



Institución Universitaria

**Diseñar un Laboratorio de Ciencias  
Forenses Digitales en el Cuerpo Técnico de  
Investigación de la Fiscalía General de la  
Nación, Seccional Medellín.**

**José Ermes Palacios Carvajal**

Instituto Tecnológico Metropolitano

Facultad de Ingenierías

Medellín, Colombia

2020

# **Diseñar un Laboratorio de Ciencias Forenses Digitales en el Cuerpo Técnico de Investigación de la Fiscalía General de la Nación, Seccional Medellín.**

**José Ermes Palacios Carvajal**

Trabajo de investigación presentado como requisito parcial para optar al título de:

**Magister en Seguridad Informática**

Director:

Msc. Héctor Fernando Vargas Montoya

Director:

Msc. Milton Javier Mateus Hernández

Línea de Investigación:

Automática, electrónica y Ciencias Computacionales

Instituto Tecnológico Metropolitano

Facultad de Ingenierías

Medellín, Colombia

2020

*(Dedicatoria o lema)*

*A mi esposa, familia, maestros y amigos.*

## **Agradecimientos**

A Dios en primer lugar por tantas bendiciones en este proceso, a mi esposa y familia por su apoyo y a mis colegas por ser un pilar en este nuevo logro universitario.

## Resumen

Es claro que la tecnología mejora nuestras vidas, los procesos y las industrias. Los diferentes avances dan un reflejo en el aumento de transacciones electrónicas como cajeros automáticos, banca virtual, comercio electrónico, transacciones en línea, etc. cada uno de estos procesos han permitido mejorar las actividades al interior de las organizaciones y fortalecer el personal. Pero así mismo, se han generado una serie de desafíos en aspectos de seguridad informática y de la información que conllevan riesgos que permiten el surgimiento del crimen cibernético, el cual da lugar a los delitos Informáticos. La falta de definición e implementación de políticas de seguridad informática, es una de las dificultades de algunas las compañías, y que se convierte en un estímulo para quienes se aprovechan de muchas falencias para ejecutar ataques cibernéticos de tipo robo de información, secuestro empresarial y posibles filtraciones de datos digitales relevantes. Esto deja a los usuarios y organizaciones expuestos a la pérdida y divulgación de datos e información reservada, así que es necesario desarrollar investigaciones que logren establecer los hechos, causas, consecuencias y agentes generadores de dichas eventualidades.

Dado lo anterior, el proyecto tiene la finalidad de crear de un laboratorio de Ciencias Forenses Digitales en la ciudad de Medellín, que permita aplicar una metodología para la recolección y análisis de evidencia digital, utilizando procedimientos que se acojan a los estándares para la gestión de incidentes en la seguridad de la información y que permitan el desarrollo adecuado de una investigación, dicho proyecto se ejecutó a través de tres fases: la situación actual de los grupos de delitos informáticos en Colombia, las características de un laboratorio Forense y los resultados del diseño de un laboratorio de Ciencias Forenses Digitales, permitiendo la obtención del diseño del laboratorio que puede ser implementado para las diferentes funciones asociadas a la investigación de delitos.

**Palabras clave:** Seguridad informática, incidente informático, informática forense, evidencia digital, análisis de evidencia digital.

## Abstract

It is a reality that technology improves our lives, processes, and industries. Different advances give a reflex of the raising of electronic transactions like ATM's, virtual bank, e-commerce, on-line transactions, etc. Each process has allowed to enhance activities within organizations and strengthen staff. Likewise, there have been generated a lot of challenges in information and informatic security that leads to risks allowing the appearance of cybernetic crimes, giving place to informatic crimes... The lack of definition and implementation of informatic security policies, is one of the difficulties in some companies that becomes a stimulus for those who take advantage of shortcomings to execute cybernetic attacks like information subtraction, bussiness secrecy and some relevant digital data filtering. This leads users and organizations exposed to data and reserved information loss or divulgation, so it is necessary to develop some investigations that could detect facts, causes, consequences and generating agents of those eventualities.

Given the above, the project aims to create a Digital Forensic Sciences laboratory in the city of Medellín, which allows applying a methodology for the collection and analysis of digital evidence, using procedures that comply with the standards for the management of incidents in information security and that allow the proper development of an investigation, said project was executed through three phases: the current situation of the groups of computer crimes in Colombia, the characteristics of a Forensic laboratory and the results of the design of a Digital Forensic Sciences laboratory, allowing obtaining the laboratory design that can be implemented for the different functions associated with crime investigation.

**Keywords:** Informatic security, informatic incident, forensic informatics, digital evidence, digital evidence analisis.

# Contenido

	Pág.
<b>1. Introducción</b> .....	<b>12</b>
<b>2. Marco teórico y estado del arte</b> .....	<b>15</b>
2.1 Marco teórico.....	15
2.1.1 Informática Forense (IF).....	15
2.1.2 Evidencia Digital .....	16
2.1.3 Delito Informático .....	17
2.1.4 Herramientas de informática forense.....	17
2.1.5 Seguridad Informática.....	18
2.1.6 Cibercrimen.....	19
2.1.7 Fiscalía General de la Nación .....	19
2.1.8 Cuerpo Técnico de Investigación CTI .....	19
2.1.9 Diseño del laboratorio.....	19
2.1.10 Manejo de la evidencia digital .....	20
2.1.11 Incidente de seguridad.....	21
2.1.12 Cadena de custodia.....	21
2.2 Estado del arte .....	21
<b>3. Metodología</b> .....	<b>25</b>
3.1 FASE 1: Situación actual de los grupos de delitos informáticos.....	25
3.2 FASE 2: Características técnicas, funcionales y procedimentales de un laboratorio de ciencias forenses digitales.....	26
3.3 FASE 3: Evaluar el diseño .....	30
<b>4. Resultados</b> .....	<b>32</b>
4.1 Fase 1: .....	32

4.2	Fase 2: Resultados de las Características técnicas, funcionales y procedimentales de un laboratorio de ciencias forenses digitales .....	38
4.2.1	Características Técnicas .....	38
4.2.2	Legislación en Colombia.....	43
4.2.3	Recolección y Manejo de la evidencia digital .....	46
4.2.4	Análisis de la evidencia digital .....	50
4.2.5	Descripción del procedimiento en el Laboratorio .....	52
4.2.6	Grado de aceptación por la comunidad técnico científica, de los procedimientos empleados.....	53
4.2.7	Instrumentos empleados para el análisis .....	53
4.2.8	Principios técnico – científicos aplicados.....	54
4.2.9	Equipo de trabajo.....	55
4.2.10	Diseño del laboratorio de Ciencias Forenses Digitales .....	57
4.3	Fase 3: Resultados de la evaluación del diseño .....	59
<b>5.</b>	<b>Conclusiones y recomendaciones .....</b>	<b>73</b>
5.1	Conclusiones .....	73
5.2	Recomendaciones .....	74
<b>6.</b>	<b>Bibliografía.....</b>	<b>78</b>



---

## Lista de figuras

	<b>Pág.</b>
Figura 1: Fases de la IF. Fuente: elaboración propia a partir de [1] y [2].....	16
Figura 2: Diagrama del proceso de evidencia digital. Fuente: Guía No. 21, Seguridad y privacidad de la información MinTIC [17] .....	20
Figura 3: Metodología para el desarrollo del proyecto de grado. Fuente: Autor.....	25
Figura 4: Procedimiento análisis evidencia digital. Fuente: Elaboración propia a partir del procedimiento general para la policía judicial de la FGN .....	51
Figura 5: Diseño de un laboratorio de Ciencias forenses digitales. Fuente propia.....	57
Figura 6: Inocencia Perdida. Fuente propia .....	71

## Lista de tablas

	<b>Pág.</b>
Tabla 1: Área y propósito.....	27
Tabla 2: Equipos, descripción y características técnicas.....	27
Tabla 3: Software y descripción .....	28
Tabla 4: Checklist .....	30
Tabla 5: Checklist – caso de estudio .....	31
Tabla 6: Resultado – Área y propósito.....	39
Tabla 7: Resultado – Equipos, descripción y características técnicas.....	41
Tabla 8: Resultado – Software y descripción .....	42
Tabla 9: Propuesta Grupos de trabajo .....	56
Tabla 10: Fijación fotográfica de la evidencia.....	62
Tabla 11: Resultado archivos encontrados en la evidencia .....	64
Tabla 12: Checklist – caso “Inocencia Perdida” .....	68

---

## Lista de imágenes

	<b>Pág.</b>
Imágen 1: Equipo en el que se realizó el procedimiento .....	62
Imágen 2: Programa FTK realizado exitosamente .....	63
Imágen 3: Ruta F:\Imagen Forense .....	63
Imágen 4: Visualización CD-ROM .....	64
Imágen 5: Visualización reporte en CD-ROM.....	65
Imágen 6: Visualización del reporte.....	65
Imágen 7: Visualización de archivo en el reporte .....	66
Imágen 8: Visualización de la evidencia.....	67
Imágen 9: Equipo forense – Actual e Ideal .....	69
Imágen 10: Individualización del sindicado .....	69

# 1. Introducción

En la actualidad, las empresas dependen en gran medida de sus sistemas información, porque a través de estos producen su trabajo diario, generan valor a través de sus datos y, en definitiva, realizan su negocio. Por lo tanto, es relevante que se realice el diagnóstico continuo del nivel de seguridad informática de la organización. Pero el hecho de no investigar posibles indicios de acceso, mal uso o fuga de información, puede generar consecuencias a futuro derivadas al daño de la imagen, pérdida de reputación o problemas económicos. Dado el alto crecimiento del crimen informático, que para el 2017 se contó con un registró en la policía nacional de Colombia de al menos 6963 denuncias por hurto a través de medios informáticos<sup>1</sup>, implica ello que tarde o temprano alguien puede acceder a sus sistemas de información y, por ende, la empresa puede estar en manos de un intruso o personal mal intencionado.

El desarrollo de éste proyecto tiene los siguientes objetivos:

## **General:**

Diseñar un Laboratorio de Ciencias Forenses Digitales en el CTI de la FGN, Seccional Medellín, que permita un adecuado tratamiento a la evidencia digital utilizando metodologías técnicas y operativas, con la finalidad de garantizar la eficacia y confiabilidad del informe de Policía Judicial

## **Específicos:**

- Determinar mediante cuestionario de carácter reservado la situación actual de diferentes grupos investigativos de delitos informáticos en Colombia, con el fin de precisar las necesidades y falencias en sus procesos de investigación.

---

<sup>1</sup> Policia Nacional de Colombia. Balance cibercrimen en Colombia 2017. Caivital. Consulta en línea el 24 septiembre de 2018 en [https://caivirtual.policia.gov.co/sites/default/files/informe\\_cibercrimen\\_2017.pdf](https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf), 2017.

- Establecer las características técnicas, funcionales y procedimentales de un laboratorio de ciencias forenses digitales, considerando lo técnico, procesal y humano, basado en estándares y referentes nacionales y/o internacionales de buenas prácticas.
- Evaluar el diseño de un laboratorio de Ciencias Forenses Digitales, a través de un set de pruebas y/o un caso de estudio en el cuerpo técnico de investigación – CTI, Seccional Medellín.

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 [30], dicha ley modificó el código penal y se crea una nueva protección, dicha ley es denominada “De la protección de la información y de los datos”, con el objetivo de preservar los sistemas que utilicen las tecnologías de la información, para lo cual, se hace necesario la implementación de diversos procesos, procedimientos y mecanismos que permitan dar cumplimiento a dicha ley, dentro de esto, todos los procesos informáticos de investigación forense digital. En consecuencia, antes de ésta ley no se registraban denuncias por hechos relacionados al crimen informático en Colombia.

Para poder responder a la demanda del crimen cibernético, actualmente el Cuerpo Técnico de Investigación (CTI) de la Fiscalía General de la Nación (FGN) en Colombia, cuenta con el talento humano, las máquinas y el software especializado para análisis de evidencia digital en las principales ciudades del país, y actualmente cuenta con un laboratorio de Informática Forense solo en la ciudad de Bogotá, pero con la novedad de no estar certificado en los procesos que validen los diferentes procedimientos orientados a estándares internacionales en temas de seguridad de la información. Teniendo en cuenta lo anterior, se hace necesario proponer el diseño de un laboratorio de Ciencias Forenses Digitales en la ciudad de Medellín - Antioquia, donde se pueda aplicar una metodología para la búsqueda y análisis de evidencia digital, mediante la aplicación de procedimientos sistémicos con técnicas procedimentales, analíticas y científicas, conocimientos legales, jurídicos y tecnológicos, para localizar, identificar, recuperar, reconstruir, validar-analizar y presentar información que pueda ser válida en un proceso penal, cuando haya ocurrido un delito informático (en términos de ley), que dicho proceso, en un futuro, pueda ser certificado bajo las normas internacionales, dando cumplimiento a la normatividad que reglamenta el manejo de los elementos materiales probatorios (EMP) y la evidencia física (EF).

Por otro lado, mediante Resolución Nro. 0-063 del 10 de marzo de 2009<sup>2</sup>, nacen al interior de la Fiscalía General de la Nación - FGN, grupos de Delitos Informáticos en cada una de las seccionales a nivel nacional, para realizar y apoyar las Investigaciones Judiciales, con ello obtener elementos materiales probatorios y evidencia física (EMP y EF) existente en medios informáticos u otros medios tecnológicos o de tipo digital.

En el año 2010, el CTI de la FGN implemento dentro de sus procedimientos una GUIA de *“Inspección, recolección y manejo de evidencia digital”*, la cual permite realizar una descripción de las actividades que se deben tener en cuenta al momento de llevar a cabo una inspección, recolección y manejo de evidencia digital, así poder detectar, identificar, clasificar, documentar, proteger y trasladar tanto elementos probatorios como evidencia digital, lo que permite efectuar una reconstrucción de los hechos ocurridos materia de investigación, sin embargo, dicha guía no establece un diseño de un laboratorio de análisis forense digital (solo un procedimiento de actuación), por lo cual, las diferentes investigaciones se realizan con un solo grupo de investigación (en campo y en el laboratorio), sin la debida separación y segregación de funciones dentro de la organización.

Así mismo, muchas de las investigaciones forenses traspasan las fronteras nacionales, por tal motivo están regidas por legislación muy diferente a la colombiana y sin los debidos procesos, se torna muy difícil establecer una buena relación en los procesos investigativos.

Éste informe final se presenta de manera secuencial en el cumplimiento de los objetivos, iniciando por un marco teórico y el estado del arte, continuando con la metodología, la cual se desarrolló en 3 fases, i) la primera, a través de un cuestionario, se preguntó a los diferentes grupos de investigación gubernamentales sobre el estado actual de los delitos informáticos, (ii)

---

<sup>2</sup> Estructura Fiscalía General de la Nación. Retrieved from <http://www.fiscalia.gov.co/colombia/wp-content/uploads/ORG4.pdf>, 2014.

seguidamente se estableció, basado en estándares nacionales e internacionales, las diferentes características que debe tener un laboratorio de ciencias forenses digitales y por último (iii) se generó una propuesta de un laboratorio y se realizó una evaluación del diseño a través de un caso de estudio, obteniendo con ello los resultados finales. Finalmente, en el documento se dan las conclusiones, recomendaciones y trabajo futuro.

En este se diseñó de un Laboratorio de Ciencias Forenses Digitales en el CTI de la FGN, se tomó como referencia la Seccional Medellín, aplicando a través de un caso de estudio, los resultados obtenidos en dicho diseño.

## **2. Marco teórico y estado del arte**

### **2.1 Marco teórico**

#### **2.1.1 Informática Forense (IF)**

La IF tiene como objetivo obtener y analizar diferentes datos e información en medios de almacenamiento o en tránsito, así, lograr demostrar con evidencia probatoria la ocurrencia de un evento de seguridad o posible delito [1]. Los mismos autores establecen que con la ejecución de los procedimientos forenses, es posible la conservación y preservación del valor probatorio, establecer el origen, destino y contenido de los hallazgos, realizar la recuperación total o parcial de datos, establecer la validez probatoria en el tiempo a través de la garantía de integridad y por último, servir como un instrumento para la presentación de los informes forenses digitales finales, que ayudarán a la toma de decisiones.

En términos generales [1], [2], las fases de la Informática Forense se ilustran en la figura 1, en la cual la primer fase es necesario realizar una identificación del incidente (definir o entender claramente el alcance), seguidamente iniciar el proceso de recolección de evidencia digital con base en el alcance planteado, para luego establecer la mejor forma de conservar la evidencia recolectada (proceso de integridad de datos), seguidamente se debe realizar un análisis de los datos recolectados, validando que sean suficientes, válidos y que logren demostrar o no el hecho

que se investiga, para finalmente, generar los informes forenses y entregarlos a los entes que lo han solicitado.



Figura 1: Fases de la IF. Fuente: elaboración propia a partir de [1] y [2].

### 2.1.2 Evidencia Digital

*“La evidencia digital es única, cuando se le compara con otras formas de “evidencia documental”. A comparación de la documentación tradicional (aquella realizada en papel), la evidencia informática o tecnológica es frágil y cuenta con la posibilidad de permitir la copia idéntica al original. Otro aspecto único en la recolección de la evidencia es la posibilidad de obtener copias autorizadas sin dejar rastro de que se realizó una copia” [3].*

Acorde a la National Institute of Standards and Technology - NIST [4], específicamente en el proyecto Computer Forensic Tool Testing (CFTT) afirma que se debe tener en cuenta un adecuado procedimiento para el análisis de evidencia, obteniendo una copia forense del medio o dispositivo original, para lo cual, los datos digitales que contiene la copia, no se deben alterar,



dado que éstos yacen en la evidencia original, porque automáticamente se invalidaría la evidencia. Por lo anterior, los investigadores deben revisar constantemente sus copias, verificando que éstas sean totalmente exactas a la original, utilizando mecanismos de validación de integridad como las funciones Hash o resúmenes matemáticos.

### **2.1.3 Delito Informático**

*“No existe una sola definición que pueda enmarcarse como admitida en todo el universo de esta conducta, pues cada país lo define de acuerdo al derecho propio según su escenario legislativo”* [5]. Acorde al senado de la república de Colombia, el delito informático [6]: *“Son todas las conductas ilícitas realizadas por un ser humano, susceptibles de ser sancionadas por el derecho penal en donde hacen un uso indebido de cualquier medio informático, con la finalidad de lograr un beneficio”*.

Algunas de las características de los delitos informáticos hacen referencia a las acciones que pueden ocasionar altas pérdidas comerciales o las ejecutan empleados con conocimientos técnicos, no se requiere de presencia física para su ejecución y puede valerse de un medio informático como medio y como fin, adicional, presentan grandes dificultades para demostrar el delito o las causas de éste, dado el alto conocimiento técnico para desarrollar las actividades informáticas [7].

### **2.1.4 Herramientas de informática forense**

Las herramientas de informática forense, por lo general, están asociadas a computadores y portátiles para llevar a cabo los análisis forenses digitales, estas herramientas pueden ser de duplicación de discos, conectividad entre ellos, adaptadores y bloqueadores, el cual permitirán realizar análisis de las pruebas de una manera rápida y sencilla.

En consideración que las diferentes imágenes forenses poseen un tamaño importante (dado que se pueden conseguir confiscaciones de discos de 500GB, 1TB o más, así como la ejecución de procesos en paralelo), éstos equipos deberán tener una alta capacidad de procesamiento de evidencia digital, para la creación y ejecución de máquinas virtuales, la creación de reportes con sus anexos indexados y recuperados, con ello, poder procesar toda la información adquirida.

En cuanto al software, se encuentran gran variedad de programas que permiten analizar, procesar y recuperar datos de una evidencia digital, pero se requiere que tengan la confianza, el respaldo y el aval internacional para realizar este proceso, por lo que este proyecto se basará en las herramientas EnCase, AccessData FTK y UFED 4PC, aunque cabe aclarar que existen muchas otras herramientas que se pueden encontrar de manera gratuita en Internet como las distribuidas por Linux, Autopsy Forensic, Helix, X-Ways Forensic, entre otros.

Guidance Software, fue fundada en 1997, desarrolla EnCase Forensic Software que es una herramienta de análisis forense para PC que ha sido el pilar del forense desde hace más de una década. El Software Forense EnCase es capaz de realizar adquisiciones, restaurar unidades de disco duro (clonar bit por bit y hacer un HDD clonado), completar una amplia investigación a nivel de disco, y crear informes extensos, entre muchas otras cosas [8].

AccessData es el principal proveedor de E-Discovery, Informática Forense de Dispositivos Móviles y Ordenadores para corporaciones, bufetes de abogados y agencias gubernamentales. Entre sus soluciones forenses digitales están Forensic ToolKit (FTK), que proporciona un procesamiento e indexación exhaustivos iniciales, por lo que el filtrado y la búsqueda son más rápidos que con cualquier otra solución del mercado [9].

Cellebrite es una subsidiaria de la Corporación Sun de Japón, Cellebrite Mobile Synchronization es una compañía israelí que se considera ser el líder cuando se trata de software forense móvil. Su principal herramienta móvil es el UFED 4PC, el cual proporciona una visión profunda de los dispositivos móviles a través de la plataforma Unified Digital Forensics de Cellebrite [10].

### **2.1.5 Seguridad Informática**

La seguridad informática, se ocupa de las diferentes protecciones técnicas que deben hacerse a los activos de información ISO [11]. Para los sistemas de gestión de seguridad es fundamental contar con los controles técnicos que permitan la reducción de los riesgos de exposición. La seguridad informática permite, a través de la implementación de diferentes controles técnicos, reducir los niveles de exposición del riesgo, con ello, los niveles de posibles impactos.

### **2.1.6 Cibercrimen**

Acorde a al proveedor de herramientas de seguridad Norton [12], es el delito por vía informática, que puede ser perpetrado por una o varias personas en muchos aspectos, como la propagación de virus a través de correos electrónicos para la venta de productos o servicios, distribución de pornografía infantil, fraude, extorsión, estafas, violación de la propiedad intelectual o robo de dinero a través de transacciones electrónicas fraudulentas.

### **2.1.7 Fiscalía General de la Nación**

La Fiscalía General nació en 1991 con la promulgación de la nueva Constitución Política y empezó a operar el 1 de julio de 1992.

Es una entidad de la rama judicial del poder público con plena autonomía administrativa y presupuestal, cuya función está orientada a brindar a los ciudadanos una cumplida y eficaz administración de justicia [13].

### **2.1.8 Cuerpo Técnico de Investigación CTI**

Es un órgano de Policía Judicial que pertenece a la Fiscalía General de la Nación [14], del poder judicial en Colombia y sus funciones principales son asesorar al Fiscal General en políticas y estrategias de investigación del delito, servicios forenses, genética y análisis criminal útil para la investigación penal.

### **2.1.9 Diseño del laboratorio**

Para lograr responder a las necesidades del CTI de la Fiscalía General de la Nación en la seccional Medellín, en el diseño del laboratorio debe predominar la seguridad, funcionalidad, eficacia y eficiencia, sobre los criterios estéticos, creando un ambiente adecuado para el tratamiento de la evidencia digital [15], [16], donde se cuente con áreas amplias, aisladas preferiblemente con seguridad biométrica solo para personal autorizado, sistema de video bajo un circuito cerrado de grabación las 24 horas y alarma de movimiento, lo anterior bajo condiciones ambientales ideales como buena iluminación, energía eléctrica regulada, control electrostático, ventilación,

temperatura y humedad apropiados para la conservación de evidencia digital, sin descuidar el cableado de red y telefónico indispensable para cada área de trabajo.

Las áreas principales son: almacenamiento, mecánica y análisis, contando con un área especial para el análisis de dispositivos móviles, el cual no tendrá señal celular.

### 2.1.10 Manejo de la evidencia digital

En Colombia, la metodología general del procedimiento de evidencia digital, se centra en cuatro pasos principales según la guía de seguridad y privacidad de la información [17], ilustrada en la figura 2.



Figura 2: Diagrama del proceso de evidencia digital. Fuente: Guía No. 21, Seguridad y privacidad de la información MinTIC [17]

Dentro del proceso, se validan y ejecutan 5 etapas, en dónde el reporte final debe condensar todo el proceso investigativo, mostrando toda la evidencia relevante que fue generada en los pasos anteriores y entregando la conclusión del análisis de datos. El aislamiento es un primer paso fundamental, que permite establecer y resguardar desde el inicio la evidencia, evitando que ésta se contamine.

### **2.1.11 Incidente de seguridad**

Es cualquier anomalía que afecte la seguridad de la información y que atente contra la confidencialidad, integridad o disponibilidad de los datos ISO [18]. Si se confirma la autenticidad del evento, se hace necesario realizar el correcto manejo de la evidencia, de acuerdo al diagrama del proceso de evidencia digital (Figura 2).

### **2.1.12 Cadena de custodia**

“Establecer las directrices del sistema de cadena de custodia colombiano, durante las diferentes etapas asociadas al hallazgo, recolección, embalaje, transporte, análisis y almacenamiento de los Elementos Materiales Probatorios y Evidencia Física (EMP y EF), con el fin de garantizar su autenticidad y capacidad demostrativa, mientras que la autoridad competente ordena su disposición final.” [19]. Para que los EMP y EF se encuentren en el laboratorio, debe ser solo con orden del Fiscal asignado al caso por el término que el determine para su análisis y entrega de resultados, de lo contrario los elementos deben permanecer en el Almacén de evidencias designado por el Fiscal General de la Nación, para la custodia permanente de los EMP y EF hasta que la autoridad competente realice su disposición final.

## **2.2 Estado del arte**

En los años 90, el FBI (Federal Bureau of Investigation), en algunas revisiones realizadas, concluyó que los elementos digitales pueden servir como pruebas muy contundentes ante un caso judicial, dado que los diferentes elementos que residen en los elementos tecnológicos pueden validar cualquier prueba e incluso pueden ser homologadas o comparadas con pruebas similares realizadas con el ADN [20], por lo que se adelantaron varios proyectos y reuniones con el fin de consolidar las herramientas y estrategias que lograran definir la evidencia digital como elementos válidos, es así, como en los años 90 se fundó la IOCE (International Organization of Computer

Evidence), con el objetivo de fortalecer las prácticas de informática forense, para 1999 se presentaron los primeros borradores sobre los principios y generalidades de lo que podría ser la evidencia digital, dentro de las cuales se destaca aquella que la establece como la *“información de valor probatorio almacenada o transmitida en forma digital”* [21]. De acuerdo con la nueva estrategia, la evidencia digital incluye diferentes sistemas de almacenamiento y servicios informáticos, por lo que dicha evidencia digital es la *“vía requerida para presentar pruebas de los hechos ocurridos en sistemas o dispositivos electrónicos”* [22].

Por otro lado, se ha propuesto una guía procedimental para la evidencia digital [23], en dicha guía se abordan diferentes temas procedimentales para reconocer, recoger extraer y proteger evidencia con una aplicabilidad en Ecuador, se plantea, a partir de diferentes referencias internacionales cómo debería ser la mejor opción de dicho procedimiento. Enmarca cada una de las fases con sus componentes, indicando cómo se podría llevar a cabo y presentando un caso de estudio para validar su aplicabilidad, sin embargo, no se aborda el tema de cómo se podría desarrollar un laboratorio técnico procedimental para el proceso.

Así mismo, las fases para el análisis y reporte de evidencia digital se abordan como una serie de pasos en su cumplimiento [24], se indica la necesidad de establecer parámetros claros en cada fase, desde la escena del crimen, pasando por la identificación de dispositivos, revisión de datos, creación del reporte hasta la entrega de la información hacia los estrados judiciales, para ello, se organiza un mapa de posibles evidencias digitales y estas se correlacionan en busca de factores comunes que desenlacen una línea de tiempo capaz de demostrar la eventualidad buscada, pero no se aborda temas que dan relación hacia almacenes de evidencia o como se articula un laboratorio para tal fin.

Ahora bien, es posible la creación de un laboratorio de análisis forense de bajo costo para una Universidad, expresando los diferentes componentes necesarios para la construcción teórica de dicho laboratorio, se plantea desde la distribución física de la sala, hasta varias versiones de hardware y software (free o de uso restringido), dichos elementos apoyan las fases de recolección, validación, análisis y reporte de los diferentes eventos de seguridad que puedan

constituir un delito, sin embargo no aborda temas como idoneidad del personal (dado que es para uso universitario y de aprendizaje), tampoco los mecanismos de control de presentación de la seguridad de la información propia del laboratorio o las consideraciones legales que pueda tener el tema [25].

Puede ser usada para probar un evento de seguridad por una investigación administrativa y/o probar un delito convencional en el que se usó un computador (como medio o como fin). La informática forense contempla múltiples procedimientos, procesos y estrategias que permitan obtener la información suficiente, relevante y necesaria para demostrar un hecho (punible o no), por lo cual acorde a [23], la informática forense debe desarrollarse como un procedimiento sistémico y organizado, que permita reconocer, recopilar, extraer, proteger e informar las diferentes evidencias digitales, pero éstas pautas los autores las aplican de forma general en los sistemas, lo que es necesario establecer el cómo debe desarrollarse para un sistema en particular.

A través de una búsqueda selectiva en Internet, se logró identificar que, en la actualidad hay varios laboratorios de informática forense, tales como:

- En Colombia:
  - (“Laboratorio de Informática Forense Fiscalía General de la Nación”) en Bogotá  
[http://centrodeinnovacion.gobiernoenlinea.gov.co/sites/default/files/26\\_laboratorio\\_fiscalia\\_general.pdf](http://centrodeinnovacion.gobiernoenlinea.gov.co/sites/default/files/26_laboratorio_fiscalia_general.pdf)
  - (“Centro cibernético de la Policía Nacional,” 2017) en Bogotá.  
<http://www.ccp.gov.co/>
  - (“Laboratorio de informática forense de la Universidad de los Andes,” 2016) en Bogotá  
<https://sistemas.uniandes.edu.co/es/infraestructura/forense>
  - (“Laboratorio forense digital Asoto Technology Group Sas,” 2016)  
<http://www.asoto.com/wp/forense-digital/>
  - (“Computo forense Internet Solutions,” 2016)  
<http://www.internet-solutions.com.co/serv.php>
  
- A nivel Internacional:
  - (“Laboratorio forense Maticca en México y Colombia,” 2017)  
<http://mattica.com/laboratorio-forense/>
  - (“Sistema Nacional de Gestión de Incidentes Telemáticos de la República Bolivariana de Venezuela,” 2017)

- <http://www.vencert.gob.ve/es-ve/>
- (“Informática forense Yanapti en Bolivia,” 2016)  
<http://www.yanapticorp.com/e1576f172c3b126ae7a6026e8995da85?id=2>
- (“Instituto Nacional de Ciberseguridad (INCIBE) en España,” 2016)  
[https://www.incibe.es/home/instituto\\_nacional\\_ciberseguridad/](https://www.incibe.es/home/instituto_nacional_ciberseguridad/)
- (“Laboratorio de criminalística en ingeniería de la Guardia Civil Española,” 2016)  
<http://www.guardiacivil.es/es/institucional/especialidades/InvestigacionCientific a/index.html>
- (“Análisis Forense de Computadoras Intrasoft en Panamá,” 2016)  
[http://www.intrasoftpanama.com/index.php?option=com\\_content&view=article &id=28&Itemid=26](http://www.intrasoftpanama.com/index.php?option=com_content&view=article &id=28&Itemid=26)
- (“Laboratorio de informática forense del FBI - Oficina federal de investigación en Estados Unidos,” 2016).  
[https://www.fbi.gov/news/stories/2009/august/rcfls\\_081809](https://www.fbi.gov/news/stories/2009/august/rcfls_081809)

Algunos proveedores de tecnología establecen diferentes parámetros de lo que ellos consideran un laboratorio forense, es el caso de la firma consultora Adalid Abogados [26], quienes ofrecen múltiples equipos técnicos que permiten la recolección y preservación de la evidencia digital, pero los clientes requieren de una estructura física y unos procesos que permitan el buen uso de dichos elementos computacionales. De la misma forma lo hacen empresas como Duriva [27], Asoto [28] y Atlas LTDA [29].

Por lo anterior, y dada las necesidades propias de la FGN, se realizó validación de los diferentes componentes y necesidades a nivel Colombia de lo que podría ser un laboratorio de análisis forense para la FGN (iniciando en la ciudad de Medellín), promoviendo de manera proactiva diferentes componentes para su creación, considerando, entre otros, personal idóneo para la ejecución de las actividades forenses, componentes tecnológicos válidos para presentar pruebas en Colombia y procedimientos para la seguridad de la información que constituye evidencia digital.



### 3. Metodología

La realización de este proyecto se dividió en 3 fases así (Figura 3):

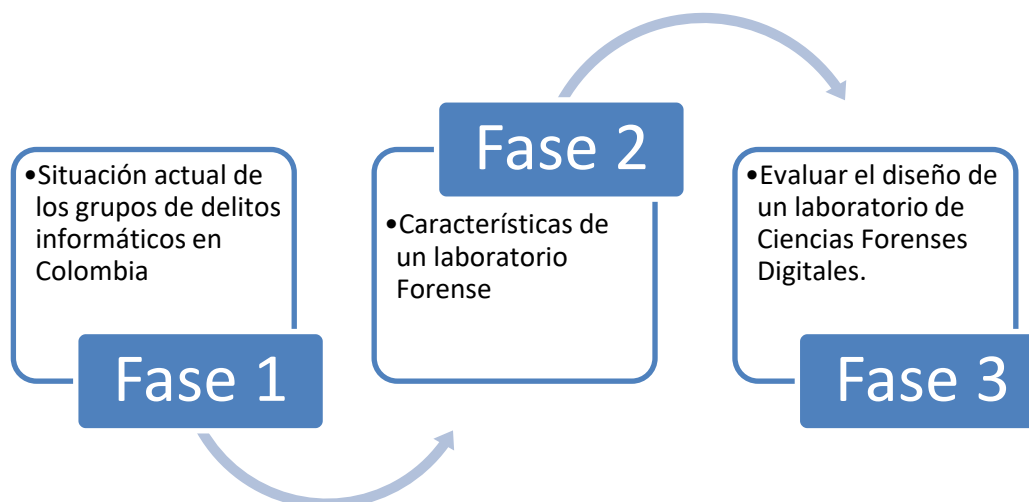


Figura 3: Metodología para el desarrollo del proyecto de grado. Fuente: Autor

A continuación, se describe cada una de las fases con las cuales se desarrolló el proyecto.

#### 3.1 FASE 1: Situación actual de los grupos de delitos informáticos.

En ésta fase, se obtuvo la información de cómo operan los diferentes grupos gubernamentales, dicha información fue recolectada a través de una encuesta, ésta, fue dirigida a funcionarios de Policía Judicial que hacen o han hecho parte del grupo de Delitos Informáticos del Cuerpo Técnico de Investigación (CTI) de la Fiscalía General de la Nación (FGN) – Seccional Medellín, con el fin de determinar necesidades y falencias en sus procesos de investigación. En total fueron 10 preguntas que se muestran en la tabla 1 y en el Anexo 1 se encuentra el formulario completo.

1. ¿Para usted que es la informática forense?
2. ¿Qué es evidencia digital?
3. ¿Qué es un delito informático?

4. ¿Para qué sirve la cadena de custodia?
5. ¿Qué es un hash?
6. Aprueba la implementación de un laboratorio de ciencias forenses digitales en el CTI de su Seccional
7. Está de acuerdo con diferenciar el Grupo de Delitos Informáticos con el de Informática Forense en su Seccional
8. Cree que es importante la creación de un plan de entrenamiento para Informática Forense (Califique de 1 a 5, donde 1 es la calificación más baja y 5 la más alta)
9. Conocimiento específico en redes y sistemas de computadores.
10. Maneja usted las siguientes herramientas: (Responda SI o NO)

De la información resultante, se realizó el análisis respectivo de las necesidades.

### **3.2 FASE 2: Características técnicas, funcionales y procedimentales de un laboratorio de ciencias forenses digitales.**

En esta fase, para obtener la información respectiva, se revisaron varias fuentes de información con el fin de obtener los requerimientos técnicos y funcionales de los laboratorios de ciencias forenses, tanto a nivel nacional como internacional.

En ésta fase se desarrollaron las siguientes temáticas: Características Técnicas, Legislación en Colombia, Manejo de la evidencia digital, Recolección de la evidencia digital, Análisis de la evidencia digital, Descripción del procedimiento en el Laboratorio, Grado de aceptación por la comunidad, técnico científica, de los procedimientos empleados, Instrumentos empleados para el análisis, Principios técnico – científicos aplicados, Equipo de trabajo y el diseño de un laboratorio de Ciencias Forenses Digitales.

A continuación, se describe la metodología usada para las temáticas:

**a) Características Técnicas**

Con respecto a los espacios físico, se realizó una descripción acorde a la necesidad, el diseño debe contemplar los requisitos, asociados al tipo de área y propósito:

Área	Propósito

Tabla 1: Área y propósito

Para la definición de equipos computacionales, se establecieron requerimientos mínimos de acuerdo al software que debe ser instalado en los equipos de cómputo, para lo cual, los equipos tendrán los siguientes detalles:

Equipo	Descripción	Características técnicas
Estación y servidores forense		
Estación portátil		
Almacenamiento de evidencias procesadas		
Bloqueadores y clonadores		
Servidor WEB		
Servidor de aplicaciones		
Servidor de procesamiento		
Servidor de bases de datos		

Tabla 2: Equipos, descripción y características técnicas

Software especializado: Son las herramientas de software que tiene los investigadores para realizar la experticia a un dispositivo de almacenamiento digital, de las cuales existen comerciales (Licenciadas) o free (Libres), para lo cual, se hace un levantamiento de la siguiente información:

Software	Desarrollador	Licencia	Descripción

Tabla 3: Software y descripción

**b) Legislación en Colombia**

Se establecido, a partir de varias respuestas de la encuesta y de la legislación colombiana como la ley de delitos informáticos -ley 1273 de 5 de enero de 2009, pornografía infantil (ley 679 de 2001) y algunas de derechos de autor (dado que son las más relevantes en cuanto a delitos informáticos), los elementos requeridos para la creación de procesos en la ejecución de las acciones respectivas.

**c) Recolección y Manejo de la evidencia digital**

Se hace una extracción del proceso para el manejo de la evidencia digital de la fiscalía, así mismo, se hace una revisión de buenas prácticas nacionales e internacionales, concatenando y entregando un procedimiento acorde a la necesidad.

**d) Análisis de la evidencia digital**

A partir de los procesos propios para el análisis de la evidencia digital, se crea un flujo para tal fin.

**e) Descripción del procedimiento en el Laboratorio**

Consiste en realizar una serie de actividades detalladas para llevar a cabo los lineamientos requeridos en el laboratorio de acuerdo a la evidencia digital allegada.

**f) Grado de aceptación por la comunidad técnico científica, de los procedimientos empleados**

Se relaciona la aceptación de los principios, métodos y procedimientos por la comunidad técnico-científica a nivel nacional e internacional.

### **g) Instrumentos empleados para el análisis**

Se indican los equipos e instrumentos fundamentales para el análisis de la evidencia digital de acuerdo a los parámetros y elementos que deben emplearse para un análisis forense.

### **h) Principios técnico – científicos aplicados**

Según la Informática forense, se mencionan los principios, métodos y procedimientos utilizados por el perito para obtener los resultados que se plasman en el informe de laboratorio, realizando una explicación clara concisa y breve del fundamento técnico científico.

### **i) Equipo de trabajo**

Para lograr los objetivos y las metas en el laboratorio se pretende realizar una división de roles al interior del grupo de delitos informáticos de la Fiscalía.

### **j) Diseño de un laboratorio de Ciencias Forenses Digitales**

De acuerdo a las necesidades físicas, ambientales y de infraestructura, se adecua el diseño de un laboratorio que garantice la integridad y seguridad de la evidencia digital.

Para la elaboración del diseño físico y sus funcionalidades, se realizó a través de la consolidación de las normas ISO 27001:2013 y las buenas prácticas establecidas por la ONAC (Organismo Nacional de Acreditación de Colombia), de ellas, se obtuvo el diseño respectivo.

### **k) Checklist de validación del diseño**

Se ha construido un checklist para la validación del nuevo diseño del laboratorio.

DESCRIPCIÓN	SI	NO
Acto urgente		
Solicitud de análisis		
Tipo de elemento (CD, DVD, USB, memoria o disco duro)		
Tipo de dispositivo (Celular)		
El elemento se encuentra con algún bloqueo		
Se cuenta con la contraseña		
El elemento se encuentra rotulado y con su debida cadena de		

custodia		
Se cuenta con medio de almacenamiento para la imagen forense		
Se cuenta con palabras claves, videos o imágenes para realizar búsquedas		
La seguridad en las instalaciones físicas para el análisis de evidencia es la adecuada		
Las herramientas forenses se encuentran actualizadas		
Las licencias forenses se encuentran vigentes		

Tabla 4: Checklist

### 3.3 FASE 3: Evaluar el diseño

En la actualidad el procedimiento que se realiza en los laboratorios estudiados, consiste en que cada investigador tiene su equipo y herramientas para realizar el análisis de la evidencia digital, por lo que en una seccional tan grande como lo es la del CTI Medellín, se repasan las actividades debido a la cantidad de casos que llegan de Antioquia y apoyo a seccionales pequeñas como Quibdó o Montería.

Este laboratorio es multiusuario con servidores web y de aplicaciones para varios investigadores, con lo cual, en esta etapa se evaluó el diseño con base en el siguiente caso de estudio, el cual ya fue juzgado (se hace un resumen de éste):

El caso de estudio tiene que ver con la recuperación y análisis de la información de una memoria MicroSD que fue incautada, la cual contenía videos sexuales de una persona adulta con varias menores de edad, éste, se ha tomado como prueba al diseño, teniendo en cuenta que ya fue judicializado y juzgado bajo un numero de noticia criminal en la ciudad de Medellín por los delitos de acceso carnal o acto sexual en persona puesta en incapacidad de resistir (acorde al art.207c.p. Agravado art. 211 n.4 de la ley 599 del 2000), el cual se realizará sobre persona menor de 14 años; acto sexual violento con menor de catorce años art.209 c.p. agravado art. 211 n.4, se realizare sobre persona menor de 14 años; actos sexuales con menor de catorce años. Art. 209

c.p.; delitos contra la vida y la integridad personal; pornografía con menores art. 218 c.p.; y secuestro simple art. 168 c.p.:

Teniendo en cuenta el caso de estudio, se procedió a realizar 2 validaciones:

1. Caso de estudio ejecutado con el proceso actual, dicho proceso indica que se debe:  
Evaluar el contenido de la memoria maca Kingston MicroSD color negra de 16GB de capacidad, con el fin de valorar el contenido de la misma (De manera detallada) y determinar si en el contenido hay alguna de las víctimas, y si en el contenido de la memoria se puede observar el presunto indiciado de la conducta penal.
2. Caso de estudio ejecutado con el proceso asociado al nuevo diseño, acorde al checklist definido en el objetivo anterior.

DESCRIPCIÓN	SI	NO
Acto urgente	X	
Solicitud de análisis	X	
Tipo de elemento (CD, DVD, USB, memoria o disco duro)	X	
Tipo de dispositivo (Celular)		X
El elemento se encuentra con algún bloqueo		X
Se cuenta con la contraseña		X
El elemento se encuentra rotulado y con su debida cadena de custodia	X	
Se cuenta con medio de almacenamiento para la imagen forense	X	
Se cuenta con palabras claves, videos o imágenes para realizar búsquedas	X	
La seguridad en las instalaciones físicas para el análisis de evidencia es la adecuada		X
Las herramientas forenses se encuentran actualizadas	X	
Las licencias forenses se encuentran vigentes	X	

Tabla 5: Checklist – caso de estudio

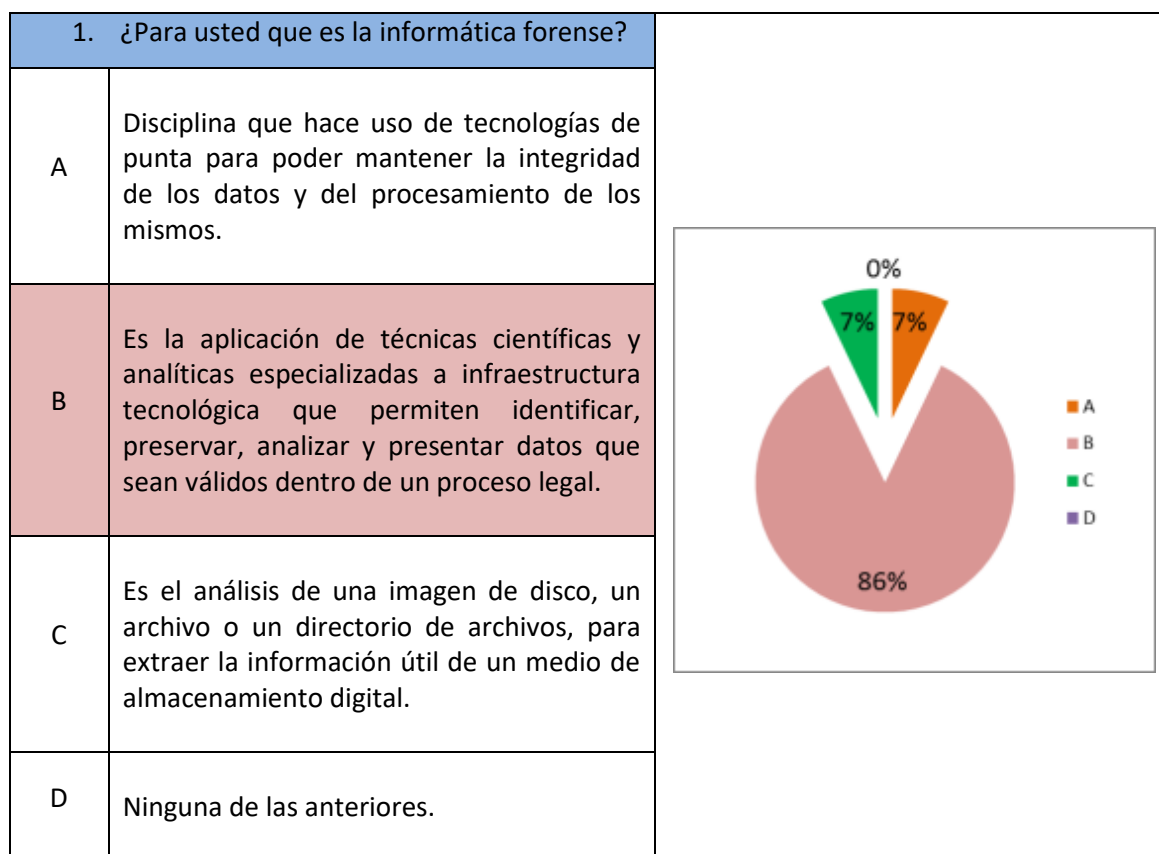
La validación del checklist en el proceso establece la forma cómo se debería realizar la prueba, con lo cual, se obtendrían los resultados respectivos.

## 4. Resultados

A continuación, se describen los resultados obtenidos con base en la metodología planteada

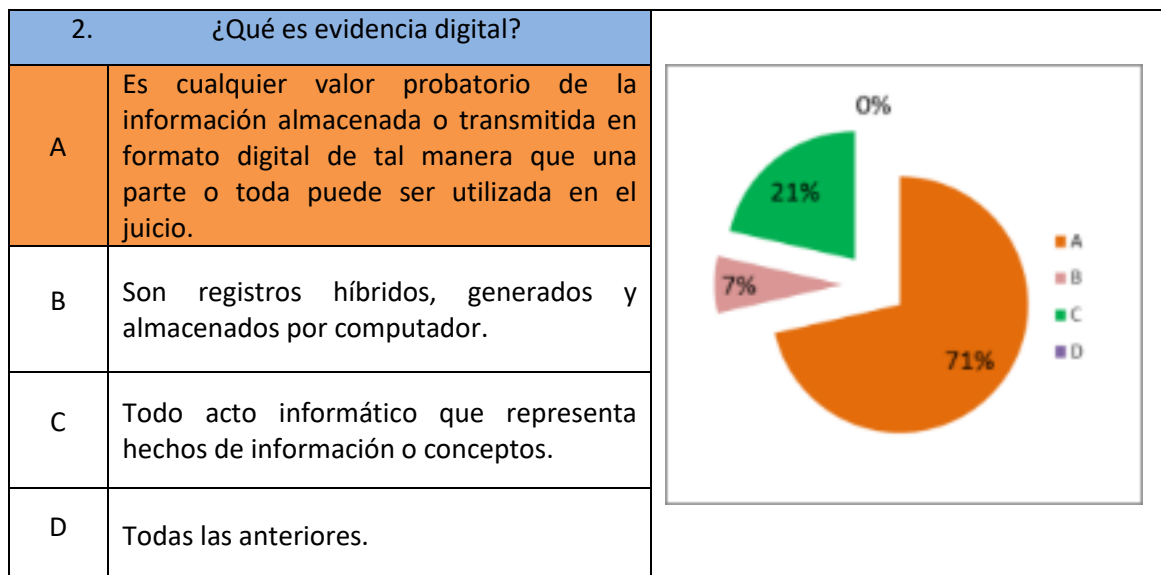
### 4.1 Fase 1:

Los resultados del cuestionario, dirigido a funcionarios de Policía Judicial que hacen o han hecho parte del grupo de Delitos Informáticos del Cuerpo Técnico de Investigación (CTI) de la Fiscalía General de la Nación (FGN) – Seccional Medellín, son los siguientes:

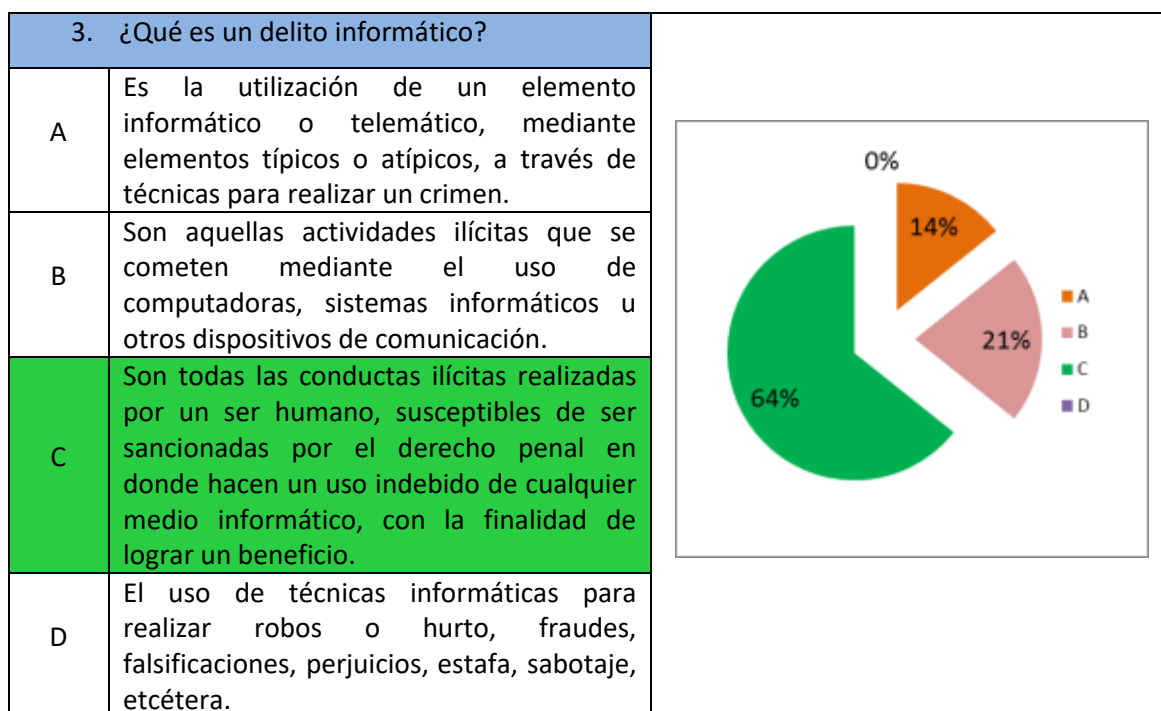


Con la respuesta a la pregunta anterior, se establece el nivel de conocimiento sobre la temática en particular, y cómo el personal desarrolla diferentes funciones considerando la formación y/o el conocimiento que adquiere. Acorde a los resultados, el 86% de las personas están enteradas y tienen el conocimiento para afrontar los retos laborales.

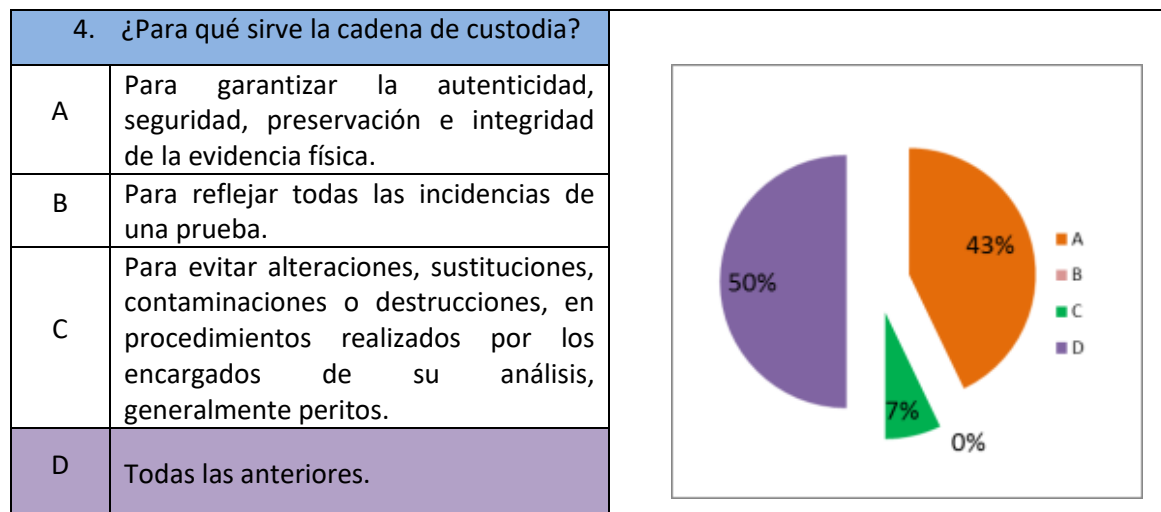




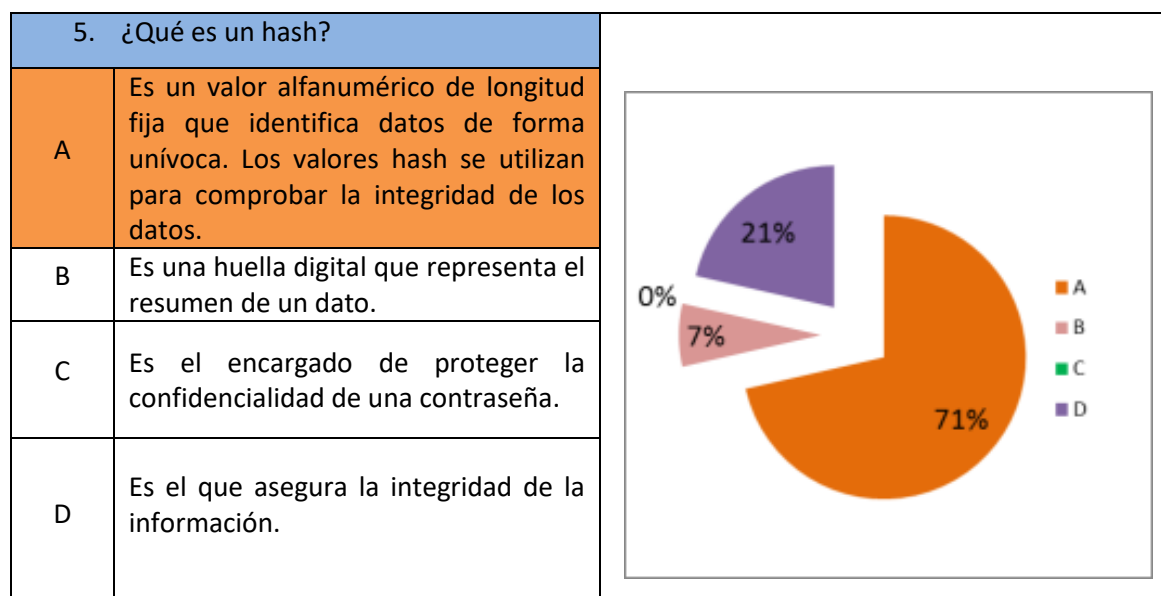
Para la pregunta No. 2, es claro el conocimiento de las personas sobre lo que es una evidencia digital, dado que el 71% de ellas reconoce la temática.



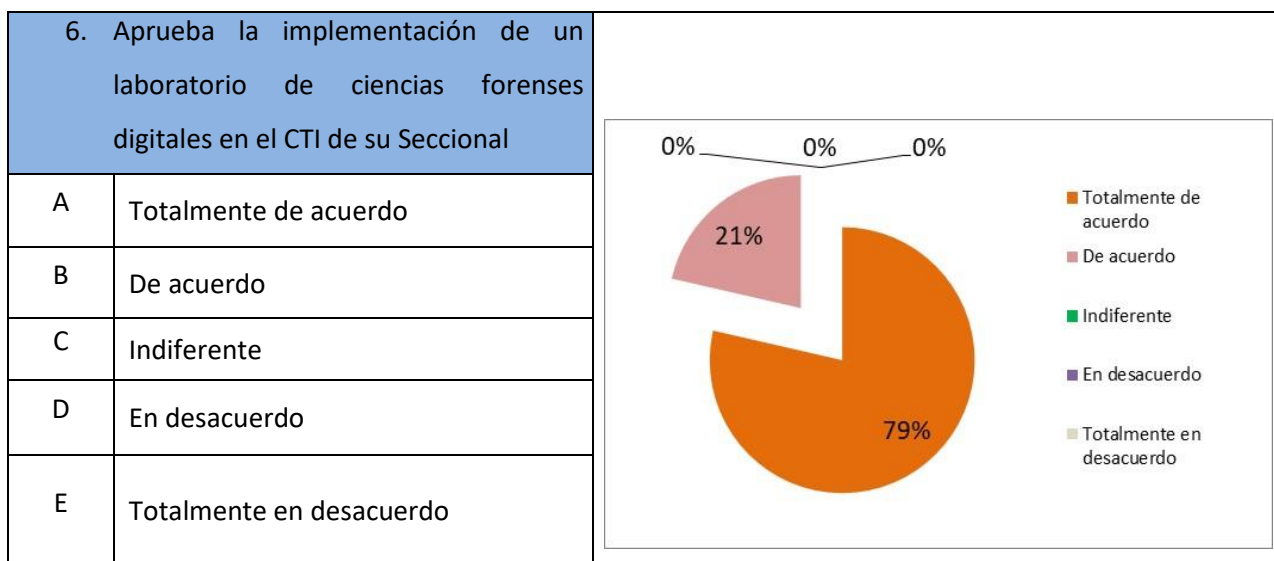
Aunque supondría que quién trabaja permanentemente en el tema de delitos informáticos le debe ser claro el tema, en la pregunta 3 el 64% de las personas seleccionaron las opciones correctas, lo que se esperaba un poco más, por lo cual, el 14% de ellas relacionan el delito informático a la utilización de elementos técnicos.



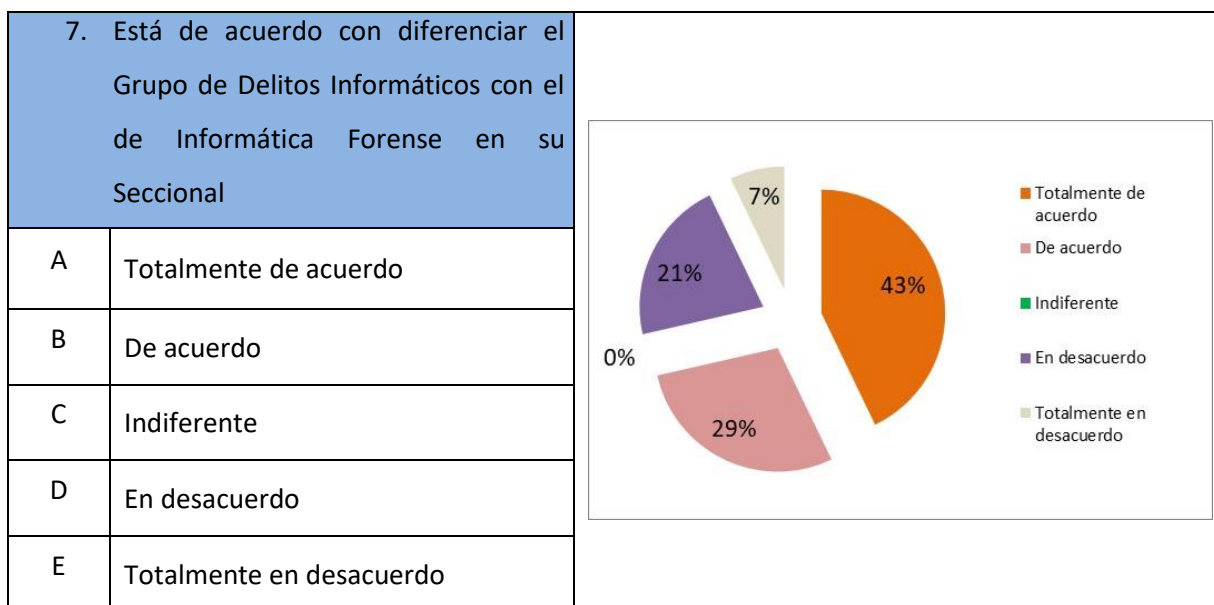
La pregunta 4 establece una necesidad clara de dar a conocer una definición coherente y homóloga de lo que es y para qué sirve la cadena de custodia, esto, en consideración que el 43% relaciona la cadena de custodia con una serie de factores, pero el 50% con todos los factores, un conocimiento dividido.



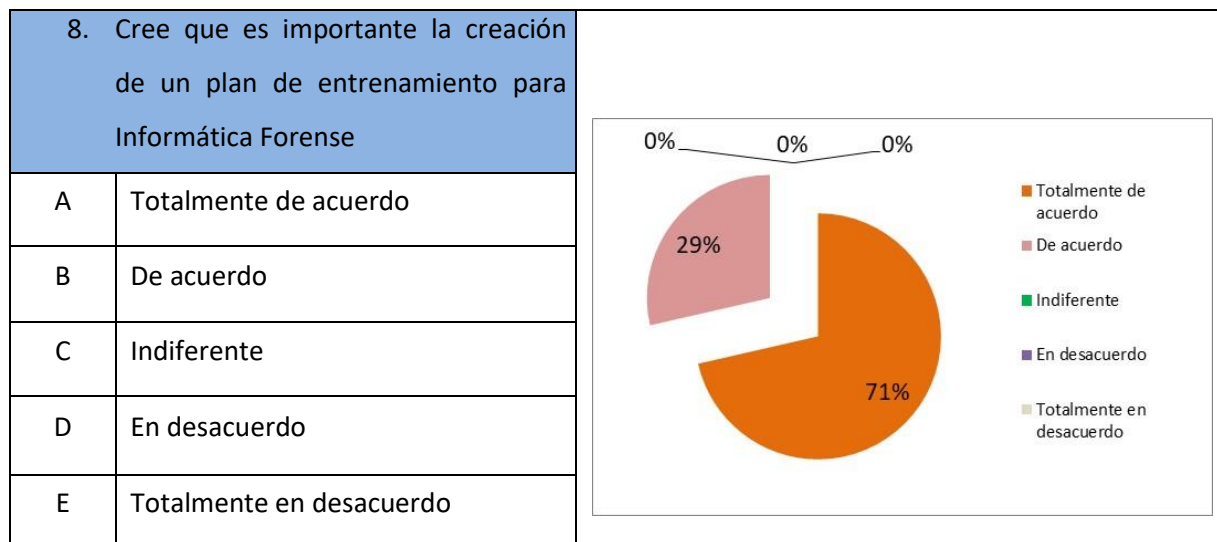
Aunque el 71% de los encuestados conocen que es un HASH, se encuentra que existe un alto grado de desconocimiento para un tema que se utiliza a diario en el Grupo.



Para está pregunta 6, con casi un 80% existe una gran expectativa para la creación de un laboratorio en la Seccional.



La pregunta 7 genera gran diferencia entre los encuestados, debido a que la mayoría de los funcionarios se encuentran cómodos en sus puestos de trabajo y prefieren realizar todas las labores tanto de laboratorio como de calle.



Con la respuesta a la pregunta 8, todos los funcionarios están de acuerdo con un plan de entrenamiento para Informática Forense, que permita establecer un plan para aumentar el nivel de conocimiento.

(Califique de 1 a 5, donde 1 es la calificación más baja y 5 la más alta)					
9. Conocimiento específico en:					
Bases de datos	1	2	3	4	5
Redes de datos	1	2	3	4	5
Programación	1	2	3	4	5
Seguridad computacional	1	2	3	4	5
Informática Forense	1	2	3	4	5

Aunque todos conocen de los temas planteados en la pregunta 9, se puede observar que los encuestados se encuentran con falencias en programación y redes de datos, pero con fortalezas en Seguridad Computacional, Informática forense y Bases de datos

(Responda SI o NO)		
10. Maneja usted las siguientes herramientas:		
ENCASE	SI	NO
FTK	SI	NO
UFED CELLEBRITE	SI	NO
WINDOWS	SI	NO
LINUX	SI	NO
MAC OS	SI	NO
RECOLECCIÓN DE DATOS VOLÁTILES	SI	NO

En esta última pregunta, observamos que faltaría capacitación principalmente en UFED CELEBRITE, y en MAC OS.

Como conclusiones generales de la encuesta se tiene:

- Se logró determinar que el grupo de delitos informáticos del CTI en la Seccional Medellín, necesita un refuerzo como plan de entrenamiento con capacitación especializada, y que cuando ingrese un nuevo integrante se someta a este plan.
- La necesidad de crear un nuevo grupo de Informática Forense como Laboratorio.
- Determinar los roles y actuaciones de los investigadores dependiendo al grupo que pertenecen.
- Para la idoneidad y pertinencia de los peritos del grupo de IF, se hace necesario que sean profesionales en áreas afines a la Informática y que su cargo sea como Profesional y no como Técnico, para que la sustentación ante un estrado judicial tenga el peso, respaldo y aprobación requerida.

## 4.2 Fase 2: Resultados de las Características técnicas, funcionales y procedimentales de un laboratorio de ciencias forenses digitales

### 4.2.1 Características Técnicas

Desde el punto de vista técnico, se valoraron las siguientes características:

- **Espacios físicos necesarios:**

El área designada para el laboratorio es parte fundamental para el desarrollo del proyecto, debido a que tiene que contar con buen espacio físico dada la cantidad de evidencia y contar con un buen nivel de seguridad requerido para tal fin, como lo es el ingreso por parte de personal debidamente autorizado, para evitar interferir en algún proceso o que se pueda presentar la pérdida de algún elemento o evidencia, las cuales se encontraran expuestas mientras se realizan las imágenes forenses. Los controles de acceso a través del tiempo han ido evolucionando cada vez con mejores tecnologías de tipo biométrico, para garantizar ingresos y registros por parte del personal a determinadas áreas. Se hace necesario contar con subniveles de acceso para espacios como el de almacenamiento de evidencias, ensamble y desmontaje de equipos y el área de análisis de imágenes forenses.

Las áreas para el laboratorio requeridas son:

Área	Propósito
Recepción	Se recibirán las evidencias debidamente embaladas y rotuladas
Almacenamiento	Almacenar las evidencias, debidamente demarcadas por caso.
Desmantelamiento	Realizar el ensamble y desmontaje de equipos
Análisis	Analizar las imágenes forenses, producto de las evidencias digitales.

Director	Tener el control administrativo del laboratorio
Cabina inhibidor de señal	Proporcionar un área sin señal para realizar el análisis de dispositivos móviles.

Tabla 6: Resultado – Área y propósito

- **Equipos computacionales:**

Para llevar a cabo los análisis de tipo digital se necesita de equipos tales como estaciones forenses (portátiles o de escritorio), duplicadores de discos duros, adaptadores, dispositivos de almacenamiento y bloqueadores de escritura.

Se establecieron requerimientos mínimos de acuerdo al software que debe ser instalado en los equipos de cómputo, para lo cual, los equipos tendrán las siguientes características:

Equipo	Descripción	Características técnicas
Estación forense	Con esta configuración de alto desempeño, se pretende realizar el procesamiento de evidencia digital, acorde a los altos volúmenes de análisis de datos, con el fin de obtener información clave para la investigación, desde la adquisición de datos hasta la generación de reportes.	Sistema Operativo: Windows 10, 64 bits Procesador: Intel® Core™ i7-3820 CPU (Quad Processor), 3.6 GHz, 10MB Intel® Smart Cache, 5 GT/s DMI RAM: 32GB PC3-12800 DDR3 1600 MHz Memory OS Drive: 256 GB Solid State Drive Data Drive: 2.0 TB 7200 RPM SATA III Hard Drive 22" WideScreen LCD Monitor with Built-in Speakers
Estación portátil	Necesaria para el procesamiento de evidencia digital en campo, donde el objetivo primordial es la realización de imágenes forenses en el lugar de los hechos.	Portátil de mínimo procesador i5 de mínimo 2GHZ de última generación, Memoria RAM de 16 GB y Disco Duro de mínimo 1 TB, Sistema Operativo Windows 10 de 64bits

Almacenamiento de evidencias procesadas	Tener capacidad de almacenamiento de las investigaciones mientras el caso se encuentra en juicio.	NAS de Almacenamiento de mínimo 30TB EN RAID10 (Evidencia procesada) Y 50TB (Almacenamiento de evidencia) en RAID5 Tarjeta de Red de 10 Gbps
Bloqueadores y clonadores	Es un equipo que realiza el puente entre la evidencia digital y el equipo forense, el cual bloquea escritura y garantiza la realización de imágenes forenses sin afectar o dañar la evidencia.	Una de las mejores empresas líder del mercado forense en el diseño y fabricación de dispositivos para recopilar, analizar y presentar datos digitales, es TABLEAU (2019)
Servidor WEB, con apache o IIS.	Equipo para visualizar la información a través de un entorno web, amigable al investigador, donde se pueden realizar consultas, búsquedas y análisis de datos, dependiendo del perfil de usuario y de los permisos otorgados a cada caso.	Procesador 16 núcleos físicos Memoria RAM de 32 GB NIC: 10 Gbps Disco Duro 1: 300 GB - 10K Microsoft Windows Server 2012 R2 64-bit en Ingles SQL - Server
Servidor de aplicaciones	Equipo que permitirá la gestión de aplicaciones de un gran sistema distribuido.	Procesador 16 núcleos físicos Memoria RAM de 32 GB NIC: 10 Gbps Disco Duro 1: 300 GB - 10K RPM Disco Duro 2: 600 GB 10k RPM Microsoft Windows Server 2008 R2 64-bit en Ingles
Servidor de procesamiento	Ejecutará las aplicaciones y será capaz de realizar las peticiones de los investigadores, compartiendo	Procesador 16 núcleos físicos Memoria RAM de 32 GB NIC: 10 Gbps



	un recurso con uno o más procesos	Disco Duro 1: 300 GB 10K RPM Disco Duro 2: 900 GB 10K Microsoft Windows Server 2008 R2 64-bit en Ingles
Servidor de bases de datos (SQL – Server)	Equipo para poder tener múltiples usuarios y que puedan acceder desde varias terminales o equipos.	Procesador 32 núcleos físicos Memoria RAM de 64 GB NIC: 10 Gbps Disco Duro 1: 300 GB - 15K RPM Disco Duro 2: 146 GB 15K RPM Disco Duro 3: 300 GB 15K RPM Microsoft Windows Server 2012 R2 64-bit en Ingles

Tabla 7: Resultado – Equipos, descripción y características técnicas

- **Software especializado:**

Son las herramientas de software que tiene los investigadores para realizar la experticia a un dispositivo de almacenamiento digital, de las cuales existen comerciales (Licenciadas) o free (Libres), como las siguientes:

Software	Desarrollador	Licencia	Descripción
Forensic Toolkit o FTK	Access Data	Comercial	Permite el escaneo de un disco duro en busca de información diversa, en donde puede ubicar correos electrónicos, imágenes, videos, zip, archivos de texto, etc. que han sido borrados, exportarlos y recuperarlos, además de búsquedas y filtros personalizados.
Encase	Guidance Software	Comercial	El software viene en varios productos diseñados para uso forense, seguridad cibernética, análisis de seguridad y uso de descubrimiento electrónico. Encase se usa tradicionalmente en el análisis forense para recuperar evidencia de discos duros incautados.

			Encase le permite al investigador realizar un análisis en profundidad de los archivos del usuario para recopilar pruebas, como documentos, imágenes, historial de Internet e información del Registro de Windows.
UFED 4 PC	Cellebrite	Comercial	Solución integral de análisis forense de dispositivos móviles, flexible y práctica para la investigación, soportado para dispositivos Android, iOS y BlackBerry
Deft (Digital Evidence & Forensic Toolkit)	Lubuntu	Libre	Es una distribución Live CD (booteable desde el CD) basada en Lubuntu, muy fácil de usar, con un grandísimo listado de herramientas forenses y con una excelente detección del hardware, que permite obtener imágenes, realizar hash, hacer análisis forense a móviles, redes y descubrir contraseñas.
Caine	Linux	Libre	Es un Live CD, que ofrece un entorno forense completo que está organizado para integrar las herramientas de software existentes como módulos de software y para proporcionar una interfaz gráfica amigable, que permite analizar bases de datos de internet, historiales, registros de Windows y archivos borrados.
Autopsy	Basis Technology Corp	Libre	Es una herramienta para el análisis de evidencia digital, que permite la creación de un caso, a través de una serie de pasos, mediante la captura de una imagen de disco, permite buscar archivos, por palabras claves, iniciales, tipo de archivos, metadatos o sectores específicos del disco, para finalmente generar reportes.

Tabla 8: Resultado – Software y descripción

## 4.2.2 Legislación en Colombia

### Ley 1273 del 5 de enero de 2009

Con la Implementación de la Ley 1273 del 5 de enero de 2009 (Senado de la república, 2019), se enmarcan nuevos retos dentro de las funciones de Policía Judicial relacionadas con el manejo de las TIC (Tecnologías de la Información y las Comunicaciones), así como la adecuada manipulación de las evidencias de tipo digital; retos que exigen un adecuado procedimiento investigativo y pericial así como personas idóneas para este tipo de actividades que poseen los conocimientos necesarios para hallar, recolectar y preservar de una manera adecuada éstos EMP o EF dentro de un marco de legalidad basado en la calidad. Como sustentación y justificación de lo anteriormente descrito se enuncian los artículos que permiten dilucidar claramente esta necesidad [30]:

- Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.
- Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.
- Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.
- Artículo 269D. DAÑO INFORMÁTICO.
- Artículo 269E. USO DE SOFTWARE MALICIOSO.
- Artículo 269F. VIOLACIÓN DE DATOS PERSONALES.
- Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.
- Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA
- Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.

### Ley 679 de 2001

Así mismo, los delitos informáticos pueden tener repercusiones y consideraciones en otras leyes como la ley 679 de 2001 [31]: "*Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores*", este delito se enmarca en el Capítulo VII, y hace referencia a la utilización de medios virtuales, utilizando redes globales de información, en los siguientes artículos:

- ARTÍCULO 33. ADICIÓNASE EL ARTÍCULO 303 DEL CÓDIGO PENAL CON EL SIGUIENTE INCISO. "Si el agente realizare cualquiera de las conductas descritas en este artículo con personas menores de catorce años por medios virtuales, utilizando redes globales de información, incurrirá en las penas correspondientes disminuidas en una tercera parte."

- ARTÍCULO 34. Adicionase un nuevo artículo al Código Penal, con el número 312A, del siguiente tenor:

Artículo 312A. Utilización o facilitación de medios de comunicación para ofrecer servicios sexuales de menores. El que utilice o facilite el correo tradicional, las redes globales de información, o cualquier otro medio de comunicación para obtener contacto sexual con menores de dieciocho (18) años, o para ofrecer servicios sexuales con éstos, incurrirá en pena de prisión de cinco (5) a diez (10) años, y multa de cincuenta (50) a cien (100) salarios mínimos legales mensuales vigentes.

Las penas señaladas en el inciso anterior se aumentarán hasta en la mitad (1/2) cuando las conductas se realizaren con menores de doce (12) años.

### **Leyes de derecho de autor**

El Congreso de Colombia decreta la Ley 23 de 1982 "Sobre derechos de autor", y es modificada por la Ley 1915 del 12 de julio de 2018 [32], el cual establece "Otras disposiciones en materia de derecho de autor y derechos conexos", y resalta la adición del siguiente artículo:

- ARTÍCULO 36. Adiciónese un párrafo 2° al artículo 271 del Código Penal, el cual quedará así:

Parágrafo 2°. La reproducción por medios informáticos de las obras contenidas en el presente artículo será punible cuando el autor lo realice con el ánimo de obtener un beneficio económico directo o indirecto, o lo haga a escala comercial.

Código de procedimiento penal "Ley 599 de 2000", el laboratorio investigará el delito referente a los siguientes artículos [33]:

- 
- ARTÍCULO 271. VIOLACIÓN A LOS DERECHOS PATRIMONIALES DE AUTOR Y DERECHOS CONEXOS. <Artículo modificado por el artículo 2 de la Ley 1032 de 2006. El nuevo texto es el siguiente:> Incurrirá en prisión de cuatro (4) a ocho (8) años y multa de veintiséis punto sesenta y seis (26.66) a mil (1.000) salarios mínimos legales mensuales vigentes quien, salvo las excepciones previstas en la ley, sin autorización previa y expresa del titular de los derechos correspondientes:
    1. Por cualquier medio o procedimiento, reproduzca una obra de carácter literario, científico, artístico o cinematográfico, fonograma, videograma, soporte lógico o programa de ordenador, o, quien transporte, almacene, conserve, distribuya, importe, venda, ofrezca, adquiera para la venta o distribución, o suministre a cualquier título dichas reproducciones.
    2. Represente, ejecute o exhiba públicamente obras teatrales, musicales, fonogramas, videogramas, obras cinematográficas, o cualquier otra obra de carácter literario o artístico.
    3. Alquile o, de cualquier otro modo, comercialice fonogramas, videogramas, programas de ordenador o soportes lógicos u obras cinematográficas.
    4. Fije, reproduzca o comercialice las representaciones públicas de obras teatrales o musicales.
    5. Disponga, realice o utilice, por cualquier medio o procedimiento, la comunicación, fijación, ejecución, exhibición, comercialización, difusión o distribución y representación de una obra de las protegidas en este título.
    6. Retransmita, fije, reproduzca o, por cualquier medio sonoro o audiovisual, divulgue las emisiones de los organismos de radiodifusión.
    7. Recepcione, difunda o distribuya por cualquier medio las emisiones de la televisión por suscripción.
  
  - ARTÍCULO 272. VIOLACIÓN A LOS MECANISMOS DE PROTECCIÓN DE DERECHO DE AUTOR Y DERECHOS CONEXOS, Y OTRAS DEFRAUDACIONES. <Artículo modificado por el artículo 33 de la Ley 1915 de 2018. El nuevo texto es el siguiente:> Incurrirá en prisión de cuatro (4) a ocho (8) años y multa de veintiséis punto sesenta y seis (26.66) a mil (1.000) salarios

mínimos legales mensuales vigentes, quien con el fin de lograr una ventaja comercial o ganancia económica privada y salvo las excepciones previstas en la ley.

Debido a que al Grupo de Delitos Informáticos llegan apoyos de todas las Unidades como Homicidios, Hurtos, Secuestro, Extorsión, Estafa, Administración pública, etc. Se vuelve una Unidad transversal, por consiguiente, la investigación se realiza a todos los artículos del Código de procedimiento penal “Ley 599 de 2000”.

### **4.2.3 Recolección y Manejo de la evidencia digital**

En el Grupo de Informática Forense se debe garantizar el manejo adecuado de los Elementos Materiales Probatorios y Evidencia Física (EMP y EF), para su examen, incluyendo los lineamientos para la recepción, manejo, custodia, identificación, protección y conservación.

“La cadena de custodia es un procedimiento que debe tenerse en cuenta desde el mismo instante que se decida realizar el proceso de evidencia forense, ya que este procedimiento, basado en el principio de la “mismidad”, tiene como fin garantizar la autenticidad e integridad de las evidencias encontradas en alguna situación determinada, es decir, que lo mismo que se encontró en la escena, es lo mismo que se está presentando al tribunal penal o comité disciplinario según sea el caso.” [34].

La Fiscalía General de la Nación [35] desarrolló el procedimiento llamado “Manual Único de Cadena De Custodia”, que contiene los pasos completos para asegurar las características originales de los elementos (evidencia) desde su recolección hasta su disposición final. La evidencia digital es aportada por un investigador de Policía Judicial al laboratorio en un contenedor debidamente rotulado y con su respectiva cadena de custodia; este debe ser recepcionado y almacenado en un lugar acorde al diseño propuesto en este proyecto para salvaguardar su integridad.

El procedimiento aplicado a la evidencia digital debe ser implementado garantizando la trazabilidad, para que brinde la confianza suficiente a quién reciba la evidencia, la cual certifica que la información contenida conserva su integridad y no ha sido alterada o modificada.

- Identificación de la fuente de información como:
  - Computador de escritorio o portátil
  - Servidor
  - Almacenamiento en la red o en la nube
  - Medios de almacenamiento digital (CD, DVD, USB, Tarjetas SD, Disco duro, etc.)
  - Dispositivos celulares
  - Dispositivos de audio o video
  
- Adquisición y obtención de los datos:
  - Si el computador se encuentra encendido, se realiza a través de herramientas forenses, para evitar la pérdida de información referente a los datos volátiles almacenados en la memoria RAM.
  - Si el computador se encuentra apagado o es un medio de almacenamiento digital, se procede a su embalaje.
  - De no haber Orden Judicial para incautar el elemento digital, se realiza una copia espejo con software y hardware especializado.
  
- Fijación de la evidencia:
  - Se debe realizar la fijación técnica del elemento utilizando los planos fotográficos de lo general a lo particular.
  
- Documentación y presentación de la evidencia:

Se utilizará el protocolo de Cadena de Custodia (Embalaje y Rotulado) para la presentación de la evidencia.

<https://www.fiscalia.gov.co/colombia/wp-content/uploads/MANUAL-DEL-SISTEMA-DE-CADENA-DE-CUSTODIA.pdf>

A continuación, se mencionan algunas fuentes que mencionan la estrategia para el manejo de la evidencia digital:

- La recolección de evidencia digital [34] amerita realizar un procedimiento de informático forense para emprender alguna acción de tipo legal, investigación disciplinaria interna o aprendizaje; donde recalca que se debe tener presente las siguientes medidas iniciales al momento de realizar el procedimiento de Identificación, Recolección, Análisis y Manipulación de evidencia digital:
  - Verificar si en realidad ha ocurrido un incidente o no (Tomado de la guía de gestión de incidentes).
  - Verificar si existe la necesidad de realizar el procedimiento de evidencia digital al incidente reportado.
  - Minimizar la pérdida o alteración de datos.
  - Llevar bitácoras de todas las acciones, con fechas y hora precisas.
  - Analice todos los datos recolectados.
  - Realice un reporte de los hallazgos.
  
- La empresa Adalid Abogados [36], afirma que, para que la evidencia digital tenga validez jurídica se debe tener una guía básica de algunos atributos para que la prueba electrónica sea realizada:
  - Autenticidad: Establece que dicha evidencia ha sido generada y registrada en los lugares relacionados con el caso, específicamente en la escena del posible delito.
  - Nivel de relevancia: Debe pertenecer al caso real, al igual que el material debe demostrar o refutar los hechos ante el tribunal.
  - Confiabilidad: Establece si los medios probatorios aportados provienen de fuentes creíbles y verificables. Esto respondería a distintos cuestionamientos que pretenden demostrar los registros electrónicos.
  - Suficiencia: Se refiere a la presencia de toda la evidencia necesaria para adelantar el caso.
  - Conformidad con las leyes y reglas de la administración de justicia: Hace referencia a los procedimientos internacionalmente aceptados para recolección,



---

aseguramiento, análisis y reporte de la evidencia digital. Si bien es cierto que los Códigos de Procedimiento Civil y Penal contienen disposiciones normativas que establecen la manera de aportar una prueba a un proceso, en el campo internacional existen iniciativas como las de la IOCE, el Digital Forensic Research Workshop, donde se establecen marcos de acción y lineamientos que cobijan la evidencia en medios electrónicos.

- La evidencia digital: Fundamentos aplicables para el abordaje de la examinación forense, hace referencia a las siguientes guías internacionales para el tratamiento de la evidencia digital [37]:
  - Guía SANS (SysAdmin Audit, Networking and Security Institute) Internacional.
  - HB171:2003 Handbook Guidelines for the management of IT Evidence
  - IOCE [IOCE0], publico “Guía para las mejores prácticas en el examen forense de tecnología digital” (Guidelines for the best practices in the forensic examination of digital technology)
  - El departamento de Justicia de los Estados Unidos de América (DoJ EEUU), publicó “Investigación en la Escena del Crimen Electrónico” (Electronic Crime Scene Investigation: A Guide for First Responders) [ElCr01].
  - El “RFC 3227: Guía Para Recolectar y Archivar Evidencia” (Guidelines for Evidence Collection and Archiving) [GuEvCo02], escrito en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group.
  
- El Servicio secreto de los EE.UU. [38] aporta un documento de buenas prácticas para el manejo de evidencia electrónica, el cual desarrolla un documento para los entes policiales, donde da a conocer los procedimientos de seguridad, y aclara que la responsabilidad de garantizar la integridad de la escena del crimen y cualquier otra evidencia potencial recaerá sobre quién la realice.
  
- La National Institute of Standards and Technology – NIST [39], ha creado una guía para integrar técnicas forenses en la respuesta a incidentes llamada SP 800-86, el cual presenta una guía para análisis forenses desde una vista de TI, no desde la aplicación de

la Ley, y enuncia que no debe usarse como una guía paso a paso, y su propósito es el de realizar actividades de respuesta a incidentes o resolución de problemas.

De acuerdo a las normas referenciadas, se hace necesario realizar la combinación de varias de ellas para definir el modelo que utilizara el laboratorio:

- Identificación, Recolección, Análisis y Manipulación de evidencia digital.
  
- Adquisición y obtención de los datos, teniendo en cuenta la Autenticidad, el Nivel de relevancia, la Confiabilidad, la Suficiencia y la Conformidad con las leyes y reglas de la administración de justicia.
  
- Fijación de la evidencia.
  
- Documentación y presentación de la evidencia a través de un informe.

#### **4.2.4 Análisis de la evidencia digital**

Para realizar el análisis a la evidencia digital, la persona encargada de realizar esta labor debe ser un perito investigador con las capacidades humanas e intelectuales que se requieren para esclarecer un delito informático, y que tenga funciones de Policía Judicial; así las cosas, el perito realizará el análisis de la evidencia digital basándose en el siguiente procedimiento (figura 4):

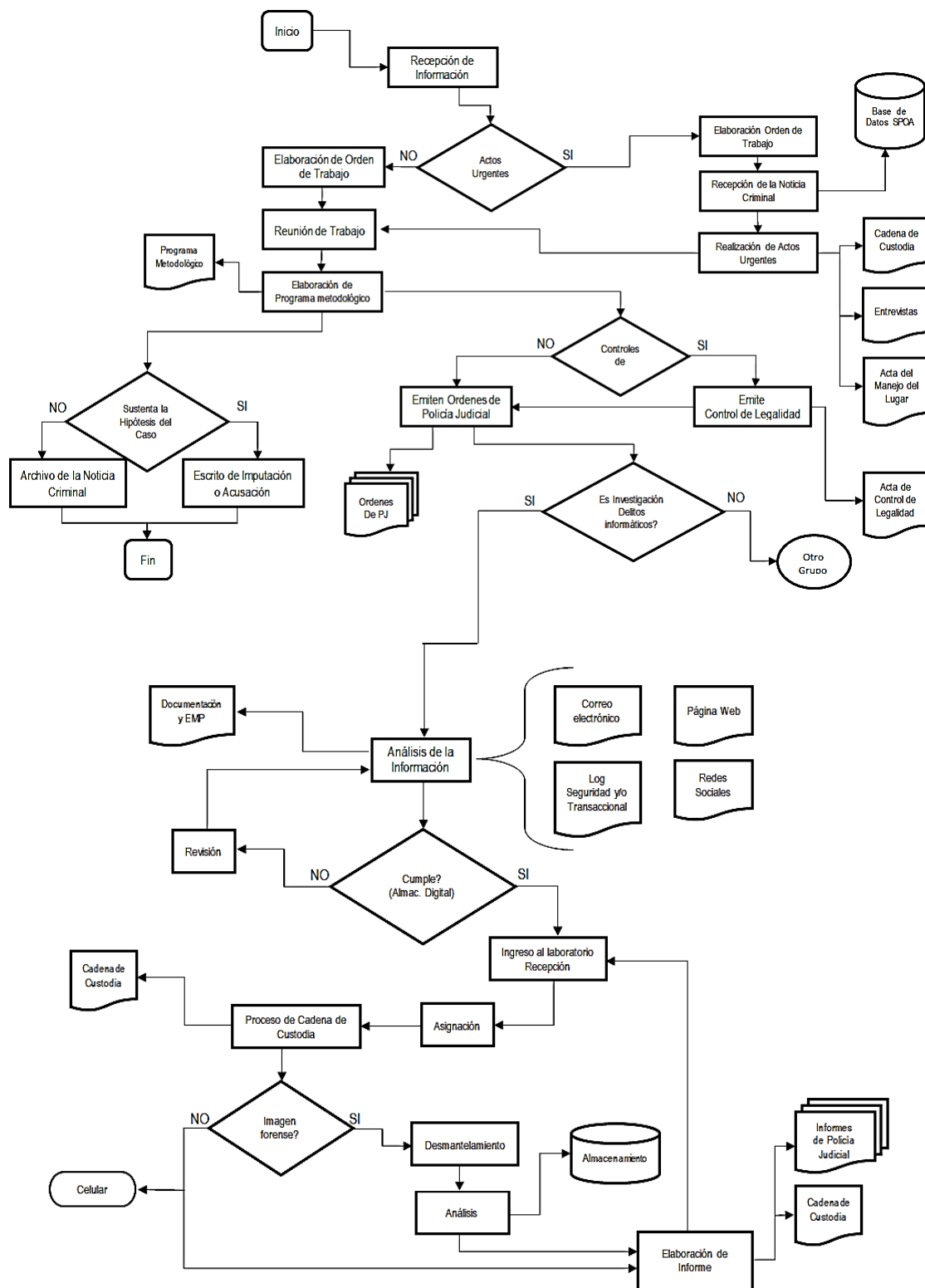


Figura 4: Procedimiento análisis evidencia digital. Fuente: Elaboración propia a partir del procedimiento general para la policía judicial de la FGN

#### **4.2.5 Descripción del procedimiento en el Laboratorio**

El procedimiento general de los temas forenses se ilustra a continuación [40]:

- Se realiza documentación fotográfica del embalaje, cadena de custodia, rotulo y EMP y/o EF motivo del presente estudio.
- Se conecta el medio de almacenamiento digital objeto de análisis, al equipo forense a través del dispositivo de bloqueo contra escritura, para garantizar la integridad de la información contenida.
- Se adquiere la imagen forense del medio de almacenamiento original y se realiza su respectiva verificación.
- Almacenamiento de la imagen forense en medios de almacenamiento digital, siguiendo lineamientos establecidos para cadena de custodia.
- Dependiendo de la investigación y si es necesario que sea entregada la evidencia original, la imagen forense, será recolectada, embalada y rotulada siguiendo los protocolos de cadena de custodia.
- Se procede al análisis de la Evidencia, sobre las imágenes previamente adquiridas y guardadas en el computador forense. En este procedimiento se realizan búsquedas en todos y cada uno de los archivos; igualmente se hacen búsquedas de archivos eliminados.
- Posteriormente se crean BOOKMARKS o MARCADORES que son básicamente carpetas donde se almacenan los hallazgos o archivos encontrados en la evidencia que puedan aportar a la investigación.
- Finalmente se genera desde la herramienta forense todos los reportes necesarios para mostrar lo hallado durante el análisis de las evidencias, así como la información relacionada al caso, a la evidencia, y a los archivos, mostrando para cada archivo el valor HASH que garantiza su integridad durante el análisis.
- Se entregan los EMP/EF a la autoridad solicitante.

#### **4.2.6 Grado de aceptación por la comunidad técnico científica, de los procedimientos empleados**

Acorde a la Organización Internacional de Evidencia Computacional – IOCE [41] los análisis se realizan de acuerdo a los lineamientos dados por la Guía Interna de Delitos Informáticos, documento estandarizado y aprobado por el Sistema Integrado de Gestión de la Calidad de la Fiscalía General de la Nación, y a los principios propuestos por la IOCE, cumpliendo con estándares internacionales usados por diferentes organizaciones privadas o gubernamentales, encargadas de velar por la seguridad informática y/o realizar investigaciones de incidentes, con la aplicación de procedimientos propios de la informática forense.

Se utilizará el Software Forense FTK [42], el cual es un software especial utilizado por la Policía Judicial a nivel mundial, ya que garantizan los procedimientos forenses, procedimientos que permiten analizar los datos de un medio de almacenamiento digital sin modificarlos, conservando así la evidencia original, intacta, tal como se recolectó en la escena del delito, el cual generara un reporte HASH para regular los archivos y los Discos imágenes.

La imagen forense será marcada como “Archivo evidencia”, el cual es una fiel copia de los dispositivos y contiene toda la información almacenada en los elementos materiales de prueba. Las herramientas forenses dan validez a la integridad de la información generando un valor HASH [43] asociado a la Evidencia, éste es una huella digital, una cadena de caracteres alfanuméricos, único para cada evidencia.

#### **4.2.7 Instrumentos empleados para el análisis**

[44] y [45] establecen una serie de parámetros y elementos que deben emplearse para los diferentes análisis forenses, entre los que se encuentran:

- Elementos de bioseguridad.
- Testigo métrico.
- Cámara fotográfica digital.
- Bloqueador de escritura para dispositivos de almacenamiento con conexión SATA, IDE, USB, etc.

- Equipo forense para el análisis de evidencia digital, adquirido por la Fiscalía General de la Nación y asignado al Grupo de Delitos Informáticos del Cuerpo Técnico de Investigación, Seccional Medellín – Antioquia.
- Software Forense AccessData FTK y/o ENCASE Forensic, para la adquisición y análisis de evidencia digital.
- Cellebrite UFED para la adquisición y análisis de dispositivos móviles.
- Otras herramientas de software, como el Programa MD5SUMMER.EXE, para calcular la Huella Digital.
- Impresora láser.

#### **4.2.8 Principios técnico – científicos aplicados**

Algunos de los principios técnicos y procedimentales aplicados, están basados en las prácticas propias del personal de CTI [46], que, de acuerdo a su experiencia, establecen una serie de procedimientos considerados buenos, lo que no implica que sea coherente con las normas y buenas prácticas internacionales.

Algunos de los procesos e informes establecen:

- La informática forense permite presentar apropiadamente las evidencias digitales ante un estrado judicial, de tal manera que las mismas no pierdan su valor probatorio. Las actividades que se realizaran corresponden a técnicas de la informática forense, cumpliendo así con los principios propuestos por la IOCE [International Organization Computer Evidence (Organización Internacional de Evidencia Computacional)], que tiene como objetivo garantizar la integridad, autenticidad, disponibilidad y confidencialidad de la información en los EMP y EF analizados.
- Una imagen forense es una copia no adulterada de una Unidad de Disco rígida u otro dispositivo de almacenamiento electrónico. Al crear una imagen forense, el Investigador garantiza Integridad de las pruebas y la capacidad de examinar los datos en un entorno controlado por un examinador forense certificado.

- Cuando se adquiere una imagen forense con un bloqueador de escritura y software forense se garantiza que la información contenida en el dispositivo físico (Disco Duro, Memoria USB, etc.) y todo lo que maneja el sistema, es una fiel copia de cómo se encontraba el sistema al momento de recolectarlo, se obtiene toda clase de archivos y los archivos borrados.
- Para cada uno de los archivos de la evidencia, se tiene la fecha de creación, fecha de modificación y la última fecha que fue ingresado en el sistema.
- A cada archivo se le saca una huella digital que permite garantizar que ese archivo no sea modificado y/o alterado.
- También garantiza que la información que se va a analizar sólo se puede visualizar, pero en ningún momento se puede modificar, borrar y/o ejecutar procesos.

Se deben analizar las condiciones humanas, físicas, ambientales y de infraestructura para la implementación del laboratorio de ciencias forenses digitales en la sede del Bunker de la Fiscalía General de la Nación, Seccional Medellín, basándonos en el nivel de percepción del equipo de trabajo y de los criterios de seguridad, ubicación área, y equipos.

#### 4.2.9 Equipo de trabajo

La propuesta dentro del diseño, permita la división de los roles por grupo así:

<b>Delitos Informáticos</b>	<b>Informática Forense</b>
<p><b>Apoyo a diligencias judiciales para la recolección de evidencia digital</b>, los cuales se embalarán, rotularán y se abrirá cadena de custodia para ser llevados al almacén general de evidencia o para estudio a la oficina de Delitos Informáticos</p>	<p><b>Análisis y/o recuperación de información de medios de almacenamiento de información digital.</b> En este asunto se incluyen todas las solicitudes y órdenes de policía judicial relacionadas con recuperación, extracción y búsqueda de información en dispositivos de almacenamiento de información digital, como por ejemplo, discos duros, memorias USB, celulares (Smart Phone), Tablet, entre otros.</p>

<p><b>Rastreo de Direcciones IP.</b> En este asunto hace referencia a las solicitudes y órdenes de Policía Judicial relacionadas con:</p> <ul style="list-style-type: none"> <li>• Encabezados de correos electrónicos.</li> <li>• Datos biográficos de correos y rastreo IP.</li> <li>• Rastreo de transacciones por internet.</li> <li>• Análisis de Páginas Web.</li> </ul>	<p><b>Duplicado de medios de almacenamiento de información.</b> En este asunto, el término contemplado para realizar la orden a la policía judicial cuando la investigación esté en etapa de indagación se requiere superior a 30 días.</p>
<p><b>Análisis de Software.</b> Dentro de este asunto se diferencian dos tipos o grupos de actividades:</p> <ul style="list-style-type: none"> <li>• Licenciamiento de Software – Legalidad.</li> <li>• Comparación de Software.</li> </ul>	<p><b>Análisis a sistemas de información o sistemas telemáticos.</b> Estas investigaciones nacen de la modificación de información sobre las bases de datos de cualquier organización privada o pública, a través de la manipulación directa del sistema de información o de la misma fuente de los datos (Base de Datos).</p>
<p><b>IRC (Respuesta a Incidentes).</b> De acuerdo con este asunto, se apoyan diligencias judiciales y/o recolección de evidencia digital en los que se requiera la participación de funcionarios expertos en el área de informática, específicamente en actividades relacionadas con la identificación, recolección y embalaje adecuados de evidencia digital.</p>	

Tabla 9: Propuesta Grupos de trabajo



#### 4.2.10 Diseño del laboratorio de Ciencias Forenses Digitales

En la siguiente gráfica se relaciona el diseño del laboratorio, el cual daría cumplimiento a los diferentes requerimientos y procedimientos técnicos para el análisis forense digital:

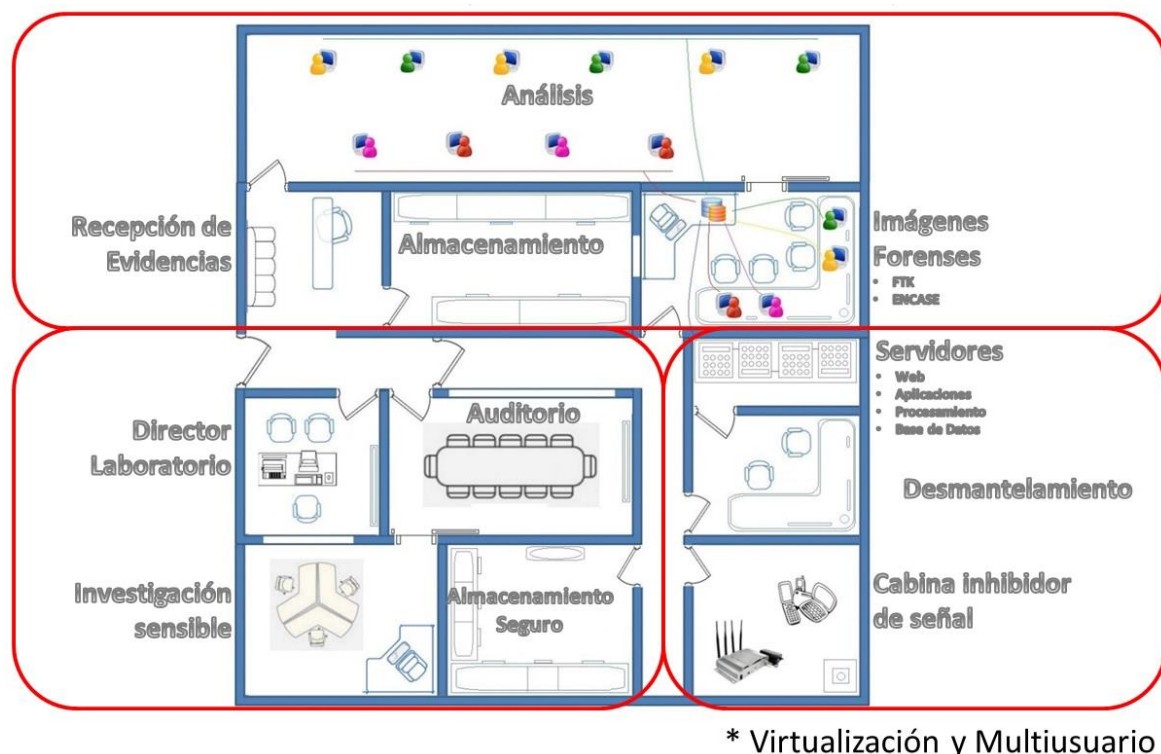


Figura 5: Diseño de un laboratorio de Ciencias forenses digitales. Fuente propia.

En la gráfica se observa el diseño del laboratorio de Ciencias Forenses Digitales, el cual comprende tres secciones descritas de la siguiente manera:

- **Sección Uno (ANÁLISIS):** Comprende el área de Recepción de evidencias, donde entregaran los Elementos para su análisis, se verificará toda la documentación y la cadena de custodia para ser ingresada al Laboratorio, contara con un área de almacenamiento, el cual tendrá armarios y estantería numerada para salvaguardar la evidencia, mientras es asignada a un perito para su respectivo Análisis.

En esta Sección se contará con un área de Análisis, y estará compuesta por varios módulos, donde cada perito podrá realizar su trabajo en estaciones de cómputo

conectadas a los servidores que tienen la información de las imágenes obtenidas de las evidencias.

Además, tendrá un área llamada Imágenes Forenses, donde se realizarán las imágenes de las evidencias allegadas al laboratorio, para luego ser procesadas.

- **Sección Dos (DESMANTELAMIENTO):** Comprende un área principal que será donde se realice el desmonte de la evidencia, por ejemplo, la sustracción del disco duro de un computador portátil.

Tendrá el área de análisis de dispositivos móviles “Celulares” que será un espacio donde no se tenga señal celular y poder realizar con seguridad la extracción y análisis de equipos móviles.

Aquí se podría ubicar un área donde estarían los cuatro servidores llamados: WEB, de Aplicaciones, de Procesamiento y de Bases de datos.

- **Sección Tres (ADMINISTRACIÓN):** Se pueden ubicar varias áreas como el Auditorio o sala de reuniones, un área de investigación sensible y un área de almacenamiento seguro para equipos, documentación, papelería, suministros o elementos necesarios para el buen desempeño del laboratorio, el cual será administrado por el Director del Laboratorio quién tendrá un área exclusiva para su trabajo.

### **Intercambio de información**

El paso de información y evidencia entre secciones solo la podrá realizar el perito asignado al caso, previo registro de la cadena de custodia, tanto física como en el sistema propio de la Fiscalía General de la Nación llamado SPOA (Sistema Penal Oral Acusatorio), la evidencia solo podrá estar en las secciones 1 y 2, y en ningún caso podrá salir del laboratorio mientras se realice todo el procesamiento de la información, para luego ser entregado a la autoridad solicitante.

La recepción de la evidencia la realiza una persona, la cual se debe registrar en calidad de custodio siguiendo el procedimiento de cadena de custodia (formatos indicados en las fotos 2, 3 y

4, en la fase 3 siguiente), y debe esperar la orden del Director de Laboratorio, quién dirá a qué Ingeniero será asignado el caso. El Ingeniero firmará en calidad de perito la cadena de custodia, para realizar el procesamiento de toma de evidencia y será quién entregue el resultado a la autoridad solicitante.

La autoridad solicitante, por lo general es un Investigador de Policía Judicial quién tiene la orden de un Fiscal o Juez para solicitar el análisis de la evidencia, deberá recibir su resultado bajo cadena de custodia, junto con los elementos o evidencias que allegó para su análisis directamente del Perito asignado al caso (si dicho perito no se encuentra, los resultados no se pueden entregar, excepto por fuerza mayor o caso fortuito).

### **Etiquetado, embalaje y clasificación de la evidencia**

Toda la información mientras esté en el proceso de valoración (investigación) debe etiquetarse como “evidencia” (foto 1 de la fase 3 siguiente), se le debe hacer el respectivo marcado en el embalaje (foto 5 de la fase 3 siguiente) y de acuerdo a la guía para la clasificación de información de la presidencia [47], por defecto dicha información es pública clasificada, por lo cual, solo tendrá acceso a esta personal autorizado, y solo puede cambiar a otro tipo de clasificación cuando existe una orden judicial o superior. Por ejemplo, podría ser *pública*, cuando el caso ya es juzgado.

## **4.3 Fase 3: Resultados de la evaluación del diseño**

Cómo se indicó, para la fase de evaluación se tomó como referencia el caso de estudio (caso juzgado), descrito en forma general y desarrollada en 2 momentos:

1. Momento 1: procedimiento actual.
2. Momento 2: procedimiento hipotético con el nuevo diseño.

### **4.3.1. Momento 1: Proceso desarrollado en el estado actual**

**Caso:** Inocencia Perdida

**Objetivo:** Evaluar el contenido de la memoria MicroSD color negra de 16GB de capacidad, con el fin de valorar el contenido de la misma (De manera detallada) y determinar si en el contenido hay

alguna de las víctimas, y si en el contenido de la memoria se puede observar el presunto indiciado de la conducta penal.

**Descripción clara y precisa de los elementos materiales probatorios y evidencia física examinados:**


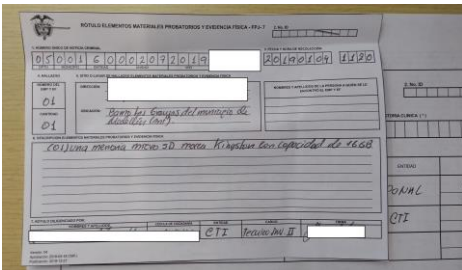
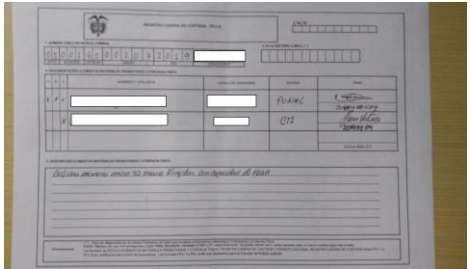
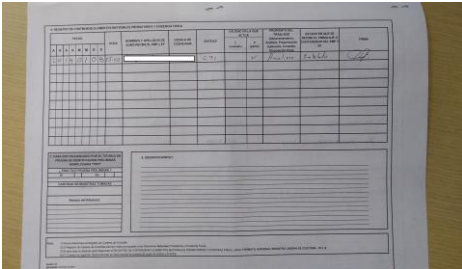


- EVIDENCIA MARCADA COMO NRO. 1: Una memoria MicroSD con capacidad de 16 GB, debidamente embalada con rotulo y su respectivo formato de cadena de custodia, color negro, con numero impreso XXBCDE-1234599.

**Descripción de los procedimientos técnicos empleados:**

- Se realiza documentación fotográfica del embalaje, cadena de custodia, rotulo y EMP y/o EF motivo del presente estudio.
- Se conecta el medio de almacenamiento digital objeto de análisis (memoria MicroSD), al equipo forense a través del dispositivo de bloqueo contra escritura.
- Se obtiene la imagen forense del medio de almacenamiento original y verificación de la imagen forense.
- Almacenamiento de la imagen forense en medios de almacenamiento digital (CD-ROM), siguiendo lineamientos establecidos para cadena de custodia.
- El medio de almacenamiento (CD-ROM), se recolecta, embala y rotula siguiendo los protocolos de cadena de custodia.
- Se extrae la huella digital, mediante el cálculo del valor HASH (algoritmos MD5) aplicado a la carpeta REPORTE que contiene toda la información extraída del (los) dispositivo(s) y que se encuentra grabada en el medio de almacenamiento (CD-ROM).
- Se entregan los EMP/EF a la autoridad solicitante.

**Descripción clara y precisa de los procedimientos utilizados durante su actividad técnico-científica:**

- Se realiza fijación fotográfica de la evidencia tal como se recibe en el Grupo de Delitos Informáticos y de cómo se encuentra al momento de extraerla de su embalaje, como se indica a continuación:

	
<p><b>Foto Nro. 1</b> Se aprecia la Evidencia en su embalaje, sellada, rotulada, con su respectiva cadena de custodia, tal y como se recibió en el Grupo de Delitos Informáticos C.T.I. Medellín.</p>	<p><b>Foto Nro. 2</b> Se aprecia el Rótulo de la Evidencia, el cual dice contener: "(01) Una memoria MicroSD marca Kingston con capacidad de 16 GB"</p>
	
<p><b>Foto Nro. 3</b> Se aprecia la parte anterior de la cadena de custodia.</p>	<p><b>Foto Nro. 4</b> Se aprecia la parte posterior de la cadena de custodia.</p>
	
<p><b>Foto Nro. 5</b> Se aprecia la Evidencia en su embalaje.</p>	<p><b>Foto Nro. 6</b> Se aprecia la memoria MicroSD marca Kingston con capacidad de 16 GB, color negro, por su parte anterior.</p>

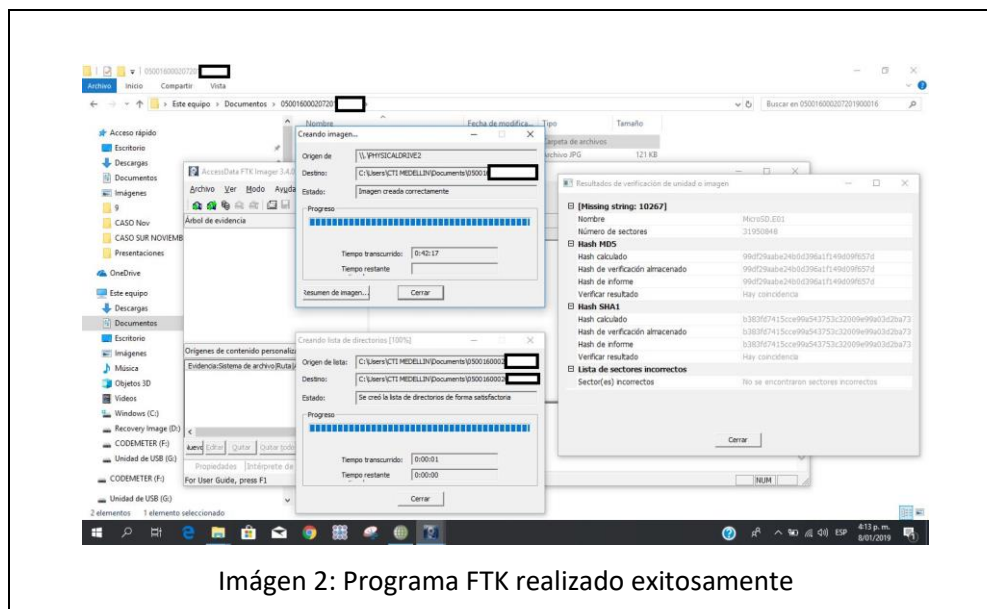
	
<p><b>Foto Nro. 7</b> Se aprecia la memoria MicroSD marca Kingston con capacidad de 16 GB, color negro, por su parte posterior</p>	<p><b>Foto Nro. 8</b> Se aprecia la memoria MicroSD marca Kingston con capacidad de 16 GB, color negro, por su parte anterior, en detalle donde se aprecia el numero impreso xxABCDE-1234599.</p>

Tabla 10: Fijación fotográfica de la evidencia

- Se procede a obtener la imagen forense de la memoria MicroSD marca Kingston con capacidad de 16 GB, color negra, con el numero impreso ABCDE-12345, haciendo uso de la Herramienta Forensic TABLEAU ESATA FORENSIC BRIDGE (El cual permite la conexión de la Memoria MicroSD Evidencia, al Laboratorio Forense con bloqueador contra escritura); así mismo, se hace Uso del Software forense FTK Imager (éste permite la adquisición de la Imagen Forense de la Memoria MicroSD Evidencia); obteniendo una extracción exitosa, como se muestra a continuación:



Imagen 1: Equipo en el que se realizó el procedimiento



Imágen 2: Programa FTK realizado exitosamente

### Interpretación de resultados:

Del ELEMENTO MATERIAL PROBATORIO Y/O EVIDENCIA FÍSICA; se genera la imagen forense con 3 archivos y un tamaño de 261 MB, el cual es almacenado en el CD-ROM que se entrega, marcado como “REPORTE MEMORIA MICROSD 050016XXX2072019XXXXX”.

- Se visualiza en la ruta F:\Imagen Forense, los archivos son los siguientes:

Nombre	Fecha de modificación	Tipo	Tamaño
MicroSD.E01	2019/01/08 4:11 p.m.	Archivo E01	267.375 KB
MicroSD.E01.csv	2019/01/08 4:11 p.m.	Archivo de valores separados por comas de Microsoft Excel	267 KB
MicroSD.E01.txt	2019/01/08 4:12 p.m.	Documento de texto	2 KB

Imágen 3: Ruta F:\Imagen Forense

- Se realiza extracción de toda la información almacenada en la memoria MicroSD marca Kingston con capacidad de 16 GB, color negro, con el numero impreso xxABCDE-1234XXX, como archivos de texto, archivos de Office (Word, Excel, PowerPoint, etc.), imágenes, audios, vídeos, redes sociales y correos electrónicos, de las cuales se puede obtener

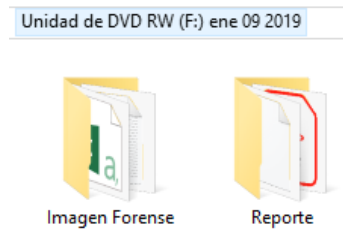
información sensible para la investigación, de la cual se exportan los siguientes resultados:

TIPO DE ARCHIVO	CANTIDAD
Imágenes	57
Phone Numbers	3
Screenshot	25
Videos	39
<b>TOTAL</b>	<b>124</b>

Tabla 11: Resultado archivos encontrados en la evidencia

Este Reporte es grabado en un (01) CD-ROM color blanco, marcado “REPORTE MEMORIA MICROSD 0500160002072019XXXXX”; debidamente embalado, rotulado y con su respectiva cadena de custodia, el cual se anexa al presente informe.

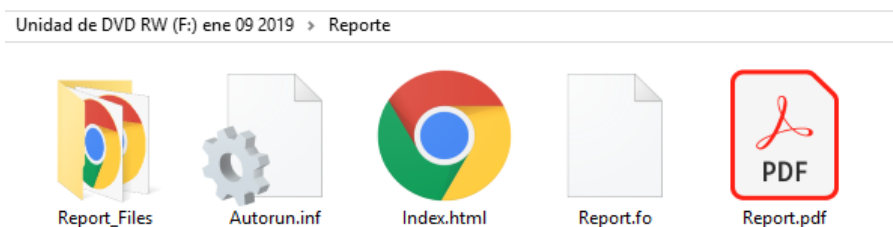
- En el CD-ROM se visualizará lo siguiente:



Imágen 4: Visualización CD-ROM

- Para visualizar el REPORTE es necesario entrar a la carpeta Reporte y se podrá visualizar de dos maneras, dando clic en el archivo Index.html para abrirlo en formato HTML o dar clic en el archivo Report.pdf para abrirlo en formato PDF, como se muestra a continuación:





Imágen 5: Visualización reporte en CD-ROM

- Si se visualiza el reporte abriendo el archivo “Index.html”, Se aprecia el reporte de los elementos anteriormente relacionados así:

**Informe FTK**

Archivo | file:///F:/Reporte/Index.html

**Información del caso**

Zona horaria para la visualización: America/Bogota

**Versión** Versión de AccessData Forensic Toolkit: 5.6.3.16

**Propietario del caso** admin

**Nombre del caso** 0500160002072019

**Referencia de caso** Caivas

**Descripción de caso** Memoria MicroSD marca Kingston con capacidad de 16 GB

**Reporte creado** 08/01/2019 06.25.21 p.m.

**Empresa** Fiscalía General de la Nación

**Investigador** Jose Ermes Palacios Carvajal

**Seccional** CTI - Medellin

**Teléfono** 4446677 ext. 1425 - 1427

**Email** jpalacio@fiscalia.gov.co

AccessData Forensic Toolkit®

**Resumen de caso**

- Información del caso
- Descripción de archivo
- Lista de evidencias

**Marcadores**

admin

- Imágenes
- Phone Numbers
- Screenshot
- Videos

**rutas de archivos**

**Propiedades de archivo**

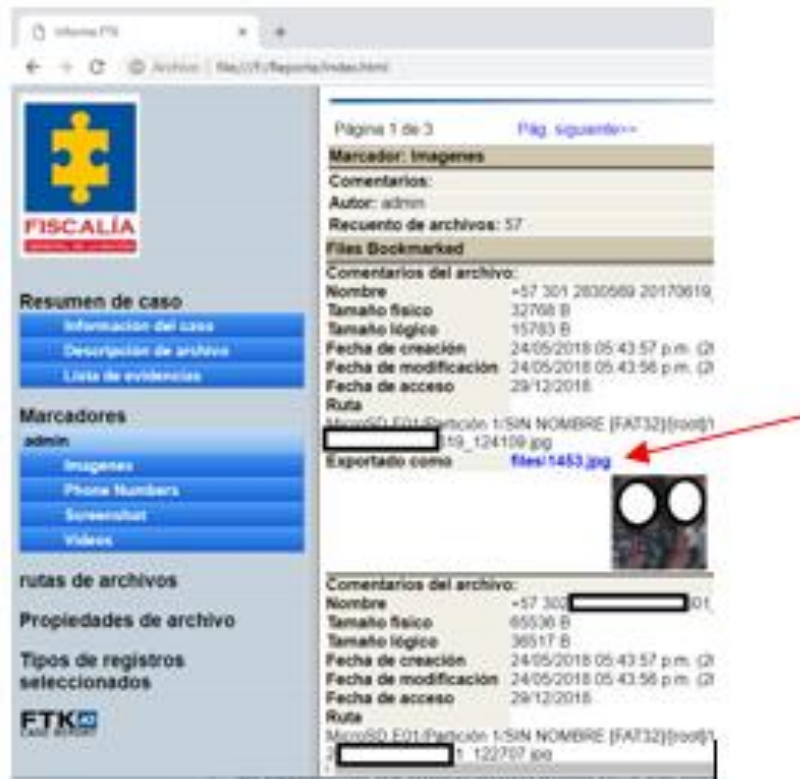
**Tipos de registros seleccionados**

**FTK**  
CASE REPORT

\*\*Para navegar se debe dar clic en los recuadros azules del menú.

Imágen 6: Visualización del reporte

Para abrir algún archivo, se debe dar clic en el enlace “Exportado como”, según indica la flecha:



Imágen 7: Visualización de archivo en el reporte

La interpretación de resultados se explica en cuanto a la extracción de información, el análisis definitivo es competencia del gerente del caso o líder de la investigación que conoce de la investigación y realizara un análisis de los contenidos de la información que en el punto anterior se extrajo.

En las imágenes extraídas de un video, se observa al presunto abusador de una menor y un elemento importante para la investigación como lo es el “casco negro con visera roja” como lo indica la flecha:



Imágen 8: Visualización de la evidencia

Luego de cotejar todas las evidencias, se entrega el informe respectivo con el análisis forense digital.

#### 4.3.2. Momento 2: Proceso desarrollado con la nueva estructura del laboratorio

Haciendo uso de la propuesta del nuevo diseño, se establecen los pasos y resultados hipotéticos de cómo obtener la evidencia digital.

**Caso:** Inocencia Perdida

**Recepción de evidencia:** A cargo de un solo funcionario con este rol, quién recibirá la documentación, verificará en el sistema y realizará la siguiente lista de chequeo:

DESCRIPCIÓN	SI	NO
Acto urgente		X
Solicitud de análisis		X
Tipo de elemento (CD, DVD, USB, memoria o disco duro)	X	

Tipo de dispositivo (Celular)		X
El elemento se encuentra con algún bloqueo		X
Se cuenta con la contraseña		X
El elemento se encuentra rotulado y con su debida cadena de custodia	X	
Se cuenta con medio de almacenamiento para la imagen forense	X	
Se cuenta con palabras claves, videos o imágenes para realizar búsquedas		X
La seguridad en las instalaciones físicas para el análisis de evidencia es la adecuada		X
Las herramientas forenses se encuentran actualizadas		X
Las licencias forenses se encuentran vigentes	X	



Tabla 12: Checklist – caso “Inocencia Perdida”

Con este Checklist, podemos observar que hace falta el documento de Solicitud de análisis, que se debe mejorar la seguridad en las instalaciones físicas para la extracción y análisis de la evidencia. En consideración con el nuevo diseño, la evidencia digital debe llevar una solicitud y ser recepcionado en el área física respectiva.

**Descripción de la evidencia, los procedimientos técnicos y de la actividad técnico-científica:**

Se conservaría como está, con la diferencia que podría sistematizarse para que el informe sea digital, para ello existen varias opciones en el mercado llamado LIMS (Sistema de gestión de información en laboratorios), el cual podría implementarse, con empresas multinacionales como: LabWare, ThermoFisher o StarLims.

El equipo forense para realizar esta labor debería estar en un área adecuada para realizar la extracción y los análisis respectivos.

ACTUAL	IDEAL
 <p data-bbox="321 688 834 779">Imagen análisis realizado el 10 de enero de 2019, por José Palacios.</p>	 <p data-bbox="862 688 1375 831">Tomado de: <a href="https://www.adalid.com/en-colombia-esta-el-laboratorio-forense-mas-moderno-del-continente/">https://www.adalid.com/en-colombia-esta-el-laboratorio-forense-mas-moderno-del-continente/</a></p>

Imágen 9: Equipo forense – Actual e Ideal

### Interpretación de resultados:

Para este caso en particular “Inocencia Perdida” se contaba con esta imagen:



La cual ayudó para la individualización del sujeto como se puede observar a través del “casco negro con visera roja”.

Por lo general los resultados son generados conforme a lo solicitado y se finaliza informando que el Investigador Líder, o conocedor del caso, debe de revisar la información que ha sido descrita en

forma general; para que detalladamente verifique su contenido, y establezca que datos u archivos son relevantes y pertinentes para la investigación.

Es decir, se entrega la información en Bruto, sin realizar un análisis de lo que conllevaría al esclarecimiento de la presunta conducta punible.

Como resultado de este acto investigativo y de otras actividades como registros, allanamientos y reconocimiento en álbum fotográfico, se materializa la captura de la persona por los delitos de ACTOS SEXUALES CON MENOR DE CATORCE AÑOS. ART. 209 C.P. en la ciudad de Medellín.

Ahora bien, el proceso general a desarrollar con base en el diseño es:

#### **1. Sección uno de ANÁLISIS:**

Una vez el personal de campo obtiene los diferentes elementos físicos que pueden servir como evidencia, se deben dirigir a la “recepción de evidencias”, allí el personal encargado debe verificar que toda la documentación este completa y que la cadena de custodia se haya conservado acorde a los manuales y procedimientos para ello.

La persona de la recepción, registra los elementos probatorios y entrega al personal de campo una constancia de recibido. Luego, llevará dichos elementos al área de almacenamiento, mientras es asignado un perito para su respectivo análisis.

Una vez se ha asignado el perito, la evidencia es extraída del almacén, y llevada a uno de los módulos, en dónde el perito hace uso de una estación de trabajo que está en red y conectada al servidor central de evidencias, así poder crear el respectivo caso en el sistema. En consideración que, dentro del proceso de análisis forense se estipula la extracción de una imagen bit-a-bit de los elementos probatorios, el perito se desplaza a la sala de “imágenes forenses”, con el fin de hacer dicha copia haciendo uso de las herramientas técnicas disponibles, con ello, poder trabajar con la copia y no con el original (evitando con ello cualquier accidentalidad).

En la figura 6, se puede visualizar el proceso global desde el personal de campo hasta la captura.



Figura 6: Inocencia Perdida. Fuente propia

Por otro lado, los elementos computacionales como las estaciones de trabajo y los servidores, están en un segmento de red aislado, reduciendo los niveles de riesgos ante ataques informáticos, así mismo, cuentan con el debido control de acceso y las líneas bases de seguridad.

El procedimiento para la extracción de las diferentes evidencias se conserva (momento 1).

## 2. Sección dos de DESMANTELAMIENTO:

En consideración que en ésta área se realizan desmontes de equipos informáticos o la preparación y análisis de dispositivos móviles (dado su diseño para no tener señal celular) y que para el caso en estudio se tiene un elemento ya extraído (MicroSD), no es necesario hacer uso de ésta zona.

## 3. Sección tres de ADMINISTRACIÓN:

Para la socialización de resultados al equipo de trabajo o los líderes, se usa esta sección, en una de las salas de reuniones se puede exponer con claridad y sin interferencia a los demás analistas, diferentes situaciones o capacitaciones que se puedan presentar. Así mismo, si se tiene un caso de extrema sensibilidad (como aquellos que puedan atentar contra algún servidor público de alto

rango, la seguridad nacional o apoyos internacionales), se puede usar el área de investigación sensible, además, sería necesario pasar la evidencia del almacén de recepción hacia ésta nueva área, previo registro en el sistema.

Se puede observar bajo el nuevo proceso y diseño físico, una debida segregación de funciones que le permite a los diferentes investigadores contar con mejores herramientas y procedimientos para el análisis forense digital, evitando errores involuntarios, sobre-escritura de archivos, pérdida de evidencia, pérdida de la custodia, más transparencia en el desarrollo de un caso.



## 5. Conclusiones y recomendaciones

### 5.1 Conclusiones

Contar con un proceso adecuado para la recepción, copia, análisis y manejo de la custodia es fundamental, toda vez que se están reduciendo posibles riesgos asociados a la segregación de funciones, falencias en la documentación, separación de ambientes, entre otros, adicional, poder contar con elementos computacionales (servidores) capaces de almacenar de forma segura los casos y las evidencias, lo cual permitirá obtener reportes y estadísticas de una manera más fiables y rápida.

Con este proyecto se logra establecer una propuesta de diseño, el cual identifica, recolecta y preserva la evidencia digital.

A través del estudio y los cuestionarios, se determinó que existe un déficit de personal capacitado y certificado en análisis forense de evidencia digital, lo cual se ve reflejado en la presentación de los resultados.

El personal de Policía Judicial que participa en los allanamientos al lugar de los hechos, no cuenta con la capacitación y experticia suficiente para realizar el tratamiento de la evidencia digital, lo cual trae como consecuencia el retraso y la posible alteración de la evidencia, el cual se vería reflejado en los resultados del laboratorio.

Para la implementación del laboratorio se hace necesaria una inversión en Hardware, Software y adecuaciones físicas, realmente necesarias para ser un laboratorio y no un grupo de delitos informáticos, como lo es actualmente.

Con la implementación del laboratorio se garantizará la autenticidad e integridad de la evidencia digital durante los exámenes forenses en laboratorio y se mejorará la agilidad y confiabilidad en los resultados de los exámenes de Evidencia Digital, contando con las herramientas y capacidades acorde al avance y evolución tecnológica permanente.

## **5.2 Recomendaciones**

Se pretende con este tipo de investigación crear un documento con el diseño acorde a las necesidades y las nuevas tecnologías para implementar un laboratorio de ciencias forenses digitales, que cumpla en su implementación con las normas base para ser certificado internacionalmente y así contribuir a la necesidad urgente que existe en el área de delitos informáticos del CTI de la FGN en Medellín.

También se busca que las evidencias recolectadas no pueden perder su validez por tratamientos inadecuados, evitando con ello que no sean legales ante un estrado judicial.

## A. Anexo 1: Tabla de preguntas

1. ¿Para usted que es la informática forense?	
A	Disciplina que hace uso de tecnologías de punta para poder mantener la integridad de los datos y del procesamiento de los mismos.
B	Es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.
C	Es el análisis de una imagen de disco, un archivo o un directorio de archivos, para extraer la información útil de un medio de almacenamiento digital.
D	Ninguna de las anteriores.
2. ¿Qué es evidencia digital?	
A	Es cualquier valor probatorio de la información almacenada o transmitida en formato digital de tal manera que una parte o toda puede ser utilizada en el juicio.
B	Son registros híbridos, generados y almacenados por computador.
C	Todo acto informático que representa hechos de información o conceptos.
D	Todas las anteriores.
3. ¿Qué es un delito informático?	
A	Es la utilización de un elemento informático o telemático, mediante elementos típicos o atípicos, a través de técnicas para realizar un crimen.
B	Son aquellas actividades ilícitas que se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación.
C	Son todas las conductas ilícitas realizadas por un ser humano, susceptibles de ser sancionadas por el derecho penal en donde hacen un uso indebido de cualquier medio informático, con la finalidad de lograr un beneficio.
D	El uso de técnicas informáticas para realizar robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera.

<b>4. ¿Para qué sirve la cadena de custodia?</b>	
A	Para garantizar la autenticidad, seguridad, preservación e integridad de la evidencia física.
B	Para reflejar todas las incidencias de una prueba.
C	Para evitar alteraciones, sustituciones, contaminaciones o destrucciones, en procedimientos realizados por los encargados de su análisis, generalmente peritos.
D	Todas las anteriores.
<b>5. ¿Qué es un hash?</b>	
A	Es un valor alfanumérico de longitud fija que identifica datos de forma unívoca. Los valores hash se utilizan para comprobar la integridad de los datos.
B	Es una huella digital que representa el resumen de un dato.
C	Es el encargado de proteger la confidencialidad de una contraseña.
D	Es el que asegura la integridad de la información.
<b>6. Aprueba la implementación de un laboratorio de ciencias forenses digitales en el CTI de su Seccional</b>	
A	Totalmente de acuerdo
B	De acuerdo
C	Indiferente
D	En desacuerdo
E	Totalmente en desacuerdo
<b>7. Está de acuerdo con diferenciar el Grupo de Delitos Informáticos con el de Informática Forense en su Seccional</b>	
A	Totalmente de acuerdo
B	De acuerdo
C	Indiferente
D	En desacuerdo
E	Totalmente en desacuerdo

8. Cree que es importante la creación de un plan de entrenamiento para Informática Forense	
A	Totalmente de acuerdo
B	De acuerdo
C	Indiferente
D	En desacuerdo
E	Totalmente en desacuerdo
9. Conocimiento específico en: (Califique de 1 a 5, donde 1 es la calificación más baja y 5 la más alta)	
Bases de datos	
Redes de datos	
Programación	
Seguridad computacional	
Informática Forense	
10. (Responda SI o NO) Maneja usted las siguientes herramientas:	
ENCASE	
FTK	
UFED CELLEBRITE	
WINDOWS	
LINUX	
MAC OS	
RECOLECCIÓN DE DATOS VOLÁTILES	

## 6. Bibliografía

- [1] G. Zuccardi, & J. Gutiérrez. Informática forense. Retrieved from [http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica Forenses/Informatica Forenses v0.6.pdf](http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica_Forenses/Informatica_Forenses_v0.6.pdf), 2006.
- [2] R.A. Proaño, A.F. Gavilanes. Guía para reconocer, recoger, extraer, proteger e informar la evidencia digital. International Conference on Information Systems and Computer Science. IEEE DOI 10.1109/INCISCOS.2017.46, pag. 188-194, 2017.
- [3] J. Cano. Estado del arte del peritaje informático en Latinoamérica, comentarios de tecnología y Derecho. 2008
- [4] NIST. Special Publication 800-101. Revision 1. Guidelines on Mobile Device. Consulta en línea en <https://csrc.nist.gov/publications/detail/sp/800-101/rev-1/final>, 2014
- [5] L. Palomá. Delitos Informáticos. (E. J. A. Morales, Ed.). Bogotá, 2012.
- [6] Senado de la república. Código penal colombiano. Actualizado el 26 de Agosto de 2018. En línea en [http://www.secretariassenado.gov.co/senado/basedoc/ley\\_0599\\_2000.html](http://www.secretariassenado.gov.co/senado/basedoc/ley_0599_2000.html), 2000.
- [7] I. Manjarrés, F. Jiménez. Caracterización de los delitos informáticos en Colombia, 2012.
- [8] Guidance Software. The Gold Standard in Forensic Investigations. Retrieved from [https://www.guidancesoftware.com/encase-forensic?cmpid=nav\\_r](https://www.guidancesoftware.com/encase-forensic?cmpid=nav_r), 2020
- [9] AccessData. Forensic Toolkit® (FTK®) and others tools. Retrieved from <https://accessdata.com/product-download/forensic-toolkit-ftk-version-6-0-1>, 2020
- [10] Cellebrite. Soluciones digitales. Retrieved from <https://www.cellebrite.com/es/pagina-principal/>, 2020
- [11] OSI. Controles ISO/IEC 27002:2013. Retrieved from <http://www.iso27000.es/download/ControlesISO27002-2005.pdf>, 2013
- [12] Norton. Retrieved from <https://co.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html>, 2019.
- [13] Fiscalía General de la Nación. Retrieved from <https://www.fiscalia.gov.co/colombia/wp-content/uploads/MANUAL-DEL-SISTEMA-DE-CADENA-DE-CUSTODIA.pdf>, 2019.

- 
- [14] Fiscalía General de la Nación. Retrieved from <https://web.archive.org/web/20081119232357/http://www.fiscalia.gov.co/pag/entidad/organig/paginas/dncti.htm>, 2019.
- [15] Guía Integral de Empleo de la Informática Forense en el Proceso Penal. Retrieved from <http://archivo2016.justicia2020.gob.ar/wp-content/uploads/2016/10/PAIF-2-versi%C3%B3n-final-registrada-2016.pdf>, 2016.
- [16] Di Iorio, Castellote, Constanzo y otros. El Rastro Digital del Delito. Retrieved from <http://www.pensamientopenal.com.ar/system/files/2018/07/doctrina46835.pdf>, 2016.
- [17] MINTIC. Retrieved from [https://www.mintic.gov.co/gestionti/615/articulos-5482\\_G13\\_Evidencia\\_Digital.pdf](https://www.mintic.gov.co/gestionti/615/articulos-5482_G13_Evidencia_Digital.pdf), 2019.
- [18] OSI. Normas ISO/IEC 270001:2013. Manual de referencia. Retrieved from <http://www.iso27000.es/sgsi.html>, 2013
- [19] Fiscalía General de la Nación. Retrieved from <https://www.fiscalia.gov.co/colombia/wp-content/uploads/MANUAL-DEL-SISTEMA-DE-CADENA-DE-CUSTODIA.pdf>, 2019.
- [20] F. Rodríguez, A. Doménech. La informática forense: el rastro digital del crimen. Consultado en línea el 24-09-2018 en <https://www.madridiario.es/noticia/210327/sucesos/la-informatica-forense:-el-rastro-digital-del-crimen.html>, 2011.
- [21] J. Cano. Admisibilidad de la Evidencia Digital: De los conceptos legales a las características técnicas. Derecho de Internet y Telecomunicaciones. (Legis, Ed.). Bogotá, 2003.
- [22] J. Cano. Admisibilidad de la Evidencia Digital: Algunos elementos de revisión y análisis. Revista de Derecho Informático, No. 061, 2003.
- [23] R.A. Proaño, A.F. Gavilanes. Guía para reconocer, recoger, extraer, proteger e informar la evidencia digital. International Conference on Information Systems and Computer Science. IEEE DOI 10.1109/INCISCOS.2017.46, 2017.
- [24] A. Varol, Y. Ülgen Sönmez. Review of evidence Analysis and reportinf Phases in digital Forensics process. 2nd International Conference on computer Science and Engineering. IEEE Pág. 923 – 928, 2017.
- [25] M. Masud, S. Akhter Hossain and S. Muhammad Rizwan. Design and Implementation of Low Cost Digital Forensic Laboratory for University. IEEE WiSPNET 2017 conference. 978-1-5090-4442-9/17 IEEE. Pág 1524-1528, 2017
- [26] Adalid Abogados. Diseño e Implementación de Laboratorios de Informática Forense. Consulta el línea el 12 de junio de 2019 en <https://www.adalid.com/servicios/forensic/disenoeimplementacion-de-laboratorios-de-informatica-forense/>, 2019.

- [27] Duriva. Empresa de seguridad. Retrieved June 12, 2019, from <https://www.peritosistemas.com/hardware-forense-laboratorio-forense-digital/>, 2019.
- [28] Análisis Forense de Computadoras Intrasoft en Panamá. Retrieved from [http://www.intrasoftpanama.com/index.php?option=com\\_content&view=article&id=28&Itemid=26](http://www.intrasoftpanama.com/index.php?option=com_content&view=article&id=28&Itemid=26) soto. Empresa de seguridad. Retrieved June 12, 2019, from <https://www.asoto.com/forense-digital/>, 2016.
- [29] Atlas LTDA. Empresa de seguridad. Retrieved June 12, 2019, from <https://www.atlas.com.co/laboratorio-de-Informatica-forense>, 2019
- [30] Secretaria del Senando de la República de Colombia. Ley 1273 del 5 de enero de 2009. Retrieved April 12, 2020, from [http://www.secretariasenado.gov.co/senado/basedoc/ley\\_1273\\_2009.html](http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html)
- [31] Secretaria del Senando de la República de Colombia. LEY 679 DE 2001 de 2001. Recuperado de [http://www.secretariasenado.gov.co/senado/basedoc/ley\\_0679\\_2001.html](http://www.secretariasenado.gov.co/senado/basedoc/ley_0679_2001.html)
- [32] Secretaria del Senando de la República de Colombia. LEY 1915 DE 2018 de Julio 2018. Recuperado de [http://www.secretariasenado.gov.co/senado/basedoc/ley\\_1915\\_2018.html](http://www.secretariasenado.gov.co/senado/basedoc/ley_1915_2018.html)
- [33] Secretaria del Senando de la República de Colombia. Ley 599 de julio de 2000. Recuperado de [http://www.secretariasenado.gov.co/senado/basedoc/ley\\_0599\\_2000.html](http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html)
- [34] MinTIC. Evidencia Digital. Retrieved from [https://www.mintic.gov.co/gestioniti/615/articulos-5482\\_G13\\_Evidencia\\_Digital.pdf](https://www.mintic.gov.co/gestioniti/615/articulos-5482_G13_Evidencia_Digital.pdf), 2018
- [35] Fiscalía General de la Nación. Manual Único de Cadena De Custodia. Recuperado de <http://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/manualcadena2.pdf>
- [36] Adalid Abogados. Diseño e Implementación de Laboratorios de Informática Forense. Consulta el línea el 12 de junio de 2019 en <https://www.adalid.com/evidencias-digitales-validez-juridica>, 2019
- [37] E. Ortiz. Evidencia Digital Fundamentos aplicables para el abordaje de la Examinacion Forense Retrieved from [https://www.researchgate.net/publication/332786161\\_Evidencia\\_Digital\\_Fundamentos\\_aplicables\\_para\\_el\\_abordaje\\_de\\_la\\_Examinacion\\_Forense](https://www.researchgate.net/publication/332786161_Evidencia_Digital_Fundamentos_aplicables_para_el_abordaje_de_la_Examinacion_Forense), 2019.
- [38] Best Practices. Retrieved from <https://www.crime-scene-investigator.net/PDF/best-practices-for-seizing-electronic-evidence-v4.pdf>, 2019.



- 
- [39] NIST. Retrieved from <https://csrc.nist.gov/publications/detail/sp/800-86/final>, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>, 2019
- [40] J. Palacios, comunicación propia, junio 19 de 2019.
- [41] Organización internacional de pruebas informáticas. Retrieved from [https://www.oas.org/juridico/english/cyber\\_links\\_ioce.htm](https://www.oas.org/juridico/english/cyber_links_ioce.htm), 2018.
- [42] AccessData FTK. Retrieved from <https://accessdata.com/products-services/forensic-toolkit-ftk>, 2019.
- [43] Kaspersky Labs. ¿Qué es un Hash y cómo funciona?. Retrieved from <https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/>, 2019.
- [44] INCIBE. Informe Anual de Actividad de INCIBE 2014. Retrieved from <https://www.incibe.es/que-es-incibe/informe-actividad/2014>, 2014.
- [45] M. Porolli. ¿En qué consiste en el análisis forense de la información?. Retrieved from <http://www.welivesecurity.com/la-es/2013/08/12/enque-consiste-analisis-forense-de-informacion/>, 2013
- [46] Entrevista realizada el 27 de agosto de 2019 al personal clave de investigación de delitos informáticos del Cuerpo Técnico de Investigación - CTI, Medellín, Colombia. 2019.
- [47] Presidencia de la república de Colombia. GUÍA PARA LA CALIFICACIÓN DE LA INFORMACIÓN DE ACUERDO CON SUS NIVELES DE SEGURIDAD. 2017. [online]. <http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/G-GD-02-calificacion-informacion.pdf>. [Accedido el] 6 mayo-2020.