

Como se puede entender a Hurtado de Barrera (2000), una investigación de corte propositivo como la pretendida en este trabajo busca argumentar sobre cómo deberían ser ciertas cosas o situaciones de la realidad con el fin de tener un funcionamiento determinado para cumplir ciertos fines; esta característica delimita de la manera más apropiada las intenciones de este trabajo, en cuanto a que se realiza una definición inicial de los servicios y ventajas que espacios como un laboratorio forense puede traer para una institución académica como una universidad; no sin antes mencionar los casos de países de la región en los cuales ya se ha dado la oportunidad para la

investigación informática y forense con resultados irregulares entre dichos casos; también se destaca que en este trabajo los protocolos y guías de funcionamiento debido cobran una vital importancia dada la ambición del estudio propositivo aquí presente.

Vale la pena delimitar los alcances que esta propuesta puede llegar a tener en un futuro, dado que se deben considerar factores externos y ajenos a ella tales como lo económico, las políticas internas de la institución potencialmente beneficiaria con el proyecto.

6.3 Procedimiento

Por último, el procedimiento planteado para esta investigación corresponde a las fases del proceso cualitativo en la medida en que, como se consideró anteriormente, es importante partir de una idea o una inquietud de investigación para ir construyendo a partir de allí el diseño metodológico. En ese sentido y con el propósito de proporcionar al lector una estructura más clara, se siguieron tres fases:

1. Planteamiento del problema: como se ha venido insistiendo, desde el área de la ingeniería se puede indagar desde diferentes aspectos para la resolución de problemas dentro de la sociedad. El planteamiento surge entonces a partir de la importancia que ha venido cobrando la práctica forense y el aporte que se puede lograr desde la academia para la creación de este tipo de

laboratorios. De esta manera, con ayuda del mismo proceso académico y la asesoría de los docentes de la institución, se planteó el desarrollo de esta tesis.

2. Recolección y análisis de datos: luego del planteamiento inicial y la búsqueda por responder a unos objetivos de investigación, se pensó en la manera más apropiada para la recolección de datos para dar respuesta a la pregunta investigativa. Así, se plantea la revisión documental como el método de recolección de información relacionado con los servicios, la infraestructura y los protocolos y guías que se han hecho al respecto de los laboratorios de práctica forense. Deslauriers (2004) considera que la revisión documental es una herramienta fundamental para cualquier investigación que configura además un punto de partida para la recolección de información. La interpretación de los datos se da en la medida en que se desarrolle una triangulación de la información presentada en el marco teórico y la funcionalidad ideal de este tipo de laboratorios.

3. Presentación de resultados: finalmente, luego del procedimiento que se ha seguido y especialmente de la recolección y el análisis de la información, se le presenta al lector una propuesta de diseño de características físicas y logísticas de un laboratorio de práctica forense para la Universidad Tecnológica de Pereira. Este diseño se va a plantea a partir de lo que se ha venido documentando tanto a nivel nacional como a nivel internacional en la materia y además busca responder al desarrollo necesario de la práctica forense en el país. El producto final será entonces el diseño del laboratorio de práctica forense, en espera de que pueda ser aplicado a un espacio real en la institución académica.

7. Resultados

Esta sección busca dar respuesta al objetivo general de diseñar un laboratorio de informática forense adecuado para satisfacer las necesidades actuales de Colombia en la Universidad Tecnológica de Pereira. A continuación, se especifican en primer lugar, los servicios que va a ofrecer el laboratorio de informática forense. Estos servicios pueden darse de manera paulatina en la medida en la que el laboratorio adquiera mayores capacidades tanto a nivel económico como a nivel de personal.

En segundo lugar, se presentan consideraciones con respecto a la infraestructura del laboratorio de informática forense y herramientas de análisis y almacenamiento de datos.

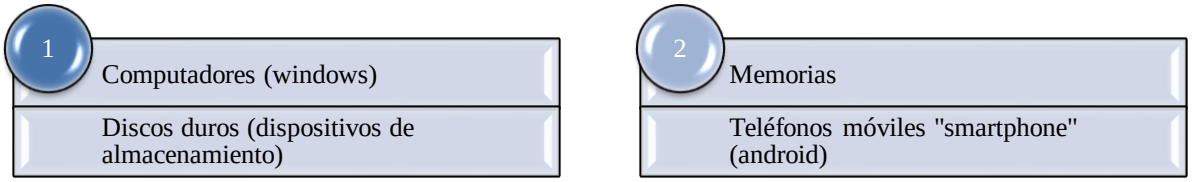
En tercer lugar, se identifican los protocolos y guías de operación que se aplican en los laboratorios de informática forense en Colombia, para garantizar el cumplimiento de los estándares de calidad y las normativas vigentes; y finalmente, las herramientas y tecnologías necesarias para la gestión del laboratorio de informática forense, incluyendo la selección de software especializado para análisis forense y la definición de los procedimientos y protocolos para su uso efectivo.

Y en cuarto lugar, se presentan las herramientas y tecnologías necesarias para la gestión del laboratorio de informática forense, incluyendo la selección de software especializado para análisis forense y la definición de los procedimientos y protocolos para su uso efectivo.

7.1 Servicios que se ofrecerán en el laboratorio de informática forense

Teniendo en cuenta las necesidades actuales del mercado y la industria, así como los avances tecnológicos, se consideraron los siguientes tipos de servicios para que sean ofrecidos por el laboratorio de informática forense de la Universidad Tecnológica de Pereira (UTP).

Los servicios que se ofrecerán en su fase inicial estarán enfocados a los siguientes dispositivos, considerados como los más fundamentales en cualquier laboratorio de informática forense:



A continuación se especifican los servicios para cada caso:

Tabla 3. *Servicios por ofrecer en el laboratorio de informática forense*

SERVICIO	DESCRIPCIÓN
SERVICIOS DE PERITAJE FORENSE	
SERVICIO DE PERITAJE INFORMÁTICO	El laboratorio ofrece los principios o fundamentos del peritaje, estos son la objetividad (tener en cuenta fundamentos éticos); conservación y autenticidad (en el proceso debe conservarse la autenticidad y originalidad de la evidencia); legalidad (el perito deberá seguir los lineamientos de la ley, además de ser correcto, preciso y eficaz en su objetivo); idoneidad (la evidencia debería ser apropiada y pertinente para el caso que se requieren); inalterabilidad (para preservar la autenticidad de los elementos probatorios, se ejecuta una debida cadena de custodia de estos); inalterabilidad y documentación) (Sampaoli, 2018).
SERVICIO DE MANEJO Y PRESERVACIÓN DE EVIDENCIAS DIGITALES.	Como se menciona entre los servicios de peritaje, cuidar la cadena de custodia permite garantizar la integridad de las evidencias; este cuidado debe garantizarse para todo el proceso investigativo, desde el inicio hasta el final, el laboratorio certifica el seguimiento de todos los pasos en este proceso de custodia, los cuales son: identificación (es el reconocimiento de la evidencia o material probatorio), recopilación de evidencia (consiste en el traslado del elemento probatorio desde el lugar inicial de los hechos hasta el laboratorio de análisis , adquisición (corresponde a la consecución o elaboración de una copia de respaldo de todos los dispositivos digitales considerados como elemento probatorio)y la mencionada preservación (como su nombre lo indica, corresponde al cuidado de la evidencia)(Ochoa, 2018).
SERVICIO DE ANÁLISIS DE *MALWARE* EN TELÉFONOS	Para este servicio, el laboratorio caracteriza el malware como un programa intruso que se instala en un equipo por medio de otro programa al que se une

SERVICIO	DESCRIPCIÓN
MÓVILES (ANDROID) Y COMPUTADORES (WINDOWS)	sin ser parte de él originalmente para así logran ingresar al sistema ordenador en cuestión, los virus, gusanos, troyanos, spyware, bonets son algunos de los nombres que reciben las clases de malware que el laboratorio está preparado para detectar y enfrentar, con el fin de evitar acciones criminales por medio del uso de estos programas "parásitos", para el caso, el laboratorio está en capacidad de detectar y eliminar malware en dispositivos telefónicos inteligentes y computadores (Agruña, 2021).
SERVICIO PARA LA DETECCIÓN DE FISHING O ROBO DE IDENTIDAD	La suplantación de identidad consiste en tomar los datos e información personales de alguien para usarlos con el objetivo de un ilícito haciéndolo pasar como propio de la víctima de suplantación ante las autoridades; este delito tiene muchas modalidades, como lo son el correo phishing, en el cual no se suplanta necesariamente a una persona, sino a una entidad u organización legalmente constituida, por medio de este correo, los delincuentes insertan una técnica conocida como email spoofin, que permite a los delincuentes esconder el verdadero enlace digital del remitente del correo para reemplazarla por el enlace de una cuenta real o legítima; también se encuentran las populares cuentas falsas en redes sociales, las cuales no pertenecen a una persona real o no son las cuentas auténticas de quien aparentan serlo, con esto los delincuentes pretenden estafar (Harán, 2022).
SERVICIO DE DETECCIÓN DE DELITOS DE ACCESO NO AUTORIZADO A SISTEMAS INFORMÁTICOS	En línea con lo manifestado a lo largo de estas líneas, los análisis digitales forenses también permiten resolver las preguntas que usualmente nacen tras hechos delictivos, ante ello, estas suelen ser "¿quién lo hizo?, ¿cuándo lo hizo?, ¿qué tanto daño hizo? Y ¿con qué lo hizo? Cabe recordar que el acceso no autorizado a información privada es uno de los delitos informáticos más comunes es, este delito es uno de los tantos actos antijurídicos que se pueden detectar y describir por medio del perito informático (Prakmatic, s.f.).
SERVICIO DE INVESTIGACIÓN POR ROBO DE DATOS , BORRADO Y FUGA DE DATOS INFORMÁTICOS	Una de las modalidades de sabotaje o uno de los accidentes más frecuentes y comunes en el manejo de información digital es el de la pérdida de información, ya sea porque un tercero, en un acto delictivo eliminó toda o parte de la información, o porque alguien, por accidente, pudo borrar parte o la totalidad de ella, el laboratorio presta sus servicios para determinar cómo pudieron ocurrir estos hechos y establecer si se trató de sabotaje (robo intencional de un tercero) o accidente (eliminación no intencional de información), además puede establecer si la información perdida fue extraída del lugar de almacenamiento en el que reposara (Atico 34, s.f.).
SERVICIO DE RECUPERACIÓN ARCHIVOS DAÑADOS EN DISPOSITIVOS.	Otro de los servicios de seguridad que ofrece el laboratorio de perito forense informático es el de recuperar o restaurar información que se ha extraviado o borrado, ya sea por error o por intención de un tercero, la recuperación de información perdida o extraviada de una unidad de almacenamiento digital se da mediante técnicas profesionales de informática para garantizar la restauración completa de la información, evitando que esta sufra alteraciones en el proceso (Perito Judicial Group - PJGroup, s.f.).
SERVICIO DE RASTROS Y LOGS DE COMUNICACIONES A TRAVÉS DE RECURSOS DE MENSAJERÍA INSTANTÁNEA Y CORREO **ELECTRÓNICO**	Un log es el registro de un suceso o evento que surge o se genera y guarda en un dispositivo informático y da cuenta sobre el funcionamiento del sistema operativo de ese dispositivo como de sus aplicaciones. En el laboratorio de análisis forense se estudian los logs con el fin de encontrar e interpretar los registros de los eventos tomados por un dispositivo informático que sea parte de una investigación en el marco de un acto delictivo, esto es, como material probatorio (Hidalgo, 2021).
SERVICIO DE ANÁLISIS DE HISTORIAL DE MENSAJES DE APLICACIONES DE	La mayoría de las aplicaciones de conversaciones en línea cuentan con la facultad de registrar las conversaciones que por intermedio de ellas se dan, esta facultad no aplica solamente para las conversaciones escritas, también lo

SERVICIO	DESCRIPCIÓN
MENSAJERÍA INSTANTÁNEA COMO CHATS, ASÍ COMO CUALQUIER OTRA FORMA DE COMUNICACIÓN ELECTRÓNICA.	hace con archivos multimedia y documentos compatibles para la aplicación; para el caso de los navegadores de internet, estos almacenan el registro de enlaces a los que accede el usuario. Para investigaciones judiciales, estos registros pueden funcionar como pruebas elementales, según sea el caso, el laboratorio, en estos casos, actúa en pro de recuperar dichas evidencias, pues a pesar de tener las aplicaciones la facultad de conservar dichos elementos, también ofrece la opción de eliminarlos, aunque dicha eliminación no es siempre definitiva, ya que, de la mano de las acciones apropiadas estos archivos o registros eliminados pueden restaurarse (Yasaca et al., 2019).

Fuente: elaboración propia, 2023.

7.2 Infraestructura del laboratorio de informática forense y herramientas de análisis y almacenamiento de datos

INFRAESTRUCTURA

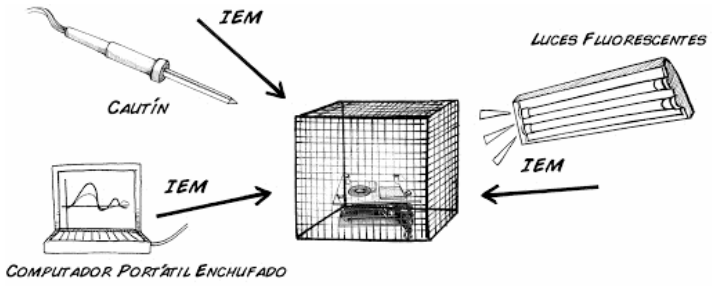
La infraestructura del laboratorio de informática forense es fundamental para su buen funcionamiento y para el cumplimiento de los servicios ofrecidos y descritos anteriormente. Teniendo en cuenta que es un proyecto que se piensa para el campus universitario, será fundamental adaptar las sugerencias de manejo de infraestructura de un laboratorio de informática forense, teniendo en cuenta que sus necesidades son particulares. En general, se deben garantizar unos requisitos generales de diseño que son aplicables a cualquier laboratorio de informática forense, esto incluye controles de acceso físico, lógico para restringir el ingreso de personal no autorizado.

La adecuación del espacio destinado para el laboratorio será un aspecto a revisar a futuro con la universidad, esto incluye su seguridad, teniendo en cuenta que se va a manejar información confidencial. Se deben definir unos perímetros de seguridad que permitan proteger cada una de las áreas que contengan y gestionen información confidencial o crítica, (esto puede incluir tarjetas de

acceso, dispositivos biométricos que permitan la identificación de todos los funcionarios, cerraduras, guardias de seguridad e incluso la instalación de un CCTV - Circuito Cerrado de Televisión , un sistema de extinción de incendios, por lo cual se recomienda adquirir extintores de espuma, , polvo químico seo, bióxido de carbono, INERGE).

Infraestructura eléctrica. Esta infraestructura es fundamental para el funcionamiento de todos los equipos digitales eléctricos para el procesamiento de la información. Fundamentalmente, el laboratorio debe tener energía eléctrica debidamente adecuada para que no haya daño de equipos por interferencia electromagnética. Guerrero y Sánchez (2013) recomiendan usar una jaula de Faraday:

Figura 1. *Jaula de Faraday*

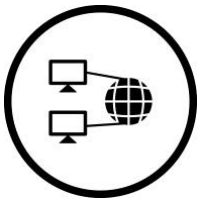


Fuente: Khurana (2018)

Adicionalmente, se recomienda tener un Sistema de Alimentación Ininterrumpida – SAI (Uninterruptable Power Supply – UPS por sus siglas en inglés) que sea complementario al suministro de energía y que además prevenga posibles saltos de voltaje.

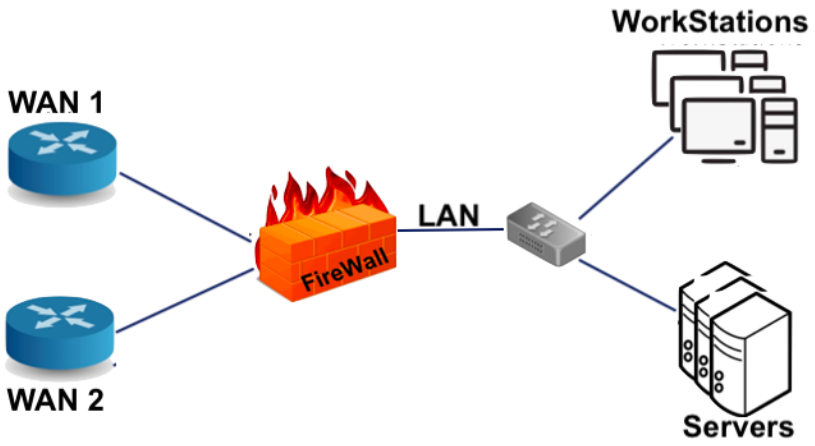
También vale la pena mencionar que las condiciones ambientales deben ser ideales para que no haya sobrecarga de los equipos por altas temperaturas. Por ellos, se sugiere adecuar un sistema refrigerado que prevenga la humedad. También, se sugiere un sistema de alarma contra

incendios. Calderón y Contreras (2021) proponen mantener un laboratorio de este tipo con una temperatura estable de 22°C y una humedad máxima del 65%.



Conectividad. En cuanto a la conectividad, el laboratorio debe contar con una conexión a internet de alta disponibilidad, por medio de transmisión guiado (cableado) para garantizar la seguridad de los datos y la evidencia. Esta conexión debe ser estable en todo el laboratorio, con altos estándares de calidad; además se recomienda tener firewalls para proteger los puertos de red, una conexión VPN que permita una extensión segura de la red de área local - LAN, sistemas de detección, prevención de intrusos que quieran monitorear la red y/o las actividades del sistema.

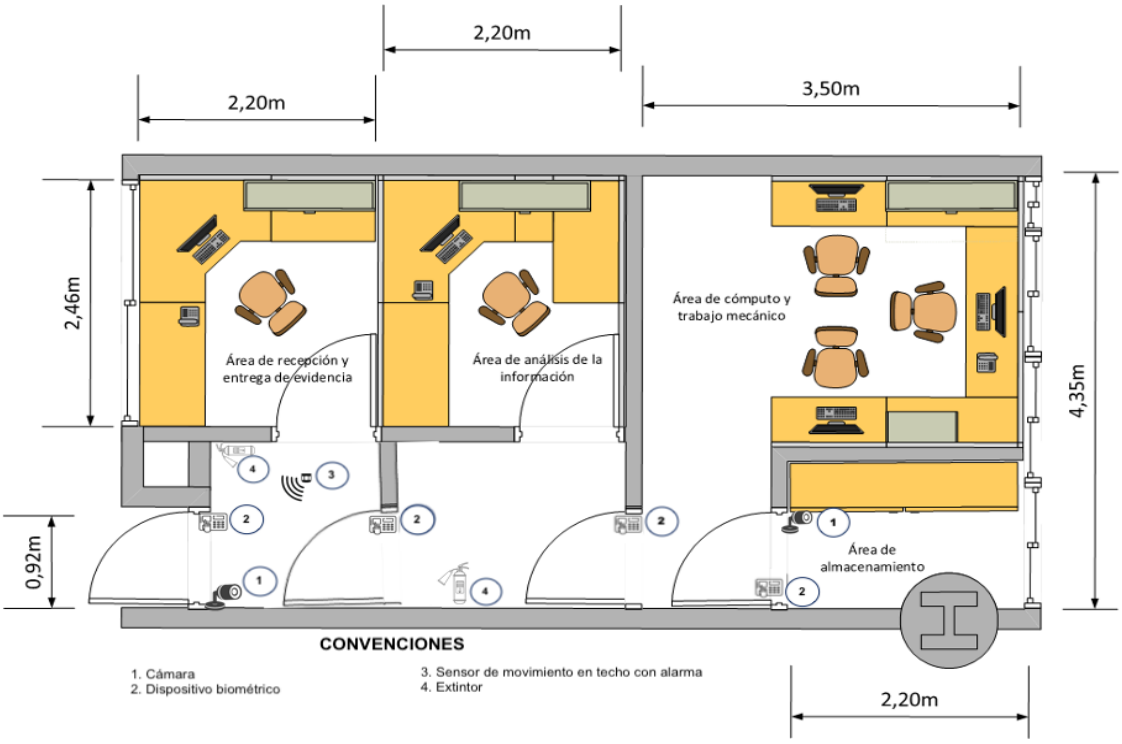
Figura 2. *Esquema básico de red para un LIF*



Fuente: Perry (2016)

A continuación, se especifican las áreas propuestas para el funcionamiento del laboratorio.

Figura 3. *Plano laboratorio de informática forense UTP*



Ubicación: UTP Carrera 27 #10-02 Bloque 15D aula 304 Barrio Álamos Pereira, Risaralda

Área de recepción y entrega de evidencia. En esta área se propone un sistema de ventanilla única para la recepción, radicación y entrega de la evidencia física de delitos informáticos. Para ello, es necesario establecer una matriz para la recepción y entrega de la evidencia física, que permita registrar la naturaleza de la evidencia y demás datos que permita identificarla. Esto debería ser firmado tanto por la persona que entrega como por la persona que recibe. Una vez admitida la evidencia, se debe almacenar de acuerdo con recomendaciones de práctica forense.

Área de análisis de la información. En esta área se llevará a cabo el procesamiento de la información recuperada de los equipos. Aquí se elaborarán informes a partir de las evidencias recolectadas. Esto es, un diagnóstico de los datos y la redacción de un informe final en el que se explique a los clientes o interesados las conclusiones y hallazgos de cada caso, así como los sistemas, técnicas y métodos empleados. Esta área también puede ser un espacio de reuniones del personal, siempre que cada caso lo requiera.

Área de cómputo y trabajo mecánico. Esta será el área donde se encuentran los equipos de cómputo y de trabajo mecánico enfocado en el montaje y desmontaje de equipos de acceso físico.

Almacenamiento. El área de almacenamiento será ideal para resguardar la evidencia recolectada y guardar su cadena de custodia. Es ideal contar con un mueble archivador que permita clasificar de manera adecuada todo el material recolectado. Así mismo, este archivador deberá ser seguro de acceso restringido. Por ser material sensible, puede llevarse un registro de acceso, de manera que haya un control del personal que accede al material, así mismo, para evitar interferencias de campos magnéticos, se sugiere adquirir contenedores antiestáticos.

EQUIPOS INFORMÁTICOS

En lo que respecta al equipo de hardware, se trata de elementos centrales para el montaje del laboratorio forense. Más allá de los elementos fundamentales, es importante considerar que para el análisis informático forense, es necesario contar con equipo especializado. Así, a

continuación, se mencionan algunos elementos básicos necesarios para la implementación del laboratorio en su fase inicial, teniendo en cuenta que el laboratorio a futuro, puede requerir otras adecuaciones y dotaciones de equipos a partir del surgimiento de nuevas tecnologías.

Se necesita al menos una impresora, cámara digital, computadores para cada trabajador (portátiles y/o de escritorio), audífonos de alta definición, programas de protección de virus, grabadora blu-ray, teléfono celular, duplicadora de discos, memorias que permitan almacenar desde 4 terabyte de información y datos:

1. **Estación de trabajo forense**: a continuación, se definen los aspectos mínimos en orden de importancia para la adquisición: sistema de almacenamiento (10TB), memoria RAM (32 GB y tecnología DDR4), disponibilidad de puertos (Thunderbolt, SATA, USB, etc.) y procesadores (intel xeon o intel Core i7); además se debe contar con teclados, monitores, mouses y demás periféricos auxiliares adecuados y de calidad.

De acuerdo con Di lorio et al. (2019):

> "Es conveniente que las Estaciones de trabajo forense cuenten en primer lugar con un disco para almacenar el sistema operativo y las aplicaciones del perito, y uno o más discos adicionales en los cuales almacenar las imágenes forenses y la evidencia digital recuperada. De esta forma, la evidencia y la información privada de aquellos que se investigue quedan siempre alojadas en dispositivos fácilmente identificables, sobre los que se pueden realizar operaciones de borrado seguro cuando finalice la investigación correspondiente" (p. 20).

2 **Clonadoras de disco**: otro de los equipos especializados en análisis forense informático Actualmente en el mercado se encuentra la Duplicadora Ditto DX Forensic.

Figura 4. *Duplicadora Ditto DX Forensic*

Fuente: WiebeTech (s.f.).

Este es un equipo fundamental para la adquisición de datos digitales para el análisis forense. Está hecha de aluminio y permite velocidades de más de 6.5 GB por minuto. Además, este aparato es ideal para el trabajo en campo, pues contiene una batería de larga duración. Permite al investigador copiar simultáneamente dos dispositivos con una interfaz que es de fácil entendimiento para el usuario. Actualmente hay varios equipos de diferentes marcas y capacidades, por lo cual es necesario hacer una propuesta económica con una cotización actualizada en el mercado colombiano, que permita hacer una inversión adecuada.

3 **Equipos de análisis forense Voom** que es un equipo que permite, sin alterar su contenido, acceder al soporte magnético.

Figura 5. *Equipo forense Voom Shadow 3*

Fuente: Ondata.

4 **Bloqueadores de escritura**, permiten la creación de imágenes forense. Así mismo, protege la evidencia forense para que no se altere durante su copia. Este es un dispositivo que garantiza la protección de la evidencia.

Figura 6. *Bloqueador de escritura*

Fuente Ondata.

5 El equipo PC-3000 Express System diseñado para el diagnóstico, la recuperación y la reparación de información que está contenida en discos duros que están dañados.

Figura 7. *PC-3000 Express System*

Fuente Ondata.

Estos son los equipos fundamentales de trabajo forense en el laboratorio. Como se mencionó anteriormente, es importante que haya un ejercicio de propuesta y cotización de los equipos esenciales para el funcionamiento del laboratorio una vez la universidad determine el inicio del proyecto, de manera que se pueda hacer una inversión adecuada.

PROTOCOLOS Y GUÍAS DE OPERACIÓN

Se mencionan a continuación algunos documentos y guías relevantes:

- ISO/IEC 27037 “Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence” de 2012, es la norma más actualizada en lo referente al manejo de evidencia digital, su propuesta se centra en 3 tipos de principios: el proceso debe ser auditable, para la cual se debe brindar evidencia suficiente, herramientas y resultados; además, este debe ser reproducible, de tal manera que se debe dar validez y su correspondiente respaldo a las acciones aplicadas; y el proceso debe ser defendible, cuidando el uso de las herramientas aplicadas.

- ISO/IEC 27042 de 2015, que garantiza la Integridad del Análisis de Evidencias Digitales en Procesos Judiciales. Esta es una guía enfocada en el manejo de evidencias digitales para

peritos informáticas. Se propone la obligatoriedad de los siguientes componentes de un informe: calificación del perito informático; información inicial; naturaleza del incidente con su respectiva fecha, hora, duración y lugar; miembros del equipo de trabajo; objetivos de la investigación; fecha y hora y lugar del trabajo; interpretación de la evidencia; hechos presentados y hallados; posibles daños de la evidencia; limitaciones de los análisis; detalle de los procesos y las herramientas;; conclusiones y recomendaciones.

- Forensic Examination of Digital Evidence: A Guide for Law Enforcement. El National Institute of Justice tiene varias guías enfocadas en el cumplimiento de la ley para el procesamiento de evidencia digital. Estas guías contienen procedimientos y protocolos de examen de apoyo para demostrar que los medios electrónicos contienen pruebas incriminatorias. Aunque no se trata de mandatos legales, son recomendaciones que se han hecho reuniendo el consenso de expertos en la materia. Estas guías se van actualizando, teniendo en cuenta el constante cambio de las tecnologías disponibles.

- Electronic Crime Scene Investigation: A Guide for First Responders, también del National Institute of Justice o Departamento Nacional de Justicia de Estados Unidos, esta guía está enfocada en la preservación de la escena de un delito electrónico a través de la protección de la evidencia. Se presentan varios ejemplos de diferentes tipos de escenas, pero haciendo la anotación de que cada escena del crimen es única. Los primeros intervinientes en las escenas de delitos electrónicos deben ajustar sus prácticas según cada escena, considerando su perfil de experiencia, las condiciones del crimen y el equipo que se considere necesario, por lo cual esta guía es esencial para este tipo de profesionales.

- Manual de Manejo de Evidencias Digitales y Entornos Informáticos de la Organización de los Estados Americanos – OAS. Es también uno de los manuales de la OAS que tiene el objetivo de brindar herramientas a profesionales para salvaguardar la evidencia de un crimen informático, especialmente policía judicial, funcionarios de la fiscalía y peritos informáticos. Así mismo, el manual busca cumplir con seis (6) principios básicos del peritaje informático: documentación, objetividad, inalterabilidad, conservación, inalterabilidad e idoneidad. Se desarrollan 8 componentes enfocados en la escena del delito, el rastro electrónico y otros aparatos electrónicos.

- UNE 71505 – Sistema de Gestión de Evidencias Electrónicas (2013). Esta es una normativa del organismo de Normalización Española que propone un sistema para la gestión de evidencias electrónicas que cumpla con los objetivos de definir conceptos de seguridad de la información; identificar relaciones entre la gestión de evidencias y de seguridad de la información; y especificar las medidas de seguridad para la gestión de la evidencia electrónica. Para esta normativa, la gestión de evidencia electrónica debe cumplir con los principios de autenticidad, disponibilidad, integridad, gestión, completitud y calidad. En general es una guía que sirve para gestionar la evidencia electrónica.

- RFC 3227 – Guía para recolectar y archivar evidencia. Creada en 2002 por ingenieros de alto nivel para la correcta recolección y archivo de evidencias en delitos informáticos. La guía establece unas convenciones relacionadas a conceptos y palabras claves en el peritaje informático, unas recomendaciones para la recolección de evidencia, actuaciones a evitar, recolección, almacenamiento, cadena de custodia y herramientas que se sugiere utilizar

para la gestión de la información. Es un documento completo y suficiente para profesionales del campo.

A nivel nacional también se encuentran documentos valiosos para el peritaje informático:

- La Policía Nacional cuenta con una serie de documentos y lineamientos para desarrollar Investigación criminalística, dentro de los cuales se encuentran una matriz de servicios, características y estándares de Investigación Criminal. La institución cuenta además con diferentes guías para manejo y gestión de la evidencia digital, para unidades de recepción de material probatorio y evidencia física, la inspección y el procesamiento del lugar de los hechos y en general para la gestión de laboratorios forenses con los que cuenta la Dirección de Investigación Criminal y la Interpol.

- STP 12657 de 2019 para la Extracción de Información a equipos celulares. Esta es una sentencia de la Corte Suprema de Justicia que especifica que la extracción de información de los celulares no necesita un control precio, pues la información allí contenida no se considera base de datos. A partir de esto, se establece que la revisión de información en sim cards no necesita de una orden judicial para el caso de la investigación de un delito informático.

- Manual del Sistema de Cadena de Custodia de la Fiscalía General de la Nación. El documento fue credo en el año 2018 y corresponde a los esfuerzos que se han hecho en el país para garantizar la cadena de custodia del material probatorio digital. Así mismo, la Fiscalía cuenta con un Manual Único de Policía Judicial. Ambas son herramientas útiles

para profesionales del campo, pues abordan todos los requerimientos normativos y legales para garantizar una buena investigación de crímenes electrónicos.

- Cartilla Evidencia Digital. Seguridad y Privacidad de la Información del MinTIC. Esta cartilla está dirigida a entidades públicas y contiene lineamientos para la realización de informática forense, adecuado a los eventos que puedan afectar la seguridad de la información.

MANTENIMIENTO GENERAL

Tan importante es pensar en los principios éticos que determinan las actuaciones de los empleados encargados del laboratorio como el mantenimiento y cuidado de los equipos e implementos de trabajo, por esto, el laboratorio debe contemplar algunos aspectos primordiales para garantizar el debido mantenimiento y adecuación de los equipos de trabajo, a saber, estos aspectos son:

Tabla 4. *Mantenimiento de equipos*

TIPO DE MANTENIMIENTO	***CARACTERÍSTICAS***	**Estaciones de trabajo**	**Clonadoras de disco**	**Equipos de análisis forense**	**Bloqueador de escritura**	**PC-3000 Express System**	***FRECUENCIA***
CORRECTIVO	Hace referencia a toda la serie de trabajos y tareas direccionados a la reparación y arreglo de los bienes tecnológicos cuyo uso ha conllevado al deterioro o daño de sus características funcionales y/o físicas. Este tipo de mantenimiento se debe realizar por personal especializado.	x	x	x	x	x	cuando se requiera

PREVENTIVO	Hace referencia a toda la serie de trabajos y tareas direccionados a la revisión y limpieza interna y externa periódica de los equipos antes de que estos inicien su periodo de fallas. El objetivo es evitar que el polvo o la suciedad interfieran con el buen funcionamiento y evitar acciones de mantenimiento correctivo, que suelen ser más costosas y que no garantizan que los artefactos recuperen el funcionamiento óptimo de su estado inicial.	MANTENIMINTO RUTINARIO: hace referencia a rutinas de limpieza externa básica del equipo realizada por el propietario del equipo y de acuerdo con las recomendaciones suministradas por el personal especializado.	x	x	x	x	x	Diario
		MANTENIMIENTO ESPECIALIZADO: hace referencia a rutinas de mantenimiento más invasivas (internas y externas), este tipo de mantenimiento se realiza tanto al hardware como al software (equipos que aplique), teniendo en cuenta las recomendaciones del fabricante. Este tipo de mantenimiento se debe realizar por personal especializado.						Anual
DISPOSICIÓN FINAL RAEE	Este es el último estadio al que alcanza a llegar un bien tecnológico, pues tras intentar el mantenimiento correctivo y no lograr reparar el artefacto, este se aísla o confina, en especial si no está constituido por elementos reutilizables, en caso de sí tener partes reutilizables, éstas se separan del todo y se clasifican para otro proceso, las partes no aprovechables son desechados en lugares adecuados especialmente para tal finalidad, como es el caso del residuos de Aparatos Eléctricos y Electrónicos (RAEE) del relleno sanitario de la ciudad. Esta disposición final aplica para cualquier aparato eléctrico y electrónico del laboratorio. Utilizar mecanismos de control para el borrado seguro de la información para aquellos equipos que lo ameriten.		x	x	x	x	x	cuando se requiera

Fuente: elaboración propia (2023).

Tabla 5. *Otros- Aclaraciones*

Bienes tecnológicos Son los aparatos que se emplean en las labores investigativas, éstos pueden estar conformados por varios elementos o artefactos físicos, como también por programas especializados para el manejo y manipulación de la información.
Vida útil Es uno de los aspectos que el laboratorio debe tener en cuenta a la hora de adquirir un bien tecnológico, ya que el tiempo en el cual uno de estos artefactos mantiene sus características físicas o de funcionamiento dentro de parámetros óptimos es un factor clave en el laboratorio.
Criterios de cumplimiento o aceptación Los criterios de cumplimientos o aceptación consisten en las condiciones o requisitos mínimos que debe cumplir, según esto, el laboratorio define si acepta o rechaz**a** el bien tecnológico al adquirirlo.
Disponibilidad

Con este criterio o aspecto, el laboratorio define, basándose en un cálculo de demora de una función o tarea, el tiempo en el que un equipo esté disponible para operar y presar el servicio para el que fue adquirido a quien lo requiera.
Característica de escalabilidad Bajo esta característica el laboratorio se permite proyectar el futuro de un bien tecnológico y calcular si este puede verse obsoleto a corto o mediano plazo y establecer estrategias frente a esto, también prever los avances tecnológicos de estos bienes para procurar estar a la vanguardia tecnológica.

Fuente: elaboración propia (2023).

SEGURIDAD DE LAS INSTALACIONES

Finalmente, es importante hablar de la seguridad del laboratorio forense, pues el acceso a este debe controlarse estrictamente, debido a la importancia de los datos que se manejan para su análisis. Las evidencias, especialmente si se trata del caso de un proceso judicial, deben protegerse desde su cadena de custodia, son fundamentales para la credibilidad del laboratorio. Como el laboratorio se proyecta como parte de un campus universitario, la seguridad se puede asegurar de diferente manera, limitando el acceso a personal específico a las instalaciones.

A partir de estas consideraciones, se sugieren las siguientes recomendaciones para limitar el acceso a los profesionales, siempre que haya una necesidad justificada:

- El laboratorio debe permanecer cerrado en todo momento, por lo cual es necesario que mantenga una buena ventilación al interior.
- El acceso debe darse a los peritos a través de tarjetas de acceso y una debida identificación biométrica. Se propone un sistema de identificación biométrica según rasgo fisiológico: huella dactilar y, de ser posible, de rostro. Así mismo, cada entrada deberá informarse mediante formulario que incluya nombre del operario, hora de entrada, firma y hora de salida.

- El laboratorio debe tener una bitácora de acceso, de manera que cada trabajador notifique su ingreso, esto para permitir una reconstrucción completa de todo el personal que accede al laboratorio.

- El laboratorio debe tener un área de almacenamiento de la evidencia, que debe contar con máxima seguridad. Es fundamental que el acceso a esta evidencia se dé de manera controlada a través de una caja fuerte, un casillero o un gabinete con llave. Así mismo, la evidencia se debe separar de los demás equipos que hacen parte del laboratorio.

- La organización del laboratorio se puede dar por áreas separadas debidamente con seguridad, de manera que no todos los profesionales puedan acceder a todas sus áreas y únicamente puedan estar en sus áreas de especialización. Para ello se proponen niveles de acceso, dependiendo de la adecuación a la infraestructura que se pueda hacer. Ver Figura 2. Plano laboratorio de informática forense UTP.

- Se sugiere la instalación de un sistema de seguridad externo que permita la vigilancia por cámaras y una respectiva alarma que se active cuando haya una amenaza de seguridad.

- Se debe considerar peligros de amenaza externa que no solo tengan que ver con el acceso no autorizado al área de trabajo, sino también con incendios, inundaciones y desastres naturales similares que pueden darse. Esto por ejemplo puede ser una consecuencia de una ventilación inadecuada del espacio y de los equipos de trabajo.

- Las amenazas a la seguridad del laboratorio también se pueden dar por medio de la filtración de virus, por lo cual es necesario que se haga un escaneo de virus de

todos los aparatos del laboratorio, así como de las unidades de recolección de la información.

- Es fundamental que los profesionales que vayan a hacer parte del laboratorio sean conscientes de las medidas necesarias de seguridad del laboratorio y hagan parte de las reglas que se establezcan para el lugar.

En definitiva, el laboratorio de informática forense debe tener diferentes sistemas de seguridad que deben ser apoyados por expertos y por los recursos que puede brindar la institución educativa. Hay que garantizar especialmente la cadena de custodia del material probatorio, especialmente si se trata de servicios asociados a la investigación de delitos. Esto dependerá del alcance del laboratorio; sin embargo, el éxito en la seguridad de la información recolectada determinará la fiabilidad del laboratorio y así mismo la confiabilidad de los clientes.

ASPECTOS CLAVES

De acuerdo con Di lorio (2019), para cuidar adecuadamente de las instalaciones se debe establecer un "sistema de cinco cinturones" cuya función es detener o bloquear una posible intromisión al laboratorio cuyo funcionamiento es el siguiente:

1° Cinturón: Disuasivo e informativo: uso de obstáculos físicos y electrónicos como cercos, carteles, rejas cámaras que alerten sobre acercamientos al laboratorio.

2° Cinturón: Detección activa: ante una intencionalidad delictiva los sistemas avisan emitiendo una alarma.

3° Cinturón: Barrera física: como su nombre lo plantea, uso de puertas, rejas, muros, cerraduras, postigos, entre otros que impidan el acceso al laboratorio mientas se emite una alerta de atención al sistema policial o de vigilancia.

4° Cinturón: Detección interna: consisten en sensores de movimiento que están conectados a un sistema de cámaras de seguridad y que controlan el ingreso al laboratorio.

5° Cinturón: Blindaje: Barreras como hormigón o acero de cajas de seguridad y muros se usan para áreas específicas del laboratorio, protegiendo la información más sensible que se encuentra almacenada.

7.3 Protocolos y guías de operación que se aplican en los laboratorios de informática forense en Colombia, para garantizar los estándares de calidad y las normativas vigentes

FUNCIONAMIENTO GENERAL

En lo que respecta al funcionamiento del laboratorio, es importante hacer consideraciones iniciales para la planeación que aquí se ha venido desarrollando. El laboratorio de informática forense pensado dentro de esta propuesta para la Universidad Tecnológica de Pereira, se piensa como parte de la práctica profesional que no solo contribuye a complementar los procesos de formación, sino también para generar un espacio de intercambio de beneficios con la comunidad. A continuación, algunas consideraciones relevantes para el planteamiento y el desarrollo del laboratorio:

1

Reconocimiento del propósito del laboratorio

En primer lugar, el objetivo fundamental del laboratorio será el de analizar evidencia forense ante la presunta presencia de un delito. A partir de la descripción de los servicios, los profesionales podrán precisar el alcance del laboratorio. Se van a cumplir con todos los requerimientos de ley, así mismo, se va a desarrollar un trabajo profesional cumpliendo con la ética profesional.

Desarrollo de áreas de enfoque específico en el laboratorio

En segundo lugar, la creación de las áreas específicas de trabajo del laboratorio, que ya se han sugerido en la sección anterior, dependerá también del presupuesto que se apruebe para la formación del laboratorio, pues es necesario dotar el lugar con diferentes herramientas de hardware y software.

Consideraciones de las limitaciones físicas, espacio y ubicación disponible

En tercer lugar, esta propuesta se puede adaptar a las instalaciones que se le presten desde la universidad. Aun así, de acuerdo con la variedad de servicios ofrecidos, se espera que el laboratorio, una vez consolidados, cuente con tecnología actualizada y de alta gama. Aun así, el funcionamiento del laboratorio deberá darse una vez se haya garantizado la seguridad de sus instalaciones desde lo ambiental, para evitar eventos desafortunados y desde lo social, para prevenir posibles infiltraciones que afecten la seguridad de la evidencia recolectada.

Determinar la capacidad de adquisición de herramientas de software

El software para trabajo específico de información que se encuentra encriptada o en discos dañados, requiere la implementación de una serie de herramientas que se describe más adelante.

Es importante considera una inversión contante para adquirir programas y sus licencias, para no exponer las labores del laboratorio con programas de acceso gratuito que muchas veces traen consigo malware, afectando la seguridad de la evidencia recolectada. Por esto, los profesionales deberán considerar los programas ideales para el funcionamiento del laboratorio y los servicios ofrecidos. Esto deberá incluirse en el presupuesto de inversión. Esto mismo aplica para los equipos de hardware.

Establecimiento de un flujo de trabajo

Se propone la organización de un equipo de trabajo multidisciplinar, es importante contar con una persona que lidere las actividades, de manera que se puedan organizar, priorizar tareas y establecer las actividades que van a permitir la culminación de cada uno de los servicios ofrecidos. Esto incluye espacios de trabajo y socialización para cada caso. La persona encargada de liderar el laboratorio debe controlar los procesos de inventario, coordinación del personal, establecimiento de los protocolos de seguridad y seguimiento de estos, cuidado de las condiciones medioambientales y en general de los informes finales de cada servicio.

APECTOS LEGALES

Cuando se menciona el aspecto de la criminalidad o el delito, se hace necesario pensar en los aspectos penales que enmarcan estos campos de la delincuencia. Con el desarrollo tecnológico también han surgido aplicaciones de estas en el mundo empresarial, no obstante, también ha

surgido un efecto colateral y es el nacimiento de nuevas modalidades delictivas, ante estas ha surgido la aplicación de informática para las investigaciones de tipo penal o forenses. En Colombia hace uso años, el hurto por medio de canales informáticos estaba tipificado como cualquier otra modalidad de robo, sin embargo, esa calidad del sistema penal colombiano ha cambiado y mediante la Ley 599 de 2000 (Código Penal colombiano), artículo 240, este tipo de robo pasó a considerarse como hurto calificado y, por ende la pena de quien lo comete puede oscilar entre 6 y 14 años, según sean los atenuantes y todos estos elementos jurídicos (Ayazo, 2019).

En este mundo globalizado por cuenta de la constante aplicación de tecnologías informáticas que surgen y se perfeccionan todos los días, la industria de Colombia ha procurado estar a la vanguardia aplicando estrategias en las que las estas sean protagonistas, a pesar de esto, la seguridad de quienes aplican estas herramientas y de las herramientas mismas no estaba garantizada ni mucho menos, es más el sistema penal y judicial colombiano no contemplaba su existencia. Ahora con la inexorable necesidad de fortalecer la seguridad en la aplicación de herramientas que buscan favorecer la productividad industrial y la calidad de vida de las personas, el sistema penal de Colombia, por medio del artículo 240 del Código Penal colombiano, se incluye una protección para el uso de tecnologías informáticas o digitales incluyendo los hurtos por esta vía en la categoría de hurto calificado, el cual conlleva penas de cárcel entre los 6 y 14 años, de hecho, para el caso específico de los hurtos que usen elementos destinados para comunicaciones informáticas las penas pueden oscilar entre los 5 y 12 años de prisión.

Cabe mencionar que el artículo 240 del Código Penal Colombiano no es el único que considera elementos informáticos, pues el 269b prohíbe a quien no tenga la preparación indicada

y la autorización, impedir o ser un hándicap para el debido funcionamiento del sistema informático, quien no cumpla este artículo podría cumplir penas entre 48 y 96 meses de prisión.

- El artículo 269c, por su parte, prohíbe expresamente la interceptación de datos informáticos, sin importar que esto se dé desde su origen o desde su destino.
- El artículo 269d castiga el sabotaje, entendido como daño, supresión o mal uso de información informática privada con 36 a 72 meses de prisión (Ortega y Páez, 2020).

El laboratorio espera estar en concordancia con el seguimiento y respeto por estos articulados del Código Penal y acompañar paso a paso la evolución que la industria colombiana que haga uso de tecnologías de la información siga teniendo con el correr del tiempo, ofreciéndole un servicio profesional que sigue los lineamientos de la ley colombiana.

ASPECTOS ÉTICOS

La ética como ejercicio particular del que hacer en relación con la existencia de los otros no es ajena a ninguna disciplina ni ciencia, de hecho, debe ser transversal, de esta manera, aunque no se garantice, sí se da un inicio a cumplir lineamientos básicos como el respeto a la ley y la dignidad.

En la evolución de la ciencia forense y la interdisciplinariedad con la informática, preparar a los futuros profesionales, técnico y tecnólogos debe pasar, en algún momento de su instrucción, por una serie de lecciones de ética, pues la labor de estos expertos estará constantemente codeándose con decisiones y actuaciones que bien podrían faltar a la ética, acto que no se puede permitir. Tal y como ocurre en el derecho, con los futuros abogados que son instruidos en ética,

toda persona que desee ser experta, sin importar el nivel, en la investigación informática forense debe pasar por los lineamientos más esenciales; a pesar de esto, la educación de fundamentos éticos en casi cualquier disciplina en nuestro país no es la más prolija. La idea de romper con esa lamentable tendencia es convertir en natural la reflexión ética en el experto en ciencia informática forense, de esta manera el ejercicio del quehacer respetando la ley y ciertos principios ante los cuales los empleados de laboratorios forenses se encuentran en el día a día será más adecuado.

El laboratorio goza de principios éticos desde su institucionalidad, el respeto por la ley y por las libertades individuales es el sello inicial de estos, el manejo responsable de la acción privada que se recibe de parte de quien solicita los servicios de apoyo en sus particulares casos judiciales, esto es, la confidencialidad como ejercicio ético.

A parte del respeto a la confidencialidad, este laboratorio adopta otros principios éticos, a saber:

El utilitarismo: el empleado del laboratorio debe iniciar su reflexión ética preguntándose sobre para qué sirve la acción que se realiza o realizará, a quien le servirá esta acción, a quién no le servirá esta acción. Traerá beneficios a una o varias personas y perjuicios a otra u otras.

Los derechos: el empleado del laboratorio debe continuar su reflexión ética asumiendo lo ya mencionado: el respeto y el acogimiento a la ley y el correcto proceder con todos los elementos que conforman un caso a apoyar.

El bien común o general: en este punto, el empleado del laboratorio debe reflexionar sobre cómo su labor contribuye a la construcción de un país en el que sus habitantes viven en la constante búsqueda de mejorar su calidad de vida.

Imparcialidad: Este aspecto establece que el empleado aplicará la ley por igual sin preferencias o beneficios clientelistas o personalistas. Esto es, aplicar la justicia, o apoyarla, sin distinciones o sesgos.

Virtud: En este aspecto, el empleado del laboratorio destacará por valores tales como la honestidad, el cumplimiento, el respeto, la compasión y la integridad, cabe resaltar que este aspecto no se determina única y exclusivamente desde la individualidad, por el contrario, se construye rutinariamente con la convivencia con la comunidad (Andrade, 2015).

PERFIL PROFESIONAL Y CAPACITACIÓN DEL PERSONAL

En esta sección, se plantean algunos fundamentos del perfil del profesional que hará parte del equipo del laboratorio:

- Director
- Perito informático.
- Personal de Apoyo

A continuación, se describe de manera global los roles mencionados anteriormente:

Tabla 6. *Perfil director*

PERFÍL DIRECTOR	
EDUCACIÓN	Ingeniero de sistemas, Informática o carreras afines.
CONOCIMIENTOS	- En informática forense. - En gestión de calidad. - En Perito Judicial - En labores de ámbitos pericial y judicial - En cultura judicial. - Complementarios en gestión de calidad, de Recursos Humanos, proyectos y seguridad.
HABILIDADES	Se espera que el director tenga aptitudes de liderazgo y trabajo en equipo; valores como la tolerancia, el respeto y la solidaridad; buena capacidad para expresarse de manera oral y escrita con buena ortografía; capacidades de gestión, planificación y administración de tareas; capacidad para trabajar bajo presión; y finalmente, capacidad para tomar decisiones, especialmente en situaciones de alta incertidumbre.
EXPERIENCIA	Experiencia en ámbitos pericial y judicial, mínimo 3 años en trabajos relacionados con su especialidad.
FUNCIONES	- Mantenimiento, gestión, organización y administración del laboratorio forense. - Mantener buenas relaciones para la gestión económica del laboratorio. - Dirigir equipos de trabajo dentro del laboratorio, promoviendo el desarrollo personal e integral de los trabajadores, a través de aptitudes de liderazgo y trabajo en equipo. - Plantear el desarrollo y los objetivos del laboratorio de informática forense. - Proponer estrategias para el uso de novedosas herramientas forenses. - Planear nuevas metas y prioridades según las necesidades del entorno. - Tomar decisiones que sean beneficiosas para el laboratorio y sus trabajadores.

Fuente: elaboración propia (2023.

Tabla 7. *Perfil perito informático*

PERFÍL PERITO INFORMÁTICO[1]	
EDUCACIÓN	Ingeniero de sistemas, Informática o Computación certificado por el Ministerio de Educación o carreras afines.
CONOCIMIENTOS	En Informática Forense, Conceptos legales, sistemas operativos, manejo de inglés, conocimientos específicos en software, hardware y/o productos según alcance del laboratorio.
HABILIDADES	Objetividad, capacidad de trabajo en equipo, proactividad, generación de propuestas, adaptación a las normas de trabajo, instrucciones específicas del oficio de perito, entre otras.
EXPERIENCIA	2 años de experiencia en cargos relacionados
FUNCIONES	Asesorar con relación a sus funciones: • **Recolección:** Recolección de Soportes de Evidencia Digital. • **Adquisición:** de Imágenes Forenses y evidencia digital. Generación de copias de medios digitales y aseguramiento de que cada imagen creada cumpla con procedimientos forenses digitales, efectuar el análisis del material, Buscar evidencia o información que describa los hechos ocurridos. • **Análisis Forense**: Extracción de evidencia aplicación, a nivel plataforma y a bajo nivel. Reconstrucción de un dispositivo. • **Tratamiento**: Análisis Forense, cuidado de la evidencia, creación y presentación de Informes, administrar el área de almacenamiento de evidencias y elementos forenses (recibir, entregar y custodiar las evidencias digitales capturadas, así como los elementos tecnológicos para las tomas de información e indexación de información) y articular las actividades de extracción e indexación de evidencia forense, garantizar que los hallazgos sean presentados de manera adecuada. • Responder por la seguridad del área del laboratorio asignada.

Fuente: elaboración propia, 2023.

Tabla 8. *Perfil personal de apoyo*

PERFIL PERSONAL DE APOYO (recepción)	
EDUCACIÓN	Técnico, tecnólogo
CONOCIMIENTOS	Cconocimiento general del funcionamiento de un laboratorio de informática forense, control de inventarios, cadena de custodia.
HABILIDADES	Objetividad, capacidad de trabajo en equipo, capacidad de adaptación a normas, efectividad, atención, buen manejo de relaciones públicas, proactividad, dinamismo, entre otras.
EXPERIENCIA	Preferiblemente en cargos similares
FUNCIONES	Recibir los casos y determinar si se pueden recibir o no, responder por la seguridad del área del laboratorio asignada, distribuir las actividades y prioridades relacionadas con cada caso recepcionado, mantener informado al director del estado de cada caso, controlar el ingreso y salida de las diferentes partes interesadas, recepcionar, radicar y entregar la evidencia y distribuirla a las personas correspondientes ubicadas en cada zona, controlar el inventario del material a peritar o peritado.

[1] Los peritos informáticos pueden ser distribuidos, y/o agrupados por temáticas, por especificidad de tareas, o por delitos de acuerdo a las necesidades del laboratorio y los servicios.

Fuente: elaboración propia (2023).

7.4 Herramientas y tecnologías necesarias para la gestión del laboratorio de informática forense, incluyendo la selección de software especializado para análisis forense y la definición de los procedimientos y protocolos para su uso efectivo.

Finalmente, una parte fundamental del laboratorio será el software que permitirá la adquisición y el procesamiento de la información. Por tal motivo, en esta última sección se presentarán las herramientas más relevantes, innovadoras e importantes para el análisis forense:

- Paraben Corporation, esta empresa es conocida a nivel mundial, enfocada en el análisis forense digital, la evaluación de riesgos y las soluciones de seguridad. Es viable analizar la oferta de esta corporación para el manejo de dispositivos de internet de las cosas, computadores y teléfonos inteligentes. La ventaja de esta plataforma es que ofrece a sus usuarios una interfaz diversa con la capacidad de trabajar con múltiples fuentes de datos.

- Sleuth Kit – es una biblioteca de herramientas forenses que además de investigar datos de sistemas de archivos, también permite la recuperación de información de discos dañados. Sus utilidades están basadas en sistemas Unix y Windows

- Opentext, es una herramienta de administración de contenido empresarial seguridad y análisis. Este programa facilita la recuperación de evidencia de múltiples fuentes y discos duros, la automatización y preparación de la evidencia, el análisis de información y la clasificación, recopilación y preservación de material probatorio. Esta es una plataforma de trabajo conocida

como Enterprise Content Management – ECM que tiene una aplicación especialmente empresarial, pero que por su gestión documental se puede usar en el laboratorio forense.

- Magnetic Forense, es una herramienta digital que presta servicios de seguridad a organizaciones públicas y privadas. Esta herramienta permite recopilar y conservar datos de los puntos finales locales antes de que estos se pierdan o se modifiquen. La utilidad de esta herramienta se centra sobre todo en el análisis de ciber ataques y otros crímenes digitales. El acceso a este software no es gratuito y ofrece actualmente una amplia gama de sub programas de acuerdo con las necesidades de cada cliente. Además, ofrecen una serie de clases de acceso gratuito y tutoriales que contribuyen a la formación de los investigadores.

- CAINE, siglas en inglés de Computer Aided Investigative Environment Live es un sistema operativo para el análisis forense de datos que presenta un conjunto de herramientas y utilidades para el estudio preliminar de la evidencia, su recolección, análisis y posterior análisis final. Este sistema operativo cuenta con varias herramientas como el Mont Manager que sirve para analizar diferentes unidades de almacenamiento; el Guymager, que permite hacer copias o réplicas de imagen de disco; Air que es una aplicación para la creación de imágenes forenses de discos.

- KROLL, herramientas fundamental para la recuperación de información y gestión de datos, así como para soluciones relacionadas con asesoramiento financiero y de riesgo. Actualmente la empresa ofrece diferentes tipos de herramientas de software, así como protocolos metodológicos.

- X-Ways, es un entorno de trabajo que es eficiente en la medida en la que no consume muchos recursos, y por ser rápido. Adicionalmente permite la creación de imágenes de disco. La ventaja de este software es que es portátil y se puede ejecutar desde una memora USB y desde

cualquier sistema operativo. Es también uno de los programas de mejor costo en el mercado, lo cual lo hace una herramienta ideal para empezar en la informática forense.

- ENCASE, herramientas ampliamente usada en el mercado del análisis forense, pues posee varias funcionalidades dentro de las cuales se puede destacar: creación de copias comprimidas de discos, lo que permite ahorrar espacio en el laboratorio; búsqueda y análisis de datos, lo cual es especialmente útil para el manejo de la información de evidencia; posee gran capacidad de almacenamiento; análisis de documentos; firmas de archivos, integración de reportes, análisis de firmas de archivos, entre otros.

- Ultimate Access Data's Tool kit, es una herramienta potente de recuperación de archivos, que se usa para hacer un examen exhaustivo de un sistema. Esto la ha consolidado como una herramienta esencial para el escaneo completo y la organización de archivos. Esta herramienta es de fácil acceso que puede ser instalado sin complicaciones por la facilidad de su interfaz que es amigable con el usuario. Se puede instalar con CD y actualmente se puede descargar directamente en la red. Su interfaz no es gratuita, pero tiene muchas facilidades de acceso.

- WINHEX, es también una herramienta de la informática forense para la recuperación de datos y gestionar la seguridad informática, es una herramienta cotidiana y de emergencia. Al igual que las demás herramientas, permite inspeccionar y modificar archivos que han sido borrados o perdidos que hacen parte de una investigación. Según el tipo de licencia, se pueden clonar discos y borrar archivos confidenciales de manera segura. En general el programa es ideal para proteger la privacidad de los discos duros y por esto es fundamental en cualquier laboratorio forense.

- Snort – Network Intrusion Detection y Prevention System, es un software de acceso libre y gratuito que permite la detección de intrusos en la red (Sistema de Detección de Instrusos – IDS). Es de código abierto. Es fundamental para prevenir ataques o actividades de redes maliciosas y

generar alertas a los usuarios. Su funcionalidad se define de tres maneras: primero, es un rastreador de paquetes tcpdump; segundo, como registrador de paquetes para la depuración de tráfico de red; y finalmente, como un sistema de prevención de intrusos en la red. La interfaz permite que los usuarios lo usen para uso personal o para uso comercial.

- Nmap, Network Mapper es una herramienta gratuita y de código abierto que es utilizada a nivel mundial para identificar y verificar posibles vulnerabilidades, escanear puestos de información y mapear redes. Aunque su creación se dio hace algunos años, diferentes programadores y desarrolladores la han mantenido actualizada. Por su eficiencia, se ha consolidado como una importante herramienta de trabajo que además es gratuita para sus usuarios. El software se puede usar en casi todos los sistemas operativos y se puede modificar y personalizar para que funcione incluso en los sistemas operativos menos populares. Se debe tener cuidado con su uso, pues muchas veces se considera que es una herramienta ilegal de piratería.

- Xplico, a través de la técnica Port Independent Protocol Identificación, el usuario puede reconstruir y recopilar información de diferentes puertos de información. El problema de este tipo de herramientas es que es limitada a ciertos sistemas operativos e interfaces. Dentro de sus servicios y protocolos se encuentran: HTTP, TCP, UDP, RTP, IRC, IPv6, Facebook, MSN, Paltalk, entre otros. Su principal funcionalidad es la de la reconstrucción de datos de aplicación de protocolo, así como el reconocimiento de protocolos en una estructura determinada de datos. Su acceso es gratuito y de código abierto, lo que lo hace ideal para cualquier tipo de usuario.

- Keylogger, es una herramienta para el seguimiento de los movimientos de teclado de una computadora. Por su naturaleza, su uso es ilícito, porque este seguimiento generalmente se hace sin el permiso del usuario. Esta herramienta puede desarrollarse tanto en una herramienta de

software como en una herramienta de hardware. Su uso es importante en un laboratorio forense, cuando se trata de un caso que así lo requiere; sin embargo, hay que tener cuidado con su uso, pues se trata generalmente de un virus (spyware) malicioso. El laboratorio también puede ofrecer servicios para bloquear la acción de este virus.

- Stellar Phoenix, es un software de recuperación de datos que han sido dañados o extraviados por cuenta de una infección por un virus malicioso, por formateo accidental de un disco o por la corrupción de un disco. Es de fácil uso y ofrece varias funcionalidades que favorecen el trabajo de investigación forense. Este es un programa que es ideal para los investigadores que están iniciando en su proceso de rastreo forense, con una interfaz sencilla de entender.

- Dcdd3, es una herramienta para el tratamiento de discos, permite controlar las funciones de disco de bajo nivel. Su ventaja sobre otras herramientas es que permite trabajar protegiendo el disco original. Permite analizar discos de grandes imágenes y finalmente, trasladarlas de manera más fácil.

- Mount Manager, su principal funcionalidad es la de examinar de manera profunda las unidades de almacenamiento que están conectadas a un disco duro sólido o SSD.

- Guymage, su principal ventaja y funcionalidad es la réplica de imágenes de disco o bit a bit.

Para tener una idea más clara respecto a las herramientas de software que se encuentran actualmente en el mercado para el análisis forense, Rada (2022) presenta un cuadro que resume la utilidad de cada grupo de herramientas de software:

Figura 8. *Herramientas de Software Forense*

Herramientas de Software Forense	
Tipo de Herramienta	**Nombre de la Herramienta**
De Disco y Captura de Datos	EnCase Forensic Imager, FTK Imager, X-Ways Forense, OSFMount Live RAM Capture, Recuva, Disk2vhd, Disk Drill, Easy NTFS Data Recovery, EaseUS Data (Partition) Recovery 9.0, Nuix Investigator, Digital Forensics Framework, SIFT, Autopsy, Wise Data Recovery, Wondershare Recoverit Data Recovery.
De Análisis de Registro	MUI Cacheview, Regripper-registry decoder
De Análisis de correo electrónico	FTK (Forensic Toolkit), Autopsy, EDB, MBOX Viewer PRO, Email Tracker Pro.
Forense de Red	Wireshark, Xplico, Tcpdump, Network Miner, TCPFLOW.
De Dispositivos móviles	Santoku, Elcolmsoft iOS Forensic, Oxygen Forensic Suite, UFED Cellebrite, OSAF, MOBILedit.
De Adquisición y Análisis de Memoria	Responder CE, Volatility, Redline, Bulk Extractor
De Recuperación de Contraseñas	Ntpwedit, ntpasswp, MailPass View, Passware
De Análisis de Malware	Microsoft Process Monitor, PDF Stream Dumper, EsetSys Inspector, Firebug, VirusTotal.
Sistemas operativos orientados a informática forense	CAINE, KALI LINUX, DEFT Linux, DEFT Zero, Linux Matriux.
De Análisis a navegadores web	MyLastSearch, FBCacheView, BrowsingHistoryView, Browser History Viewer, ImageCacheViewer
De funciones específicas: hash y comprobación de integridad	HashMyFiles, QuickHash, Exiftool

Fuente: Rada (2022).

El laboratorio debe apoyarse en los recursos financieros para acceder a programas especializados; por lo tanto, para su fase inicial se contemplan las siguientes opciones.

Con el tiempo y la consolidación de los servicios se podrá adquirir software y equipos más especializados.

Tabla 9. *Software forense*

SOFTWARE	CARACTERÍSTICAS	TIPO		Guía /manual / protocolo
		Gratis	Código abierto	
AUTOPSY	Búsqueda y análisis de malware. Esta plataforma de acceso por código abierto permite el análisis de dispositivos móviles y otros medios digitales. Además, permite analizar dispositivos de almacenamiento de datos como discos, celulares, tarjetas de memoria, entre otros. Permite procesar la información (recuperar archivos borrados, historial de navegación, artefactos de internet, indexar (palabras claves). Además, funciona a través de sistemas operativos: Windows, Linux, Mac, Free BSD y OSx.	X	X	https://sleuthkit.org/autopsy/docs/user-docs/4.0/
FTK IMAGER	Crear imágenes forenses (copia bit a bit del medio de almacenamiento) Este programa permite a los investigadores crear copias exactas de los dispositivos de almacenamiento, esto en el caso de análisis seguros y controlados para no alterar la información original. Adicionalmente, el programa permite: - Creación de imágenes forenses. - Cuidado integral de la imagen. - Búsqueda de las palabras claves. - Sustracción de archivos específicos.	X		https://www.exterro.com/ftk-product-downloads
GHIDRA	Programa para el análisis de malware. Permite el análisis de virus, códigos maliciosos y otros tipos de malware para entender la vulnerabilidad de los sistemas y las redes. Esta herramienta sirve para realizar ingeniería inversa de binarios que incluye un descompilador y una interfaz de usuario completa.	X	X	https://htmlpreview.github.io/?https://github.com/NationalSecurityAgency/ghidra/blob/stable/GhidraDocs/InstallationGuide.html
VOLATILITY	Búsqueda y análisis de datos volátiles de memoria RAM. Permite la extracción de información de artefactos digitales, como la memoria RAM de los computadores.	X	X	https://github.com/volatilityfoundation/volatility/wiki/Volatility-Usage
WIRESHARK	Analizador de protocolos de red. Su principal utilidad se centra en la captura de paquetes de red, esto permite analizarlos en tiempo real y fuera de línea. Es fundamental para el análisis de la red y como consecuencia, para salvaguardar su seguridad. Permite el acceso a múltiples plataformas y sistemas operativos. Los archivos	X	X	https://www.wireshark.org/docs/wsug_html/

SOFTWARE	CARACTERÍSTICAS	TIPO		Guía /manual / protocolo
		Gratis	Código abierto	
	capturados también se pueden comprimir para ahorrar espacio en el disco, facilitando el rendimiento del laboratorio forense.			

Fuente: elaboración propia (2023)

8. Conclusiones

Para cerrar este ejercicio investigativo de alcance propositivo, a continuación, se presentan las conclusiones del trabajo que buscan responder al objetivo de diseñar un laboratorio de informática forense adecuado para satisfacer las necesidades actuales de Colombia en la Universidad Tecnológica de Pereira.

Así, en primer lugar, respecto a los servicios que se consideraron adecuados para la creación y desarrollo de un laboratorio de informática forense. Se encontraron dos tipos de servicios: unos enfocados a la informática forense en general que hace parte fundamental de la tarea de peritaje informático y el manejo de evidencias digitales. Y otros, enfocados en servicios en el sector de la gestión de servicios empresariales, relacionados con el manejo de problemáticas de fuga de información, espionaje empresarial, mala gestión de los recursos empresariales y del personal asociado a una organización. A pesar de que se presentó una amplia gama de servicios, lo cierto es que se espera que estos servicios se vayan ofreciendo en la medida en la que se vayan presentando mayores recursos para el fortalecimiento del laboratorio.

En segundo lugar, en lo que respecta a la infraestructura del laboratorio, las herramientas de análisis y almacenamiento de datos, se tuvieron varias consideraciones: que es necesario contar con un espacio amplio y seguro en el que se puedan organizar diversas áreas de análisis forense, se seleccionaron tres fundamentales: área de análisis de la información, área de cómputo y trabajo mecánico y área de almacenamiento de la evidencia. A partir de las consideraciones hechas en este apartado, se puede concluir la importancia que tiene la seguridad de las instalaciones, pues se trata del manejo de información sensible que en muchos casos está involucrada en procesos de

investigación. Así mismo, se consideró necesario pensar en un área de trabajo con buenas condiciones ambientales, eléctricas y digitales.

Es importante que el cuidado sea integral y que los trabajadores e investigadores que vayan a acceder al laboratorio sean cuidadosos y sean identificados de manera rigurosa para evitar la fuga de información. También se analizó la incidencia de la universidad en la garantía de la seguridad de los espacios físicos. Como se trata de un proyecto propuesta, el espacio escogido dependerá de la disposición y la capacidad de la universidad y de su campus.

En tercer lugar, se identificaron los protocolos y guías de operación que permitirán el cumplimiento de estándares de calidad y normativas vigentes. Este fue un ejercicio de reconocimiento de la integridad de la labor de un informático forense, pues se trata de acceder a información de carácter confidencial y el acceso a recursos que generalmente son invasivos. Según la normatividad vigente, este laboratorio que surge de un ejercicio investigativo, reconoce el cumplimiento de toda la normatividad vigente y la profesionalidad de los investigadores que hagan parte del proyecto. Se espera que los servicios que apoye el laboratorio vengan de la mano con entidades y organizaciones que requieran de una intervención profesional.

Finalmente, para el último objetivo se especificaron las herramientas y tecnologías necesarias para la gestión del laboratorio de informática forense, incluyendo la selección de software especializado para análisis forense y la definición de los procedimientos y protocolos para su uso efectivo. En la búsqueda de información se encontró una gran cantidad de herramientas de software de acceso gratuito y otras de pago que contribuyen a la recolección, almacenamiento y gestión de información codificada de diferentes fuentes de almacenamiento. En general, estas herramientas se pueden organizar según su funcionalidad: de disco y captura de datos; de análisis

de registro; de análisis de correo electrónico; de dispositivos móviles; de adquisición y análisis de memoria de recuperación de contraseñas; de análisis de malware; sistemas operativos orientados a informática forense; de análisis de navegadores web; y de funciones específicas: hash y comprobación de integridad.

En general, la búsqueda de información para la planeación del diseño de un laboratorio de informática forense mostró que se trata una tarea compleja que requiere pensar fundamentalmente en un espacio bien adecuado a las áreas más relevantes del análisis forense; también la articulación de profesionales capacitados ética y profesionalmente en esta labor; y finalmente, la inversión en herramientas de software y hardware para el análisis forense de nivel profesional.

9. Recomendaciones

Finalmente, se formulan a continuación algunas recomendaciones para el trabajo a futuro a partir de los hallazgos hechos, sus limitaciones y alcances. Al tratarse de un proyecto propuesta para el diseño de un laboratorio de informática forense, su desarrollo dependerá de la gestión de la universidad para incorporar a sus instalaciones un laboratorio que preste este tipo de servicios. Aun así, se trató de un ejercicio de revisión de la información que puede ayudar en futuras investigaciones al reconocimiento del estado de arte de herramientas necesarias para el diseño de un laboratorio de informática forense.

Para el planteamiento de un laboratorio forense, se recomienda a los investigadores que consideren que se trata de un ejercicio complejo que requiere la inversión de recursos para la adecuación de espacios y la dotación de equipos de software y de hardware. Se espera contar con tecnología de vanguardia e innovadora y por esto es necesario validar constantemente el uso de nuevas herramientas y nuevas metodologías de trabajo. Así mismo, se deben evaluar las necesidades del mercado y el contexto colombiano en cuanto a desarrollo de este tipo de proyectos. Además de incorporar mecanismos de control para garantizar la integridad, confidencialidad y la disponibilidad de la información como por ejemplo la NTC-ISO-IEC 27001:2022 y GTC-ISO-IEC 27002:2022.

A futuro, se recomienda a los profesionales en investigación forense mantenerse actualizados en normas de seguridad y manejo de información sensible en procesos de investigación y peritaje forense. Así mismo, dada su importancia y la variedad de servicios que puede ofrecer un laboratorio de informática docente, las instituciones educativas deberían contar con estos espacios para afianzar la alianza que tienen con la comunidad y las problemáticas que

los rodean. Puede resultar efectivo promover más proyectos de esta naturaleza que provean toda la información relacionada con el diseño y montaje de un laboratorio de informática forense.

Un área que representa muchas ventajas es el empresarial, que se beneficia de la informática forense para reforzar la seguridad dentro y fuera de sus instalaciones. Las instituciones educativas pueden fortalecer la formación profesional a través de la práctica dentro de estos laboratorios.

10. Referencias

Agruña, S. (2021). *Análisis forense de una infección por malware* [Universitat de Barcelona]. https://diposit.ub.edu/dspace/bitstream/2445/182840/2/tfg_sergio_agruña_alvarez.pdf

American Academy of Forensic Sciences. (2021). *Forensic chemistry*. https://www.aafs.org/

Andrade, J. (2015). *Códigos de ética y responsabilidad profesional en la computación forense*. Aandrade. https://aanndrade.wordpress.com/2015/02/16/codigos-de-etica-y-responsabilidad-profesional-en-la-computacion-forense-2/

Ayazo, P. (2019). *Uso de la Informática Forense aplicada a Delitos Informáticos en la industria colombiana*. [Universidad Nacional Abierta y Distancia - UNAD]. cholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=Funcionalidad+Familiar+en+Alumnos+de+1°+y+2°+grado+de+secundaria+de+la+institución+educativa+parroquial+“Pequeña+Belén”+en+la+comunidad+de+Peralvillo%2C+ubicada+en+el+distrito+de+Chancay+-+periodo+2018&btnG=

Barros, F. de, Kuhnen, B., Serra, M. da C., & Fernandes, C. M. da S. (2021). Ciências forenses: principios éticos e vieses. *Revista Bioética*, *29*(1), 55–65. https://doi.org/10.1590/1983-80422021291446

Bustamante, J. (2021). Avances de la informática forense en Colombia en los últimos cuatro años. *Ingeniería Investigación y Desarrollo*, *20*(1), 69–78. https://doi.org/10.19053/1900771x.v20.n1.2020.13384

Calderón, C. A. C. (2021). Buenas prácticas en Informática Forense para el procesamiento de evidencia digital o información electrónicamente almacenada. In *Publicaciones e Investigación* (Vol. 15, Issue 2). https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/5245/5293%0Ahttps://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/5245

Cámara de Comercio de Bogotá. (2019). *Seguridad de la información en las empresas: principales desafíos.*

Creutzburg, R., Sanchez, M., Flores, J., Chapela, C., & Ricalde, C. (2016). Seguridad Informática y Análisis Forense Digital. *Computación e Informática*, *4*(3). https://www.researchgate.net/profile/Reiner-Creutzburg/publication/303974058_Seguridad_Informatica_y_Analisis_Forense_Digital/links/57611dda08ae244d037219e2/Seguridad-Informatica-y-Analisis-Forense-Digital.pdf

Cuevas, F., & Sánchez, J. (2018). Informática forense: retos y perspectivas. *Tecnura*, *22*(54), 55–67.

Darahuge, M. E., & Arellano, L. (2016). *Manual de informática forense III. Gestión integral de la prueba documental informática para operadores del Derecho*. Errepar. https://books.google.com.br/books/about/Manual_de_informática_forense_III.html?id=1-3LxQEACAAJ&redir_esc=y

Di Lorio, A. H., Castellote, M. A., Constanzo, B., Curti, H., Waimann, J., Lamperti, S. B., Giaccaglia, M. F., Cistoldi, P. A., Podestá, A., Iturriaga, J. I., Greco, F., Alberdi, J. I., Ruiz Del Angeli, G. M. ., Trigo, S., & Nuñez, L. (2017). El rastro digital del delito. Aspectos técnicos, legales y estratégicos de la Informática Forense. *Universidad FASTA*, 556. http://redi.ufasta.edu.ar:8082/jspui/handle/123456789/1593

Di Lorio, A. H., Constanzo, B., Podestá, A., & Giordano Lerena, R. (2019). InFo-Lab : Desarrollando Tecnología Nacional en Informática Forense. *JAIIO - SIE*, *2451–7534*, 193–208.

Di Lorio, A. H., Constanzo, B., Waimann, J., & Podestá, A. (2016). *Guía Integral De Empleo De La Informática Forense En El Proceso Penal*.

Di Lorio, A. H., Mollo, M., Cistoldi, P., Lamperti, S., Giaccaglia, M. F., Malaret, P., Vega, P., Iturriaga, J. I., & Constanzo, B. (2016). Consideraciones para el diseño de un Laboratorio Judicial en Informática Forense. *REDI - Repositorio Digital de La Universidad FASTA*, 1–6. https://www.researchgate.net/publication/324064283_Consideraciones_para_el_diseno_de_un_Laboratorio_Judicial_en_Informatica_Forense

Di lorio, A., Lamperti, S., Coppes, L., & Constanzo, B. (2019). Guía técnica para el diseño de laboratorios judiciales de informática forense. *3era InFoConf*. https://www.researchgate.net/publication/338554754_Guia_tecnica_para_el_diseno_de_laboratorios_judiciales_de_informatica_forense

Espinoza, M. (2019). Informática forense: una revisión sistemática de la literatura. *ReHuSo: Revista de Ciencias Humanisticas y Sociales*, *4(2)*, 112–128.

Fiscalía General de la Nación. (2020). *Anuario estadístico 2019.*

Frisch, H., & Severi, S. (1995). Forensic Science. *Hormone Research*, *43*(4), 121. https://doi.org/10.1159/000184254

Garrido, A., Álvarez, L. A., & Martínez, A. (2020). Diseño e implementación de un laboratorio forense en una universidad de México. *Revista Iberoamericana de Educación*, *83*(1), 59–76.

Gómez, J., & Rincón, J. (2020). Informática forense en Colombia: estado del arte. *Sistemas & Telemática*, *18*(49), 67–85.

Gómez, J. A. (2022). *Laboratorio virtual de informática forense*. Escuela de INGENIERÍA INFORMÁTICA (SEGOVIA).

González, C., & Cañón, J. (2017). *Monografía informática forense* [Pereira : Universidad Tecnológica de Pereira]. https://hdl.handle.net/11059/8320

González, F. G., González, J. S., & Téllez, L. (2019). Laboratorios de informática para mejorar el proceso de cumplimiento fiscal de Colombia. *Revista Científica*, *3*(36), 325–340. https://doi.org/10.14483/23448350.14958

Guerrero, J. M., & Sánchez, L. (2013). *Requerimientos para el diseño de un laboratorio de análisis forense digital enfocado a pequeñas y medianas empresas de Colombia*. Universidad Piloto de Colombia.

Harán, J. (2022). *Qué es el robo y suplantación de identidad*. Welivesecurity. https://www.welivesecurity.com/la-es/2022/05/11/que-es-robo-suplantacion-de-identidad/

Hern, P., Herrera, H., & Sebasti, L. (2019). Automated management of operational activities in forensic computer laboratories. In *Universidad Nacional de Río Negro* (Vol. 18, Issue 2). Universidad Nacional de Río Negro.

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación*. McGraw Hill España.

Hidalgo, M. (2021). El dilema del píxel espía: cuando usar sistemas de seguimiento de correos electrónicos es ilegal. *El País*. https://elpais.com/tecnologia/2021-02-27/el-dilema-del-pixel-espia-cuando-usar-sistemas-de-seguimiento-de-correos-electronicos-es-ilegal.html

Hurtado de Barrera, J. (2010). *Metodología de la Investigación. Guía para la comprensión holística de la ciencia*. Quirón Ediciones. https://doi.org/10.2307/j.ctv2vdbtsb.5

International Association of Forensic Sciences Education. (2016). *Best practices for forensic science education*. https://www.iafse.org/best-practices-for-forensic-science-education/

Kaspersky. (2021). *Informe de Ciberseguridad 2021 de Kaspersky.*

Khurana, A. (2018). *The uses of a Faraday cage – an electrochemist's point of view*. https://lab-training.com/the-uses-of-a-faraday-cage-an-electrochemists-point-of-view/

Lázaro, O., & Pérez, G. (2021). Estructura de un laboratorio de Informática Forense para la Dirección de Seguridad Informática. *Revista Cubana de Ciencias Informáticas*, *16*(4), 1–10.

Lefebvre, A., & Spruit, M. (2021). Laboratory Forensics for Open Science Readiness: an Investigative Approach to Research Data Management. *Information Systems Frontiers*, *25*. https://doi.org/10.1007/s10796-021-10165-1

Lerena, R., Di lorio, A., Podestá, A., & Constanzo, B. (2016). InFo-Lab, un laboratorio mixto de investigación y desarrollo de tecnología en Informática Forense. *Universidad FASTA*. http://redi.ufasta.edu.ar:8082/jspui/handle/123456789/1565

López, Ó., Amaya, H., & León, R. (2019). Informática forense : generalidades, aspectos técnicos y herramientas. *Revista Universidad de Los Andes*, 1–22.

Ministerio de Justicia y Derechos Humanos. (2016). *Laboratorios Regionales de Investigación Forense*. http://www.saij.gob.ar/docsf/ediciones/libros/Laboratorios_Regionales_de_Invest._Forense.pdf

Miranda, E., Bernardis, H., & Riesco, D. (2019). Ingeniería de Software al Servicio de la Informática Forense y la Evidencia Digital. *Universidad de San Luis. Dto de Informatica*, *1*. http://sedici.unlp.edu.ar/handle/10915/104037

National Institute of Justice. (2017). *DNA forensics*. https://www.nij.gov/topics/forensics/evidence/dna/Pages/welcome.aspx

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

Oviedo, J. (2015). *Aspectos relevantes de la informática forense en la actualidad y su importancia* [Universidad Piloto de Colombia]. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2923/00002055.pdf?sequence=1

Pacheco, H. E., & Moreno, J. L. (2012). *Esclarecimiento de hechos delictivos usando informática forense* [Universidad Nacional de Trujillo]. http://dspace.unitru.edu.pe/handle/UNITRU/1437

Perito Judicial Group. (n.d.). *Recuperación de datos de medios informáticos - Informática Forense*. https://peritojudicial.com/recuperacion-de-datos/

Perry, S. (2016). *Applying the Critical Security Controls to a Digital Forensics and Incident Response Lab Network GIAC GSEC Gold Certification*. SANS Institute.

Policía Nacional de Colombia. (2021). *Policía Nacional logra la captura de 61 personas por delitos informáticos*. https://www.policia.gov.co/noticia/capturado-delito-hurto-informatico-enriquecimiento-ilicito-y-lavado-activos

Prakmatic. (n.d.). *Identifica las incidencias en sistemas informáticos con un análisis forense*. https://www.prakmatic.com/analisis-forense-investiga-las-incidencias-en-tus-sistemas-informaticos/

Qureshi, S., & Ramprakash, R. (2022). Role Of Crime Laboratories: Scope And Prospective In Criminal Investigation - Survey Based Analysis. *Journal of Mountain Research*, *17*(1). https://doi.org/10.51220/jmr.v17i1.15

Rada, K. (2022). *Herramientas De Análisis Forense Digital Orientadas a Infraestructuras TiC Como Medio De Investigación En Delitos Informáticos*. Universidad Nacional Abierta y a Distancia - UNAD.

Rada, K. (2022). *Herramientas De Análisis Forense Digital Orientadas a Infraestructuras Ti Como Medio De Investigación En Delitos Informáticos*.

Rivas, L. (2014). *Ciencia Forense*. INACIPE - INSTITUTO NACIONAL DE CIENCIAS PENALES.

Sampaoli, J. (2018). *Peritaje informático: marco teórico-practico*. Pontificia Universidad Católica de Argentina.

Sica, S., & Julio, M. (2021). *Suplemento CICA Multidisciplinario Julio - diciembre 2021* (Vol. 5).

Silva, R. S. S. da, Costa, C. F. de M., & Junior, C. M. D. (2019). Uma Aplicação do Lean Office (LO) na Informática Forense do Instituto Geral de Perícias de Santa Catarina (IGP-SC). *Tópicos Em Administração*, *25*. https://doi.org/10.36229/978-85-7042-151-7.cap.02

UNIR. (2021). *Confidencialidad en seguridad informática: claves para garantizarla*.

UNIR. (2021). *Informática forense: en qué consiste, ámbitos de aplicación y perfiles profesionales*. https://www.unir.net/ingenieria/revista/informatica-forense/#:~:text=La informática forense se refiere,un procedimiento legal o administrativo

Vargas, H., Solano, D., & Roldán, M. (2022). Investigación forense digital en entidades del Estado colombiano: acercamiento a la Ley 1952 de 2019. *Revista Logos Ciencia & Tecnología*, *15*(1), 122–140. https://doi.org/10.22335/rlct.v15i1.1698

Velasquez, R., & Davalos, F. (2016). *Informática forense y su influencia en la calidad de servicio en el centro de cómputo de la Universidad Tecnológica de los Andes*. Universidad Tecnológica de los Andes.

Wickenheiser, R. A. (2021). Reimagining forensic science – The mission of the forensic laboratory. *Forensic Science International: Synergy*, *3*. https://doi.org/10.1016/j.fsisyn.2021.100153

Wiebetech. (n.d.). *Ditto DX Forensic FieldStation*. https://wiebetech.com/products/ditto-dx-forensic-fieldstation/

Yasaca, S., Cajo, G., Cajo, B., & Mesías, I. (2019). *Evidencias Digitales en la Investigación Forense Informática*. Escuela Superior Politécnica del Chimborazo. http://cimogsys.espoch.edu.ec/direccion-publicaciones/public/docs/books/2019-09-19-211754-91 Evidencias Digitales en la Investigación Forense Informática.pdf

Yudistira, I. W. A., & Widijowati, R. D. (2023). Evidence Using Forensic Laboratory in Revealing the Crime of Murder. *Journal of Law, Politic and Humanities*, *3*(3), 330–342. https://doi.org/10.38035/jlph.v3i3.225